Mediterranean Journal of Basic and Applied Sciences (MJBAS)
Volume 6, Issue 1, Pages 20-26, January-March 2022

Artificial Neural Network Model for Intrusion Detection System

Yusuf Musa Malgwi[1], Ibrahim Goni[2] & Bamanga Mahmud Ahmad[3]

[1,2]*Department of Computer Science, Modibbo Adama University, Yola, Nigeria.*
[3]*Department of Computer Science, Federal University, Lafia, Nigeria.*
Email: yumalgwi@mautech.edu.ng[1], algonis1414@gmail.com[2] & mabamanga@gmail.com[3]

DOI: http://doi.org/10.46382/MJBAS.2022.6103

Article Received: 14 November 2021 *Article Accepted: 20 February 2022* *Article Published: 16 March 2022*

ABSTRACT

Artificial Intelligence (AI) breakthroughs in the last few years have accelerated dramatically as a result of the industry's vast technological use. Neural Networks (NN) is one of the most vital areas of AI, as they allow for commercial use of features that were previously not accessible via the use of computers. The Intrusion Detection System (IDS) is one of the areas in which Neural Networks are being extensively investigated to provide comprehensive computer network security and data confidentiality. During the realization of this work Artificial Neural Network (ANN) were used to shape the proposed model using a realistic CICIDS2017 dataset retrieved from the Canadian Institute for Cyber-Security (CIC) website. Following implementation and testing, it was discovered that the new model performs exceptionally well, with an average. In addition, the receiver operator characteristic curve (ROC) has a 9.999 % area under the Receiver Operator Characteristic Curve (AUC). Finally, it was discovered that the new model is exceptional and has a high level of accuracy. The new model will aid in an improved knowledge of various orders in which IDS research has been conducted. It will be useful for those working on AI-based solutions in IDS and similar domains. It is possible to enhance the new model's detection capabilities to incorporate all other lingering forms of incidents in this actual datasets, which contains all real-time and existing incidents.

Keywords: *Machine learning, Intrusion detection systems, X-IIoTID dataset, Hyper-parameter optimization, Security, Artificial neural network.*

1. Introduction

A class of Machine Learning-based systems known as Artificial Neural Networks (ANN) is mathematical systems that mimic the learning process of human brain. It appears to be computational intelligence technique that has been applied in so many areas including computer and network security (Shenfeld, Day, and Ayesh, 2018).

Since last decades neural network are applied to intrusion detection system. It's a very broad issue, with a variety of techniques taken into account to protect against various attack vectors. Since 2009, there have been evaluations of the concept of utilizing ANN to help irregularity identification and malicious software exposure (Sani, et al., 2009). In terms of factual influence, it is apparent that ANN is one of the most advanced technologies. The widespread application of ANN in mobile solutions, automotive, IoT, health care, and the defense industry distinguish it as stimulating know-how that is extremely adaptive across industries (Ayonya *et al.*, 2021).

This has a significant influent on a variety of studies involving the use of ANN in security and privacy offices, such as Intrusion Detection Systems (IDS) and network monitoring software. A new generation of better productivity of algorithms and ANN parameters are described by Almási, Wozniak and Cristea (2016).

Intrusion Detection Systems (IDS) are security check points that conduct audits to systems and network operations for any suspicious activity and policy violations (Tran, Sarker and Hu, 2018).

Basically Intrusion Detection Systems (IDS) are classified into two types; network-based and host-based, respectively, Buczak and Guven 2016).

The aim of this research is to use neural network technique and create an Intrusion Detection System (IDS).

2. Literature Review

Camastra, Ciaramella and Staiano (2013) classified techniques to IDS modeling based on artificial intelligence. The four categories of ML and SC defined are supervised learning-based methods, unsupervised learning-based methods, statistical modeling-based methods, and ensemble-based approaches. Supervised learning-based methods are the most common type of ML and SC. The first method is used to detect known attacks, whereas unsupervised techniques are utilized to detect new invasions. To track user performance and assess whether it deviates from what is considered "normal," a statistical modeling-based method is utilized. In contrast, the ensemble-based technique mixes many models to improve accuracy and efficacy.

