ENHANCEMENT OF NETWORK SECURITY BY USE MACHINE LEARNING

AHMED RAHEEM HASAN

A project report submitted in partial
fulfillment of the requirement for the award of the
Degree of Master of Electrical Engineering with Honours

Faculty of Electrical and Electronic Engineering
Universiti Tun Hussein Onn Malaysia

JUNE, 2019

DEDICATION

I would like to thank my parents RAHEEM HASAN and NAJJLA NOURI for giving me ethical support while I were doing this project. They always guided me to make sure I could finish my project on time and complete it successfully.

I also would like to thank my friends for their concern and help for completing my project successfully with giving suggestions and discussing together to solve the problem during my project; without them, I could not have completed this project on time.

ACKNOWLEDGEMENT

Praise and thanks be to **Allah** for the blessings of mind and health and "conciliating me" for completing this thesis. I would like to express my sincere gratitude to my supervisor **Dr. NAN BIN MID SAHAR** for giving me the proper of advice, guidance and encouragement for my research. He gave me many opinions and ideas for the research and writing of this thesis. Through his patience, motivation, enthusiasm and immense knowledge, I managed to complete this project perfectly and successfully!

In addition, I would like to thank my parents **RAHEEM** and **NAJJLA** for giving me ethical support while I were doing this project. They always guided me to make sure I could finish my project on time and complete it successfully.

To UTHM and the Faculty of Electrical and Electronic Engineering staff Thanks for providing me with an excellent research environment and the proper resources to undertake this research. To the Iraqi government and all Universities: Thank you for supporting me to complete my master's degree. Finally yet importantly, I would like to thank a person who contributed to completing my final thesis directly or indirectly. I would like to acknowledge him/her for helping, which was necessary to complete this.

Furthermore, I also would like to thank my friends for their concern and help for completing my project successfully with giving suggestions and discussing together to solve the problem during my project; without them, I could not have completed this project on time.

ABSTRACT

This research is about the design and simulation on enhancement network security using machine learning. The design use MATLAB coding to show the simulation. The coding is designed in a way that there is an attack of malicious to destroy the data. Because there is a machine-learning scheme in the security, the system have done automatically protect the data and hence the data is recovered at the end of the system. The important study in this research is the machine learning with deep learning system to enhance the security. This put the system into artificial intelligent system. By trains the system, the security can be enhanced. The next incoming data have done checked and the system was identify whether it content errors or fake data. By the end of the research, graphs and animation system have done shown to demonstrate the basic operation of the enhance network with machine learning system.

From the analysis in the simulation results, one can see that the ANNDL is the best algorithm of machine learning process. This method uses many layers to compute or process the data. The time taken to reach the accuracy is also short with less number of iteration. The ANNDL uses iterations method to detect the data, do matching and identify the data. If the data is 100% matched, then the accuracy increase to 1%. As more and more iteration take places, the accuracy have done increased. Thus, it is suggests to have high number of iterations.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Background of Study

Network security becomes more and more important as technologies for information technology being improved. The security here is refers to protection of user information like message or data. The message or data can comes from wired network, radio frequency (wireless network) or even the fiber optical network.[1][2].

Today, many networks have installed with firewalls or some sorts of protection mechanism to prevent data stolen, hacking of data from third party and loss of data due to illegal intruding the network. The computer systems in finance, especially in banks are even more sensitive because they are programmed to do transactions every day. Such computer stored the monetary information as well as personal data of user and the company information. These data and transaction should be protected to avoid lost or complains by users. [3]. by looking into the network security currently available, many systems use antivirus, anti-scammer and other software to against the attack from malicious. The malicious not only limited to virus, but also the adware, malware and other harmful program that comes from the networks.[4].

In this research, the propose idea to enhance the security network is by means of using machine learning. Machine learning be part of ASI (Artificial Super Intelligence where in this research it have done be added into the security network research. By general definition, the machine learning is a system or algorithm that learn the previous behavior of data and make decision intelligence. Machine learning developed from artificial intelligent. It is believed that when the machine undergoes the learning process, it gains the experience. When next task is assign the machine to do, it recall from the experience and make decision to do it. The terms 'make decision

to do it' refers to the action that the machine have done take. The machine either take the resources from the storage to action on it or make a new variable to improve the system. Depends on how intelligence the system programmed by the programmer.

