AN IMPROVED ARTIFICIAL NEURAL NETWORK MODEL FOR DETECTION OF SOURCE OF CYBER ATTACKS

Gift Chukwuneyem Okwuokenye L. N. Onyejegbu, F. E. Onuodu, Augustine Ugbari

Abstract— Artificial neural network (ANN) is an assembly or nexus of interconnected processing elements or nodes whose functionality can be compared to the human brain. This ability is achieved by adaption and learning from existing patterns and using the learned pattern to detect and predict the next similar pattern in future occurrence and activity. In this project, neural network system was developed for detecting and tracking the source of cyber- attacks using selected ports in which cyber data is fed into the system. The analysis and design was done using structured system analysis and design methodology (OOADM), due to its direct computing-oriented features which are sequential in nature. ANN is computational based and using MATLAB programming language. The pattern of cyber- attacks (data sets) was used in training the system so that it can learn and then track and detect future attacks. The result shows 95% accuracy in detection of cyber- attacks in the ports used in testing the system. This work could be beneficial to hospitals, to schools, to financial institutions, to security agencies and any other organisation that deals with cyber security.

Index Terms— Artificial, Network, Neural, Detection, Cyberattack, Security, Analysis

1 INTRODUCTION

Information drive the world and these ranges from simple data to stored relational databases and to big data stored in small, medium and large computer systems across the globe. Modern data are in form of text used for decision making, signals used to trigger various equipment which include Manufacturing, Hospital and even Military hardware. Sending wrong signals or changing stored text can lead to wrong machine reaction or users taking wrong decisions. Removing the stored data or blocking signalling channel can also lead to breakdown in office operation and equipment response. Assuming in a war scenario, plane engines are disabled, radar capability to dictate plane arrivals are disable while electronic tanks as well as missile launchers cannot trigger. The best thing is simply to surrender.

These capabilities have been made possible by organized cyber-attackers including some government secrete agents.

Cyber-attack can be considered as any activity lunched by an individual or group of individuals against a computer networks with the objective of compromising the privacy, reliability and accessibility of data in that network [1].

Any attack that impedes the privacy, reliability or accessibility of the system or data it holds a server or any system on a network can be referred to as a cyber-attack. [2].

Cyber-attack is can still be referred to any form of hostile activity against the information located with computer systems, the configurations of network infrastructure or internet enabled devices. This may be undertaken by individuals or organizations by several means of unethical methods often initiated from an anonymous source that may monitors, changes, steals, or eliminates a particular target data/resource by hacking into the compromised system. Attacks of this natured may be referred to with different names such as Cyber campaign or cyber terrorism based on in varying circumstances. Cyber-attacks take place at a various range with the aim of compromising the contents of whole system by the installation of a malicious code on a target machine.

The level of sophistication in cyber-attacks is fast on the raise with devastating consequence as demonstrated recently in the Stuxnet worm attack [2]. The RansomeWare attack in April 2017 actually got many computers down and the WanaCry Virus attack which followed the following month in May 2017 also damaged many hospital systems.

.

1.1 Aim and Objectives

The aim of the study is to develop a neural network system for detecting and tracking the source of Cyber-attacks. The objectives include to:

1. Design a neural network (deep learning) system for detecting and tracking source of cyber-attacks.

2. Implement the system using MATLAB programming language and KDD dataset as the databases

2 LITERATURE REVIEW

2.1 Related Works

In the development of cyber-attack the attack pattern has always being the challenge. In neural network learning the various attack patterns are very critical in building a durable system. According to Shiffman (2012), learning in ANN comes as a result of altering the weight with some kind of learning algorithm. The target is using the training data to make sure that the system learns the pattern that is hidden in the data. Learning is very important in Artificial Neural Network as an adaptive system that can change its internal structure based on various information passed to it. In training the system there are many algorithms that can be applied.

