Available online www.jsaer.com

***Journal of Scientific and Engineering Research*, 2020, 7(1):154-162**

Research Article

ISSN: 2394-2630
CODEN(USA): JSERBR

Detection of Unauthorized Intrusion in a Network Using Feedforward Neural Network

Williams D. Ofor[1]*, Mercy Nwanyanwu[2]

[1]Department of Computer Science, Rivers State University, Nigeria
[2]Department of Computer Science, Port Harcourt Polytechnic, Nigeria
*Corresponding Author: williams.ofor@ust.edu.ng, Tel.: +2348032621382

Abstract Intrusion detection system is very important in a computational environment. The increase in computing techniques, communications among devices and computer network has made the computational environment subject to external attacks. This project presents an Unauthorized Intrusion Detection in a Network with Neural Network technique to classify the different class of anomalies/ malicious behaviours into Dos, U2R, R2L and PROBE. The implemented system uses the feedforward backpropagation neural network to classify the NSL-KDD Cup '99 dataset with an average accuracy of 99.29% and a mean square error of 1.2e-3.

Keywords malicious, abnormal attack, feedforward, backpropagation

Introduction

With the inventions of more internet connectivity and technologies; the rapid development of network security problems cannot be overly emphasized. These challenges are getting more serious with each passing day [1]. In this modern era everything is going to be digitized, so, a single movement on the internet need security for data that are shared on the network [2]. Research conducted by Cisco reports that there are currently 10 billion devices connected, compared to the world population of over 7 billion and it is believed it will increase by 4% by the year 2020 [3].

Due to heavy use of the Internet, the importance of information protection has been increased. As such, there is no defined method of interjection deduction. It can be considered as pattern matching problem that differentiate between network attack, abnormal network behaviours, and normal network behaviours. Any Group of activities which try to compromise on the reliability, accessibility, confidential or privacy of resources is known as interjection or interruption. An intruder is an attacker, person or group of people who initiates the activities during interruption. Attackers can be from within the network, person who have the access to use system with normal user rights or someone who uses a hole in some OS to escalate their access level or admin rights. It can be from outside of the system or network that is someone on another network or even in some other country who exploits a weakness, vulnerability in an insecure network service on the system to take unauthorized entry and access of the trust network [4].

Network Based Intrusion Detection System (NIDS)

An intrusion in a network is an unauthorized access to a network with the intension to cause a harm or acquire confidential information that is not supposed to be for public consumption. An intrusion detection system (IDS) is a security detection system put in place to monitor networks and computer systems. There are two types of intrusion detection system namely: Host Based Intrusion Detection System and Network Based Intrusion Detection System. This paper presents the network-based intrusion detection system. Network-based IDS

(NIDS) is placed on clog point of the network control. It observes a real-time network traffic and analyses it to detecting unauthorized intrusions or the malicious attacks [5].

Artificial Neural Network

Artificial Neural Networks are computing technologies which was conceived in the early 1940s and then industrialized in the Artificial Intelligence (AI) region [6]. It is similar to how neurons are organized in layers in the human brain cells, neurons in neural networks are often prearranged in layers as well [7]. The intricacy of real neurons is highly abstracted when modelling artificial neurons. These, basically consist of inputs (like synapses), which are multiplied by weights (strength of the respective signals), and then computed by a mathematical function which determines the activation of the neuron.

In a bid to improve efficiency in the use of technologies in data storage and information retrieval, the internet technology is exploited which in turn exposes this information to unauthorized users. However, misuse or outright attack on network systems is a challenge faced by organizations and how to detect and stop these intruders (otherwise known as hackers) from gaining access to the systems network. The main aim of the paper is to detect intrusion in a network using neural network with the objective to design and implement an intrusion detection system using neural network, to prevent malicious attacks to a network and to obtain dataset for the training of the neural network.

The rest of the paper is organized as followed: section I contains introduction of the detection of unauthorized intrusion, Section II contains the Related Work of the proposed system, section III contains the materials and methods, section IV gives description of the result and discussion of the proposed system, section V concludes the research work.

