International Journal of Advance Industrial Communication and Cyber Security Systems 2022

MODELING OF NEURO BASED STRATEGY FOR MITIGATION OF CYBER THREAT ON 4G WIRELESS NETWORK USING ARTIFICIAL INTELLIGENCE TECHNIQUE

[1]Mba J.C., [2]Asogwa T.C.

[1,2]Enugu State University of Science and Technology

chiomajulietmba@gmail.com, yayoengine@yahoo.com

Abstract

This paper presents modeling of neuro based strategy for the mitigation of cyber threat on 4G wireless network using artificial intelligence technique. The aim was to develop an intelligent botnet detection firewall for the security of 4G network using machine learning. This was achieved using data collection of botnet, feature extraction, artificial neural network, training and classification. The neural network based botnet detection algorithm was modeled with self defining equations and then implemented on a 4G network using Simulink. The result of the algorithm was measured with Receiver Operator Characteristics (ROC), Mean Square Error (MSE) and validated with tenfold cross validation approach. The True Positive Rate from the ROC is 0.9989 while the MSE is 2.7054e-5. The implication of the result showed that algorithm was able to detect botnet correctly with an accuracy of 97.6%.

Keywords: Botnet, 4G network, Cyber Attack, Regression, Server, ANN, Throughput

I. INTRODUCION

The design of 4G network has five security models to protect the various layers of the network architecture. According to Liyanage (2015), these security models were designed with encryption technology, but the limitation of this security technique like lack of adaptivity, unreliability, etc provides backhole for attackers and has remained a major problem resulting to major threats like botnet, wormhole, malware, etc. (Eze et al., 2022; Mizuno et al., 2017) which lead to issues of denial of service and eventual shutdown of the server. This has resulted to many problem like loss of information, theft, lack of integrity among other issues and require urgent solution. The benefit of solving these problems will provide reliability, confidentiality, integrity among other merits to the stakeholders. The aim of this research is the modeling of neuro based strategy for the mitigation of cyber threat on 4G wireless network using artificial intelligence technique. The importance of this research cannot be overemphasized as it will provide countless number of benefits to the stakeholders like the administrators of 4G network, the public and private enterprises which depends on this Ethernet platform to store and communication vital information. This paper will also provide reliable security model for cyber security experts and administrators which can be recommended and also deployed for the security of 4G networks in other domains.

2. THEORY OF BOOTNET

The Botnet used four key components which are the botmaster, command and control

server, botcode and the zombies to attack a network Shamsul and Yahwant (2018). The botmaster is the hacker who organized and inflicts the attack based on domain flux technique to connect, command and control server (i.e a Common Computer (C&C) used by cyber criminals for cyber attack. This C&C server transmits botcode which is the botnet malware to devices (Zombies) which are then used to attack the targeted server or any internet of things device. The attributes of this botcode and their descriptions are presented in the table 1; while systematic review of relevant impact of botnet and techniques used to combat them was presented in table 2;

Table 1: Data attributes of BotNet (Shamsul and Yahwant, 2018)

Features	**Description**
Variance of payload size in time window	Useful for finding DOS evasion techniques employed in the communication between Bots and C&C consisting in sending fake packets
Ratio between in packets and out packets	Bots are not managed by humans and are programmed to respond to sets of commands they receive.
Number of packets	Some botnets maintains connections by sensing large packet per time window
Packet size (Bytes)	It revealed the typical characteristics of the network protocols and refers to the entire flow
Number of packet less then 320bytes	This is used in peer to peer botnet or C&C communication
Average payload size	In legitimate traffic this value is higher then botnet flow

Table 2: Systematic Review of Literature

Author	**Technique**	**Work done**	**Research gap/Limitations**
Eljona et al. (2016)	Machine learning	In the study 4G network was the center of attraction as it has recorded many online threats since its evolution. The study developed an unsupervised machine learning algorithm using neural network to mitigate this cyber threat on 4G network.	The study achieved detection accuracy of 89.73%, but leaves room for more improvement.
Gagnon and Fanadi (2017)	Artificial neural network	The study collected data of 4G network and train with neural network algorithm to mitigate blackhole.	The accuracy achieved is 89.78% which is good but can be improved
El-Sayed and Feras	Hybrid artificial	This work advanced fuzzy classifier and generic algorithm as a hybrid approach to	92% accuracy

(2015)	intelligence	provide optimal solution to cyber-attack	
Sulaiman et al. (2021)	Support Vector Machine	This researched applied the Support Vector Machine technique for the mitigation and detection of Cyber-Attack over a 4G data communication and transmission network using data collected from KDD dataset.	The result achieved an attack detection accuracy of 90%
Ettiane et al. (2018)	Encryption	This work described and identified some of the various methods of detecting and preventing DDoS on a communication network in order to establish a secure connection on a mobile network for mobile devices.	85% accuracy but not adaptive
Sulaiman and Al-Shaikhli (2014	Cryptographic algorithms based on different factors	The study analyzed the various cryptographic techniques usually applied to ensure security in data transmission over a 4G network. These was simulated with MATLAB toolbox and evaluated.	The result showed that the proposed algorithm is preferred for the security of packet and not the network.
Ronaldo et al. (2020)	Encryption technique	This work combined Advanced Encryption Standard (AES), Blowfish algorithm and Triple Data Encryption Standard (3DES) for the cryptographic method and then implemented with Matlab	The result achieved detection accuracy of 92% which is good, but leaves room for improvement.