Rana et al. (2017) studied a semi-supervised learning strategy based on Fuzziness for intrusion detection. Only labeled samples are used in supervised learning approaches to make a classifier work better, also, collecting satisfactory labeled data is time-consuming and needs help from experts in the field. Unlabeled samples, on the other hand, many real-world situations make it easy to get what you need. Semi-supervised learning (SSL), which is similar to supervised learning systems, solves this problem by allowing a large number of unlabeled examples to be combined with identified samples to develop a more accurate classifier.

Dias, et al. (2017) used Artificial Neural Networks for Computer Network Intrusion Detection Systems. Intrusion Detection Systems (IDS) is a form of Intrusion Detection System (IDS) that detects unauthorized access which is widely used by network managers since it is seen to be vital in maintaining network security. One potential stumbling block is that such systems are usually built on signature systems, making them highly reliant on updated databases and hence ineffective against novel threats (unknown attacks). The research reported in this study suggests an IDS system built on the KDDCUP'99 dataset and an Artificial Neural Network (ANN). Experiments indicate that the suggested system achieved an overall accuracy of 99.9% when it comes to classifying pre-defined kinds of intrusion attempts, which is a very good result when compared to previous methods.

Nisioti et al. (2018) provide an all-encompassing survey of unsupervised algorithms for intrusion detection and attacker attribution. The results reveal that IDS has progressed from simple detection to correlation and attribution in recent years. As a result, powerful data analytics processes can be used to identify the attacker. In addition, the study proposes that there are already attack classes be expanded by three new classifications related to outgoing network traffic. But, the results of each technique employed in IDS vary due to the dataset and procedures used.

Shenfeld, Day, and Ayesh (2018) used artificial neural networks to evaluate intelligent intrusion detection systems. The article offers a unique technique for detecting malicious network traffic that makes use of artificial neural networks and can be employed in intrusion detection systems that do deep packet inspection.

The suggested artificial neural network system can accurately distinguish benign from destructive network traffic when fed a variety of benign network traffic data (dynamic link library files, and a variety of other miscellaneous files such as logs, music files, images, and word processing documents) and malicious shell code files obtained from an online exploit and weakness repository. Anna, Mariusz, and Jacek (2019) researched the use of neural networks to intrusion detection systems. Intrusion detection systems are one of the sectors in which neural

networks are frequently investigated to improve data privacy and overall computer and network security. The essay conducts a comprehensive assessment of the recent literature on the use of neural networks in intrusion detection systems, as well as surveys and fresh technique recommendations. Additionally, there are fundamental definitions of neural network topologies, types of intrusion detection systems, and training datasets.

Michal and Marek (2021) are also working on an intrusion detection method based on an improved artificial neural network. A wide range of ANN configurations is compared. The researchers tested their algorithms on two benchmark datasets: NSL-KDD and CICIDS2017. Finally, on an existing benchmark dataset, the most successful arrangement obtains 99.909% of multi-class classification accuracy.

The suggested approach by Kanimozhi and Prem (2019) is designed to detect a botnet attack that poses a serious threat to financial institutions services and banking. The suggested solution was developed using artificial intelligence on a realistic cyber defense dataset (CSE-CIC-IDS2018), the most recent IDS Dataset released by the Canadian Institute for Cyber Security (CIC) in 2018, hosted on AWS (Amazon Web Services).

Artificial intelligence, which allows machines to mimic human behavior, is one of the most recent emerging technologies, and the intrusion detection system is the most significant component utilized to identify cyber-intruders or criminal actions (IDS). Artificial intelligence is also important in detecting intrusions and is commonly regarded as a superior method of adapting and constructing IDS. Neural network algorithms are a new artificial intelligence approach that can be used to solve real-time challenges in the current world.

Mokhtar *et al*., (2021) give a detailed research and study of the literature's proposed Intrusion detection and features extraction systems based on SVM. It begins by outlining the fundamental principles and background information concerning security assaults, intrusion detection systems, and SVM classifiers. It then goes on to give taxonomy of SVM-based IDS systems and explain how various classes of SVM classifiers have been used to detect various types of abnormalities and intrusions. It also addresses the major contributions of the examined schemes, as well as the algorithms and methods that can be used in conjunction with the SVM to enhance the detection rate and accuracy of the system. It also addresses the major contributions of the examined schemes, as well as the algorithms and techniques that can be used in conjunction with the SVM to improve the detection rate and accuracy. Ultimately, the SVM-based IDS methods' various features and drawbacks are examined.