Paulo et, al. (2010) in their work on Octopus-IDS constructed 30 x 30 SOM map and used DARPA dataset for the training. When they retested in pre-deployment they collected data from the real network traffic by developing their own packet sniffer. During training they used batch training algorithm that has a training length of 100 and starting radius of 15. They were successful in classifying the IP packets in three classes which includes intrusion, possible intrusion or normal. The only challenge of their system is the level of accuracy which was low making some traffic to be wrongly classified while others were well classified. In a cyber-attack case this can result to fatality [3].

In the work of Haijun et, al. (2007), Kohonen Neural network layer was introduced to reduce the false negative rate. There work targeted denial of service (DOS) and hacker probe. According to Haijun et, al., Kohonen Neural Network is necessary at the first layer for separation since it supports unsupervised learning. They held that it can separate known patterns, generalize the patterns and detect variations of attacks. The challenge identified in this work is that their model is less complex in selection of configuration parameters this is linked to the number of hidden layers, number of nodes for each layer and the transfer function. It could be said that an improvement in these parameters could greatly affect the result positively.

According to Bhavin and Bhushan (2012), adding another layer could improve the function for pattern detection in Neural Network. In their work on dynamic change learning rate in Back Propagation Neural Network (BPNN), they seriously held that the performance of a given BPN depends on the learning rate [4] (r). On the occasion that r is assumed to be a constant, it results to the local minimum and proceeds to slow convergence rate.

On the contrary if r is small value, the Neural Network training times moves up in flat sections of the error surface. On the other hand if r is a big value then higher training time will result in gradient area. Bhavin and Bhushan (2012) in their work decided to initialize the step value r at the first instance, and if there is increase in the error after a given iteration time, the iteration is made invalid. In that case the step value is expected to multiply with a value of b (<1), as r (t+1) = br(t), and the iteration is repeated again. If the error goes down, the iteration is prove to be valid, so the learning rate multiplies with a value of a (>1), as r (t+1) = ar(t). This scheme is expected to improve the slow convergence rate. Notwithstanding, Bhavin and Bhushan (2012) adjusted the learning rate when the system error of the iteration is not up to the expectation. The only challenge of the work is that it concentrated on simplified attacks whose pattern have already been known but the system have challenges in learning from relatively new patterns which is actually the real nature of cyber-attacks [4].

2.2 Artificial Neural Network (ANN)

ANN has an attractive ability that makes the network useful to model non-linear relationships and does not rely on restrictive assumptions implicit in BS model. The only input for an ANN is historical data that enables the network lean the relationships between inputs that characterize the phenomena being mode. ANN is frequently applied to statistical analysis and data modelling. Therefore, they can be used for forecasting because ANN is very sophisticated modelling techniques capable of modelling extremely complex functions (Dhal, 2013).

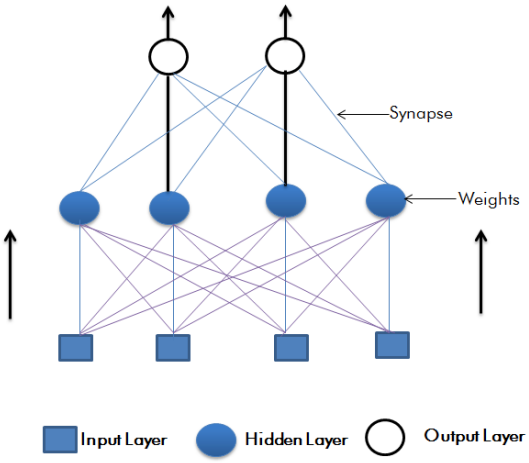

Fig. 1.1: The ANN Layers (Source: [5])

In figure 2.1 the Layers of the Artificial Neural Network is shown with the Input Layer at the lowest level: This is the level where the neural network is expected to receive the various attack patterns that will be feed into the system. This layer is

- *Gift Chukwuneyem Okwuokenye*, *masters Student, Computer Science in University of Port Harcourt, Nigeria,, +23470383379195. E-mail: giftokwukenye@gmail.com*
- *L. N. Onyejegbu, Senoir Lectureer, Department of Computer Science in University of Port Harcourt, Nigeria,. E-mail nneka2k@yahoo.com*
- *F. E. Onuodu Senior lecturer, Department of Computer Science, University of Port Harcourt, Nigeria, E-mail: friday.onuodu@uniport.edu.ng*
- *AUGUSTINE UGBARI, Lecturer, Computer Science department, University of Port Harcourt, Nigeria E-mail; ugbari@gmail.com*

closely followed by the second layer were the weight is infused into the system. The weights are based on the degree of impart that they will have on each of the factors that are evaluated. The higher the impact the higher the weight that is used on the factor to cover for the influence expected from the factor in detecting the pattern and possibility of an attack.