3. METHODLOGY

The methodology employed artificial neural network to develop an algorithm for the detection of botnet in 4G network. Data of botnet was collected and then trained with the neural network algorithm using back propagation to generate the neuro based firewall deployed on the eNodeB of 4G for the security of the network against threat. The implementation was achieved with Simulink environment. The research methods were discussed as follows;

3.1 Data collection

This is the data collected to train the artificial intelligence technique proposed and develop the security model. The primary source of data collection is the CyberSOC Company located at Abuja, Nigeria (a cyber security firm) which provided 15 Gigabit (sample size) of Botnet infected WLAN data. The secondary source of data collection is the Github repository which provided the Botnet CIADA dataset. These data were extracted and used to develop the security model proposed.

3.2 Data extraction

This is the process of drilling the features of the botnet data collected into a compact feature vector for training. This was done using statistics and feature extraction

toolbox which was developed using histogram oriented gradient method in (Asogwa and Ituma, 2018). This drill the feature vectors of the botnet into statistical values and then stored for training process.

3.3 Artificial neural network

The machine learning algorithm proposed to solve this problem is the neuro based strategy formulated from artificial neural network adopted from Eze et al. (2022). This has been used in many works reviewed to address this problem of cyber threat, but due to the deep configuration of the network suffers issues of latency on the network. To address this problem, the researcher propose a feed forward configuration of the neural network which is a much simpler network form, but very effective in training, learning and making accurate decisions. This was used to train the extracted data from the Botnet data collected. The neural network presents the structure of the neurons and how they are interconnected in the hidden layers for the computation of the botnet feature vectors and then produce the desired output for the classification of the attack. These neurons have weights and bias function which are activated before feeding to the hidden layers using an activation function. The function of the activation function is to ensure the feature vectors of the botnet data are within a compatible format in the scale of -1 to 1 as in the hyperbolic tangent activation function used for this work.

3.4 Training and the neural network botnet detection algorithm

This process involves learning the neurons with the Botnet feature vectors for the pattern recognition. The feed forward neural network developed in the previous section was feed with the training dataset and then make to learn the botnet data pattern using a training algorithm. The training algorithm adopted for this training process is the back propagation algorithm. This was used to adjust the neurons to learn the botnet features and then generate the neuro botnet detection algorithm.

3.5 Classification of the threat

Before training the neural network, the dataset was divided into three sections which are the test, training and classification sets in the ratio of 70:15:15 and then simultaneously trained, test and validated by the neural network tool. The training process provided the neuro botnet detection algorithm which was used for the classification of botnet.

4. MODELING

The artificial neural network was modeled starting with single neuron model which is the building block of the neural network via multiple inter connection of the neurons. The block model of a single neuron is presented in the figure 1;

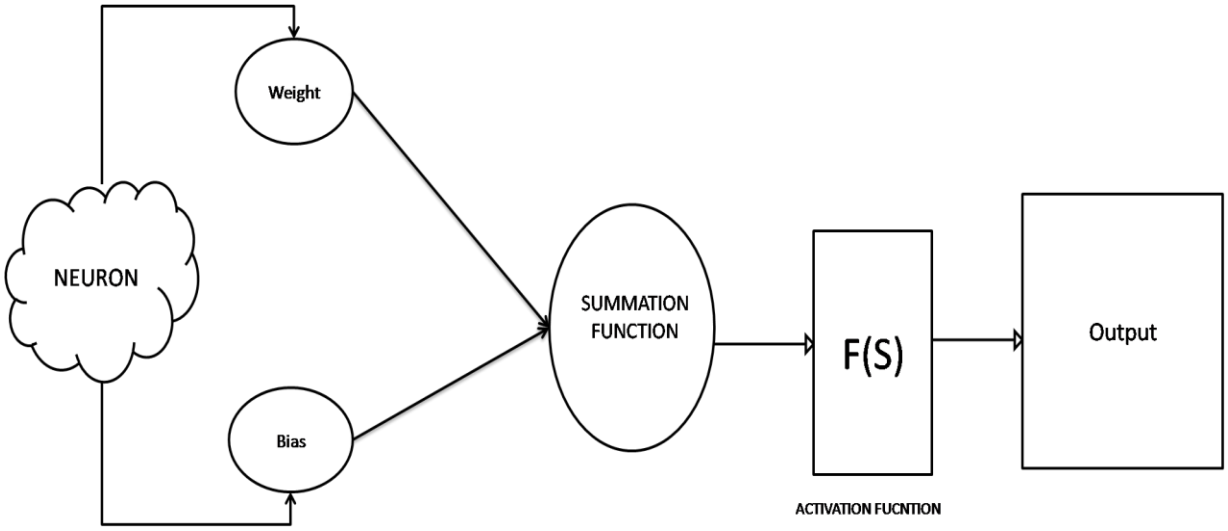

Figure 1: Model of a single neuron

The figure 1 presented the model of the single neuron which ahs weight, bias and activation function. The weight and the bias are inside the neurons while the activation function was used to maintain balance scale on the data feature vectors from the neuron for better training performance without convergence. The activation function type used in this neural network model is the tansigmoid function which ensures that the data scale do not exceed (-1 to 1).