For machine learning that applied to the cybersecurity, it look into the following: [5] User behavior

- Https and DNS request
- Files and executable
- Network traffics
- Harmful and unknown codes injection

All the tasks mentioned above are automatic without user manually trigger the machine learning to work. The machine learning embedded into computer system is transparent to all users. It may be part of the window solution, Linux operating system and Apple MAC operation system. Depending on the developers on how they develop the software.

1.2 Problem Statement

The current network security systems are still relies on firewall and antivirus software [6] Most of these software only fight with harmful program or codes that appears in user terminal.

Today, many antivirus and antimalware software work on recorded malware or virus names in the database. New virus or new malware, the software unable to detect. There is no system in the antivirus or antimalware that can record the new virus and malware so that it can fight for next encounter. Thus, the antivirus or antimalware can say is limited version or not mean for this intelligence system [7]. Not only the problem on unable record the new names of virus or malware, the current antivirus or antimalware also cannot monitor the traffic in the network. This might because the design of the software not mean for this purpose [8].

In network, traffic monitoring and control is also part of the cybersecurity. If the traffic of the network not monitored, the data send out might get lost or collide with other data. Hence, this creates unnecessary time spend on sending the data [9]. With network traffic monitoring system, data can be prevented to send out. The data

only able to send out when the network is idle. This mechanism is something like MAC (Media Access Control) [10].

For firewalls, the design of this system is to prevent unauthorized login into the user terminal or server. This is the original function of the firewall [11]. Today, there is a slight improvement on the firewall. The firewall can block most of the threats, but still other threats like adware could not block completely. For example, some basic installer comes along with threats like Chronometer. This ' Chronometer' is a harmful advertisement Apps. It automatic install into user terminals and automatic appears on the desktop without user instructions. Every time it appears, it block the user browser and disturb the user works. So sad to say that until now, none of the firewall in window 10 and above can block this adware [12]. This also means that the firewall is not intelligence enough and it cannot update itself whenever it is necessary.

With machine learning applied into the network, it can help to analyze the data flow in and out from the user terminals [13]. Apart from that, it also helps to update its information to learn new data and control the machine to make decision. The process of learnings are the difficult part. From literature reviews [14], there are five learning tasks for the machine-learning algorithm. These five learning tasks are supervised learning, semi-supervised learning, active learning, unsupervised learning and reinforcement learning. The detail of these learning have done explained in chapter two and chapter three.

After the learning tasks are complete, the system actively monitoring the data flows from the network to the terminals or from the terminals to the networks. The next thing the system has to do is make prediction and decision. The prediction is an advance level for the machine learning system compare to the decision making. The decision making usually is done using 'if-else' function block in algorithm or in programming. The decision is made based on the programmed data or those data have stored in the computer [15]. If the decision-making check that the input data match on what it has stored in the system, then the next task have done executed directly without alter the data or make improvement to the data.

On the other hand, for prediction, the algorithm is slightly complicated. Apart from making decision, the data have done sent for improvement through a 'process'. Once this improvement is done, the new data tell the computer what to do. Thus, this is the difference between decision-making and prediction [16]. The Figure 1.1. Show to us usage ratio of machine learning algorithm in all applications.

