NIJBAS
Publications 2024

OPEN ACCESS
ONLINE ISSN: 2992-5797
PRINT ISSN: 2992-6122

NEWPORT INTERNATIONAL JOURNAL OF BIOLOGICAL AND APPLIED SCIENCES (NIJBAS)

Volume 5 Issue 2 2024

https:/doi.org/10.59298/NIJBAS/2024/5.2.516011

Security Model for the Detection of Distributed Denial of Service Attack (DDoS) at the Access Layer in Cloud Reference Architecture

Etuk, Akaninyene Udo and Okoye, Francis

Department of Computer Engineering Enugu State University of Science and Technology (ESUT), Nigeria.
Email: ibomatai1970@gmail.com; francisced@esut.edu.ng

ABSTRACT

DDoS attacks on the cloud have become an emerging problem, which calls for an intelligent protection solution for information, communication and computing resources. Cloud reference architecture as a new technology with wider access facility, the access layer in the reference architecture becomes grave to numerous security challenges, and it is mostly exploited by the attacker using compromised computers to launch DDoS attack which affects its performance by shutting down some services. Many security frameworks have been proposed in the past, but they are not enough to provide security solution for accurate detection and control of DDoS attack at the access layer. Intelligent security model based on artificial neural network was developed to detect and control DDoS attack at the access layer. DDoS dataset obtained online was used to train and test the intelligent security model using MATHLAB workspace. Simulated results implemented and generated with receive operator characteristic analyzer (Roc) showed a true positive rate of 98.2% to detect and control DDoS attack at the access layer and a false negative rate of 0.02%. The inclusion of additional parameters to determined and identifies the source of the attack, whether it is lunch from outside or inherent within the reference architecture is recommended.

KEYWORDS: Reference Architecture, Access Layer, Distributed Denial of Service (DDOS), Artificial Neural Network's (ANN's)

INTRODUCTION

Cloud reference architecture is a distributed and decentralized network that is self-sustaining based on deployment model [1, 2, 3, 4]. The access layer which is the aperture provide the integration for interfaces and network within and outside the reference architecture. Access from remote or mobile devices makes the architecture internet enabled at all times. A typical cloud reference architecture of cloud computing is depicted in figure 1.

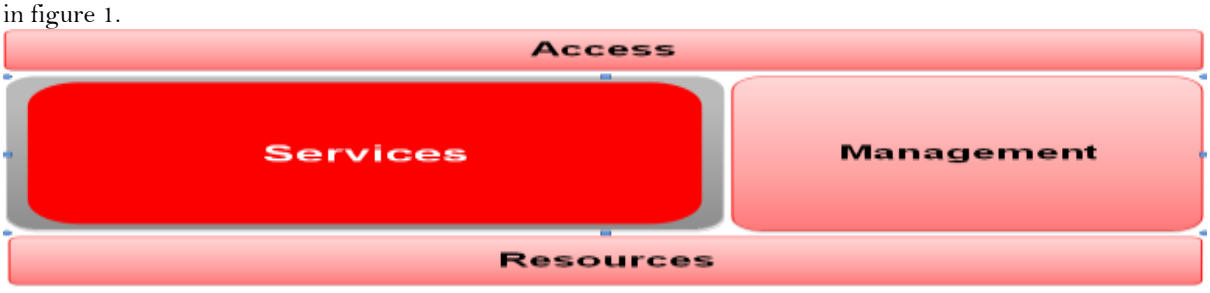

Figure 1: Logical block diagram of reference architecture

The access layer is the layer where all pre-requisite security policies are created and enforced with enabling template for the management of IP addresses and ports. It provides security constraint for communication in the reference architecture. Since it connects with other network such as the internet, hence, the access layer provides a multi-hop connectivity. The reference architecture is a generic high-level theoretical foundation of cloud computing [5] It determines the needs, structures, architectural attributes/functions and processes of the cloud, and can be deployed either as private, public or hybrid model. In the entire deployment model, the reference architecture are susceptible to severe security challenges by hackers [6], as a result, functional and