Ziadoon et al., (2021) offered machine learning (ML) methods for developing anomaly-based IDS (AIDS). The study uses ten prominent supervised and unsupervised machine learning techniques to find effective and efficient ML–AIDS of networks and computers. The supervised machine learning algorithms include the artificial neural network (ANN), decision tree (DT), k-nearest neighbor (k-NN), naive Bayes (NB), random forest (RF), support vector machine (SVM), and convolutional neural network (CNN), while the unsupervised machine learning algorithms include expectation-maximization (EM), k-means, and self-organizing maps (SOM). Several models of these algorithms are described, and the turning and training parameters of each approach are explored to achieve the best classifier evaluation feasible. Unlike other research, this one assesses the performance of 31 ML-AIDS models by measuring their true positive and negative rates, accuracy, precision, recall, and F-Score.

3. Method

The suggested methodology employs an Artificial Neural Network (ANN) to detect malicious attacker entry. The ANN is built by learning from a machine that mimics the learning pattern of genuine neural systems, such as biological systems. The systems work with intelligence, receiving inputs that are supposed to be presented in the human brain's linked neurons.

Additionally, a botnet was employed, which is a sort of attack (derived from the words "robot" and "network") or malware that enables an operator to remotely control and guide a system. By tracking and collecting consumer information, the botnet is used to do some criminal and damaging acts, including data theft, most notably in the banking and finance industries. Personal information such as usernames, passwords, and other credential information is stolen.

In the training phase, a cyber-dataset was pre-processed, and all entities and features were translated into numeric features. The model was then trained for Artificial Intelligence, and the detection accuracy was confirmed in the testing phase. The proposed Artificial Intelligence was built using Multi-Layer Perceptron (MLP). When it comes to attribute or feature scaling, Perceptron is gentle. As a result, scaling your data is recommended.

On the other hand, the Perceptron is composed of at least one spare input, a bias, an activation function, and a resulting output. The auto encoder recognizes the inputs (120 features extracted from the CICIDS2017 dataset gathered by the Canadian Institute for Cyber-Security (CIC)), applies a few weights, and the activation unit creates the output (attack or normal). The neural network of our framework can be defined as a collection of perceptual layers that generate multi-layer perceptions.

The process of optimizing a neural network is a large undertaking that takes a long time to accomplish. The method was carried out using the GridSearchCV Optimization approach and hyper-parameter optimization. The hyper-parameters evaluated for tuning are alpha, which can be a contrast of multiple regularization parameter values, and hidden layer sizes, which is an alternate parameter for tuning. With 10-fold cross-validation, it runs in parallel and iterates. The model is made up of two levels. We classified the grouping as "Benign or Malicious" as the outcome in the proposed structure.

4. Implementation

The experiments were carried out with the MATLAB Neural Network Toolbox version 2017b, which includes algorithms, pre-trained models, and apps with one hidden layer for constructing, training, visualizing, and modelling neural networks (also known as shallow neural networks) and neural networks with multiple hidden layers (called deep neural networks). A grid search procedure was used to find the optimum structure for the model, A multi-layer perceptron (MLP) with multiple convolutional layers of 30 hidden neurons each is the optimum structure (in terms of classification accuracy) for ANN. The classifier designs were evaluated using 10-fold cross-validation in ANN structure optimization. The Receiver Operating Characteristics curve was used in this study since it is one of the most widely used assessment metrics for determining the accuracy of any classification model to see the process of classifying multi-dimensional data.

Mediterranean Journal of Basic and Applied Sciences (MJBAS)
Volume 6, Issue 1, Pages 20-26, January-March 2022

5. Result

When the ratio of True Positive to False Negative is graded at estimation points, a Receiver Operating Characteristics curve is created. The curve illustrates how successfully the binary classifier differentiated between the two classes, Benign and Malicious, and it is shown in Figure 1. When the classifier model is run on a sample of 1109654 records with 80 features, it is optimized using 10-Fold Cross-Validation to produce the curve.