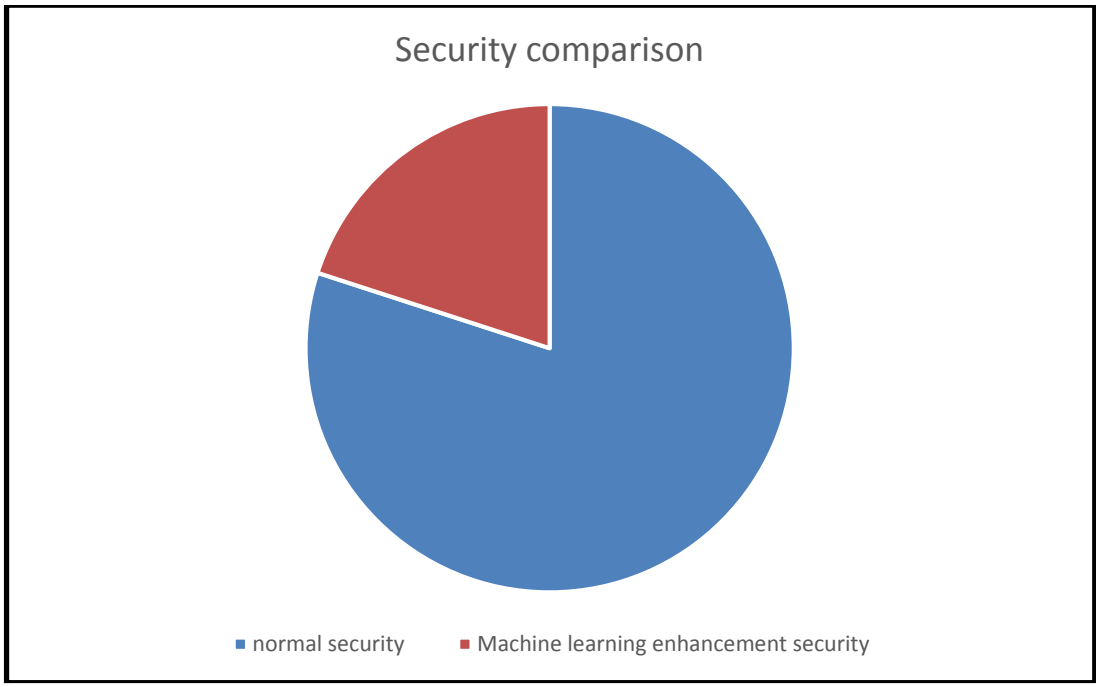

Figure 1.1: Comparison between normal security and enhance security system [16].

1.3 Objectives

The objectives of the research are:

(i) To simulate the machine learning system using five set of random data.

(ii) To analyze between Supervise Method and ANNDL Method in Parameter speed.

(iii) To do compare between Supervise and ANNDL in speed, lost and Accuracy.

1.4 Scopes of the Research

The scope of the research was cover the following areas.

(i) Machine learning algorithm design.

(ii) Implementation of machine learning algorithm into the network.

(iii) Add the noise attack to the system.

(iv) Use MATLAB coding to show the system operation.

The first task has to do before go further the research is to learn the machine learning. After this, apply the machine learning into security.

For this machine learning application in security, it might be difficult to implement. To able continue the research, more references from the published papers and textbooks should carried out to get the idea and solutions. Referring to other people works are important because it helps to kick off the research and give clear direction on the progress of works. Once the idea is obtained, the modeling or design works carry out. In this part, a clear software tool must be defined to design the system. MATLAB software tool have done proposed to use in this research. Other software tools might be used if they are found useful in this research.

1.5 Motivation

This main purpose to develop this research is to motive the innovative idea on the improvement of cybersecurity system. The main improvement area is to make the system more intelligence with the use of machine learning. This has become the challenge in the system design and research. With new improvement and new idea, the network turn into more intelligence and more secure. Not only, it helps to manage and protect the personal information especially for those users who make transaction every day.

It is hopes that with this new intelligence system, the complaint issues from users about threats and other computer hacking systems have done less and eventually drops to zero.

It is also hopes that the new intelligence system can be commercialized locally and even globally.

1.6 Contributions

The main contribution of this research is on cybersecurity system. The research can help users and companies improve the security in their electronic communication systems. The contribution also helps in traffic control in the network. By monitoring the traffic, user always have a secure and clear communication path to send and receive data.

1.7 Aims of Study

The main aims of the study is the machine learning application in network security. The use of machine learning to improve the cybersecurity by looking at data flows, detection on user behavior, block the harmful program and make prediction or decision on next actions.

1.8 Thesis Structure

This report consists of five chapters in total. Chapter one is introduction, chapter two is literature review, chapter three is methodology, chapter four is results and discussion and chapter five is conclusion and recommendation.

Chapter one reviews overall idea and concept of the research. This chapter mainly discuss about the machine learning in general and its application in cybersecurity. The chapter also presents the problem statements, objectives and the scope of the research.

Chapter two reviews the theories and papers related to the cybersecurity. This chapter discusses various ideas people have talk about the machine learning and cybersecurity.

Chapter three shows the methodology of implementation the research. The chapter shows the steps, software tools and model of the networks. The coding and flowcharts about the algorithm also have done presented in this chapter.

Chapter fours presents the results and discussion. This chapter shows the simulation results and discuss in detail about the outcomes.

Chapter five conclude the research works and state the future improvement of the research.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

This chapter review the theories related to the network security as well as the machine learning. Most important things show present is the ideas behind about the machine learning applied to the network in security. At the end of the chapter, a list of published papers have done shown. These papers are related to the machine learning and application of machine learning in network security.