Related Work

A review of related literature was done through the theoretical framework, empirical studies and related literature.

1. *Theoretical Framework*

The theoretical framework allows explicit statement of assumption and address the why and how question of the research. [4] illustrated that prediction system for intrusion detection is the heart of prediction engine that analyses data and outputs the predictions on the data. The system is also able to know if data record is normal or affected by any attack. [8] also explained that an intrusion detection system can be a device or a software that monitors network or system activities for malicious activities or a user violates the policies put in place by the network administrators. How to identify various network attacks was presented by [9] especially, unforeseen attacks, which is unavoidable. According to [10] the processes of identifying internal and external user who intend to do something that is not authorized against the computer system is IDS. This also identifies legally connected users who intend to misuse their privileges. [7] presented signature-based and anomaly-based IDS as one aspect of an effective network security monitoring strategy but that NIDS has been criticised to generate large number of false positive and false negative signatures.

2. *Review of Empirical Studies*

This author developed a hierarchical offline anomaly network IDS that was based on distributed time-delay which aim was to solve hierarchical multiclass problem on (DoS, U2R, R2L and Probe attacks) detected by dynamic neural network [11]. [12], describes how incoming packets to the network are captured in a packet sniffer and analysed with the packet signatures extracted and discretized using K-means clustering algorithm. The performance and evaluations are performed by using a set of benchmark data from a KDD dataset and the consistency of the data was checked whether the source and destination address of data where same or not [13]. The authors [1] also used the KDD Cup 99 dataset to evaluate network flow and analysis on intrusion detection and it provide good comparison for their IDS model. To improve performance of IDS with real-time network traffic, a large-scale realistic intrusion detection was sponsored by the US Défense Advanced Research Projects Agency (DARPA) in 1998 and DARPA database was then designed to evaluate performance of IDS for more than two months of network traffic from US Government site [14]. [15] also designed and implemented a real-

time monitoring and detection of intrusion activities in network traffic data from DARPA dataset. Their training model and evaluation was performed by Root Means Square (RMS) error analysis.

3. Review of Related Literature

A fuzzy neuro system for IDS was proposed by [4]. They created a prediction model, an engine that analyses the data according to the model and only false predictions were fed back to model tuner to automatically tune the model. [16] implemented IDS with Genetic algorithm that detect various types of network intrusions and performance measurement. [17] detected intrusions considering the behaviour of the intruding element that is different from authorised user behaviour. [18] focused on the technology, development and strategic importance of intrusion detection system as it applies to network. [1] addressed this issue with convolutional neural network which used dataset from the KDD Cup 99 dataset and did two dimensionalization processing on the test data to bring more convenient convolutional neural network learning. [19] detected network intrusion using data fusion. They brought out some issues and proposed a research direction in data fusion. Statistical anomaly and rule - based misuse models were used.

Materials and Methods

The proposed Detection of Intrusion System in a Network using Neural Network was developed with the MATLAB scientific programming language and follows the structured system analysis and design method (SSADM). This technique sets standards for systems analysis and application design using a formal systematic approach to the design of information system and it can make investigation and design more complete.

Hence, it is designed to enable the detection of unauthorized access in a network system. This is achieved by the neural network technique. Figure 1 presents the architectural design of the system.