OPEN ACCESS
ONLINE ISSN: 2992-5797
PRINT ISSN: 2992-6122
normal services will cease with the capacity of the reference architecture greatly overwhelmed or sometime shutdown. Some of the most frequent attacks launched in reference architecture according to [7] are account or service hijacking, malicious Vm creation, customer-data manipulation, insecure Vm migration and denial of service (DoS). Security and performance of the architecture are the most addressed and evaluative issue considering the amount of data reserved in it and shared network resources [8]. However, among all these attacks, the denial of service (DoS) attack is regarded as the most hazardous attack. DOS attack is a major security challenge in the emerging cloud computing technology [9]. DoS attack can be described as an attack designed to prevent some cloud services or resources from optimizing their normal services. The problem becomes more complicated when the attack traffic is from multiples sources. This type of attack is known as distributed denial of service attack (DDoS) [10]. Therefore once the reference architecture is attacked by intruders with DDoS attack patterns, it ceases to deliver normal service which cripples it performance and can undermine the services of the target system by sending extremely massive quantity of data packets to the target system or networks through the access layer. As a result, the bandwidth resources are consumed at the target system, rejecting legitimate request for resources [11]. This makes it harder to discriminate large volume of attack traffic from transient burst of normal traffic. Since the main problem associated with DDoS attack has to do with overwhelming the bandwidth with access request, with the use of botnets to ultimately cripple the saver or take down the network, consequently to protect the reference architecture from malicious traffic and defend it against known DDoS indicative patterns, it is important to detect and control the DDoS incident at the access layer which will block the attack traffic from reaching the target machine and also keep the access layer from becoming part of the botnet [12]. Notorious tools and devices employed in the cloud among networks engaging internet for computing, communication and database management are HULK (HTTP Unbearable Load King), LOIC (Low Orbit Ion Cannon). DDOSIM – Layer7 DDoS simulator, SEM (Solarwinds Security Event Manager) RUDY and Pyloris (Behal and Kumar, 2016). Basically, volume-based attack, protocol attack and application-layer attack are the three most prevalent DDoS migrated attack against the reference architecture, which can be launched internally or externally, that make it far harder to identify the DDoS attack from the attack source before it reaches its target system [13]. Therefore, if this DDoS attack is not detected and controlled at the access layer, it will translate to various complications and sometimes shutdown the architecture. Hence the need for this study, which will concentrate on the development of Intelligent Security Model, based on artificial neural networks (ANN's) that will be fast, brilliant, strong and dependable model for detecting and controlling the identified DDoS attack in reference architecture. To realize early detection and control of the DDoS attacks, normalized data set will be used to train the artificial neural network to establish the profile for normal traffic based on the training algorithm. The main purpose of using ANN based intelligent security model in the detection and control of DDoS attack is that, it has the competent of detecting any distributed attack using specialized pattern [14]. The model will regulate access, thus preserving the privacy and probity of information stored or transmitted in the cloud reference architecture.

Literature Review

DDoS assaults can be detected in real time using an Artificial Neural Network model described by [15]. In order to distinguish between DDoS attacks and legal traffic, important parameters (such as source, IP addresses, packet lengths, destination ports, and the sequential number of packets) were extracted. The constructed Artificial Neural Network (ANN) model was trained using parameter values. As a result of this research, an attack model was designed to detect TCP, UDP, and ICMP protocol-based attacks on the internet. DDoS attacks were detected with 98 percent accuracy using the evaluation model. However, it was not possible to identify the sort of DDoS assault based on these parameters at the access layer of reference model. Based on traffic patterns generated by the DDoS attack source, [16] developed a technique for detecting DDoS attacks. This trend joined with identified factors such as Port number, time to live (TTL), formats & port numbers. These data were used to develop a correlation coefficient approach for determining known traffic parameters [17]. Only legitimate traffic may be detected using the traffic analysis technique. This was viewed as a flaw in the method's design. Another major flaw in this presentation was the data set used for the research, which was obtained in 1998 and was therefore too old to be of any use. The features of traffic (such as protocol description, the variety of devices that sign - ups, the volume of traffic generated, and the integration of numerous IP-based services, such as IPTV and VoIP) have shifted dramatically as a result of the removal of significant data. Recurrent Neural Function (RNF) ANN was used by [18] to detect DDoS attacks. They employed parameters including typical payload size, data packets number, packet arrival time variance, and packet size variance to construct a detection algorithm. The created DDoS attack detection approach was 96.5 percent accurate in one data set and 98.2 percent accurate in a second data set, according to simulation. The method based on simulation was shown to be successful, but with a significant lack of accuracy in detecting and controlling DDoS attacks at the access layer. According to [19], a paradigm for ensuring the integrity of cloud reference architecture was suggested using security patterns. Maintaining a misuse pattern with threats and security inventory is the security pattern's primary goal. It also incorporates security best practices, which outline how to counter the known dangers and weaknesses. However, it was found that much of the defense/misuse patterns against identified threats did not solve this problem, particularly the DoS attack which had little or no influence, as most of the Defensive line pattern handles attack at target system, not at access layer. [20] in their work proposed a defense

OPEN ACCESS
ONLINE ISSN: 2992-5797
PRINT ISSN: 2992-6122

mechanism to detect and filter DDoS attacks against the cloud, but fail to mention implementation detail especially at the access layer. [21] presented the Oracle Security Reference Architecture which created three partition of data security, fraud detection and compliance, it was mapped for a particular product with no commitment to vulnerable nature of the access layer. The PCI-Compliant cloud reference Architecture of [21] only look at the fundamental framework for securing cloud that compliant with PCI DSS standard. It uses specific product of the company to define security defense based on the four primary layer, but there was no information on threat analysis that affect each layer of the architecture.

MATERIAL AND METHODS

1. Collect dataset online from CICDDOS2019
2. Celeron-quad-core Intel N3450
3. Windows XP professional X64 edition
4. Mathah 6.5 program (Matworks programming tools)
5. Neural Network Architecture Software-Apache-2.0-(Neuroph).
6. Regression Analyzer.