The pattern can be either a recurrent pattern or a feedforward pattern. The pattern often decides which attack is feasible at any given moment. The pattern used to connect to the artificial neural network also influences the behaviour of the neural network and its ability to track situations for which it is deployed to handle. The architecture of the neural network also has a role to play in deciding the pattern of connection of the ANN. Simple pattern of the connection is illustrated in figure 2.2.

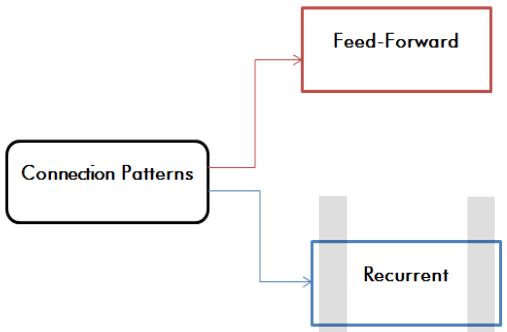

Fig. 2.2: Simple Pattern of connections on ANN (Source: Yousefpour, 2007)

In figure 2.3 a detail of the Feed-Forward and the Recurrent. The Feed-Forward pattern includes different layers of perceptron; the Single Layer Perceptron (SLP), the Middle Layer Perceptron (MLP) and the Radial Basis Function (RBF). The Middle Layer Perceptron (MLP) is the most popular in usage among the various model of the feed-forward and will be discussed further. The Recurrent on the other hand is made up of the Competitive Networks, the Kohonen's SOM, the Hopefield Network and the Art Models.

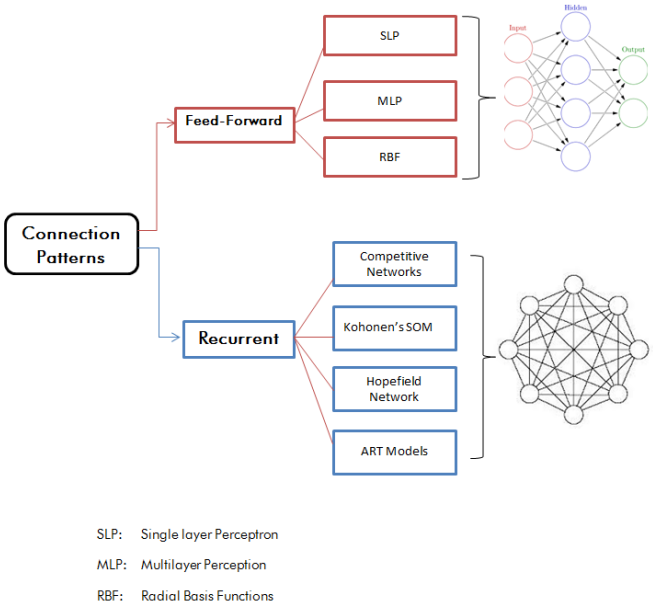

Figure 2.3: Detail Pattern of connections on ANN (Source: **[5]**)

3. MATERIALS AND METHODS

The methodology used in the system analysis, design and development of the system in this thesis is the object-oriented Analysis, Object-oriented Design and Object-oriented development commonly referred to as OOADM. The methodology breaks down the components of the system based on the objects that surround the system and using the object components builds the new system around the identified objects. The new system will have relationships, activities and even dependences around the identified objects. Messages for the performances of any identified activity will be delivered to objects which will interact with the corresponding method to make sure that the activity is carried out within the system. When there are existing components outside of the system message can also be delivered to it to perform certain actions and return corresponding result back to the calling method or class. In other to achieve a well-organized system, section of activities will be categorized into classes in such a way as to make each group of activity and the processes accompanying them compact.