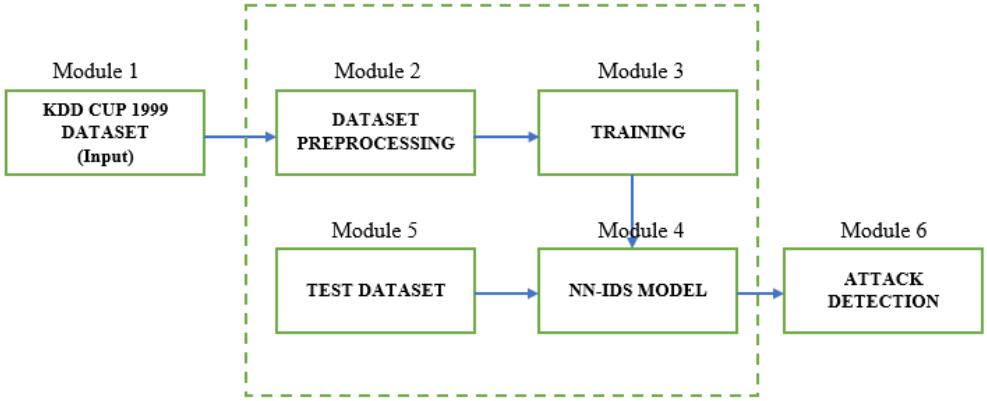

Figure 1: Architecture of the Proposed System

The system architecture that Figure 1 presents six different modules which are: the input module, pre-processing module, training module, test module, neural network model module and the attack detection module. These modules contribute to the successful development of the system.

Data from the KDD Cup '99 dataset is used as the input to train and test the system. The process design of the system can be seen in Figure 1 bounded by the dotted rectangular line that include 4 separate modules which are: Module 2 (Dataset pre-processing module), module 3 (Training module), module 4 (NN-IDS model module) and module 5 (Test Dataset module). These constitute the processes though which the system follows achieve detection of attacks on the network.

Dataset Pre-processing (Module 2)

The dataset is pre-processed for better classification. The technique that was used for pre-processing the NSL-KDD Cup 99 dataset is normalization. This technique prepares the dataset for better identification and classifications reducing dimensions and irregularities. Training a neural network requires numeric data and the dataset has a combination of alpha-numeric data hence, the need for normalization.

Dataset Training (Module 3)

The NSL-KDD dataset with 42 attributes is used in this empirical study. This dataset is an improvement over KDD'99 data set from which duplicate instances were removed to get rid of biased classification results. The dataset gotten from the NSL-KDD Cup '99 requires training for the NN to be able to learn between normal use and anomaly or misuse. Hence, the training of the dataset is necessary for the proposed system model. A percentage from the dataset is used in the training process.

NN-IDS Model (Module 4)

This is the Neural Network model that was created for the Intrusion Detection System (IDS). The model is implemented to train and recognise unauthorized access and or malicious use to a network system. The figure 2 represents the schema of FFBP neural network that was used in the training process.

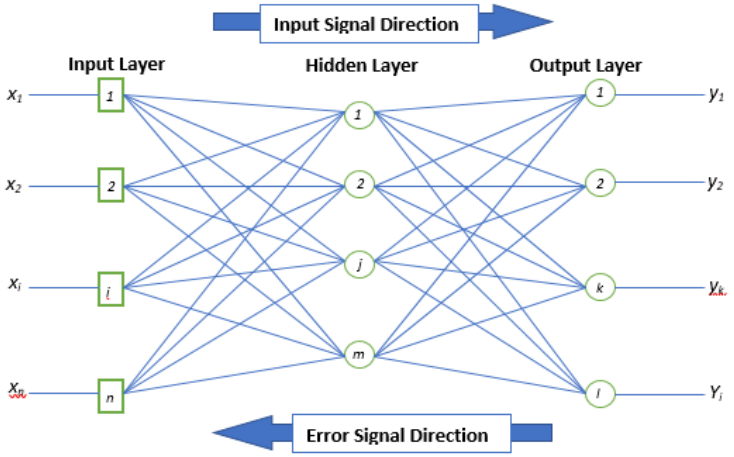

Figure 2: Architecture of the Feedforward Backpropagation Neural Network

Figure 2 is a feedforward backpropagation neural network architecture with an input layer (with input variable x) that feeds in the system data which comprises the various packets that passes through the network nodes. The hidden layer is where all the manipulations on data are carried out. The calculations of the output of the neurons in the hidden layer is done using the sigmoid activation function which is given by:

$$Y_j(p) = \text{sigmoid}\sum_{i=1}^{n} [x_i(p)*w_{ij}(p) - \theta_j] \quad 1$$

Where y is the output result of the system and x is the input data, *w* is the weight value respectively. The symbol θ is the correction needed only in the hidden layer, n is the number of inputs of the neuron j in the hidden layer. Sigmoid, is the activation function (Sigmoid(s) = 1 + 1/e^s, where e is the base of the natural algorithm). To calculate the actual output of the neurons in the output layer is seen in the equation 2.