Analysis of the Proposed System

From the reviewed literatures, DoS attack was identified as the main threat to the reference architecture. This attack affects the access layer of the cloud reference architecture as the most exposed part of the cloud networks by inducing traffic using multiple fake IP address generated from the attack host, thereby over powering the cloud architecture, which eventually shuts it down [14]. It was observed that various security approaches have all been proposed to solve this problem in the cloud. However despite the successes, issues from poor performance and their inability to completely detect a DoS attack at the access layer against the cloud architecture in particular. Hence there is need for a reliable security model which is intelligent and can completely protect the reference cloud architectures against DoS attack at the access layer. The researcher proposed to achieve this based on Artificial Neural Network (ANNs) technique [16]. The technique has been employed in almost all the field of human endeavors to tackle various forms of challenges based on classification of regression approaches. Artificial Intelligent (A.I) mimics human behavior by collecting data of the case study problem, learning from the data and making correct predictions with high accuracy. Therefore in the proposed system, dataset of DDoS attack vectors will be collected and learn the intelligent system technique to be used to generate a reference attack model which will be used to detect future security threat channeled towards the cloud [17]. This will enable real time and intelligent protection of the cloud reference architecture at the access layer and guarantee data privacy and effective database management.

Design of intelligent security model based on ANNs

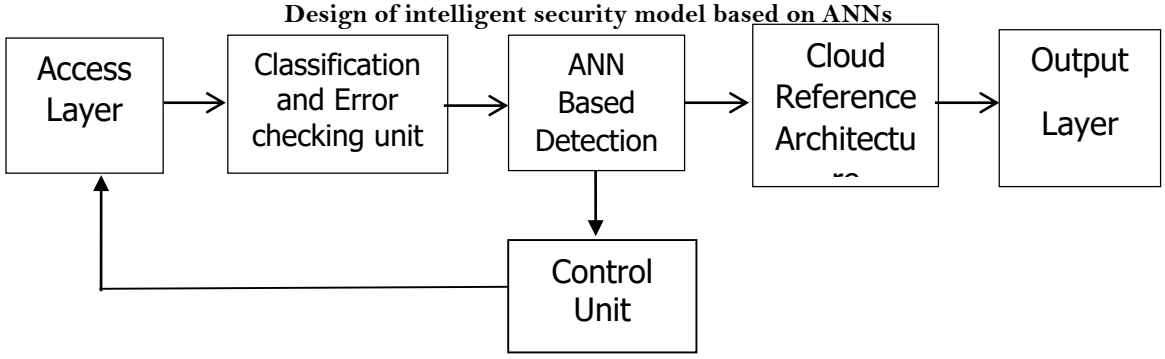

Fig 2: Block diagram of intelligent security model based on ANNs technique

In this section a new ANNs technique to detect and control the DDoS attacks at the access layer in cloud reference architecture is described. To develop a model which secure the access layer from DDoS attacks, two important stages must be implemented, classification/error checking and Detection/Control unit. In most recent research, packets of data are migrated direct to the target system without detection and control mechanism; but with application of artificial neural network based on training algorithm, all packets must be classified according to establish pattern before it is forwarded for detection [15]. It will not be processed principally on used protocol alone but will be subjected to other zero error checking protocol, thus allowing detection and control of malicious flow of data to be separated from normal data packet. The block diagram of figure 2 describes the proposed intelligent security model based on ANN's technique [16]. The access layer, the input layer of the model, where specific security policies are configures and enforces before passing the input to the classification and error checking unit. At the classification and error checking unit, the packets of data and information are classified and learned before being forwarded to the intelligent security model, where each entry represents the number of packets. At this stage the classification/error checking unit acquire information about the architecture and detection algorithm based on pattern [17]. The characteristic feature of data packets analyzed are source/destination IP address source and source/destination port and information about used protocol (UDP, DNS and SYN). In reference architecture they are multiple ways to train the ANN to classify

OPEN ACCESS
ONLINE ISSN: 2992-5797
PRINT ISSN: 2992-6122

the traffic pattern, in this case BP (Back propagation) will be deploy [18]. The classification is done independently of the detection. This approach allows information on the trained ANNs to detect DDoS attack because the algorithm based on trained pattern will check for traffic characteristics which equally increase the precision of the algorithm. At the intelligent security model, the behavioral Patterns are extracted from the data packets regarding abnormalities in terms of source IP address, destination port, etc., based on the features extracted, with the transformation of the intelligent security model during training, the given packets of information is detected and control as normal or infected packet. The control unit protects the end-users when malicious attack is detected [19]. The precision of the control unit depend on the amount of information of the attack that is acquired by the model during training. Once the given packets of information is detected and classified as a normal packet, Access is granted to the cloud which is referred to as the servers, but if it is detected as a useless packet of dataset, it is being controlled and returned to the input unit for reclassification. The output layer in artificial neuron networks is the last layer of neurons that produces designed outputs for the model [20].

