Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Ola et al. Vol 2, Issue 1, 2025 Publication Edition

Deep Learning-Based Network Intrusion Detection Using CNN and Enhanced UNSW-NB15 Multi-Class Dataset

Research Article https://stem.techspherejournal.com

Author(s) Details

A. G. Ola*[1], O.D. Alowolodu[2] and A.H. Afolayan[3]

[1]Polytechnic Digital Library, Federal Polytechnic Ado-Ekiti, Ekiti State, Nigeria

[2,3] Department of Computer Science, Federal University of Technology Akure, Ondo State, Nigeria.

https://doi.org/10.5281/zenodo.15495192

*__Corresponding author's email__: ola_ag@fedpolyado.edu.ng

ABSTRACT

The need for sophisticated intrusion detection systems (IDS) has grown owing to the significant security risks and network attacks brought on by the proliferation of network devices or nodes such as computers, laptops, smart phones and others on the internet for data and information exchange. Deep learning has proven to be quite effective in a variety of disciplines and can handle large amounts of data. Security experts are therefore working to incorporate deep learning into an intrusion detection system. Multiclass model is designed for classifying network traffic into multiple attack categories. Several studies have been conducted on this subject, resulting in a wide variety of methods. Most of these approaches use predefined features extracted by an expert in order to classify network traffic. In addition, the UNSW-NB15 dataset was created in several distinct files and labelled using binary classification. The goal of this study is to separate the entire dataset into nine multiclass models and determine the highest network attacks from the dataset. The study examined how well deep learning performed in two classification categories (Binary and Multi-Class) using the improved UNSW-NB 15 dataset. The findings of the study discovered that Generic and Exploit Network Attacks from UNSW-NB 15 dataset contained highest network attacks. The model's training accuracy increases gradually while the validation accuracy improves up to 96.04% in multi-class classification.

Keywords: Deep learning, CNN, Intrusion detection system, UNSW-NB15.

1 Introduction

The rapid and advanced development in Information and Communication Technology (ICT) has made communication to be instant and easily accessible. The need for sophisticated intrusion detection systems (IDS) has grown owing to the significant security risks and network attacks brought on by the proliferation of network devices or nodes such as computers, laptops, smart phones and others on the internet for data and information exchange (Ahmed, Mohammed and Ahmed, 2024). Network security has grown significantly in recent years due to the rapid growth of cutting edge ICT technologies as 5G communications, mobile internet, Internet of Things (IoT), cloud computing, grid computing, and big data (Ola, 2024). Recent increases in internet usage have resulted in advancements in computer networks, with large volume of data being transferred on a daily basis. Edeh (2022) predicted that by 2023, there would be a rise in the quantity of IP-connected devices generating a substantial amount of IP traffic, reaching up to 4.8 ZB. In the era of COVID-19 in the year 2020, there was a high introduction of new attacks typically due to the entire world's population increases in the use of internet services. The socio-economic facets of human endeavor, such as communication, business, education, and entertainment, benefited from the availability of the Internet. People's daily lives have been changed by this service, particularly with the use of Internet of Things (IoT) devices in smart cities. (Mebawondu, 2023).

An intrusion is an intentional and unauthorized effort, whether successful or not, to breach, access, manipulate, or misuse valuable assets, potentially rendering them unreliable or unusable (Ola, 2024). An intrusion detection system (IDS) is a security tool designed to detect unauthorized intrusions into computer systems and networks. Vakanski (2021) described a Network Intrusion Detection System (NIDS) as a security system utilized to protect networks from unauthorized intrusions. To prevent potential breaches, network intrusion detection systems (NIDS) must continuously monitor network traffic for any unusual activity that could violate security policies or compromise the confidentiality, integrity, and availability of the network.

Current IDSs based on signatures intrusion detection cannot detect unknown or new threats. Anomaly IDSs that utilize Machine Learning (ML) methods lack scalability when dealing with large datasets, and their runtime increases with dataset size, requiring significant computational resources to meet runtime demands (Edeh, 2022).This is as a result of network intrusion by cyber-criminals to steal confidential information from users on the internet. Vakanski (2021) asserted that network security is crucial for every organization, as all computer systems are susceptible to security vulnerabilities.