$$Yk(p) = \text{Sigmoid}\sum_{i=1}^{m} [x_{jk}(p)*w_{jk}(p) - \theta_k] \quad 2$$

Where m is the number of inputs of neuron in the output layer. The system is trained with FBPNN to acquire the knowledge of normal activities and attacks for anomaly detection attacks.

Test Dataset (Module 5)

The test dataset is fed into the already trained NN model for detection and classification. During the training process, a percentage of the dataset was used for the training. The remaining dataset is now used to test the model for performance evaluation of accuracy.

Use Case Design

This shows the interactions between users of the system (i.e. actors) and the system during the execution process, it represents the different use cases the user is involve with. It captures graphically the system functionality and interactions between the user (referred to as actor) and the system. The Figure 3 below shows the categorized interactions of the execution process of the system.

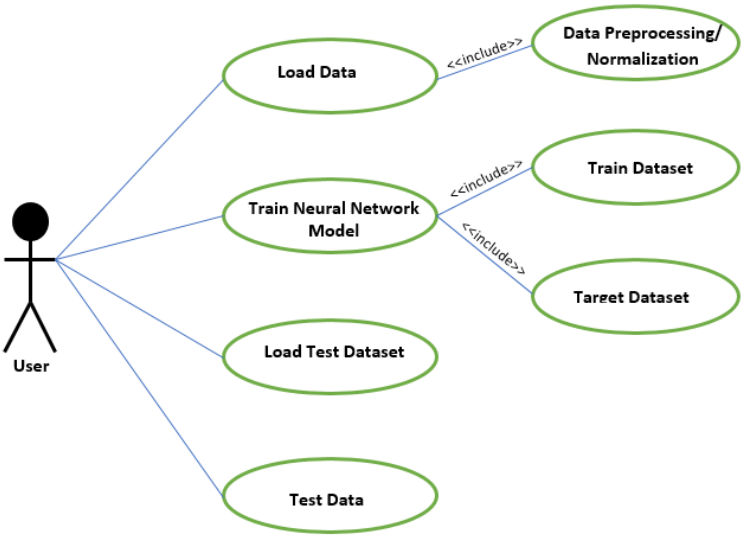

Figure 3: Use Case Design of the Proposed System

The user (actor) in Figure 3 performs the functions as illustrated. He/ she loads the dataset in the system which automatically calls the pre-processing module. After that has been accomplished, the user performs the training of the neural network model that gets the dataset and separate it into training data and target dataset. The test dataset is then loaded into the system and the testing of the system is then executed.

Implementation Architecture

The proposed system allows user to load in the dataset to train and the test-set to test the system with. Figure 4 present the implementation architecture followed in successfully executing the developed system.

Figure 4: Implementation Architecture of the Proposed System

The user of the system in Figure 4 loads the dataset after and pre-processes the loaded dataset into training dataset and target dataset. The pre-processed dataset is then trained in the Neural Network algorithm into a model. The user the loads the test data to test the trained model on the test data and the result are displayed on the screen.

Results & Discussion

System Testing

The system was tested using part of the dataset gotten from the KDD Cup '99 website. After training the system/ model, 70% of nine thousand (9000) records that was extracted from the corrected version overall dataset and analyzed. Figure 5 and 6 demonstrate the implementation of the developed system. They present successful loading and pre-processing of the dataset after which, the loaded data was trained. The test data was loaded and tested giving outputs on the different types of attacks present in the test dataset file as shown in Figure 6.