Design Flow Chart of Intelligent Security Model

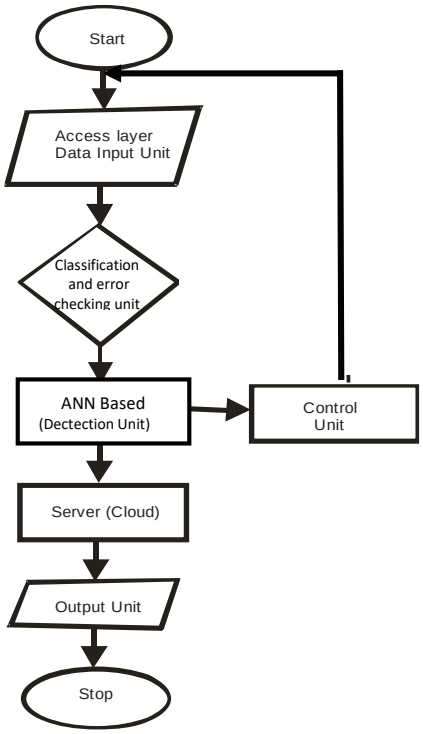

Figure 3: Design flowchart of Intelligent Security Model as shown in figure 3

The DDoS Detection and Control flowchart

The DDoS detection and control flowchart in figure 4 is used to present and explain the overall workflow of the entire system integrated with the intelligent security model as shown in figure 2.

OPEN ACCESS
ONLINE ISSN: 2992-5797
PRINT ISSN: 2992-6122

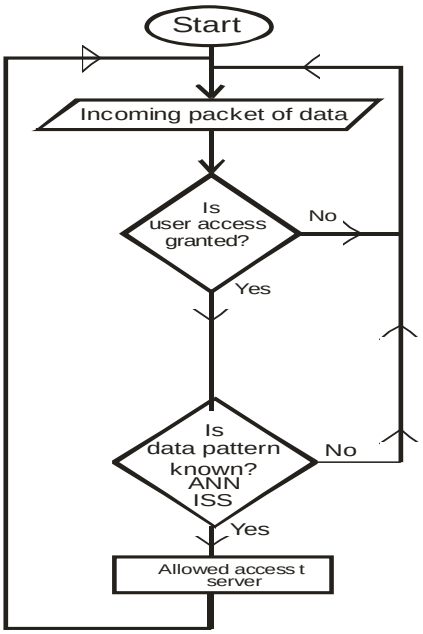

Figure 4: Detection and Control of DDoS attack flowchart

The flow chart presents the data flow from the access layer showing the transmission of packet via intelligent security system to the cloud. From the flowchart it was revealed that before any packet gets to the cloud, it is trained and tested with the intelligent security model as shown in figure 2. The artificial neural network was used to develop an intelligent DDOS security model using the DOS dataset to learn the network on the features and attributes of DDOS packet patterns. This intelligence by the network is used to detect the packet flow from the access layer. The detection process in simple, if the packets are infected with DDOS attributes, the dataset is isolated from the cloud or else access is allowed to the server.

Source of DDoS Dataset

To collect the necessary dataset of the attack vector for training the artificial intelligence technique proposed for this research. CCIDDOS2019 data was chosen [6]. This dataset includes traffic patterns from 12 modern DDoS attacks of (NTP, DNS, 2DAP, MSSQL, NetBIOS, SNMP, SSDP, UDP, UDP-Lag, WebDDoS, SYN, TFTP), in addition to normal traffic. The dataset was processed, normalized to serves as input for the intelligence security model. A sample of 20 network traffic dataset were selected from CCIDDoS2019 for the purpose of this research. For the purpose of this research, collected dataset were analyzed, sorted out to allow for identification of patterns that will separate such into class of (DNS, UDP and SYN) and normal network traffic. For the purpose of detection and control of DDoS attack, normalization and classification of dataset was carried out to place the identified parameters in digital ratio [14]. Such values of the identified parameter were calculated and place in digital form which was used as an input in the developed ANN's model. Model validation was conducted using computer simulation, the implementation of this type of intelligent system for the purpose of detection and control of DDoS attack provide a high accuracy for the desired output [13]. This study is limited to three types of DDoS dataset protocol namely: DNS, UDP and SYN. The dataset was selected using a specialized characteristics of DDoS attack listed in table 1, the attack classes of this dataset cover the following DDoS traffic for this research, DNS, UDP, SYN and normal traffic.

OPEN ACCESS
ONLINE ISSN: 2992-5797
PRINT ISSN: 2992-6122

Table 1: DOS dataset Parameters

Patterns	Description	Data Type
Average Packet time interval	This is when the time interval for each transmission are close to zero seconds, indicating multiple	Continuity type
Average Packet flow size	They have the same packet size usually less than 100bytes	Continuity type
Protocol type	When transmitting with multiple protocols like TCP, UDP, UP or more at once	Integers
TCP SYN response	No server response acknowledgement	Discrete type
Destination IP	Similar IP destination within short time	Continuity type
Average packet flow rate	DDoS is sending large packet flow in order to disable the server	Discrete type
Land connection	This is labeled as 1 if connection is from same host or 0 if otherwise	Binary
Packet size variance	When Massive number of packets are transmitted to the server in small time frame	Continuity type
IP flood	This is flooding the server with numerous IP at once	Continuity type

Data normalization: The initial dataset collected is not suitable for input in the ANN because of the sample size of data type of each parameter. Data normalization allow representation of each parameter value in the (0,1) interval and quantities value of a qualitative. Normalization was carried out according to equation 1 which formalize the notion of imbalance through the Pielou index (Araujo et. al, 2021).

$$J \frac{1}{In\ S} \sum_{i=1}^{S} \frac{ni}{N} In \frac{ni}{N} = \frac{H}{In\ S} \quad \text{..... (1)}$$

Where we have S distinct classes, each C_i has n_i elements and the complete data set has N samples. In equation (1), H is the Shannon Entrophy. The Pielou Index normalizes entrophy by its maximum (In S), so that the values are confined between 0 and 1. In this case, 0 represent the largest possible balance (the samples are divided equally between classes). Note that the Pielou Index are applicable to both sets with binary and multiclass labels [12].

