Intrusion Detection in a Network using Feedforward Neural Network

[1,]Selai Maisea, [2]Chindika Mulambia, [3]Yasmin Chuupa Essa, Dr Jabir Ali[4]

Sharda University, School of Engineering and Technology, CSE Department
Sharda University, School of Engineering and Technology,CSE Department
Sharda University, School of Engineering and Technology,CSE Department
Sharda University, CSE Department

Date of Submission: 12-01-2023 Date of Acceptance: 25-01-2023

ABSTRACT: *This paper is aimed at detection of unauthorized intrusion in a network using feedforward neural network. MATLAB a scientific programming language in relation with SSADM (Structural System Analysis and Design Method) as methodology in carrying out this research. Related literature on the detection of unauthorised intrusion in a network were reviewed. The research concluded that in a computational environment, the intrusion detection system is crucial. The expansion of computing methods, device communications, and computer networks has exposed the computational environment to outside threats. A Neural Network technique for Unauthorized Intrusion Detection in a Network to categorise the various classes of anomalies and malicious behaviour into Dos, U2R, R2L, and PROBE. The implemented system classifies the NSL-KDD Cup '99 dataset with an average accuracy of 99.29% and a mean square error of 1.2e-3 using a feedforward backpropagation neural network.*

KEYWORDS:Neural Network, Feed Forward, Intrusion Detection, Intrusion Prevention

I. INTRODUCTION

The rapid change in network security is becoming an alarming issue which cannot be ignored easily as a result of improvement in internet connectivity and daily invention of technologies gadgets are invented. The growing rate of technologies are becoming an issue of worry on daily basis Liao, H. (2013). Due to digitalization of almost everything in this present era, there is need to beef-up security in our internet to ensure our data are safe. Liao, H. (2013). Currently, almost Ten Billion different types of devices were connected to the networks, which is even higher to world population of seven billion, and there is likely to increase by 10% by 2025. Because of the widespread of internet access, the need to secure information has become a subject of discussion Saraswathy, V. R. (2018).

An individual or group of individuals whom interrupt or attack the activities of a network is called an intruder. Attackers may originate from within the network, have regular user rights to the system, or use an operating system vulnerability to gain administrative access. An insecure network service on the system can have a weakness or vulnerability that someone on another network or even in another country can take advantage of to access the trusted network without authorization Awasthi, I. & Fatima, I. (2018).

Unauthorized access to a system with the purpose of causing harm or obtaining private information that is not meant for public consumption is referred to as an intrusion. I, Awasthi (2018). A security detection tool used to keep an eye on computer networks and systems is called an intrusion detection system (IDS). Host-based and network-based intrusion detection systems are two different types of intrusion detection systems. This paper introduces the network-based intrusion detection system. The network control point where the network-based intrusion detection system (NIDS) is installed is congested. It continuously monitors and examines network traffic to look for malicious or unauthorised intrusions. Hodo, E (2016).

II. LITERATURE REVIEW

Ratnawat, N. & Jain, A. (2014) proposed a fuzzy neuro system for IDS. The model predicted was designed to analyse data but, it wasn't able to provide the expected feedback. Naser, A. (2012) came up with the idea of Genetic algorithms in detecting different categories of network intrusion and as well measure the functionality. Prabhu, G. (2014) conducted a research in which he can to realize a strange behaviour of intruded element which is contrary to the function authorised by the user. Asif, M. K. (2013) came up with a logic to detect the technological development, strategies and significant of intrusion in relation to networks. Liu, Y., Liu, S. & Zhao, X. (2017) resolved this issue using KDD Cup 99 dataset in order to come up with more efficient convolutional neural network.

Artificial Neural Network.

Artificial neural networks are attempts to mimic the network of neurons that make up the human brain so that the computer may learn things and make judgments in a fashion that is comparable to that of a person. Programming common computers to behave like interconnected brain cells is required to create ANNs. Autade P. S (2018).

III. MATERIAL AND METHODS

For the purpose of this research, an intrusion detection system using neural network was proposed. MATLAB a scientific programming language was used which works in relation to SSADM (Structural System Analysis and Design Method). The method is considered because it provides accurate results in system analysis and application design.