The model in the figure 1 was used to develop the interconnected neural network architecture which was feed with the data collection of botnet model in table 1 to train the neurons of the bonet and generate the botnet detection algorithm. the nodel of the neural network was configured considering the number of input attributes of the botnet features with a training algorithm which enables the neurons learn the botnet patterns was presented in the figure 2;

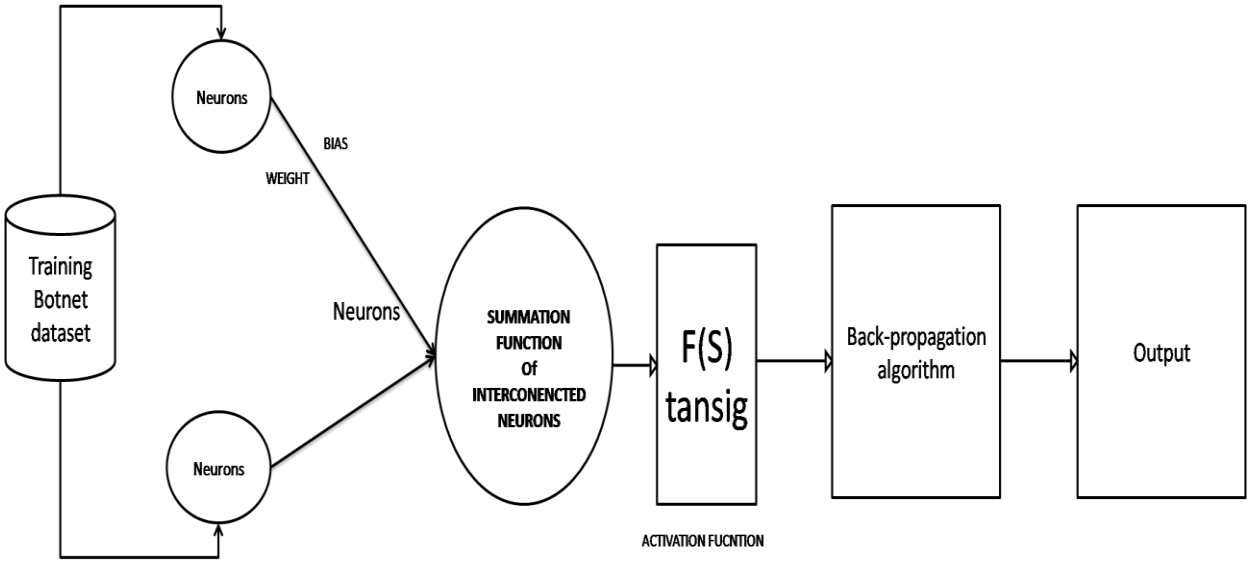

Figure 2: The model of the Neural Network

The figure 2 presented the model of the neural network architecture which was used to train the botnet data. Then neural network was also configured with the training parameters in table 3 for the setting of other parameters inspired from the testbed characterized. The training process employed back propagation training algorithm adopted from (Eze, 2022) to learn the neurons of the data and then make time series detection of botnet.

Table 3: Training Parameters

Parameters	Values
Training epochs	6
Size of hidden layers	20
Training segments	15
No. delayed reference input	23
Maximum feature output	2
Maximum feature input	23
Number of non hidden layers	12
Maximum interval per sec	2
No. delayed output	1
No. delayed feature output	2
Minimum reference value	-0.7
Maximum reference value	0.7
Time	0.05sec

It has to be noted that the neural network on its own divided that input botnet into training and test set when the data was loaded (this happens inside the neural network toolbox). The aim was to train and then use the test set to check the reliability of the algorithm in making time series classification of botnet using performance evaluation tools such as Mean Square Error (MSE) and Regression. These parameters will be discussed later in the next chapter to analyze the efficiency of the algorithm developed. The data flow chart of the training process to generate the algorithm for the detection of the botnet is presented in the figure 3;