The use of Artificial Intelligence (AI), including Machine Learning algorithms and Deep Learning methods, in Network Intrusion Detection has begun to yield significant outcomes. Deep learning approaches are particularly advanced, capable of addressing constraints inherent in conventional machine learning techniques. Network Intrusion Detection (NID) also finds application in various other cyber security domains such as Denial of Service, Backdoor detection, Reconnaissance, malware detection and classification, file type recognition, spam detection, insider threat detection, network traffic analysis, botnet detection, user authentication, detection of false data injection attacks, verification of human key-strokes, and identification of drive-by download attacks (Ola, 2024).

1.1 Network Attack Types in UNSW-NB 15 Dataset

According to Moustafa (2016), Network attack types can be categorized into nine groups, namely:

1. Fuzzers: This attack involves an attacker trying to uncover security vulnerabilities in a program, operating system, or network by bombarding it with extensive inputs of random data in an attempt to cause it to crash.
2. Analysis: This category includes various intrusions that infiltrate web applications through methods such as port scans through ports, emails like spam, and web scripts such as HTML files.
3. Backdoor: A method to circumvent normal authentication procedures, allowing unauthorized remote access to a device and providing a covert entry point to plaintext data while attempting to remain unnoticed.
4. DoS: An attack that disrupts computer resources by overwhelming memory or making them excessively busy, thereby preventing authorized requests from accessing a device.
5. Exploit: A series of instructions that leverages a flaw, bug, or vulnerability, exploiting unintended or unexpected behaviour on a host or network.
6. Generic: A method that targets any block-cipher by utilizing a hash function to create collisions, regardless of the block-cipher's specific configuration.
7. Reconnaissance: This refers to probing or gathering information about a computer network to circumvent its security controls.
8. Shellcode: This attack involves an attacker injecting a small piece of code, typically originating from a shell, to gain control over the compromised machine.
9. Worm: This attack involves the attacker replicating itself to propagate onto other computers, often utilizing computer networks and exploiting security vulnerabilities on target computers to gain access.

Convolutional Neural Network (CNN) is one of the fundamental algorithms in deep learning, was developed to emulate the human visual system (HVS). A convolutional neural network (CNN) is a type of multi-layer artificial neural network widely applied in intrusion detection (Alowolodu et al 2020). At its core, a CNN is structured around the convolutional layer, which is pivotal for processing data. This layer involves several components: input data, a filter, and a feature map

(Mayank, 2020). Typically, a CNN comprises three main layers: convolutional, pooling, and fully connected layers. Figure 1 shows the Generic Architecture of CNN.

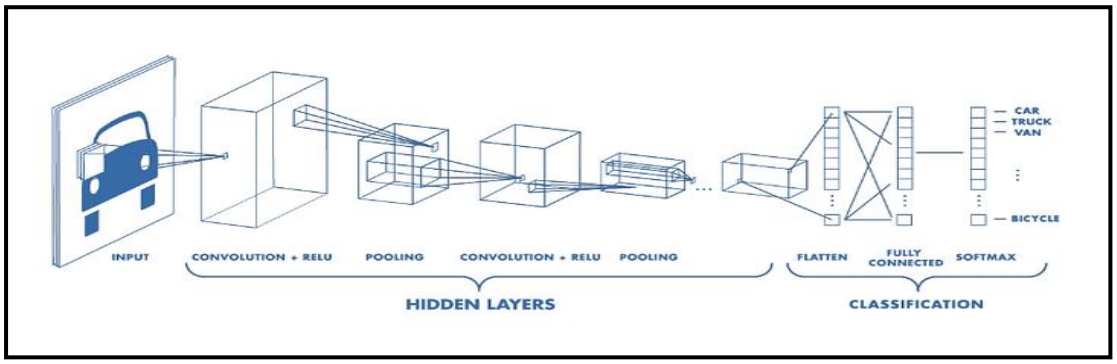

Figure 1: Generic Architecture of CNN (Mayank, 2020)