Traffic classes (Legitimate and DDoS) included in this study are defined based on the analysis of collected datasets. With the analysis of the observed dataset, it was identified that traffic parameters which values are subsequently used as input to the ANN with the aim of detection and control of legitimate DDoS traffic. Parameter used for detection are packet arrival time, source IP address (source) destination IP address (Destination) used protocol and packet length [14]. The reason for the application of the selected parameters in the development of model is based on previous studies and the association with displayed parameter set.

System Implementation

This research aims to develop an Artificial Neural Networks techniques at the access layer of a cloud reference architecture, to detect and control DDoS attacks [16]. The intelligent security model which is based on ANN. The algorithm used in Training and Learning our proposed security model is back propagation. It is best in terms of classification and error checking analysis with respect to ANN. The implementation work in two stages. Training and testing of the model with the obtained dataset. Since the model is adaptive in nature, thus the classification decision of the incoming traffic is the testing stages is based on the training stage. The security model will produce the best result, if they are trained progressively with all types of data [18]. This set of data contain normal, DNS, UDP and SYN. In the training stage, input vector are passed to the model with their designed output. During testing of the model, same values of the learning rate is applied. Moreso, same steps of feed-forward used in training are followed in testing to generate the output from the output layer nodes. Unlike

OPEN ACCESS
ONLINE ISSN: 2992-5797
PRINT ISSN: 2992-6122

training the model input vectors used for testing are provided without designed output values. The system was implemented using the design models developed, neural network architectural toolbox, dataset, and Mathlab program [19]. In the Mathlab environment integrated with neural network toolbox with dataset uploaded for training and testing into the intelligent security model. Back propagation learning algorithm was integrated into the model using machine learning tools as shown in figure 5.