.

3.1 Existing System model

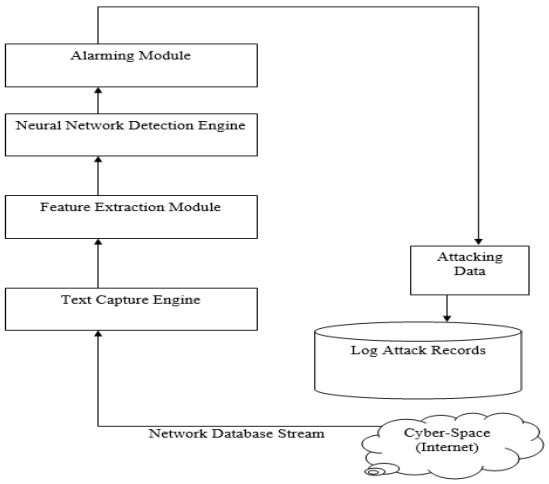

Fig. 3.1: Architecture of the Existing Cyber-Attack Detection System [4].

It is important to express the fact that efforts have been made in the work of [6] as well as in the work of Aggarwal and Sharma (2015) in the development of cyber-attack detections. Their work is the bases of the discussion of the existing system and from there we intend to build on the areas that we have identified some lapses. In the work the design was based on Back Propagation Neural Network (BPNN). In the architecture of the existing system specified in figure 3.1 the neural network classification engine distinguish the intrusive action by analysing and processing the data by the feature extraction module. Once the system detects aggressive behaviour it warns the users and records attack-related information [7]

3.2 Proposed System model

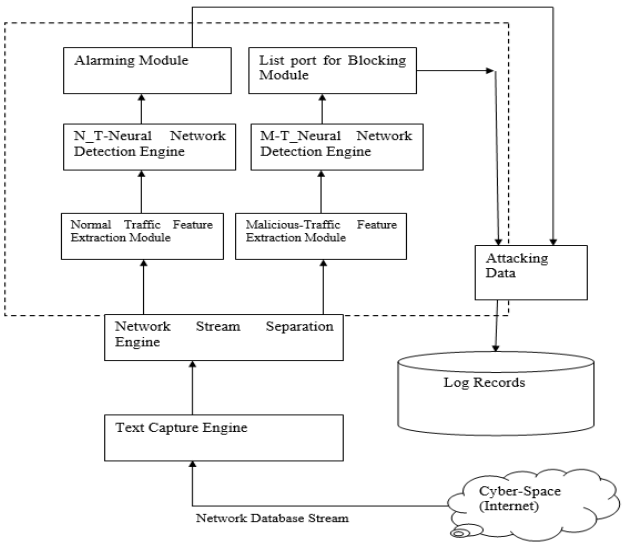

Figure 3.2: Architecture of the Proposed System

In the proposed system, the network stream is received normally by the text capture engine which is similar to what happens in the existing system but after that instead of sending the data to the feature extraction module as in the existing system it is rather split into two mainly the Malicious-Traffic Extraction Module andNormal-Traffic Extraction Module.

The separation was done to enable the system easily train the data and register the behavior of the data separately the behaviour of the Malicious-Traffic can be used to track other data set from the general population which are either normal or malicious. If any traffic matches the malicious data behaviour then the Neural Net detection engine can easily track it for blocking or for listing its URL for blocking by the artificial neural network blocking engine.
The blocking engine makes sure that any stream of data from various sources that displayed treats found in the malicious trained data will be selected and the source uniform resource locator of data is listed and presented to the system module responsible for blocking malicious sources. Cyber Attackers often use malicious channels in attacking systems which are often their targets. This is illustrated in the analysis of the proposed system in figure 3.2.