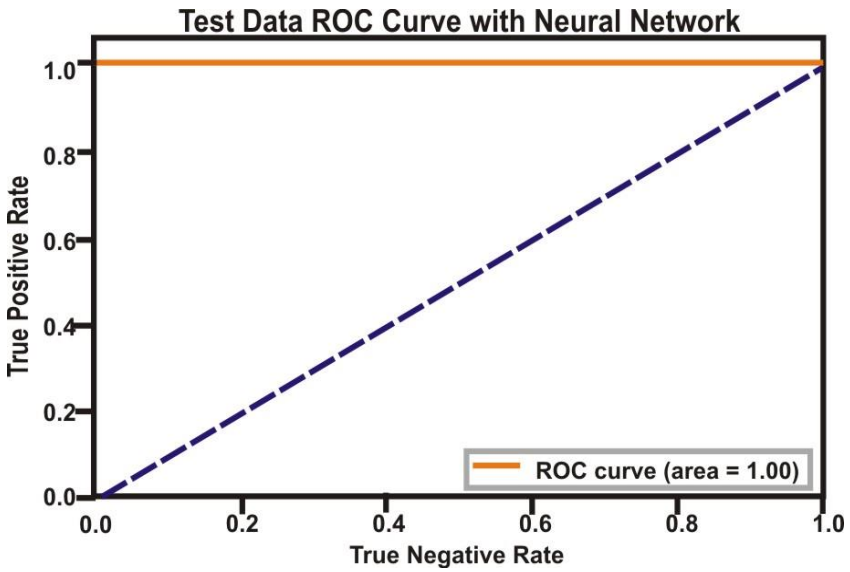

Fig.1. Receiver Operating Characteristics (ROC) curve

The Area under Curve (AUC) score (that is, the region under the Receiver Operating Characteristic (ROC) curve) indicates the overall implemented performance of the binary classifier. More points equal better performance for the classifier model, and the higher the score the better the performance. The AUC SCORE, on the other hand, is 0.999. In Figure 2, there is a Confusion Matrix that shows the number of positive and negative forecasts, as well as the computation of Benign and Malicious occurrences in this model, with the beneath graph exposing samples with a high proportion (100%). It distinguishes between benign and malicious botnets.

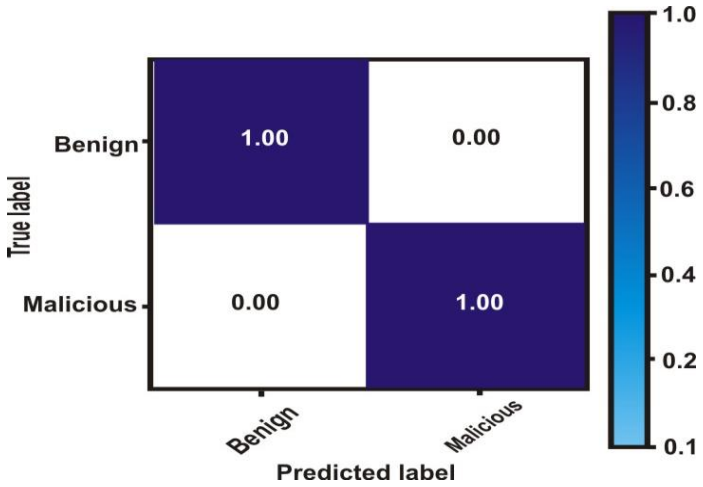

Fig.2 Neural Network Confusion Matrix

The Classification and Accuracy report of the proposed model is summarized as shown in the table 1 below:

Table 1. Classification Report of Neural Network

Performance Metrics	Training Data	Performance Metrics	Test Data
Accuracy	1.0	Accuracy	0.9997
Precision	1.0	Precision	1.0
Recall	1.0	Recall	1.0
F1	1.0	F1	1.0
AUC	0.0	AUC	1.0

Table1 indicates that the Model Training Accuracy is 1.0 and the Model Testing Accuracy is 0.9997.

6. Conclusion

The new model performs exceptionally well, with an average of 99.97% accuracy score and an average of 9.999% Area under Receiver Operator Characteristic Curve (ROC). The new model will aid in a better comprehension of various orders where IDS research has been conducted. It will be useful for those working on AI-based solutions in IDS and similar domains. Using this dataset, which includes all real-time and current incidents, the new model may be extended to detect all other lingering forms of attacks.

Declarations

Source of Funding

This research did not receive any grant from funding agencies in the public, commercial, or not-for-profit sectors.