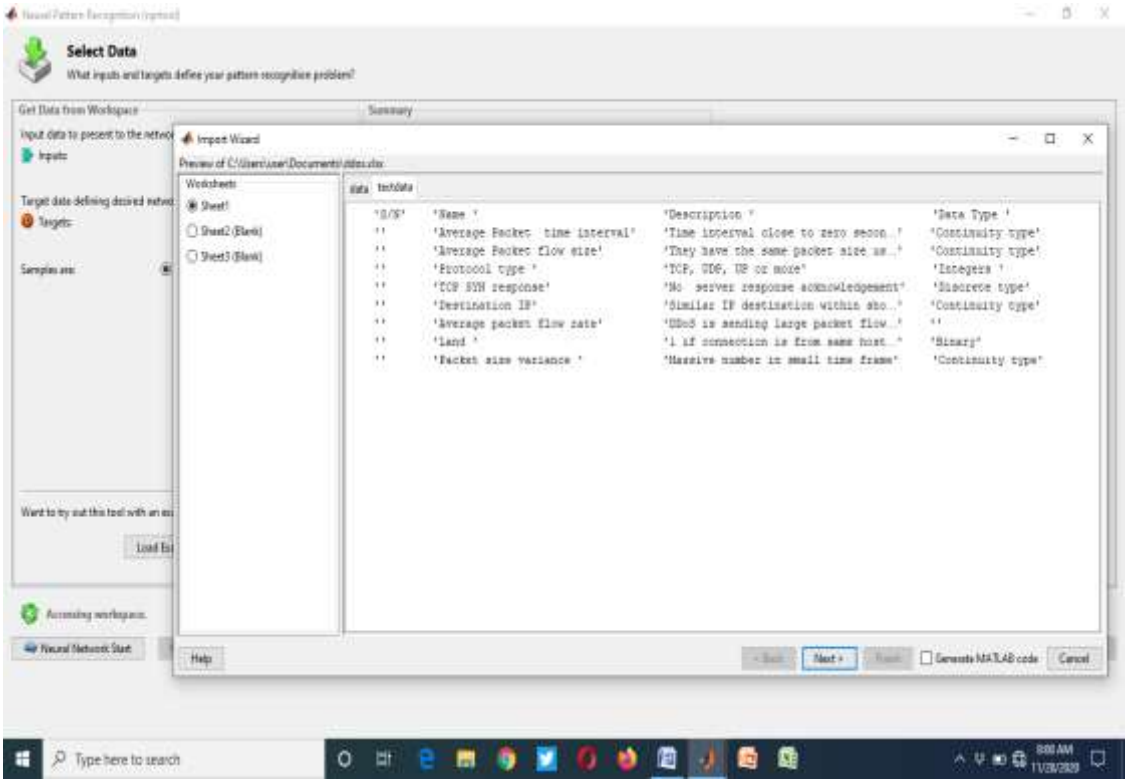

Figure 5: Snapshot of uploading the DDoS dataset into the Mathlab workspace

From the work space in figure 5, the DDOS dataset was uploaded and arranged as inputs to be feed to the neural network architecture for training via the neurons. These inputs have weights, bias and activations function to transform the data into designed output [8]. The Multilayered intelligent neural networks designed in figure 2 with input neurons to facilitate the training and activation of the features are transformed using the summation and activation functions to produce designed output, [18]. These models is implemented as shown in figure 5 with collected dataset from CICDDOS2019, Celeron-quad-core intel N3450, windows XP professional X64 edition, Mathlab 6.5 program (Mathworks programming tools, Neural Network Architecture software – Apache 2.0 (Neuroph) and Regression Analyzer. At this point the DDOS data features have been converted from packet data into statistical values of zeros and ones and ready for training. In the training process, the neural network adjusts the weight and bias functions of each neuron until the network learns the features. This training process was achieved using the training algorithm presented earlier prior to this (Back propagation algorithm). The training algorithm automatically splits the feature vectors into training, testing and validation sets before training. This training process using the back propagation algorithm automatically adjust the weights of each neurons while simultaneously checking the epoch values until the best training result is achieved and the reference model is generated for future detection. The training processes are evaluated using confusion matrix, receiver operator characteristics curve, among other measurements tools as shown in figure 6.

OPEN ACCESS
ONLINE ISSN: 2992-5797
PRINT ISSN: 2992-6122

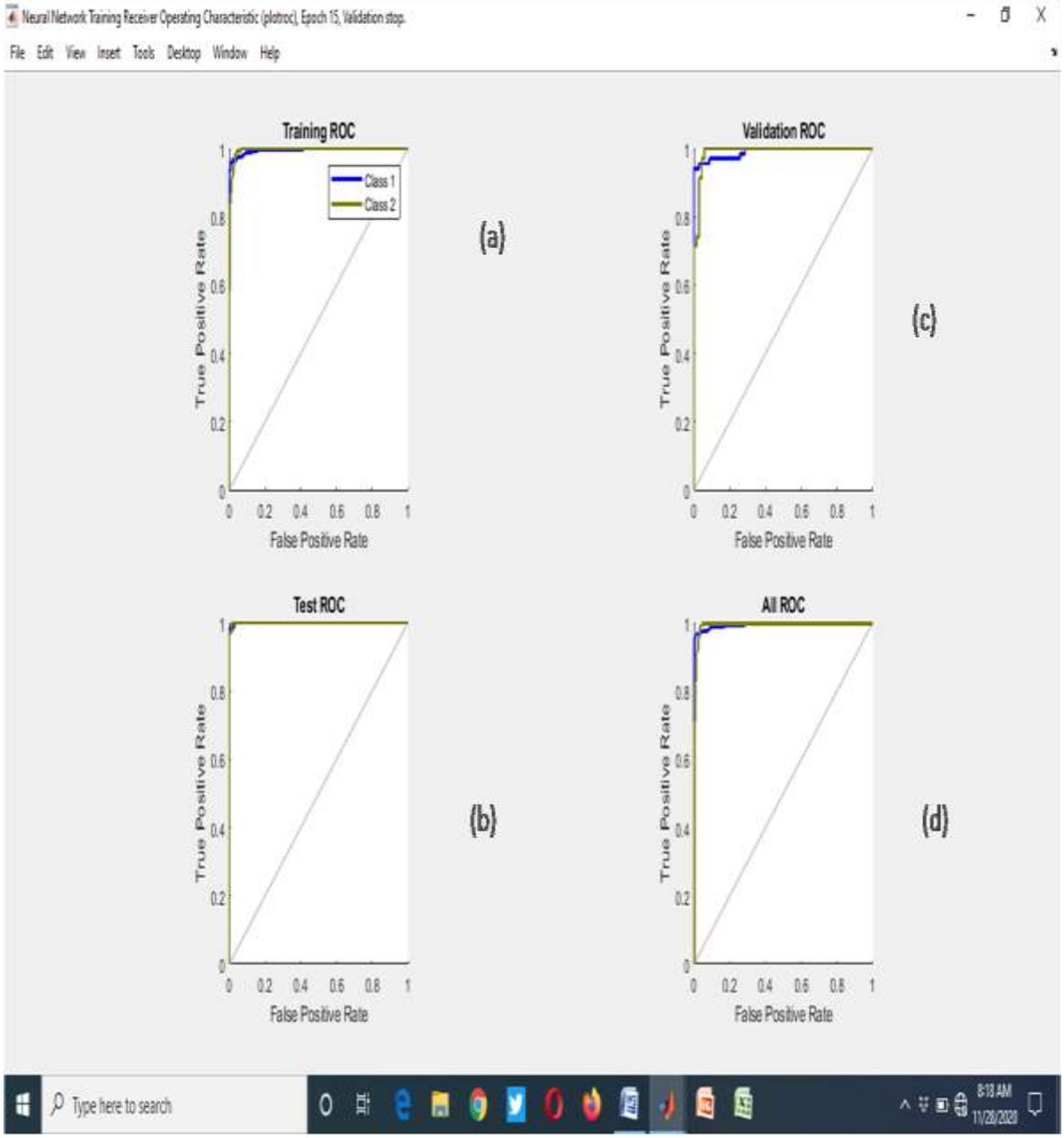

Figure 6: Regression result (a) Training RoC (b) Test RoC (c) Validation RoC(d) All RoC