In figure one (1), its shows a system architecture design on how unauthorised access is detected in a network system.

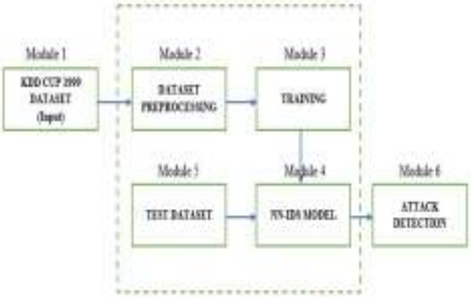


Figure 1: System architecture design

As shown in figure one, it contains six distinct modules namely: the input, pre-processing, training, test, neural network model, and attack detection modules respectively. The designed system is trained and tested using data from the KDD Cup '99 dataset. Figure 1 depicts the system's process design, which is bounded by a dotted rectangular line and includes four distinct modules. at the system employs to detect network attacks.

Pre-processing of Datasets (Module 2)

The dataset has been pre-processed to improve the classification. Normalization was the technique used to pre-process the NSLKDD Cup 99 dataset. By reducing dimensions and irregularities, this technique is used because it organised dataset for proper classification and identification.

NN-IDS model (module 4)

In this model, an intrusion detection system is built and train to detect unwanted access or any malicious attempt to the network system. The schematic of the FFBP neural network used in the training process is shown in Figure 2.

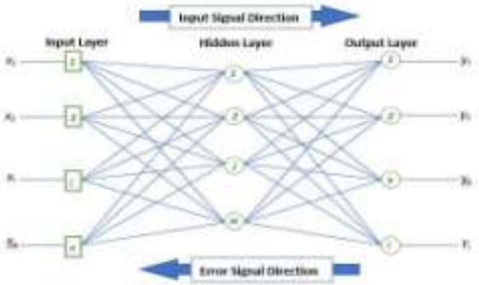


Figure 2: Architecture diagram of Feedforward Backpropagation Neural Network

From the figure 2, it has three layers namely; Input, Hidden and Output layers. The input layers consist of x variable, output y variable and the hidden layer were the logical manipulation takes place. The calculation of hidden layer's neurons' output is done using the sigmoid activation function. Mathematically $Y_j(P) = Signoid\sum_{i=1}^{n}[x_i(p) * w_{ij}\ (p) - \theta j]$ ……………..1

Where;
y = result of system output
x = input data to the system
w = weight value
θ = hidden layer correction required.
n = inputs numbers of neuron j in the hidden layer.

The activation function is Sigmoid (s) = 1 + $\frac{1}{e^s}$

Where; e = is the natural algorithm's base.

$Y_j(P) = Signoid\sum_{i=1}^{m}[x_{ik}(p) * w_{jk}\ (p) - \theta k]$……………………………………………..2

Equation 2 express how the actual output of the neurons in the output layer is calculated.

where m is the total number neurons in the inputs and output layer's.

Test Dataset (Module 5)

The system is trained with FBPNN to learn about typical activities and attacks for attacks on anomaly detection.

Case Study Design

The design is used to represent various cases the user is involved and depicts the interactions between users and the system during the process of execution. This graphically illustrates how the system functions and how an actor and the system communicate. The categorised interactions of the system's execution process are shown in Figure 3 below.

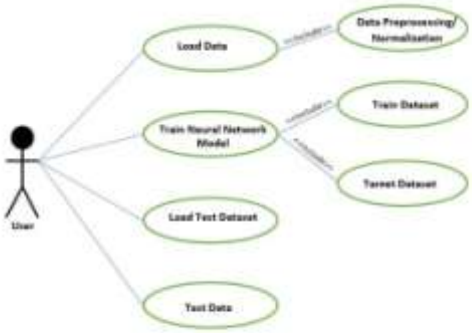


Figure 3: Use Case Proposed System's Design

The user (actor) in Figure 3 carries out the indicated tasks. The pre-processing module is started when he or she enters the dataset into the computer system. After that, the dataset is obtained and split into training and target datasets, and the user trains the neural network model. The system is then tested after being loaded with the test dataset.