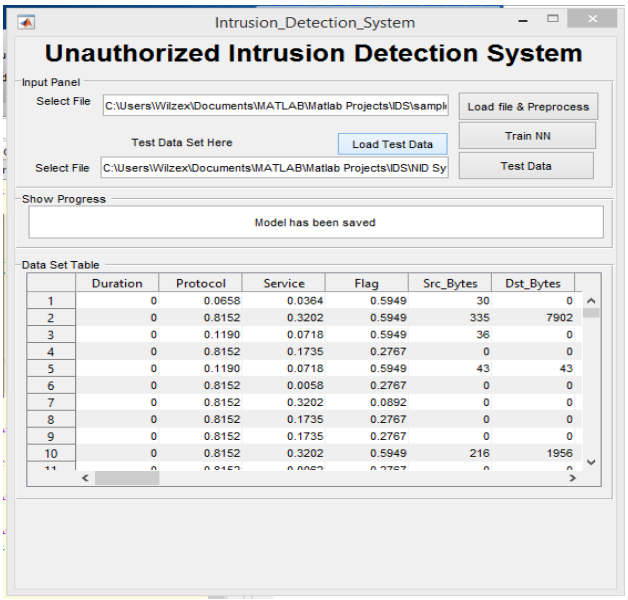

Figure 5: loaded data with a successfully trained model of the proposed system

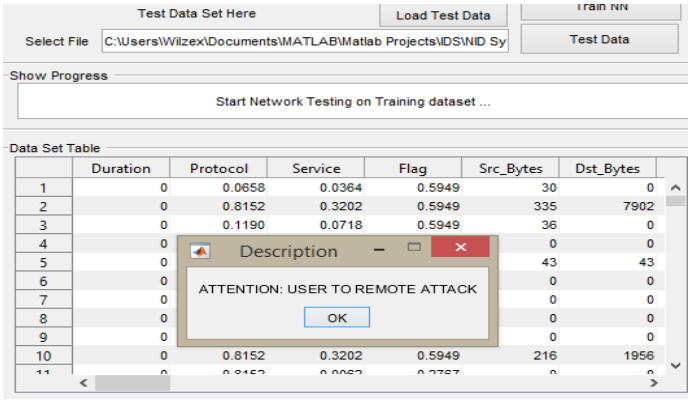

Figure 6: implementation of test dataset and result display

The system was tested against the different types of attack which are: Denial of Service Attack (DoS), User to Root Attack (U2R), Remote to Local Attack (R2L) and Probing. The statistic is further shown in Table 1 as shown below

Table 1: Test Result for the Neural Network System

Attack Class	No. of Pattern for each Class	No. of Classified Pattern for each Class	Percentage Classification
Normal	3000	3000	100%
DoS Attack	1500	1455	97.9%
U2R Attack	1500	1470	98.7%
R2L Attack	1500	1485	99.8%
PROBE	1500	1485	99.9%
Total	9000	8895	99.29%

The Table 1 shows that the result of Neural Network after training and testing. The goal of the training was met at 125 epoch (Iterations) and it produces a mean square error of 1.2e-3 and a total percentage classification of 99.29% as represented in the graph in figure 7.