Over a decade, Machine Learning (ML) and Deep learning (DL) techniques have been subjected to extensive research in developing Intrusion Detection System (IDS) using various intrusion detection datasets. The most common among the datasets are the KDD99 and NSL-KDD intrusion detection datasets.
Moreover, the deep learning architecture which does not require any of the features engineering technologies such as (e.g., feature selection methods…etc). Therefore, this study utilizes Deep Learning techniques, specifically Convolutional Neural Networks (CNN), for detecting Multi-class Attacks with *UNSW-NB 15 Dataset*. The accuracy and loss of Deep Learning algorithms utilized for binary, multi-class classification on network intrusion detection is determined.

2 Research Methodology

The research methodology will be in four (4) phases: data acquisition, data preparation, classification and evaluation phases. The datasets for this research were generated primarily by the University of New Wales Networked Based 2015 (UNSW-NB 15) Intrusion Detection Datasets from online Repository provided by Kaggle. Data Preparation includes cleaning of data, handling missing values, statistical summaries, categorical feature conversion, normalization and exploratory data analysis. The classification phase will involve designing the drive-by download attack modelling using deep Learning. In this phase, the prepared network datasets would be classified as normal or multi-class and drive-by download using Convolutional Neural Network (CNN). The research methodology will be in four (4) phases: data acquisition, data preparation, classification and evaluation phases. The datasets for this research were generated.

3 Proposed Model

The proposed model will be implemented using the Tensorflow python library. The fourth phase involved model evaluation using standard metrics. Convolutional neural networks run a mathematical operation called convolution. Equation 1 describes the CNN mathematical model on the UNSW-NB15 dataset.

$$x_i^a = \phi\left[\sum_{i \in k_i} x_j^{a-1} * w_{ji}^a + b_j^a\right] \quad (1)$$

Where,

$x_i^a$is the attribute i map of the convolution layer a.
ϕ Represents the Activation Function
$k_i$is the input attribute set of the layer (a-1)
w_{ji}^as the connection weight between attribute i of the convolution layer and attribute j of the layer (a-1)
$b_j^a$the deviation in the related layer

The layer that follows the convolution layer is the pooling layer. Reducing the size of the attribute map is the major objective of the pooling layer. The pooling layer operation ensures the identification of significant attributes, minimizes data complexity, and increases the tolerance of the network against environmental changes. The pooling layer can be presented as demonstrated in Equation 2.

$$x_i^a = \phi\left[\beta_i^a c\left(x_i^{a-1} + b_i^a\right)\right] \quad (2)$$

The c demonstrated here indicates the sub-sampling function
b indicates the weighting matrix
The classification operation is performed through the fully connected layer following the convolution layer and pooling layer. Equation 3 demonstrates the output function of the fully connected layer.

$$y^m = \phi[w^m x^{m-1} + b^m] \quad (3)$$

The m demonstrated here indicates the layer index while
y^mdemonstrates the output of the fully connected layer
$x^{m-1}$is the input of the fully connected layer
$b^m$is the deviation

The proposed methodology has been divided into modules as follows:

Data Acquisition Phase:

Step 1: Download the Dataset and import the library:
Step 2: Loading of the essential library needed to build the model.
Step 3: Dataset Splitting (70% for Training and 30% for Test Datasets and to cross-validate the CNN algorithm).

Data Preparation Phase

Step 1: Cleaning of data,
Step 2: Handling missing values,
Step 3: Statistical summaries,
Step 4: Categorical feature conversion,
Step 5: Normalization and
Step 6: Exploratory data analysis.

Classification Phase with CNN NID Model.