2.2 Reviews the Modern Network Security Systems

Computer network is important for communications. The networks can have many topologies and the way they implemented based on available technologies. The modern networks are LAN (Local Area Network), WAN (Wide Area Network) and WSN (Wireless Sensor Network). There are also other types of networks [17].

The LAN is a small network where the number of workstations (user terminals or user computers) are connected via a bus of cable or in a small area. The LAN has one server. All the workstations are connected to the server for internet access. For wireless LAN, the same implementation and configuration of network applied accept that the connection is wireless. In Wireless LAN, each workstation have its own antenna or wireless access point. The main access point is a server or a gateway. All users' workstations are connected to the gateway and share the same frequency in communication. The communication not interfere on each other because frequency hopping is applied. The frequency hopping is a MAC (Media Access Control)

mechanism where it controls the workstations access into the communications channel and prevent data collision or busy of the network.

The WAN is a network where it has a huge number of workstations all connected together. WAN can have multiple servers for workstations to access into internet. In fact, the internet network itself also classified under the WAN category. Like in LAN, WAN also can have wireless implementation. The wireless radio coverage in WAN is larger than LAN. The coverage could reach kilometer away. The wireless BTS (Base Transceiver Station) is the main access point for the communication. It receives and transmits the data. It also acts as a station to broadcast the communication signals. Thus, BTS is a duplex communications device. The latest network, which exists now, is due to the IOT technology, called WSN. The WSN is mainly for 5G network. Today, all the 5G communication devices have this IOT technology. The main function of IOT is to receive and transmit the sensor data. The implementation is based on wireless technology.

With more and more sensors exist in an area, and then a network is formed. All the sensor networks are wireless. This is because the sensors have to support mobility of terminals and makes convenient for user to receive data signal at any time and at everywhere. All the networks mentioned above have differences topologies of connections. Generally, the network topologies are Ring, Mesh, Star, Fully connected, Line, Tree and Bus. Figure 2.1 illustrates difference types of topologies for current networking.

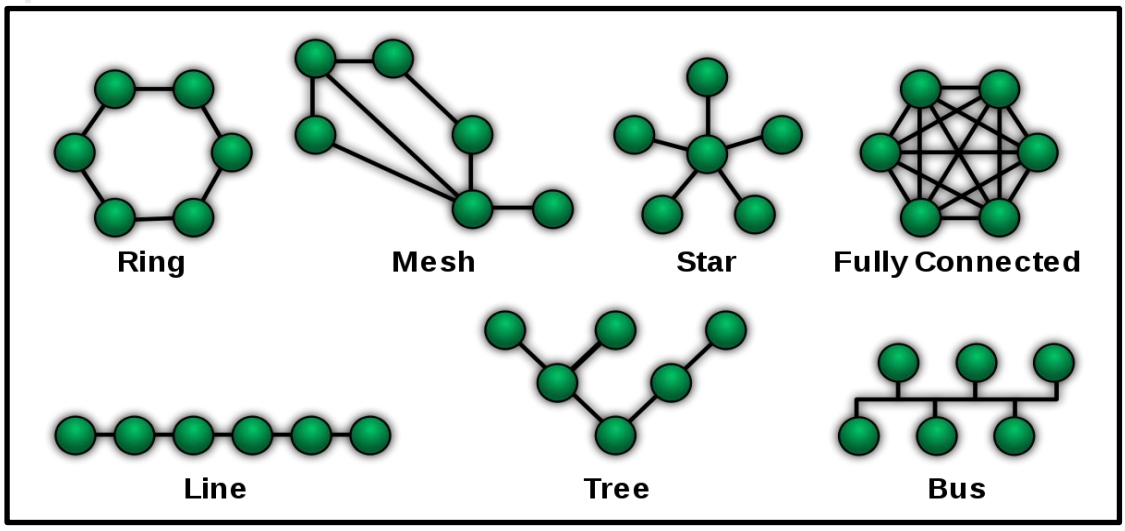

Figure 2.1: Seven types of network topologies [18].