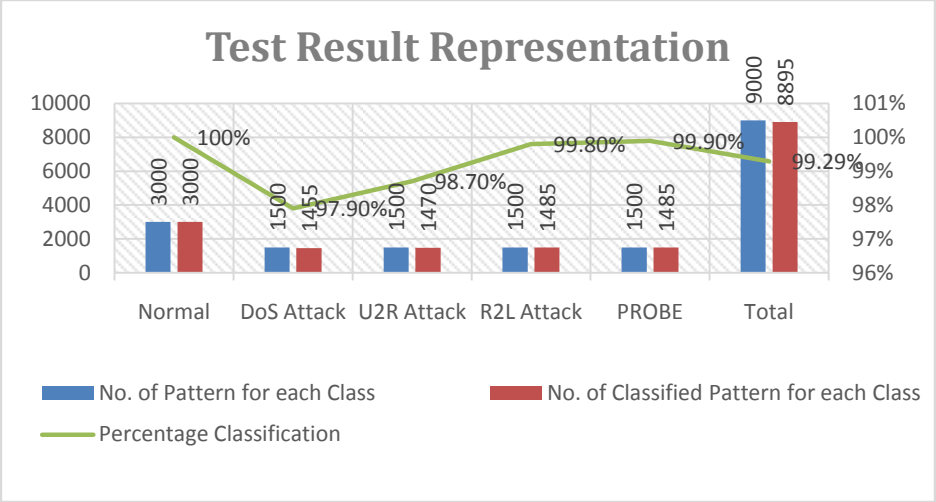

Figure 7: Graphical Representation of the Test Result for the Neural Network System

Figure 8 presents the validation plots of the developed system from the Neural Network. It shows the mean square error of 20 epochs. From the plot, we noticed that the validation line (green) matches the best line (black dotted line). Indicating that the system performed excellently in classifying the various class or attacks.

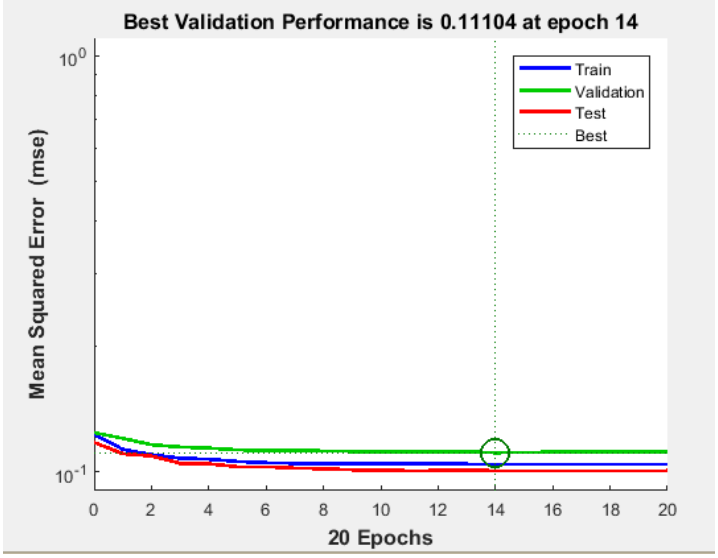

Figure 8: Validation Diagram of the Proposed System

The neural network learns to perform task by considering examples, generally program with task-specific rules. It uses the feedforward backpropagation based Neural Network to train the data for identification of intrusions. The main goal of ANN is to transfer all inputs into the network to outputs, indicating the treats involved during executions.

After training the system/ model, 70% of nine thousand (9000) records that was extracted from the NSL-KDD data set overall dataset and analyzed. The system was tested against the different types of attack which are: Denial of Service Attack (DoS), User to Root Attack (U2R), Remote to Local Attack (R2L) and Probing. The goal of the training was met at 14 epoch (Iterations) and it produces a mean square error of 1.2e-3 and a total percentage classification of 99.29%.

Conclusion

An unauthorized Intrusion System is a software that monitors malicious activity in a network. After study and analysis, an intelligent software was developed based on the NSL-KDD Cup '99 dataset which has live network data of both malicious activities and normal operations. Therefore, making the developed neural network an effective and efficient model for detection of suspicious activities in the network.

After the execution of the system, a total of 8895 patterns/ classes were classified including normal behavior totaling 3000. The percentage classification of attack for the different type are: DoS attack 97.9%, U2R attack 98.7%, R2L attack 99.8% and probe 99.9% with an average accuracy of 99.29% and a mean square error (MSE) of 1.2e-3. The proposed system focuses on intrusion detection and the system can be enhanced to other aspects of security. Intrusion prevention can be built into it to stop all intruders to the network from accessing data from the organization.