Step 1: Normal Classification
Step 2 Multi-class Classification and

Evaluation

Step 6: Evaluation

3.1 Multiclass Classification Implementation and Testing

Multiclass model is designed for classifying network traffic into multiple attack categories. The Multiclass classification of the deep learning techniques is implemented and tested. First, the classification is based on the UNSW-NB15 training dataset for multiclass for Fuzzer (6062), Analysis (677), Backdoor (583), DoS (4089), Exploit (11,132), Generic (18,871), Reconnaissance (3496), Shellcode (378) and Worms (130) records. Then the evaluation of the built model was based on a test dataset of Fuzzer (18,183), Analysis (2000), Backdoor (1746), DoS (12,264), Exploit (33,393), Generic (40,000), Reconnaissance (10,491), Shellcode (1133) and Worms (44) records to test the performance of the newly created models. These datasets are in CSV format and are used based on a target of the multiclass classes only. The classification, testing and evaluation, and results of CNN, are implemented. Upon completing 20 epochs of training for the Multiclass classification CNN model, the results are as in the Figure 2 and Figure 3.

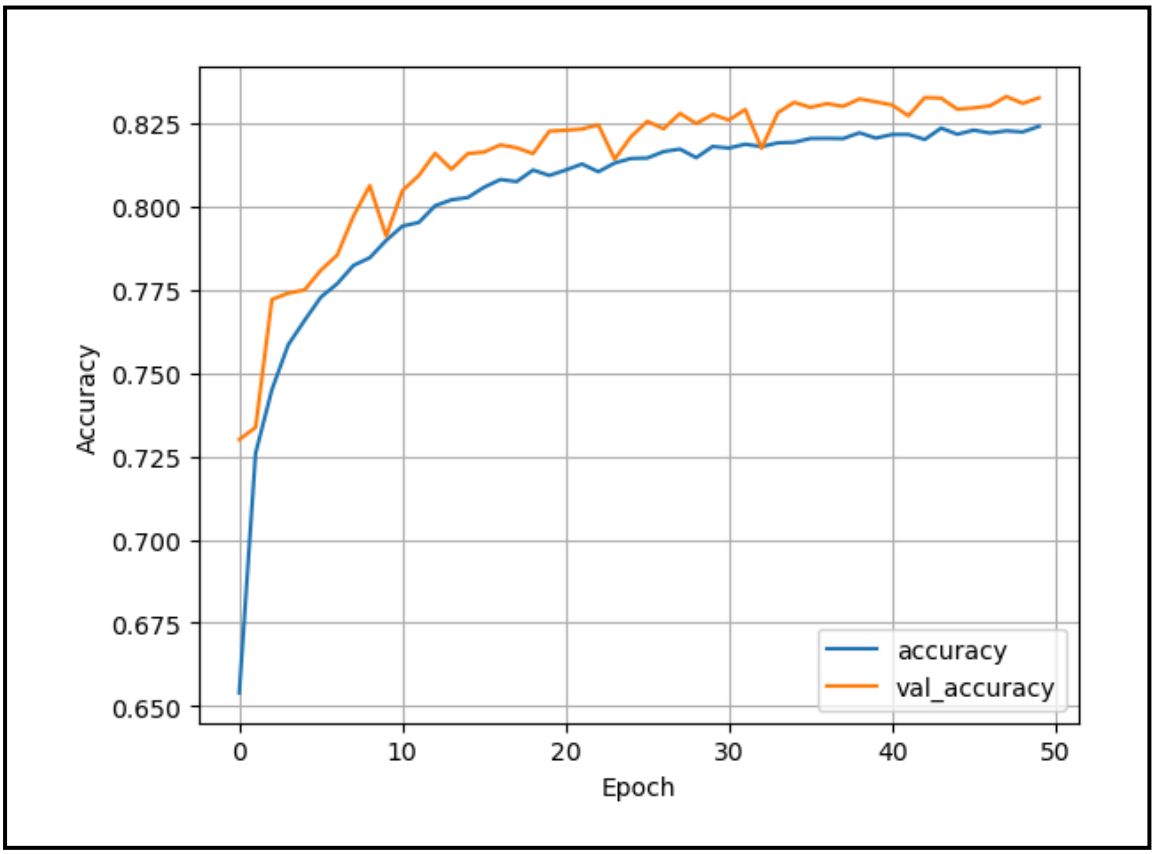

Figure 2: Graph showing the increase in accuracy value of the Multiclass classification model over 20 epochs