- The ring topology is the network where all the workstations are connected in circular pattern. The communication among all the workstations are take turns. This means that there is a mechanism like the one 'token' is send to the ring. Once this 'token' grabbed by one of the workstations in the network, the workstation can start to communicate with others. When the communication is completed by that workstation, the 'token' is then released into the network and ready for the next grab.
- The mesh topology consists of workstations, which they all connected into a mesh. The message have done distributed into the network from top to down. The media access control have done a chosen mechanism to control the communication in the network.
- The star topology also called centralize topology where all the workstations are connected to one main server. This server control the communication among all the workstations. One disadvantage of this network is that, if the main server down, then all the communication down or affected. The advantage of this topology is that, it is easy to implement.
- The fully connected topology is a complex network where all the workstations are connected to one and another. This connection does not relies on the main server. All the workstations are free to communicate on each other. If one workstation fails, not affect the entire network.
- The line topology is the simplest type of topology. The line could be a backbone of wire where it connected all the workstations together. This kind of network has a disadvantage on the line connection where if the line is breakdown, all the communications also breakdown. For wireless communication, this kind of topology is not suitable. However, for URLLC (Ultra-Reliable Low Latency Communication) wireless communication, this could help [19].
- The tree topology is a network that distribute the message from one workstation to another other. The message is sending through propagation method where it pass down and going through other workstations before reaching the destination.
- The bus topology is a simple topology where all the workstations are attached to the bus (a connection points). The bus topology requires MAC mechanism

to control the message send and receive from the network. The primitive LAN network is using this kind of connection.

All the networks present above are used in data or message communications. The data is the important parameters in the network. They have to deliver to the right destination, safely received and appears in original as the one send from the sender. The data should not lost or disappear in the network or altered by someone in the network. If this case happens, that means the network is not secure. None secure network always give problem to the users. The data not only lost, but there are other things exist to disturb the workstations. These things are virus, malware, adware and other harmful programs which received by the workstations. All these should be blocked or filtered in the networks.

Unfortunately, the current networks are not strong enough to fight against these viruses and unwanted programs. There is a gap to improve the current network. The current network securities are divided into many types. The available securities are access control, antiviruses' software, behavior analysis, email security, firewalls, intrusion prevention, mobile device security, VPN (Virtual Private Network), Web security, Wireless security and network segmentation [20].

2.2.1 Access Control Security

The access control security also called network access control where it prevents unauthorized person access into the network. The control usually using a page or a software in user terminals. Whenever user connects to the network, a message dialog pop up and asking for user name and password. This message dialog is the access control point.

When user key in correct password and username, he or she is allowed to enter the network and start their communications. The disadvantage of this access control security is that, if everyone knows the password and username, he or she can enter the password easily. If the user carries the virus, then the virus attack the whole network. Another disadvantage of this access control is the weakness of using username and password. Recently, there is a software develop to hack the password and username. The software like "Data doctor", "Gmail Hacker" and "Account Hacker" are the commonly used software to hack the password and username [21].

2.2.2 Antivirus Software

As mentioned before, this software is not potentially protect the user terminals or network affected by the virus. This is because the virus is updated from day to day. Unless the antivirus software is too intelligence and able to update the virus quickly, then it should be no problems to against the viruses. [22]

Today, virus is no more prevail computer worm. This is because most of the virus causing computer damage and the virus makers could not get anything or could not get benefit the damage. The most prevail computer worm now called adware. This is a powerful computer worm where it drags the user to payment site and making user unconsciously make payment without any reason. The worm displays attractive information automatically and ask user to pay for it. In some cases, the worms display threaten message, like "your computer is attacked by 1000 virus" or it automatically scan the user computer and display the summary of threats found on user computer. By doing this, users start worry and the worm drag them to payment site and ask them to buy an antivirus software to kill all the threats. The payment sites are fraud. Most of them take the money and run. [23]

Therefore, the entire antivirus today are lousy and unable to block the adware. Another disadvantage of antivirus is unable to differential good .exe and bad .exe file. Many antivirus software seems like to block all the .exe files. As long as they detect the file extension name has .exe, then they block or kill. This is a big disadvantage of all the current antivirus.

Frankly speaking, many .exe files are good programs. They are not viruses. They are user application software where it is presented in .exe. Therefore, if this good .exe file is deleted by the antivirus software, user not able to install the software. Another file called 'crack', also not a virus. Unfortunately, many antivirus software treat it a virus and kill files. It is sad to say that not all the antivirus software are intelligent enough to identify whether the file is a virus or not. Many of them take action on kill or block.