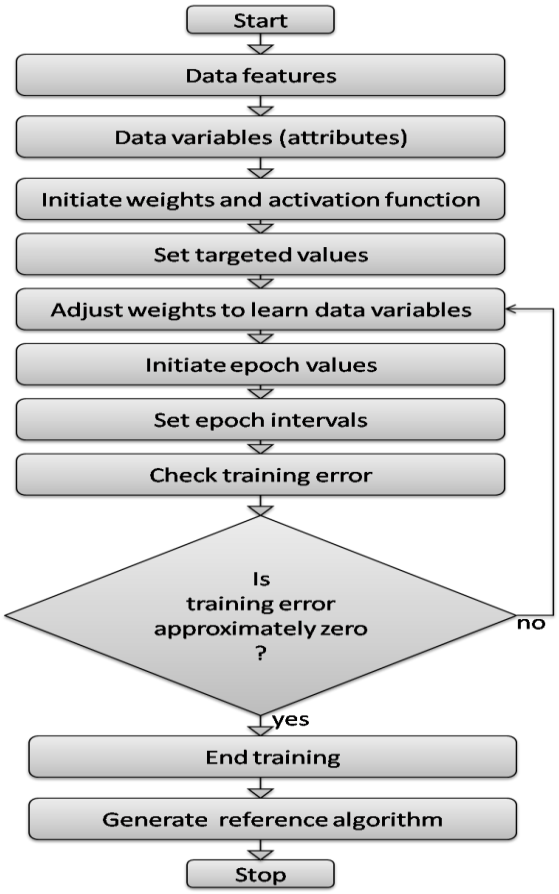

Figure 3: Flow chart of the back-propagation algorithm

The figure 3 presented the neural network data flow chart, showing how the input data feed to the neurons were activated and trained by the training algorithm to generate the reference botnet detection algorithm. During the training process, the weight of the neurons were adjusted by the back propagation algorithm based on the reference bias values which is the targeted function to make sure the patterns of the botnets were learnt. The pseudo code of the algorithm was presents as;

Start

1. *Load botnet dataset*
2. *Identify botnet attributes by neurons*
3. *Configure neural network model in figure 2*
4. *Initate training algorithm (Lavernberg back propagation algorithm)*
5. *Initiate activation fucntion (Tansig)*
6. *Initate epoch values and starting interval*
7. *Initate performance evaluaiton fucntions (MSE and Regression)*
8. *Train the neural network*
9. *Check training performance at each epoch interval*
10. *If*
11. *Least MSE and best R value = true*
12. *Then*
13. *stop training*
14. *Else*
15. *Return to weight (Back-propagation)*
16. *Adjust value*
17. *Retrain*
18. *Apply step (9;10;11)*
19. *Do*
20. *Until*
21. *Step (11) is true*
22. *Then*
23. *Stop Trianing*
24. *Generate botnet algorithm*
25. *Allow new data*
26. *Classify new data collected with botnet algorithm*
27. *If*
28. *pattern the same as algorithm = true*
29. *flag as botnet*
30. *Else*
31. *Allow throguhput*
32. *Return*
33. **End**

5. SYSTEM IMPLEMENTATION

The system was implemented using neural network application programming software in Simulink. The tool was configured with algorithm developed and then used to build the neural network based botnet detection firewall. The neural network tool was loaded with the botnet data and then configures the neural network model as in figure 2 using the setting in table 2. The training algorithm in figure 3 was then selected to train the neural network and generate the neuro botnet firewall as in figure 4;

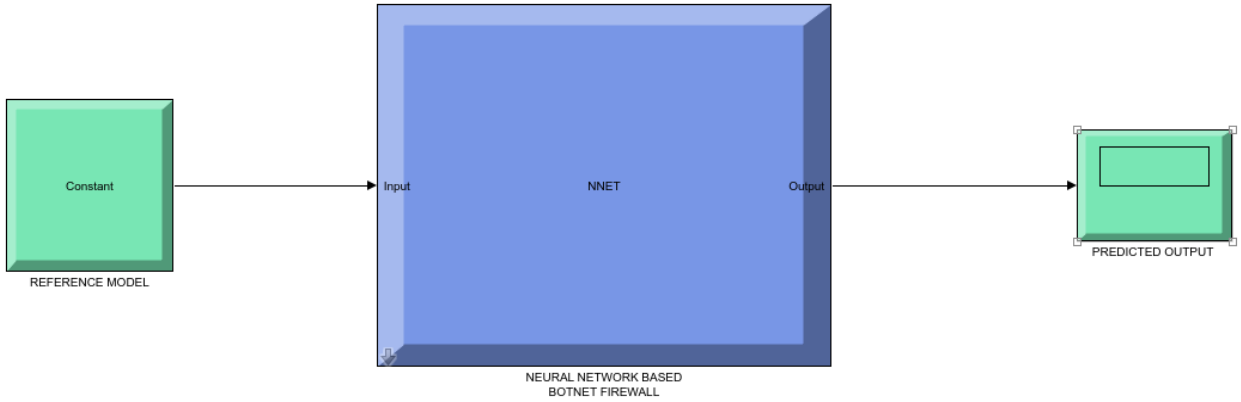

Figure 4: The Simulink model of the neuro inspired botnet firewall developed

The figure 4 presented the simulink model of the neuro inspired botnet firewall developed for the mitigation of botnet on wireless network. The firewall was integrated on a 4G network as showed in figure 5 and simulated with the parameters in table 4.