SIMULATION RESULT

This section presented the results of the ANN based intelligent security model developed using MATHLAB. The system developed was integrated on the reference cloud architecture and tested via simulation using DDoS dataset [7]. The result generated and analyzed revealed that the training performance was perfect without overshoot and credit to the back propagation algorithm used. The system was also tested with DDoS routed packet data and the result showed that the Intelligent security model was able to detect, control and isolate the threat before access to the cloud with a true positive rate of 98.4%, with the best result achieved at epoch 9. The result revealed that the new intelligent security model is very intelligent with improved detection accuracy [14].

OPEN ACCESS
ONLINE ISSN: 2992-5797
PRINT ISSN: 2992-6122

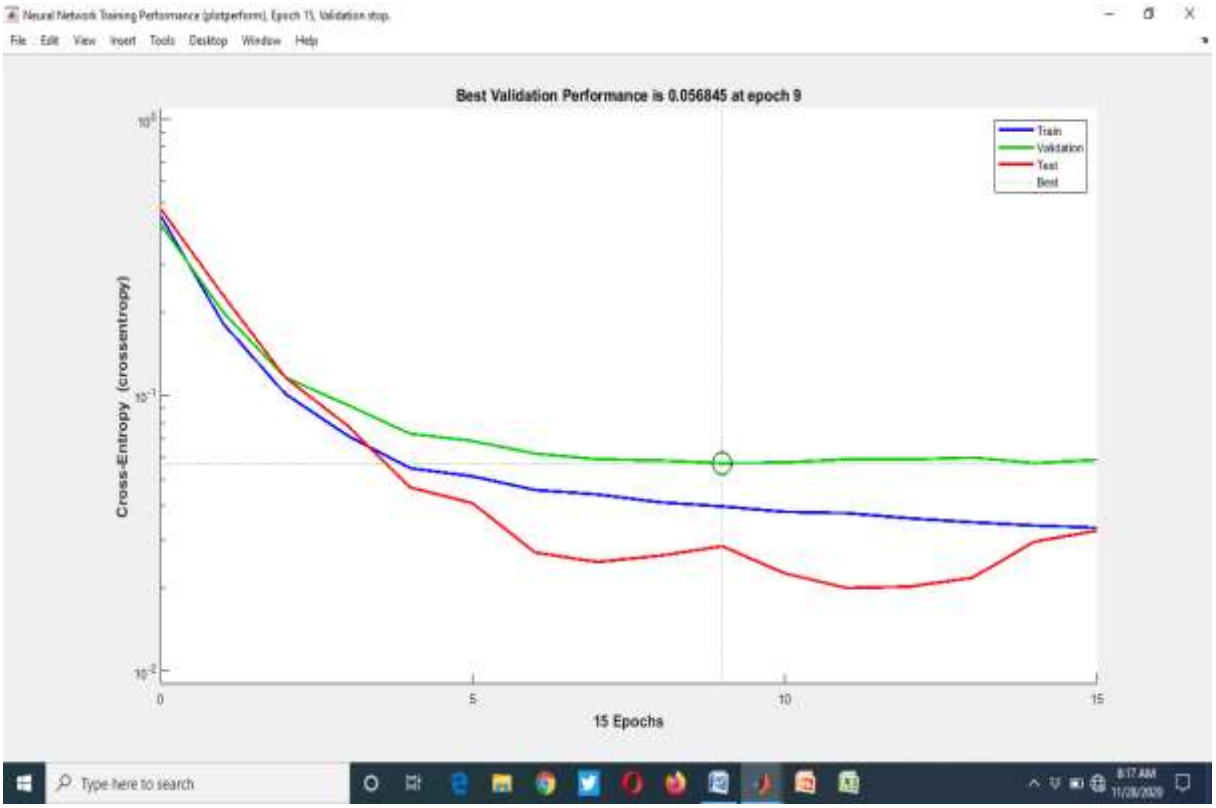

Figure 7: Snapshot of Neural network training performance

CONCLUSION

In this study we proposed on intelligent security model that will detect and control distributed denial of service attack (DDoS) in a cloud reference architecture [20]. The proposed system is designed to be implemented at the access layer in a cloud reference architecture. Our proposed system ISM detect incoming UDP and DNS traffic intelligently into its classified categories, that is normal, or abnormal traffic, by using ANN. Simulation results and performance analysis proved that the intelligent system models is brilliant, strong and dependable than other previous works which center on the security solution on the target machine [21]. Our future work will be focused on tracing the source of the attack whether it is outside or inherent within the cloud reference architecture and with additional parameters to enable it detect the source of the attack.