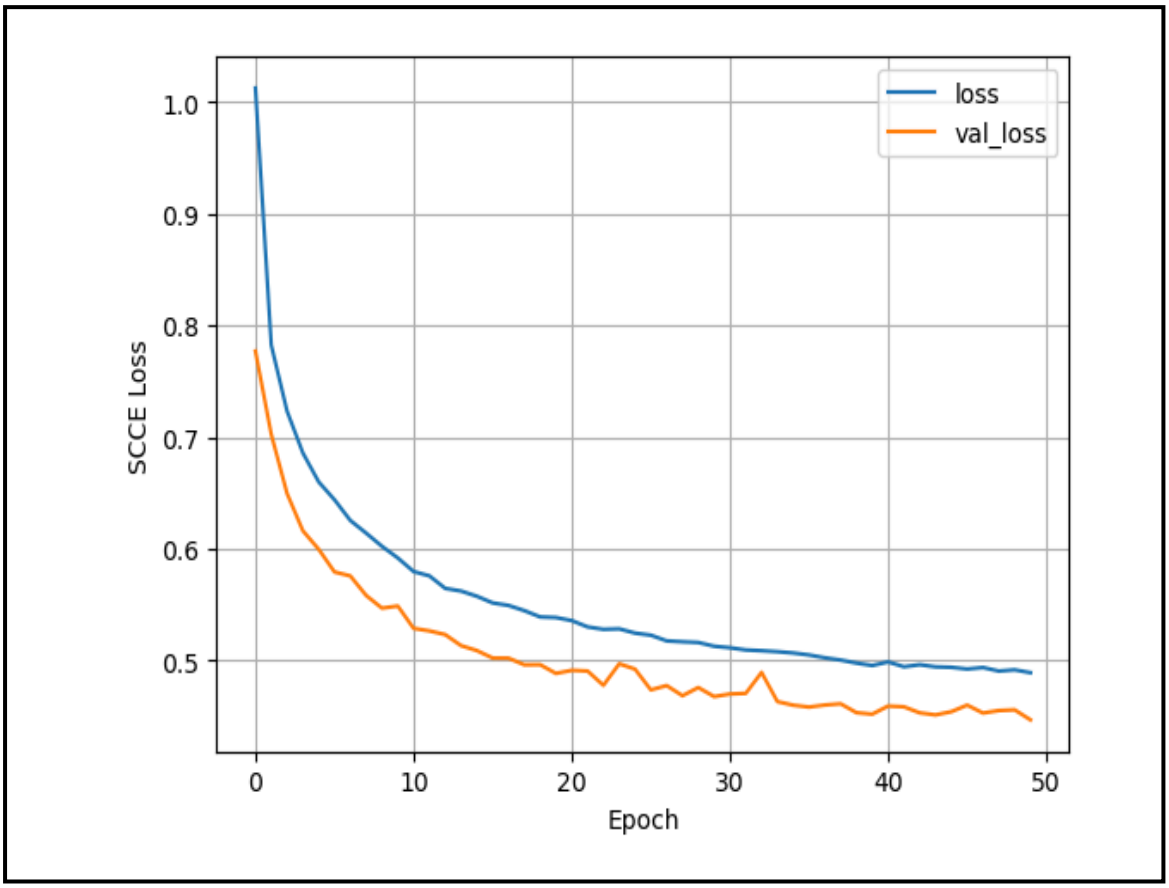

Figure 3: Graph showing the decrease in loss value of the Multi-class Classification over 20 epochs

Table 1: Results Obtained from the Multiclass Classification:

S/N	Metrics	Multiclass Classification
1	Training Accuracy	95.36%
2	Validation Accuracy	96.04%
3	Training Loss	0.1101
4	Validation Loss	0.1034