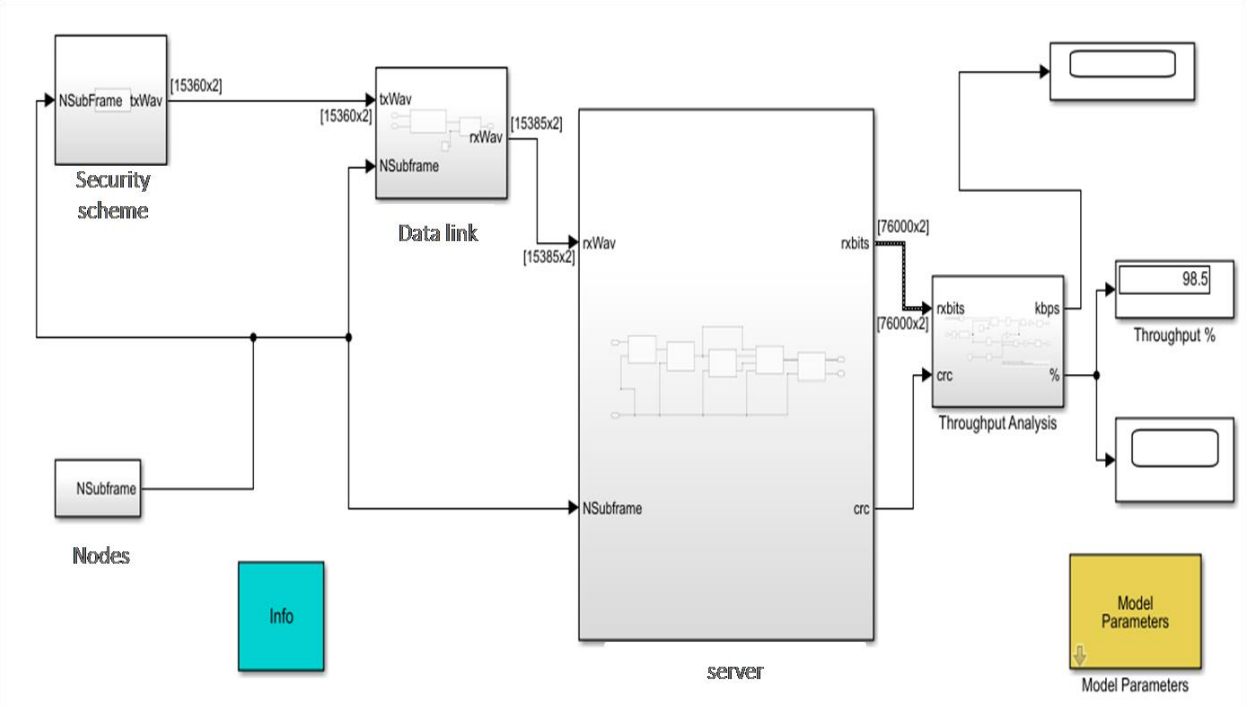

Figure 5: The Simulink model of the protected 4G network

The figure 5 presented the model of the improved 4G network with the firewall developed and installed with the gateway for the protection of the network against botnet.

The check the quality of service implication of the algorithm, the network was simulated with the performance of the testbed table 4 and the results all reported in the section.

Table 4: simulation parameters

Parameters	**Values**
Communication standard	IEEE 802.11g
Monitoring system IP	172.32.3.99/25
Simulation time interval	0.0020ms
Modulation type	16 and 64 QAM
The Resolution bandwidth	12 kHz
Power	2.2W
Gateway	172.32.3.1
Duplexing scheme	Time division multiplexing

6. PERFORMANCE OF THE NEURO INSPIRED ALGORITHM

The section presented the results of the botnet detection algorithm developed. The was measured using MSE to read the amount of error which occurred during the training and testing process. While the Receiver operator characteristic (ROC) analyzer was used to measure the ability of the algorithm to detection incoming botnet packet and flag off as an attack or threat. These MSE and ROC were analyzed with hope of achieving the ideal values which are equal or approximately zero for MSE and equal or approximately True Positive Rate (TPR) of one for the ROC as presented in figure 6;