2.2.3 Behaviour Analysis

The behavior analysis is part of the network security system. This system is developed to trace the user behavior on the network. It monitors the URL that user often visits and files that often downloaded by the user. Through the behavior analysis, the system helps to avoid user goes into harmful pages and download the harmful files. The system recommend the best URL and files for the user to download. This help to avoid user computer attacked by the virus or worm.

Behavior analysis is quite a complicated mechanism. Example of network behavior analysis is shown in Table 2.1. [24].

Table 2.1: Example of network behaviour analysis and how it detects the threat.

Normal	Abnormal	Examples
Server accept requests service from workstations	more than 1000,0000 request per second or per minutes	Problem: TCP SYN flooding
A user connects to few workstations in a network	more than 10000 connection happen to the same destination	Problem: SQL slammer
The source address is not the same with destination address	The source address is same with destination address	Problem: LAND attack
Traffic rate in the region is around 200 Mbps	More than 200 Mbps found appears in the network	Problem: Generic traffic flooding

From the network behavior analysis, the system operates on the statistical analysis where it detects user visits the sites, use the data rates and other things that user log in to the network. All this behavior have done counted based on number of times users make it. If one day or sudden changes of the behavior, then system know that, it must be the worm or scammer who attack the network.

2.2.4 Email Security

Currently, there are also many software developed to protect the users' email. Email security now becomes more and more important. The email scammer protections can help to block the scammers, illegal URL and other harmful program. Email security works on email communications only. This is the main disadvantage of email security. It also helps to block the threats and other harmful program from the browser. [25]

2.2.5 Firewalls

Firewalls are the system to filter out unwanted data flows into the personal computer or flows into the networks. Firewalls have been used many years by many companies and by many personal computers. The functions of the firewalls are:

- To protect the workstations from the attack of threats
- To protect data lost
- To secure the communication

Many firewalls do their tasks as based on their definitions. This put the firewalls have limitation on blocking or filtering some threats. The adware and malware still unable blocked by firewalls. Below shows the lists of adware and malware that could not filtered by firewalls [26]:

- Delta search
- B lyrics
- BetterBuys
- ChatZum
- Chronometer
- Do-search

All these adware attacks the browsers and making annoying pop up even offline is implemented in the workstation. When adware or malware attack the browser, the effects are:

- Could not search a complete information as compare with Google search.
- Little information appears in the search engine.
- Most of the information are related to buy and sell.
- Blocking user to use other search engines.

REFERENCES

1. P-KuanHoong, I. Tan, and C. YikKeong, “G Nutella N Etwork T Raffic M Easurements and,” Int. J. Comput. Networks Commun., vol. 4, no. 4, pp. 1701–1706, 2012.
2. M. T. Nehete and V. G. Wagh, “Network Security and Authentication in Communication,” pp. 30–32.
3. S. Prabhakar, “Network Security in Digitalization: Attacks and Defence,” Int. J. Res. Comput. Appl. Robot. www.ijrcar.com, vol. 5, no. 5, pp. 46–52, 2017.
4. S.- Volume and G. Kumar, “& Management Technology Network Security Attacks – An Overview,” vol. 1, no. 5, pp. 195–198, 2014.
5. V. Ford and A. Siraj, “Applications of Machine Learning in Cyber Security Applications of Machine Learning in Cyber Security Methodology,” no. October 2014, 2015.
6. Lau Kim Boon, Jenny.C and Voon. K.S., "Design and Implementation on Antivirus and Antimalware Software", IEEE Trans on Computer Technology, Vol. 4, Issue 1, pp. 1 – 10, 2015.
7. Sandra.L, Dinita.K and Sukima. M, "The World Issues About Cybersecurity", International Journal on Computer and Technology, Vol. 8, Issue 3, pp. 5 – 15, 2016.
8. Jason.W, T.T.K and Boysted. N, "Network Security Enhancement and Protection", IEEE Trans on Computer Technology, Vol. 14, Issue 10, pp. 6 – 12, 2017.
9. Mohammed. A, Roslin.C and Kafai.M, "The Modern Network Security Systems", IEEE Trans on Computer Technology and Engineering, Vol. 16, Issue 13, pp. 18 – 27, 2017.
10. Janet Ong and Chan.S.H, Introduction to Computer Network, McGraw-Hill, New York, 2016.