References

[1]. Liu, Y., Liu, S. & Zhao, X. (2017). Intrusion detection algorithm based on convolutional neural network. *DEStech Transactions on Engineering and Technology Research*, (iceta).

[2]. Awasthi, I. & Fatima, I. (2018). Analysis of Intrusion Detection System Using Machine Learning. *International Journal of Advanced Research in Computer Science*, *9*(Special Issue 2), 133.

[3]. Hodo, E., Bellekens, X., Hamilton, A., Dubouilh, P. L., Iorkyase, E., Tachtatzis, C. & Atkinson, R. (2016, May). Threat analysis of IoT networks using artificial neural network intrusion detection system. In *2016 International Symposium on Networks, Computers and Communications (ISNCC)* (pp. 1-6). IEEE.

[4]. Ratnawat, N. & Jain, A. (2014). A novel intrusion detection system using neural-fuzzy classifier for network security. *Int. J. Emerg. Technol. Adv. Eng*, *4*(6), 900-905.

[5]. Ponkarthika, M. & Saraswathy, V. R. (2018). Network intrusion detection using deep neural networks. *Asian Journal of Applied Science and Technology*, *2*(2), 665-673.

[6]. Veselý, A. & Brechlerova, D. (2009). Neural networks in intrusion detection systems. *Agriculture journals. cz*, 156-165.

[7]. Hijazi, A., El Safadi, A. & Flaus, J. M. (2018). A Deep Learning Approach for Intrusion Detection System in Industry Network. In *BDCSIntell* (pp. 55-62).

[8]. Shwetambari R. P. & Pradeep D. (2013). Classification of Attacks in Network Intrusion Detection System *International Journal of Scientific & Engineering Research* 4(2), 1-5

[9]. Autade P. S. & Kalavadekar P. N (2018). Review on Intrusion Detection System using Recurrent Neural Network with Deep Learning. *International Research Journal of Engineering and Technology (IRJET)*, 05(10), 1385- 1388

[10]. Ahamad, T. & Aljumah, A. (2014). Hybrid approach using intrusion detection system. *International Journal of Engineering Research & Technology*, *3*(2).

[11]. Ibrahim, L. M. (2010). Anomaly network intrusion detection system based on distributed time-delay neural network (DTDNN). *Journal of Engineering Science and Technology*, *5*(4), 457-471.

[12]. Rana, A., Pandey, R. R., Londhe, S. & Mohankar, P. (2015). Intrusion Detection and Attack Classification Using K Means Algorithm and Artificial Neural Network. *International Journal of Engineering and Management Research (IJEMR)*, *5*(2), 326-330.

[13]. Davikrishna, K. S. & Ramakrishna, B. B. (2013). An artificial neural network-based intrusion detection system and classification of attacks.

[14]. Planquart, J. P. (2019) Application of Neural Network to Intrusion Detection. SANS Institute Information Security Reading Room, 1.

[15]. Sodiya, A. S., Ojesanmi, O. A., Akinola, A. &Aborisade, O. (2014). Neural network-based intrusion detection systems. *International Journal of computer applications*, *106*(18).

[16]. Hoque, M. S., Mukit, M., Bikas, M. & Naser, A. (2012). An implementation of intrusion detection system using genetic algorithm. *arXiv preprint arXiv:1204.1336*.

[17]. Prabhu, G. N., Jain, K., Lawande, N., Kumar, N., Zutshi, Y., Singh, R. & Chinchole, J. (2014). Network intrusion detection system. *International Journal of Engineering Research Application*, *4*(4), 69-72.

[18]. Asif, M. K., Khan, T. A., Taj, T. A., Naeem, U. & Yakoob, S. (2013, April). Network intrusion detection and its strategic importance. In *2013 IEEE Business Engineering and Industrial Applications Colloquium (BEIAC)* (pp. 140-144). IEEE.

[19]. Li, G., Yan, Z., Fu, Y. & Chen, H. (2018). Data fusion for network intrusion detection: a review. *Security and Communication Networks*, *2018*.