3.3 Process model Design

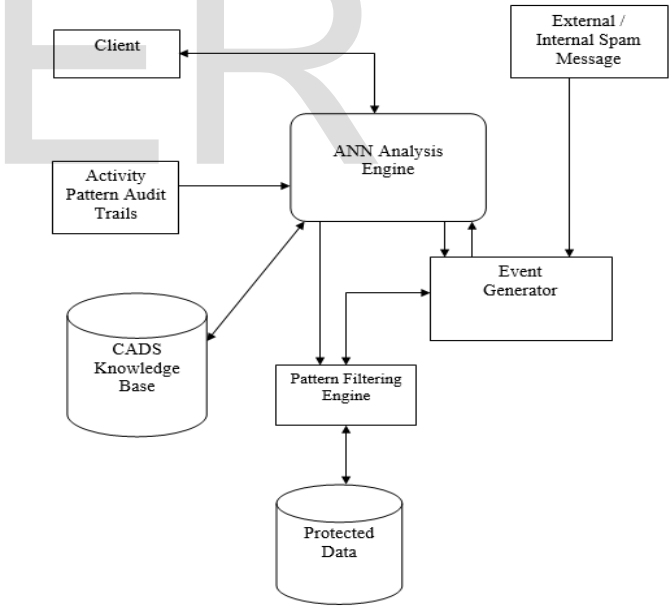

Fig. 3.3: Process model Design of the CADS

In figure 3.3 the client system log has information about the local internet activity going on the client machine before the client visits the CADS system. The log is usually accumulated using cookies or session controllers and they are stored on the client machine without the explicit knowledge of the system user. On visiting the CADS this log is accessed by the system and feed into the Artificial Neural Network (ANN) Analysis Engine. The

analysis engine also uses the activity pattern audit trail which is a list of audited behaviour of spamming activity as at when the ANN training begins. Since the ANN training is progressive it is also important that the audit trails are re-injected whenever changes occur in the pattern of the hacker. Once the system has learned a pattern it stores it in the CADS knowledge base.

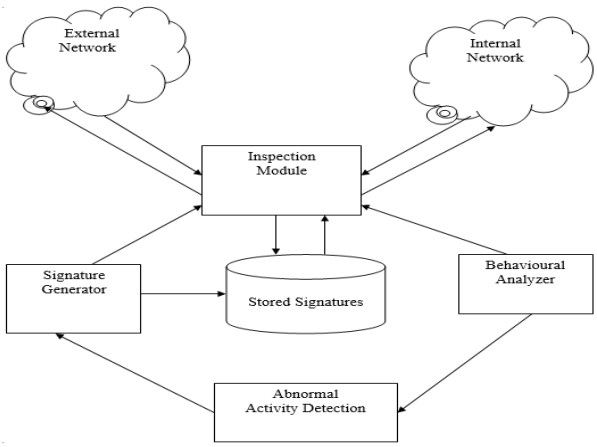

Fig. 3.3: Model of Inspection in the Cyber Attack Detection System

The Intrusion Detection System (IDS) module is based on stately static signature detection technology. This technology comes equipped with periodic signature updates with provision for emergency updates in cases when newly discovered high-risk attacks are in progress. Behavioural-based real-time signature expertise are utilised in Network Behavioural Analysis (NBA). As a result, a threshold for the networks normal behaviour is set including its running application and user behaviour are mapped in the system

4 RESULT AND DISCUSSION

4. 1 Result Discussion and System Documentation

The execution of the system is triggered when the user clicks run on the tool bar. This starts the execution by loading the data and waiting for a keyboard tap to proceed at each pause point. The process is followed by the loading of the initial weights of the neural network and evaluating the Sigmoid Gradient of the ANN. This is illustrated in figure 4.4. The processed data in the Matlab worksheet is presented in figure 4.2.