11. Lily.G and Franky Liew, Computer Network and Security, Prentice-Hall, New York, 2015
12. Teh.D.Y and Ying Lau, Basic Computer Network Security, Longman, New York, 2014.
13. Hans.F, Kwong.C.F and Lious. J, "Applied Machine Learning in Cybersecurity", IEEE Trans on Network Security, Vol. 45, Issue 32, pp. 10 – 32, 2017.
14. Tie Shan and Tzi Ying, Introduction to Machine Learning and Network Security, Wiley & Sons, London. 2016.
15. Okira. H, Kirakasi. L, Advanced Computer Network Security, Oxford Press, London, 2015
16. Vivient. A, Fatimah.M and Norazlina. M, "Design and Simulation on Machine Learning Algorithm", International Journal on Computer Networks, Vol. 56, Issue 30, pp. 47 – 67, 2016.
17. Tan Chu Lam, Computer Networks, Prentice-Hall, New York, 2013.
18. Xiao Hui, Basic Computer Network and Communications, Prentice-Hall, New York, 2014.
19. Kok Cheng Hua and Janet Ong, "Simulation on URLLC Networks with IoT Technology", IEEE Trans on Electronic Communications, Vol. 89, Issue 60, pp. 50 – 68, 2014.
20. Tion.J, Lee.F.O and Boystad.L, "Modeling and Design a Virtual Private Network", International Journal on Communications, Vol. 88, Issue 54, 2016.
21. Thomas.G, Advanced Network Security, Pearson, New York, 2017.
22. Ramirez, Jose Bernardo Quintero, Julio Canto, and Alejandro Bermudez. "Scanning files using antivirus software." U.S. Patent Application No. 15/920,090.
23. Gan, Chenquan, and Xiaofan Yang. "Theoretical and experimental analysis of the impacts of removable storage media and antivirus software on viral spread." *Communications in Nonlinear Science and Numerical Simulation* 22.1-3 (2015): 167-174.
24. Ooi Wan Cheng, Lily.T and Maggie. V, "Simulation on Behavior Algorithm for Advanced Networks", IEEE Trans on Electronic Communications, Vol. 100, Issue 75, pp. 59 – 84, 2015.

25. Huang, Jen-Wei, Chia-Wen Chiang, and Jia-Wei Chang. "Email security level classification of imbalanced data using artificial neural network: The real case in a world-leading enterprise." Engineering Applications of Artificial Intelligence 75 (2018): 11-21.
26. Fatin.M, Norazlina.M and Huang. W, Introduction to Wireless Communication Networks and Security, Pearson, New York, 2015.
27. A. Shaghaghi, M. A. Kaafar, and S. Jha, "WedgeTail 2.0: An Intrusion Prevention System for the Data Plane of Software Defined Networks," pp. 849–861, 2017.
28. Syed.A, Mohammed.A and Han. J, "Overview of Mobile Security Systems", International Journal on Computer and Mobile Networks, Vol. 123, Issue 32, pp. 90 – 120, 2016.
29. Donita.K and Liew. H, Basic Virtual Private Network, Longman, New York, 2016.
30. Hansen, Marc R. "Asymmetrical Challenges for Web Security." U.S. Patent Application No. 15/202,755.
31. Zou, Yulong, et al. "A survey on wireless security: Technical challenges, recent advances, and future trends." Proceedings of the IEEE 104.9 (2016): 1727-1765.
32. Nasrin.M and Ema.T, The Machine Learning and Implementation, McGraw-Hill, New York, 2014.
33. Lee.G.S, Beisay.L and Lau.K.B, "Mathematical Analysis on Machine Learning Algorithm", International Journal on Computer Technology, Vol. 66, Issue 80, pp. 347 – 447, 2016.
34. J. Bennett and S. Lanning, "The Netflix Prize," 2007.
35. S. Kumar, X. Gao, I. Welch, and M. Mansoori, "A Machine Learning based Web Spam Filtering Approach," pp. 973–980, 2016.
36. M. Zamani and M. Movahedi, "Machine Learning Techniques for Intrusion Detection," pp. 1–11.
37. L. y Taylor and Francis Group, Data Mining and Machine Learning in Cybersecurity. 2011.