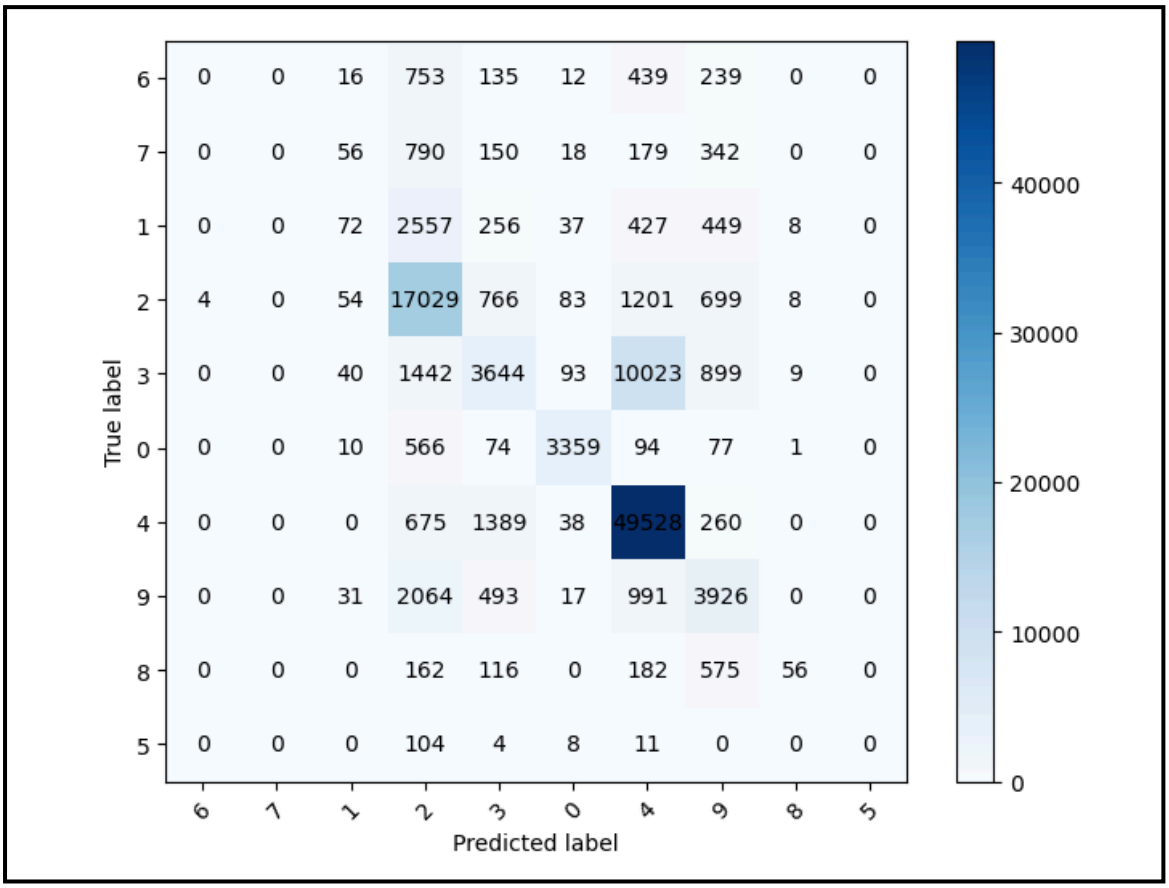

Figure 4: Confusion Matrix for the CNN test Multiclass Classification

Results obtained from the Multiclass classification processes performed by using the convolutional neural network (CNN) in the UNSW-NB15 dataset are presented in Table 1.1. The model's training accuracy increases gradually while the validation accuracy improves up to 96.04%. The training loss decreases as the model learns from the data. The model's performance seems reasonable, but further evaluation on unseen data is needed to assess its generalization ability. Higher accuracy suggests better generalization, while a lower accuracy indicate issues with overfitting or the model's inability to handle the complexity of the test data. Further analysis and fine-tuning may be required to improve the model's performance.