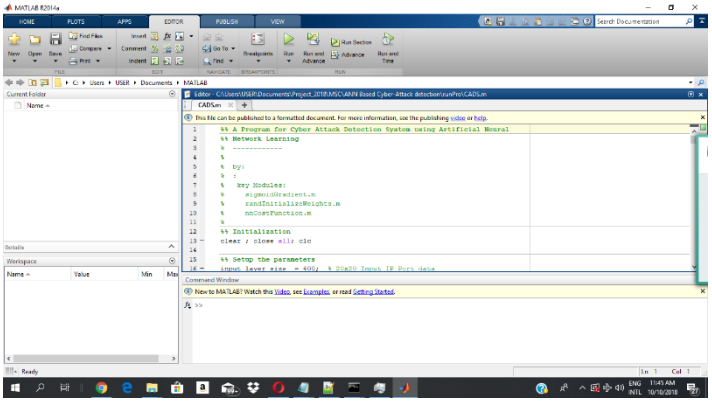

Fig. 4.1 The Matlab IDE showing Graphical Tools

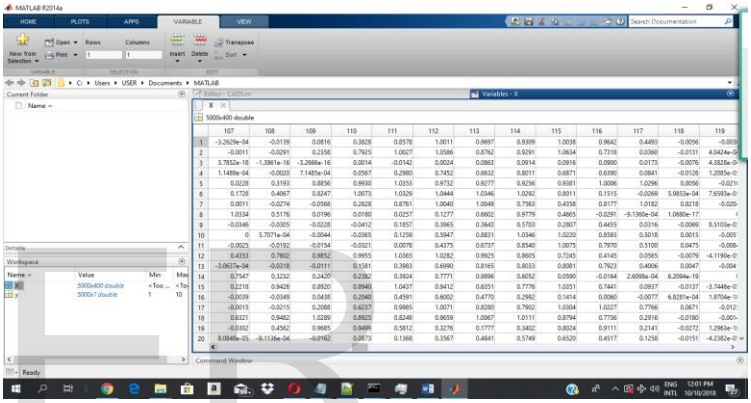

Figure 4.2: Processed Data inside Matlab Worksheet

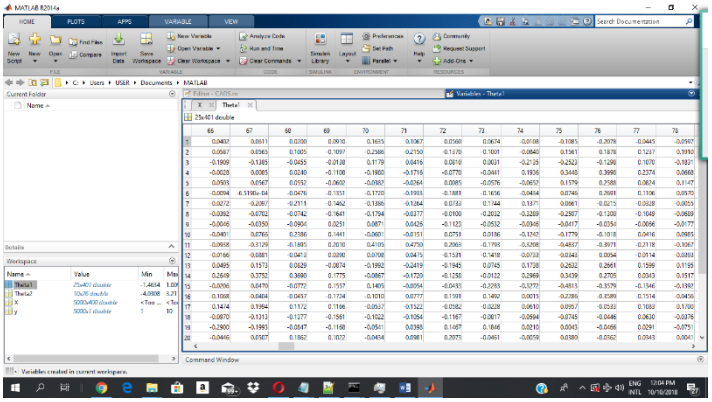

Fig. 4.3: Initial Weights data used to Train the Neural Network

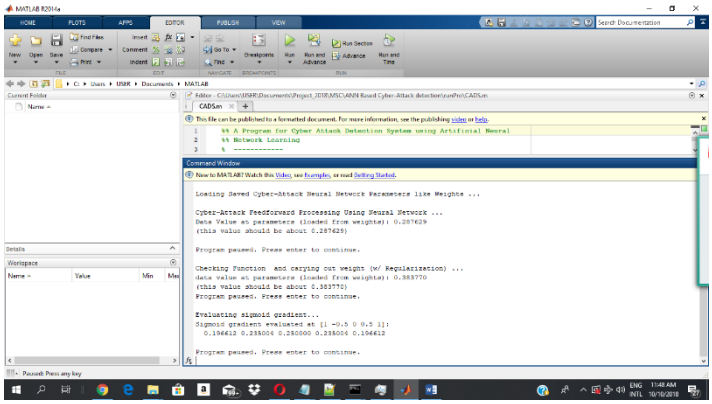

Fig. 4.4 Showing the Initial weight and the Evaluated Sigmoid gradient

The values of the weight of the neural network keep changing in the training phase to adapt to the training data so that the performance of the whole Cyber-Attack detection system will be constantly improved. As there are 50 inputs (based on KDD dataset, every data flow in the network has 50 different feature values), after the training phase each input will have a corresponding weight value. In total 50 weights will be saved in the input layer, which are ready to be used to conduct the detection task. This is illustrated in figure 4.3 and figure 4.4.