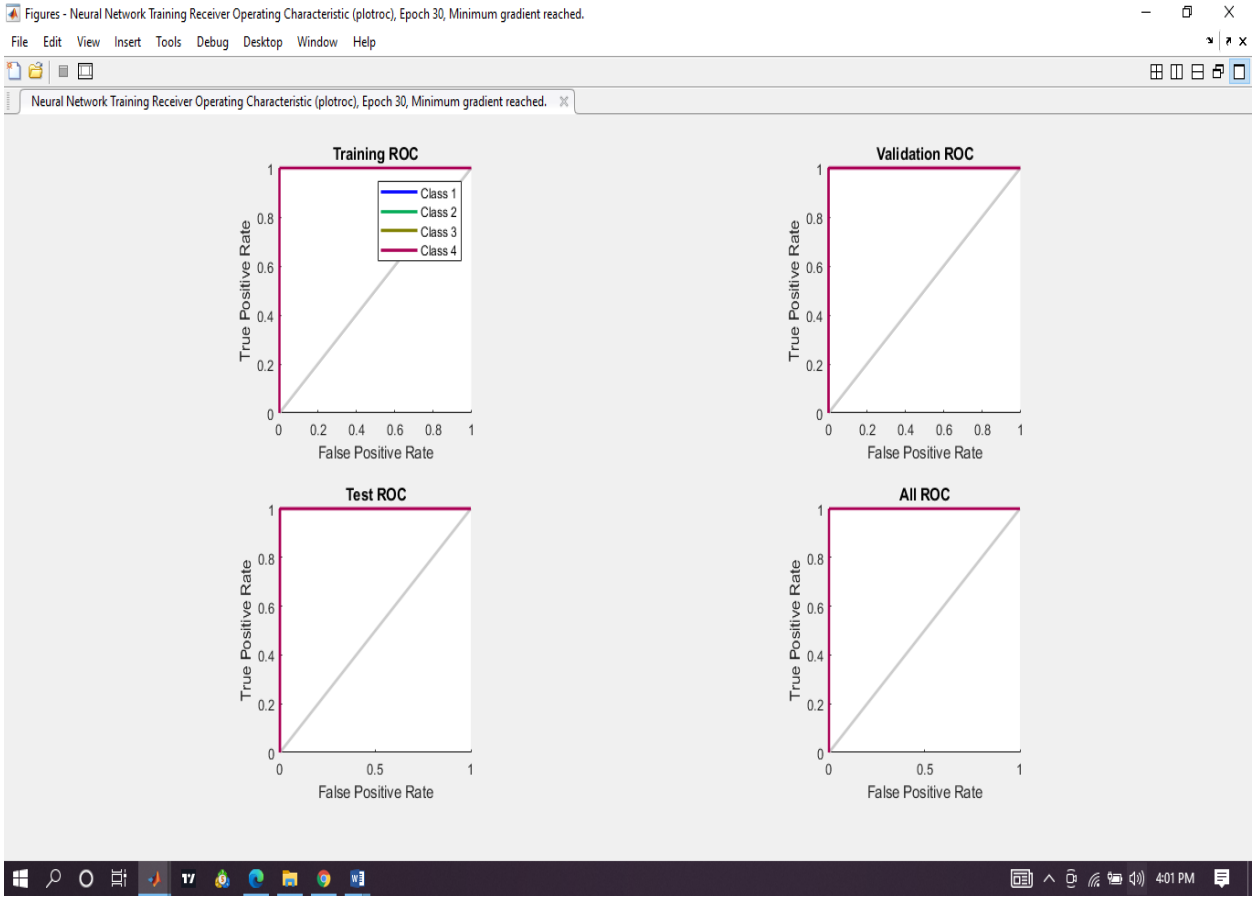

Figure 6: ROC performance of the neural network algorithm

The figure 6 presented the ROC performance of the algorithm. This was achieved using the average between the training , testing and validation regression result as shown to score the overall regression value of the algorithm as TPR =1. Although this regression is impractical due to some external factors in real live situations, but in simulation as shown it is possible and it implies that in reality, the algorithm was able to detection botnet instantaneously. The next result presented the MSE performance of the algorithm as shown in figure 7;