3.2 Performance Evaluation

The performance evaluation metrics expected to be derived in the research are Specificity, Sensitivity, Positive Predicted values (PPV), Negative Predicted values (NPV), and Accuracy.

With reference to equation 1 – 3; from the confusion matrix, TP = 5985, FP = 872, FN = 967 and, TN = 1983

1. Sensitivity (Recall) : Sensitivity = TP / TP+ FN = 5985/5985+967 = 96.71%
2. Specificity = TN/TN+FP = 1983/198+872 = 1983/5985+872 = 87.21%
3. PPV (Precision) = TP/TP+FP = 5985/5985+872 = 87.21%

4. NPV = TN/TN+FN = 1983/1983+967 = 96.69%
5. Accuracy = (TP +TN)/ (TN+TP+FN+FP) = (5985+1983)/(1983+5985+967+872) = 81.20%
6. F1-Score= 2TP/2TP+FP+FN = 0.86%

The results are tabulated in Table 2 for the Final Result after Performance Evaluation of the Multiclass classification CNN NIDS model

Table 2: Performance Evaluation CNN deep learning model for detecting Drive-by Download Attacks

%Sensitivity	%Specificity	% PPV	% NPV	% Accuracy	% F1-Score	% Loss
96.71%	87.21%	87.21%	96.69%	81.20%	0.86%	18.8%

In the result, Sensitivity or recall value is greater than the Specificity of 87.27 %. This indicated that the model predicted well. The accuracy of 81.20% shows there are error rates of about 19% is existing in the model. The sensitivity of 96.71% shows the model's true positive rate can be very sensitive to detect any attack. The specificity of 87.21 % indicates the true negative rate is moderately okay

4 Conclusion

This work presents deep learning models based on CNN as an intrusion detection system, for intrusion detection system in computer environments. The UNSW-NB15 enhanced benchmark dataset was applied with a convolutional neural network deep learning model. Further, the development of Multiclass Attack categories were evaluated using metrics based on accuracy and loss. The experimental results of proposed deep learning models show its superiority for detecting abnormal events using the improved UNSW-NB15 dataset compared with earlier techniques that have been developed on the same dataset. In the future, we plan to extend this study to deploy the framework in a real environment with further findings and explanations.

References

Ahmed, A., Mohammed, Y. and Ahmead, M. (2024). Deep-Intrusion Detection System With Enhanced Unsw-Nb15 Dataset Based On Deep Learning Technique. Journal of Engineering Science and Technology

Alowolodu, O. D., Adetunmbi, A. O., Mebawondu, J. O., and Mebawondu, O. J. (2022). A Review of Deep Learning Techniques for Network Intrusions Detection towards Efficient Model Developments. IEEE Nigeria 4th International Conference on Disruptive Technologies for Sustainable Development (NIGERCON), 2022, pp. 1-5, doi: 10.1109/NIGERCON54645.2022.9803080.

Ebru, K. (2022). Network Intrusion Detection with A Deep Learning Approach. A Thesis Submitted To the Graduate School Of Informatics Of Middle East Technical University.

Edeh, D. I. (2022). Network intrusion detection system using deep learning technique. Master of Science, Department of Computing, University of Turku.

Mayanki, M. (2020). Convolutional Neural Networks, Explained. Towards Data Science

Mebawondu, J.O. (2022). Development of an Ensemble Deep Learning Network Intrusion Detection System. PhD Proposal Seminar, Department of Computer Science, Federal University of Technology Akure Nigeria

Mebawondu, J.O. (2023). Development of an Ensemble Deep Learning Network Intrusion Detection System. PhD Proposal Seminar, Department of Computer Science, Federal University of Technology Akure Nigeria

Moustofa, N and Nygard, O. (2020), Convolutional Neural Networks with LSTM for Intrusion Detection. EPiC Series in Computing, Proceedings of 35th International Conference on Computers and Their Applications, Volume 69, 2020, pp 69-79.

Ola, A.G. (2024). Detection of Drive-by Download Network Attack using Deep Learning Approach. MTech Thesis, Department of Computer Science, Federal University of Technology Akure Nigeria