In the output layer, the iteration numbers and the error between the real result and desired result can be obtained. In the whole training process, it was found that though the error value did not keep decreasing after each single training circle, the general trend did decrease which means the CADS performance is being improved.

Technically speaking, when the error becomes less than 0.001, the ANN is considered ready to be used. In figure 4.5 the use of the ANN was illustrated the ports where designated from 0 to 9 and any port that the data pattern matches the attack pattern is simply reported and the port number is displayed to show that the CADS actually worked. The accuracy of the system clearly shows 95% which is high enough.

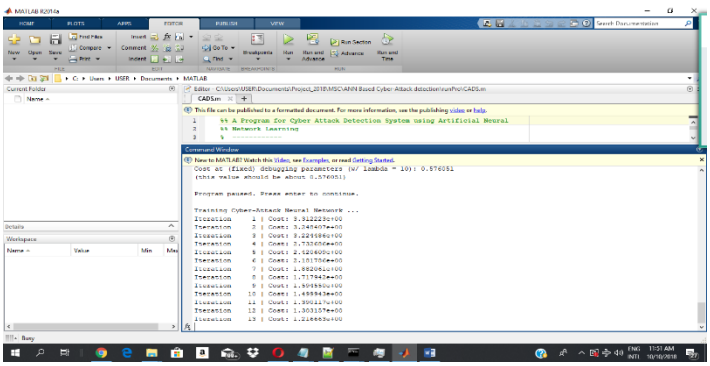

Figure 4.5: Training of the ANN for 50 features of the CAD System improving the weight