Competing Interests Statement

The authors declare no competing financial, professional and personal interests.

Consent for publication

Authors declare that they consented for the publication of this research work.

References

Anna, D., Mariusz, P. and Jacek, R. (2019). A survey of neural networks usage for intrusion detection systems. Journal of Ambient Intelligence and Humanized Computing, https://doi.org/10.1007/s12652-020-02014-x.

Almási A-D, Woźniak S, Cristea V et al (2016) Review of advances in neural networks: neural design technology stack. Neurocomputing, 174: 31–41. https://doi.org/10.1016/j.neucom.2015.02.092.

Ayonya, P., Vijay, K. C., Sunakshi, S. and Suneel, Y. (2021). An Optimized Deep Learning Framework for Network Intrusion Detection System (NIDS). Authorized licensed use limited to: Indian Institute of Information

Technology. Downloaded on September 01, 2021 at 05:54:42 UTC from IEEE Xplore. Restrictions apply. DOI: 10.1109/EnT50437.2020.9431266.

Buczak AL, Guven E (2016) A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Commun Surv Tutor., 18:1153–1176. https://doi.org/10.1109/COMST.2015.2494502.

Camastra F, Ciaramella A, Staiano A (2013) Machine learning and soft computing for ICT security: an overview of current trends. J Ambient Intell Humaniz Comput., 4: 235–247. https://doi.org/10.1007/s12652-011-0073-z.

Dias, L.P., Cerqueira, J. J. F., Assis K. D. R. and Almeida, R. C. (2017). Using Artificial Neural Network in Intrusion Detection Systems to Computer Networks. 978-1-5386-3007-5/17/$31.00 ©2017 IEEE.

Kanimozhi, V. and Prem, J. T. (2019). Artificial Intelligence based Network Intrusion Detection with hyper-parameter optimization tuning on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing. Publishing services by Elsevier B.V.

Michał, C. and Marek, H. (2021). Intrusion detection approach based on optimized artificial neural network. 2021 Elsevier B.V. Neurocomputing, 452 (2021) 705–715.

Mokhtar, M., Tarik, A. R., Sarkhel, H. T., Adil, H. M. A., Quan, T. T., Moazam, B., Amir, M. R. and Mehdi, H, (2021). A comprehensive survey and taxonomy of the SVM-based intrusion detection systems. Journal of Network and Computer Applications 178 (2021) 102983.

Nisioti, A., Mylonas, A., Yoo, P. D. and Katos, V. (2018)"From intrusion detection to attacker attribution: A comprehensive survey of unsupervised methods," IEEE Commun. Surv. Tutorials Surv. Tutorials, vol. 20, no. 4, p. 3369, 2018, [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8410366/.

Rana, A. R. A., Xi-Zhao, W., Joshua, Z. H., Haider ,A. and Yu-Lin, H. (2017). Fuzziness based semi-supervised learning approach for intrusion detection system. Journal of Information Sciences 378 (2017) 484–497 http://dx.doi.org/10.1016/j.ins.2016.04.019 0020-0255/© 2016 Elsevier Inc. All rights reserved.

Sani, Y., Mohamedou, A., Ali, K., Farjamfar, A., Azman, M. and Shamsuddin, S. (2009). An overview of neural networks use in anomaly intrusion detection systems, IEEE Student Conference on Research and Development (SCOReD) 2009 (2009) 89– 92, https://doi.org/10.1109/SCORED.2009.5443289.

Shenfeld,A., Day, D. and Ayesh, A. (2018). Intelligent intrusion detection systems using artifcial neural networks, ICT Express (2018), https://doi.org/10.1016/j.icte.2018.04.003.

Tran NN, Sarker R, Hu J (2018) An Approach for Host-Based Intrusion Detection System Design Using Convolutional Neural Network. In: Hu J, Khalil I, Tari Z, Wen S (Eds) Mobile Networks and Management. Springer International Publishing, Cham, pp 116–126.

Ziadoon, K. M., Robiah, Y., Nazrulazhar, B., Salama, A. M. and Cik, F. M. F. (2021). Benchmarking of Machine Learning for Anomaly Based Intrusion Detection Systems in the CICIDS2017 Dataset. IEEE Access, VOLUME 9, 2021 Digital Object Identifier 10.1109/ACCESS.2021.3056614.