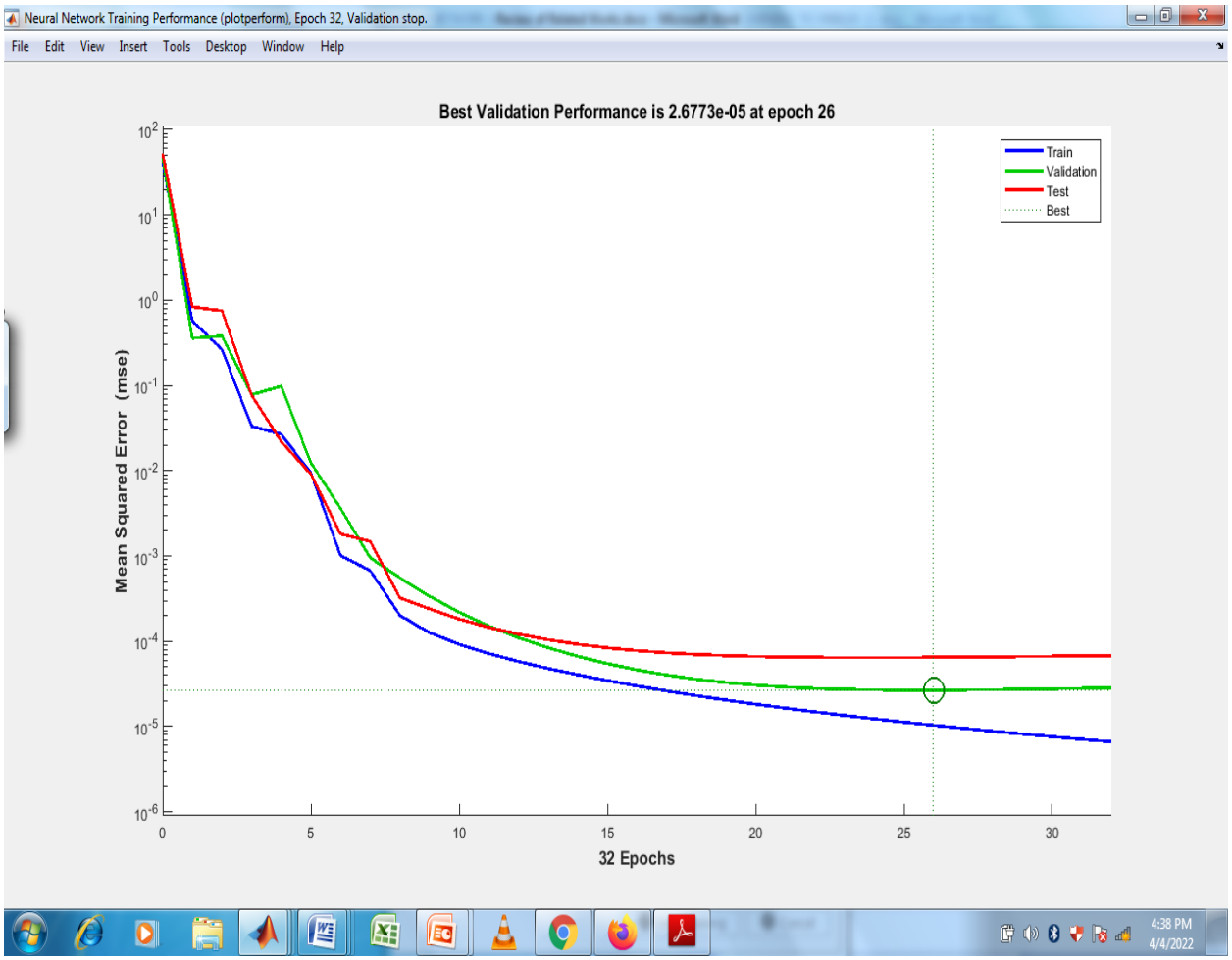

Figure 7: MSE performance

The figure 7 presented the MSE values measured with the average of the training, test and validation set and at intervals of epoch until the least MSE was achieved at epoch 26 which is 2.6773e-5. The implication of this result showed that minimal error was recorded at the training of the algorithm showing that the neural network properly learnt the botnet data for the detection of time series attack on the 4G network. The detection accuracy of the botnet algorithm developed was also evaluated using confusion matrix as shown in figure 8;

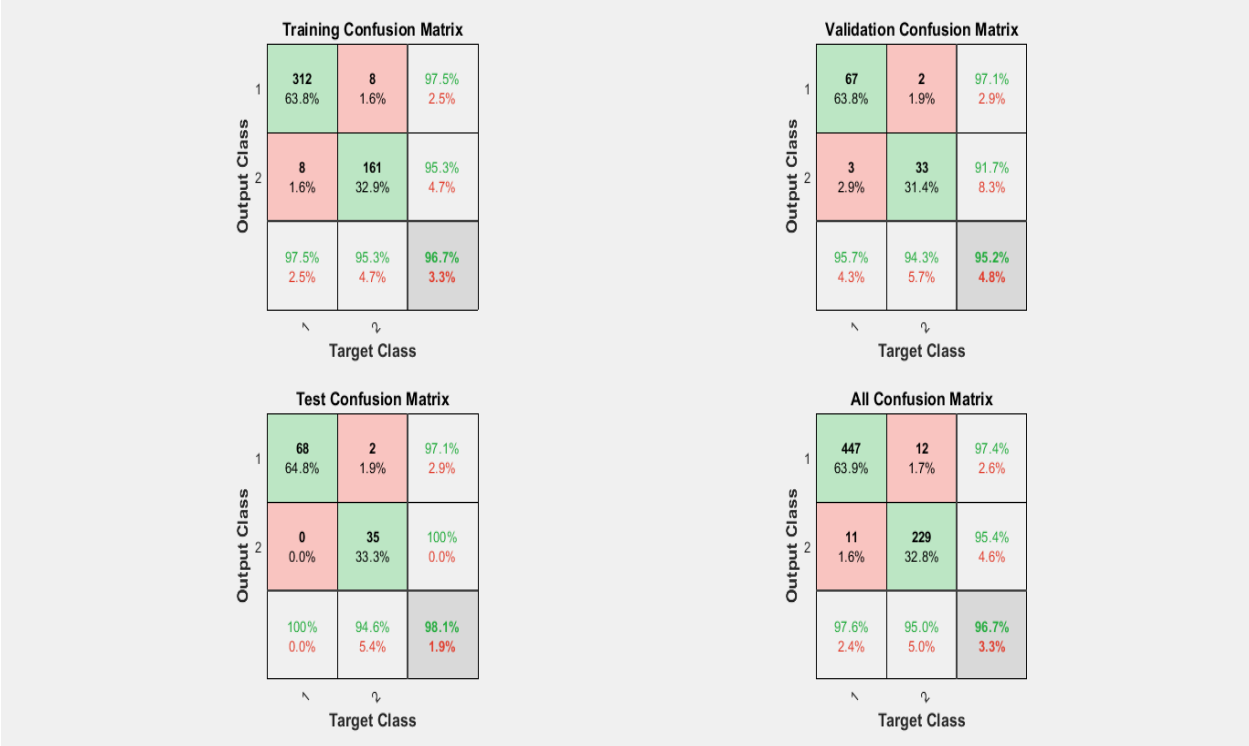

Figure 8: Confusion matrix

The figure 8 presents a confusion matrix used for the evaluation of the botnet detection accuracy and from the overall confusion matrix performance it was uncovered that the threat detection accuracy is 96.7%. The implication of the result showed that the algorithm developed learns the pattern o the botnet correctly and was able to correctly classify the attack on a 4G network.