REFERENCES

1. Saied, R. E. Overill, and T. Radzik, (2014) "Artificial Neural Networks in the Detection of Known and Unknown DDoS Attacks: Proof-of-Concept." Commun. Comput. Inf. Sci., Vol. 430, pp. 300-320.
2. An Oracle white paper (2021), "Cloud References Architecture." Oracle Enterprise Transformation, solution series.
3. Bilal Hikmat Rasheed, M. Sivaram, D. Yuvaraj and A. Mohamed Uvaze Ahamed, (2019): An improved Novel ANN Model for Detection of DDoS attacks on Networks, International Journal of Advanced Trends in Computer Science and Engineering. Vol. 8 No. 1.4.
4. Chappelle D (2013): "Security in depth reference architecture, release 3.0 White paper, Oracle Corporation,Redwood Shores, CA, USA, URL http://www.oracle.com/technetwork/topics/entarch/oracle-wp-security-ref-1918345. Pdf
5. Chonka A, Xiang Y, Zhou W, Bonti A (2011) Cloud Security defence to protect cloud computing against http-dos and xml-dos attacks. J Netw COmput Appl 34(4): 1097-1107, DOI 10.1016/j.jnca.2010.06.004.
6. Cisco, HyTrust, VMware, Savvis, Coalfire (2011) Pci-complaint cloud reference architecture. White paper, Payment, Cisco Systems.
7. Dragan perakovic, Marko perisa, Ivan Cvitic and Sinasa Husnjak, (2017) "Model for Detection and Classification of DDoS Traffic Based on Artificial Neural Network". Telfor Journal, Vol. 9, No. 1
8. Eduardo B. Fernandez (2015) "A security Reference Architecture for Cloud System. Department of Computer Science and Engineering, Florida Atlantic University, Boca Raton, FL, USA. http://www.cse.fau.edu/~ed
9. Fernandez, E. B. &Monge, R. (2014). "A security reference architecture for cloud systems," in ACM ICSA 14. Sidney, NSW, Australia: ACM.

OPEN ACCESS
ONLINE ISSN: 2992-5797
PRINT ISSN: 2992-6122

10. Fernandez, E. B., Monge, R. and Hashizume Keiko (2015) "Building a Security Reference Architecture for Cloud Systems"
11. Sharafaldin, A. H. Lashkari and A. A. Ghorbani, (2019) "Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy," *IEEE 53rd International Carnahan Conference on Security Technology*, Chennai, India, Doi: 10:.1109/CCST.2019.8888419
12. Muhammad A. Khan, S. Khan, Bilal Shams and Jaime Lloret. (2015) "Distributed flood attack detection mechanism using artificial neural network in wireless mesh networks" Security and communication Network/Volume 1. Issue 15/p2715 – 2729.
13. Narendra Mishra, R. K. Singh and S. K. Yadav (2022) "Detection of DDoS Vulnerability in Cloud Computing Using the Perplexed Bayes Classifier" Computational Inteligence and Neuroscience Volume 2022, Article ID 9151847, 13 pages https//doi.org/10.1155/2022/9151847.
14. NIST Cloud Computing Security Working Group, (2013) "NIST Cloud Computing Security Reference Architecture", Working Document.
15. Pedro Henrique Hauy Netto de Araujo, Andersn Apercido Alves da Silva, Norisvaldo Ferraz Junior, Fabio Henrique Cabrini, Alsessandro Santiago dos Santos, Adilson Eduardo Guelfi, Sergio takeo Kofuji, (2021), "Impact of Feature Selection Methods on the Classifications of DDoS Attacks using XGBoost", Journal of Communication and Information Systems, Vo.36, No.1.
16. R. Karimazad and A. faraahi (2011), "An Anomaly-Based method for DDoS Attacks Detection using RBF Neural Networks," in International Conference of Network and Electronics Engineering, , vol. 11, pp. 44-48.
17. Sonia Rani and Neetu Sharma, (2014): A Security Integrated Data Storage Model for Cloud Environment, International Journal of Computer Science and Mobile Computing
18. Sunny Behal and Krishan Kumar, (2017): Characterization and Comparison of DDoS Attack tools and traffic generators – A Review, International Journal of Network Security, Vol. 19, No.3, PP. 383-393 (DOI: 10.6633/IJNS. 201703.19(3).07)
19. T. thapngam, S. Yu, W. Zhou, and S. K. Makki, (2014) "Distributed Denial of Service (DDoS) detection by traffic pattern analysis, "Peer-to-peer Netw. Appl., vol. 7, no. 4, pp. 346-358.
20. Thuy-Anh Nguyen, Hai-Bang Ly, Hai-Van thi Mai, and Van Quan Tran (2021); "On the Training Algorithms for Artificial Neural Network in Predicting the Shear Strength of Deep Beams. University of Transport Technology, Hanoi 100000, Vietnam,.
21. Xin Zu, Yongqiang Sun and Zunguo Huang, (2007): Defending DDoS Attacks using hidden Markov Models and Cooperative Reinforcement Learning.

CITE AS: Etuk Akaninyene Udo and Okoye Francis (2024). Security Model for the Detection of Distributed Denial of Service Attack (DDoS) at the Access Layer in Cloud Reference Architecture. NEWPORT INTERNATIONAL JOURNAL OF BIOLOGICAL AND APPLIED SCIENCES,5(2):51-60.
https:/doi.org/10.59298/NIJBAS/2024/5.2.516011