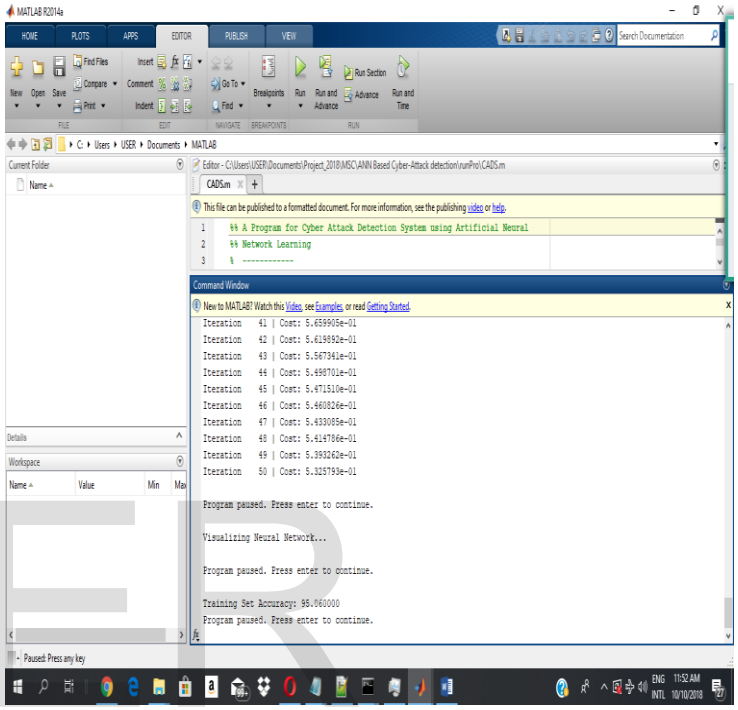

Figure4.6: Iteration done to improve the weight of the ANN

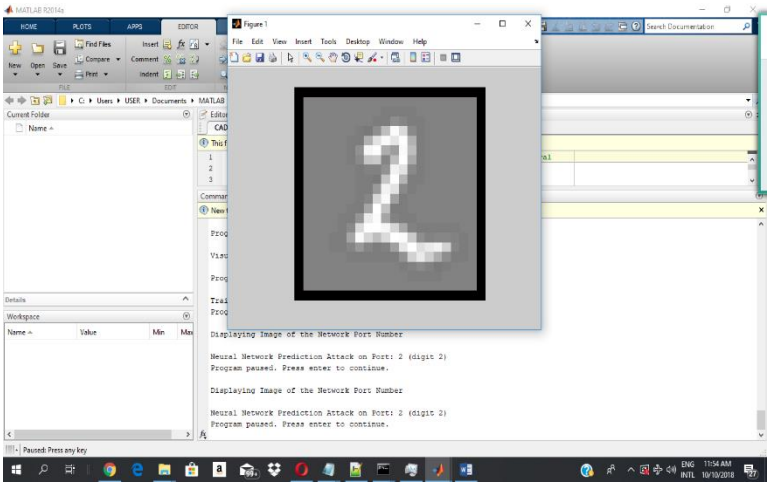

Figure 4.7: Executed CADS ANN showing the network port number of Attack

[7]

In the application developed in the project, we can activate the start by directing the data to where the ANN can easily locate the data and execute it. The folder where the application was stored should also be the folder where the data is sent, however if the data is in a separate location then it must be well specified in the code so that the system can locate it and load it to memory when execution starts.

5. Conclusion

In conclusion, we have been able to design a cyber-attack detection system via neural network technology. The designed system was represented using models developed in the system. An application was equally developed based on the design provided in the work. The developed application was tested using data from KDD set with the desired features required to provide required behaviour training from the neural network in the system. The testing was done in other to evaluate the system using the data available. In all the thesis was able to successfully develop a good cyber-attack detection system using artificial neural network and successfully detect network infiltrators by reporting the port in which such attack is targeted. The application developed in this project can be deployed in many network environments to detect cyber intruders and possibly deter them from carrying out malicious attacks on users' network.

6. Recommendations

We recommend the work developed in this project to developers of cyber security detecting systems. We equally recommend the work to researchers who are interested in making further research that can extend the work done on this project to cover more extensive features more than the once covered in this research. Advanced researchers who are working on neural network and those who wish to apply neural network to other systems will equally find the research in this thesis useful.

.

7. Contribution to Knowledge

Neural Network has been applied in different areas but in this work, we have made some significant contributions in the following ways:

1. Applied neural network in cyber-attack using feature classification based on the data collected.
2. Determination of network port where an attack pattern has been identified.
3. Development of the cyber-attack application detection system.

8. REFERENCE

REFERENCES

[1] B. Andreea, "Cyber-Attacks – Trends, Patterns And Security," in *7th International Conference On Financial Criminology (13-14)*, Oxford, United Kingdom: Wadham College., 2015.

[2] F. Vince, Cyber Attacks: Prevention and Proactive Responses., nil: Practical Law Publishing Limited and Practical law Company, 1., 2011.

[3] V. M. a. J. d. S. F. Paulo M. Mafra, "Octopus-IIDS: An Anomaly Based Intelligent Intrusion Detection System," IEEE, nil, 2010.

[4] S. a. B. H. T. Bhavin, "Artificial Neural Network based Intrusion Detection System: A survey," *international Journal of Computer Application,* vol. 39, no. 6, pp. 13-18, 2012.

[5] M. A. A. &. Z. X. Yousefpour, "Electrophoretic deposition of porous hydroxyapatite coatings using polytetrafluoroethylene particles as templates.," *Materials Science and Engineering,* vol. 27, no. 5-8, pp. 1482-1486, 2007.

[6] B. a. T. B. H. Shah, "Artificial Neural Network based Intrusion Detection System: A Survey," *Journal of Computer Applications,* vol. 39, no. 6, pp. 13-18, 2012.

[7] P. a. S. ,. S. K. Aggarwal, "Analysis of KDD Dataset Attributes-Class wise for Intrusion Detection.," *ScienceDirect Procedia Computer Science,* vol. 57, no. nil, pp. 842-851, 2015.