Implementation of Architecture Design

The system allows the user to load the dataset, train and test the dataset respectively, as shown in Figure 4

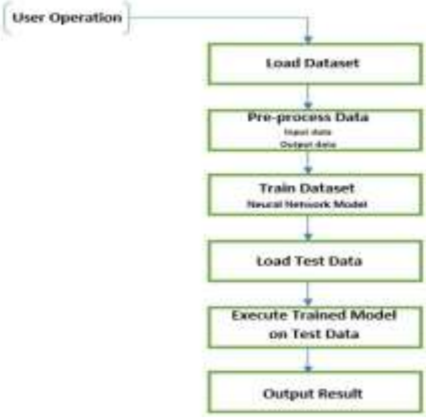


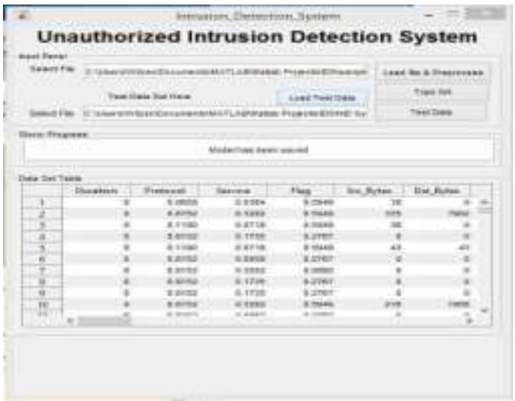
Figure 4: Proposed Architecture design system

After pre-processing the dataset into training and aim datasets, the system's user in Fig.4 loads it. A model is then created using the Neural Network algorithm using the pre-processed dataset. The trained model is then applied to the test data by the user, who then see the results on the screen.

IV. DISCUSSION OF RESULTS

Testing

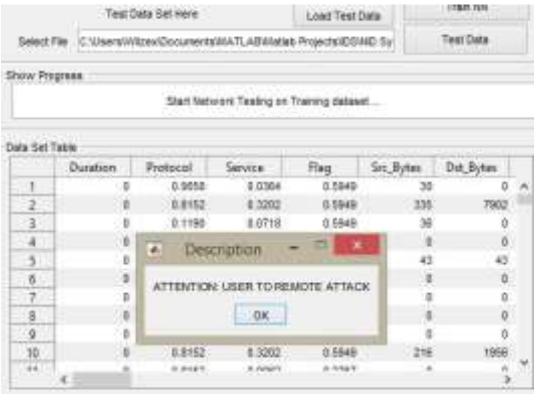
Data from the KDD Cup '99 website were used for the system's testing. 70% of the nine thousand (9000) records from the whole dataset of the revised version were extracted and analysed after the system/model was trained. Figures 5 and 6 depict the implementation of the created system. They do training on the loaded data after successfully loading and pre-processing a dataset.


Intrusion_Detection_System

Unauthorized Intrusion Detection System

Figure 5: Trained model system with loaded data

Figure 6, shows various types of attacks after the test data were loaded and tested.



C:\Users\Wilzex\Documents\MATLAB\Matlab Projects\IDSIMD Sy

Start Network Testing on Training dataset....

	Duration	Protocol	Service	Flag	Src_Bytes	Dst_Bytes
1	0	0.9658	0.0304	0.5949	30	0
2	0	0.8152	0.3202	0.5949	335	7902
3	0	0.1198	0.0718	0.5949	38	0
4	0				0	0
5	0				43	45
6	0				0	0
7	0				0	0
8	0				0	0
9	0				0	0
10	0	0.8152	0.3202	0.5949	216	1958

ATTENTION: USER TO REMOTE ATTACK

Figure 6: Obtained Result after Implementation of test dataset.

Multiple attack techniques, including probing, remote to local, user to root, and denial of service, were used to test the system. The table below displays the statistical analysis as it is.

Types of attack	No. of Pattern	No. of Classified Pattern	Percentage
Normal	3000	3000	100%
DoS	1500	1455	97.9%
U2R	1500	1470	98.7%
R2L	1500	1485	99.8%
PROBE	1500	1485	99.9%
Total	9000	8895	99.29%

Table 1: Test outcome conducted for the Neural Network System

Table 1 shows the results of the Neural Network following training and testing. After 125 epochs (iterations), the educational aim was achieved with an average square error of 1.2e-3 and a total percentage classification of 99.29%, as illustrated in Figure 7.