38. Dubey, Doradha.L and Sinha.K, "Applied Machine Learning in Image Processing and Data Mining", IEEE Trans on Digital Signal Processing, Vol. 90, Issue 12, pp. 8 - 29, 2016.
39. M.H. Rashid and Cryil.W, "Fast Image Processing Method Using Machine Learning and Artificial Intelligent", IEEE Trans on Digital Signal Processing, Vol. 22, Issue 1, pp. 78 - 100, 2014.
40. P.C. Sen, Mohan. M and M.S. Jamil, "Image Processing Method using Machine Learning", International Journal on Engineering and Technology, Vol. 10, Issue 18, pp. 77 - 102, 2017.
41. Joseph Vithayathil, Artificial Intelligent with Machine Learning, McGraw-Hill, New York, 2018.
42. David.C and Kok Chong Meng, Applied Artificial Intelligent, McGraw-Hill, New York, 2017.
43. Chrysis G.C, Basic Artificial Intelligent, Prentice-Hall, New York, 2016.
44. K.B. Pasalkar, Fundamental of Artificial Intelligent, Prentice-Hall, New York, 2017.
45. S.K. Datta, Introduction to Artificial Intelligent, Pearson, New York, 2016.
46. R.J. Acosta and R. Bauer, Basic Artificial Intelligent System, Pearson, New York, 2017.
47. M. Allman and V. Paxson, Advanced Artificial Intelligent System and Applications, Prentice-Hall, New York, 2016.
48. P. Conforto, G. Losquadro and S. Floyd, "Big Data Mining Using Neural Network Deep Learning (NNDL)", IEEE Trans on Digital Signal Processing, Vol. 19, Issue 21, pp. 43 - 53, 2017.
49. L. Gauthier, G. Malkim and J. Mogul, "Complex Data Mining Using Nueral Network Deep Learning", IEEE Trans on Digital Signal Processing, Vol. 31, Issue 17, pp. 1 - 67, 2017.
50. M. Mathis and T. Sherpard, "Simulation on Artificial Intelligent Using Deep Learning Method", IEEE Trans on Digital Signal Processing, Vol. 45, Issue 80, pp. 4 - 26, 2018.
51. G. Patel and P. Robertson, "Simulation on Neural Network Deep Learning usign MATLAB", International Journal on Engineering and Technology, Vol. 77, Issue 90, pp. 28 - 56, 2016.

52. F.Dovis and E. Stare, Basic Machine Learning and Introduction to Artificial Intelligent, McGraw-Hill, New York, 2017.
53. C. Perkins and R.C. Reinhart, Introduction to Deep Learning of Machine Learning, McGraw-Hill, New York, 2018.
54. Y.F. Hu and R.E. Sheriff, Apply Neural Network Deep Learning in Image Processing, Oxford Press, London, 2017.
55. V. Obradovic and W. Stallings, Introduction to Neural Network Deep Learning System, ey & Sons, London, 2016.
56. J.De Vriendt and P. Lucas, Fundamental of Neural Network Deep Learning, Pearson, New York, 2015.
57. Tocci. M and Luglio. T, Advanced Neural Network and Deep Machine Learning, McGraw-Hill, New York, 2017.
58. E. Berruto and P. Diaz, "Design and Implementing Neural Network Deep Learning in Image Processing", IEEE Trans on Digital Signal Processing, Vol. 90, Issue 100, 2015.
59. ian. T and Ooi.G, "Apply Machine Learning in Security Network", IEEE Trans on Computer Networking, Vol. 67, Issue 33, pp. 108 - 110, 2017.
60. F. Delli Priscoli, Computer Network with Neural Network Technology, Pearson, New York, 2016.
61. E. Del, D.C. Cox and X. He, "Data Protection Scheme Using Neural Network", IEEE Trans on Digital Signal Processing, Vol. 94, Issue 55, pp. 77 - 120, 2017.
62. N.E. Kruijt and A.R. Modarressi, "Design and Implementation of Code Extraction for Matching Learning", International Journal on Engineering and Technology,
63. 1M. Werner and A. Jahn, Introduction to Data Communication and Processing, McGraw-Hill, New York, 2016.
64. L. Bahl, C. Berron and Ting Sii Ying, "Data Corruption and Attacked By Virus Issues", IEEE Trans on Data Communications, Vol. 99, Issue 1, pp. 14 - 97, 2016.
65. V.M. Jovanoic, Basic Data Communications, McGraw-Hill, New York, 2017
S. Lin and D.J. Costello, Advanced Data Communications, Pearson, New York, 2016.