6.1 Validation of the algorithm

Having successfully evaluated the performance of the algorithm developed with MSE and TPR and achieved good results, the system was validated using tenfold cross validation technique which iterative evaluated the system performance in tenfold and compute the average as shown in the table 5;

Table 5: Validation of the Results

S/N	MSE	TPR
1	2.6773e-5	1.0000
2	2.0254e-5	0.9978
3	2.1975e-5	0.9886
4	2.5845e-5	0.9982
5	2.9333e-5	0.9978
6	2.1566e-5	1.0000
7	2.0752e-5	1.0000
8	1.7536e-5	0.9738
9	2.1466e-5	0.9984

10	2.8975e-5	0.9977
Average	2.7054e-5	0.9989

The table 5 presented the validation result of the algorithm developed for the detection of botnet. The aim here was to check the reliability of the algorithm and ensure it maintain optimal botnet detection performance over time. The result showed that the average TPR is 0.9989 while the MSE is 2.7054e-5. The implication of the result showed that the TPR and MSE were as expected indicated good botnet detection performance.

6.2 Comparative analysis

The comparative analysis compared the performance of the new algorithm developed with neural network and other algorithm developed for the detection of cyber threats in wireless network as shown in table 6;

Table 6: Comparative analysis

Author	**Technique**	**Accuracy**
Eljona et al. (2016)	Artificial neural network	89.73%
Gagnon and Fanadi (2017)	Artificial neural network	89.78%
El-Sayed and Feras (2015)	fuzzy classifier and generic algorithm	92%
Ettiane et al. (2018)	Encryption	85%
Sulaiman et al. (2021)	Support Vector Machine	90%
New technique	Neuro inspired algorithm	96.7%.

The result showed that the performance of the new algorithm developed was better than the conventional algorithms. This was because the feature of the data was extracted so as to generate enough vectors for training unlike the other algorithms.

7. CONCLUSION

Cyber security has remained one of the most discussed topic in this 21st century. This was due to the rapid transformation in the information and communication technology viz Internet of Things (IoT). However, this offering of IoT also presented the need for optimal security as more data are uploaded and stored in the cloud on daily basis. Intruders target the cloud server to steal information or deny user access using botnet as one of the most used attack model. This research has solved this problem via the development of an intelligent firewall using neural network and botnet data collected from a case study testbed. The security firewall was implemented with simulation and tested. The result showed that the algorithm was able to protect the network against botnet at high accuracy.

REFERENCE

Asogwa T.C and Ituma C. (2018)"Machine learning based digital recognition of identical twins to support global crime investigation" [J] IJLTEMAS; Vol (7), Issues 12, ISSN 2278-2540, pp 18-25.

Eljona Proko, Alketa Hyso, Dezdemona Gjylapi (2016). Machine Learning Algorithms in Cyber Security. CEUR-WS.ord/vol-2280/paper-32.pdf

El-Sayed M. El-Alfy and Feras N. Al-Obeidat (2015). Detecting Cyber-Attacks on Wireless Mobile Networks Using Multicriterion Fuzzy Classifier with Genetic Attribute Selection. Hindawi Publishing Corporation Mobile Information Systems Volume 2015, Article ID 585432, 13 pages http://dx.doi.org/10.1155/2015/585432.

Ettiane, R., Chaoub, A., & Elkouch, R. (2018). Robust detection of signaling DDoS threats for more secure machine type communications in next generation mobile networks. In Electrotechnical Conference (MELECON), 2018 19th IEEE Mediterranean (pp. 62-67). IEEE.

Eze E.M., Ituma C., Asogwa T.C., Ebere U.C. (2022)"Development of Machine Learning Based Security Algorithm for 4G Network against Botnet" International Journal of Research and Innovation in Applied Science (IJRIAS) volume-7-issue-2, pp.70-75

Gagnon F., Esfandiari B. (2017) "Using Artificial Intelligence for Intrusion Detection. In Proceeding of the Conference on Emerging Artificial Intelligence Applications in Computer Engineering, Amsterdam, Netherlands. pp. 295-306.

Liyanage, M., Ahmad, I., Ylianttila, M., Gurtov, A., Abro, A. B., & de Oca, E. M. (2015). Leveraging LTE security with SDN and NFV. In Industrial and Information Systems (ICIIS), 2015 IEEE 10th International Conference on (pp. 220-225). IEEE.

Mizuno, S.; Hatada, M.; Mori, T.; Goto, S. (2017) Bot Detector: A robust and scalable approach toward detecting malware-infected devices. In Proceedings of the 2017 IEEE International Conference Communications (ICC), Paris, France; pp. 1–7.

Ronaldo, F., Pramadihanto, D., & Sudarsono, A. (2020). Secure Communication System of Drone Service using Hybrid Cryptography over 4G/LTE Network. In 2020 International Electronics Symposium (IES) (pp. 116-122). IEEE.

Shamsul H., Yahwant S. (2018) "Botnet detection using machine learning"5th International conference on parallel distribution and grid computing" pp.1-15.

Sulaiman Yousef Alshunaifi, Shailendra Mishra and Mohammed Abdul Rahman AlShehri (2021). Cyber-Attack Detection and Mitigation Using SVM for 5G Network. Intelligent Automation & Soft Computing DOI:10.32604/iasc.2022.019121

Sulaiman, A. G., & Al Shaikhli, I. F. (2014). Comparative study on 4G/LTE cryptographic algorithms based on different factors. International Journal of Computer Science and Telecommunications, 5(7), 7-10.