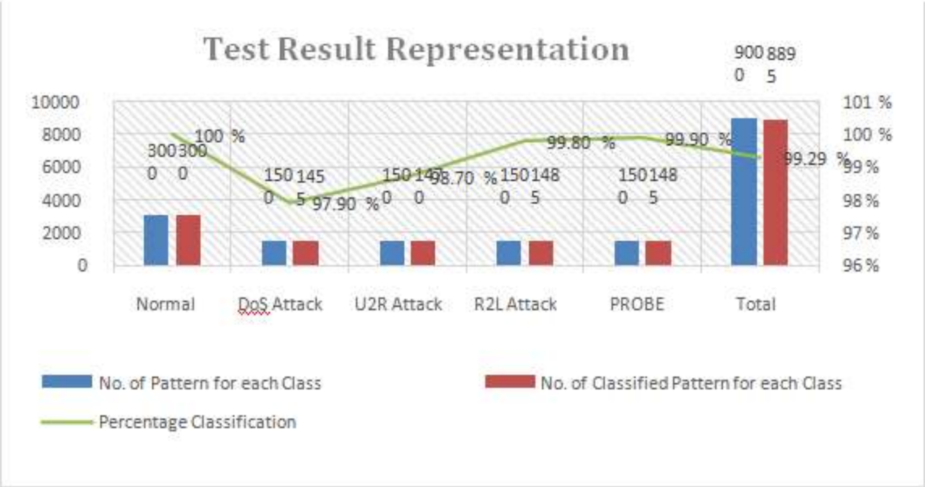


Figure 7: Test Result Representation

Figure 8 depicts the validation plots for the network-developed system that a neural network was used to create. The average square error across 20 epochs is shown on the plot graph. The graph shows that the best line corresponds to the green validation line (black dotted line). demonstrating that the system classified the different sorts of attacks better than expected.

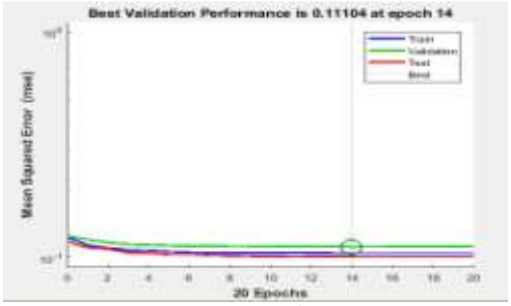


Figure 8: Validation plots for Networked system

The neural network is programmed to perform tasks by analysing problems that have been pre-programmed with task-specific rules. It trains the data for intrusion detection using a feedforward backpropagation-based Neural Network. Artificial neural networks' main objective is to translate network inputs into outputs that reveal the risks present during executions. 70% of the nine thousand (9000) records retrieved from the NSL-KDD data set total dataset had been reviewed after the system/model had been trained. A variety of attacks, including DoS, User to Root (U2R), Remote to Local (R2L), and Probing, were tested against the system. The training objective was achieved after 14 epochs (iterations), with a mean square error of 1.2e-3 and a total percentage identification of 99.29%.

V. CONCLUSION

An unauthorised intrusion system is software that monitors malicious activities on a network. Intelligent software was developed using live network data from harmful and lawful actions within the NSL-KDD Cup '99 dataset, based on investigation and analysis. Because of this, the developed neural network works as a reliable and effective model for spotting suspicious behaviour within the network. A total of 8895 patterns and classes, including 3000 instances of typical behaviour, were found once the system had been properly executed.

The proportion of attacks for the different categories are as follows: 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 suggested system concentrates on intrusion detection but can bemodified to incorporate additional security features. To stop all network intruders from accessing

VI. 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.

[20]. Liao, H. J., Lin, C. H. R., Lin, Y. C., & Tung, K. Y. (2013). Intrusion detection system: A comprehensive review. Journal of Network and Computer Applications, 36(1), 16-24.

[21]. 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.

[22]. 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.

[23]. 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.

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

[25]. 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

[26]. (IRJET), 05(10), 1385- 1388

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

[28]. 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.

[29]. 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.

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

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

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

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