Intrusion Detection System Based on Network Port Statistics Using Multilayer Perceptron and Deep Learning Approaches

Purnima Miazy
Department of Computer Science
and Engineering
University of Chittagong
Chittagong -4331,Bangladesh
miazypurnima@gmail.com

Muhammad Anwarul Azim
Department of Computer Science
and Engineering
University of Chittagong
Chittagong -4331, Bangladesh
azim@cu.ac.bd

***Abstract*—The proliferation of the Internet of Things (IoT) faces significant challenges in terms of network security. The confidentiality of data and stability at the network layer are at risk because of the increasing expansion in the development of IoT devices, which creates a broad attack field for malevolent cybercriminals and may result in more damaging assaults.**

This paper gives a thorough investigation into intrusion detection utilizing the UNR-IDD dataset, which bases its findings on network port information. We offer two unique approaches for improving intrusion detection efficiency over existing machine learning (ML) algorithms, using Multilayer Perceptron (MLP) and Convolutional Neural Network (CNN) algorithms, respectively. We employed three feature engineering techniques—Principal Component Analysis (PCA), Analysis of Variance (ANOVA), and Mutual Information—in addition to employing MLP as the baseline model to improve the effectiveness of the IDS system. Additionally, hyperparameter tweaking was done to make the model's parameters as efficient as possible.

The suggested MLP-based technique obtains an accuracy of 83% after rigorous testing, whereas the CNN-based approach obtains an accuracy of 85.7%. These astounding findings demonstrate the efficacy of deep learning models in intrusion detection applications, prevailing against traditional ML methods. This study advances network security in the face of growing internet hazards by offering insightful information on the development and use of successful IDS systems.

***Index Terms*—Intrusion Detection, Network Statistics, MLP, CNN, Anova, PCA, Mutual Information, Deep learning.**

I. Introduction

Systems for detecting network intrusions (IDS) are essential for securing computer networks against unwanted and harmful activity. To improve the detection skills of IDSs, researchers have investigated a number of strategies throughout the years, including machine learning (ML) and deep learning (DL). Network intrusion detection has made extensive use of machine learning (ML) methods, including decision trees, support vector machines (SVM), and random forests, which have shown remarkable effectiveness in identifying known attack patterns. However, with network assaults becoming more sophisticated and complicated, there is a need for more sophisticated methods to increase the precision and effectiveness of IDSs. In order to prevent these assaults from occurring, the development of a reliable and effective intrusion detection system (IDS) for cybersecurity has become a critical issue. An intrusion detection system examines network traffic for any behavior that may be suspect, investigates it, notifies the system, and then searches the network traffic once again. Data exchanged and transferred via a network may be vulnerable to many types of assaults, which an IDS can detect. Several cyberattacks were thoroughly examined as part of this inquiry [1].

Because of its capacity to automatically discover hierarchical representations from data, deep learning, a branch of machine learning, has attracted a lot of interest. Multilayer perceptron (MLP), convolutional neural networks (CNNs), and recurrent neural networks (RNNs) are examples of deep neural networks that have shown extraordinary performance in a variety of fields, including pattern identification, image recognition, and natural language processing. The use of DL approaches in network intrusion detection has a lot of potential for solving the problems brought on by new and unpredictable attack patterns.

Recent studies have shown that deep learning (DL) approaches, such as MLP and CNN, outperform classical ML algorithms for network intrusion detection. MLP models may successfully capture the deep interactions between network characteristics by combining hidden layers and nonlinear activation functions. This enables them to identify previously unidentified assaults and decrease false positives.CNN is a strong framework for deep learning which is currently gaining momentum in a variety of fields, spanning image and signal processing, in addition to MLP. CNN models are extremely good at detecting spatial connections in data. In the context of network intrusion detection, CNN may use its organizational framework to derive significant characteristics from network port information, boosting the detection mechanism's effectiveness and resilience.

This study seeks to develop network intrusion detection to give useful insights into the use of MLP and CNN algorithms for intrusion detection based on network port information. The results will help in the creation of more effective and reliable IDSs to defend computer networks against new threats by illuminating the capabilities and constraints of deep learning methods in tackling the changing issues of network security.

II. Related Work

The growth of communication technology, the availability of gadgets, and the development of computational systems are all contributing to the Internet of Things (IoT) explosive growth. The researchers are now concerned about IoT security as a result of this. An examination of recent research in IoT security, its trends, and unresolved challenges is provided by Wan Haslina Hassan in his article [2]. Additionally, they discuss IoT-based system management, policy enforcement, privacy, integrity, and confidentiality.

IoT security concerns and IoT attack surfaces were covered by Mohammed Ali Al-Garadi in this survey [3]. The potential applications of machine learning and deep learning in IoT security are thoroughly examined and explored. They contrasted the approaches at the conclusion of each paragraph based on their usability, benefits, drawbacks, and numerous applications for IoT security. In a later section of this survey, the applications of ML and DL algorithms are discussed in order to protect the key IoT layers. Finally, they discuss concerns, obstacles, and potential future directions relating to the employment of machine and deep learning approaches in successfully safeguarding IoT systems in accordance with data learning methodologies.

As cyber threats grow and become more sophisticated, network security has become a major concern for enterprises. Traditional rule-based intrusion detection systems are limited in their ability to identify innovative threats and can create a large number of false positives. This is where machine learning comes in, bringing numerous significant advancements and increasing the effectiveness of NIDS.

A network intrusion detection technique centered on anomalies was established by Meftah [4] utilizing the UNSW-NB15 dataset. They split their strategy into two key phases. They determine the essential characteristics for machine learning applications using a variety of techniques, including Recursive Feature Elimination and Random Forests. Then, they use several data mining methods, such as SVM, GBM, and Logistic Regression, to do a binary analysis to hunt for aberrant traffic. The support vector machine approach gave them the greatest accuracy score, 82.11%. To improve the accuracy of identifying threat patterns, they then inserted the SVM results into a collection of polynomial classifications. Particularly, researchers assessed the effectiveness of Naive Bayes, Decision Trees, and Polynomial SVM. It was decided to adopt a two-phase mixed categorization method, which boosted the accuracy of the results by up to 86.04%. This work may be improved by creating a novel classification method or by applying deep learning methods to a large number of examples.

Om H [5] presented a hybrid model that incorporates k-Means with the k-nearest neighbor and Naive Bayes classifier techniques. For attribute selection, this model employs an entropy-based feature selection technique. It uses the k-means clustering approach to group data (five clusters are employed) and then uses the k-nearest neighbor (KNN) and Naive Bayes classification algorithms to find intrusions. The model demonstrates a superior method to k-Means alone. The author also conducted their experiment using the KDD99 cup data set.

Deep Learning models and approaches have been successfully used for a variety of tasks, including object identification, illness diagnosis, picture recognition, self-driving vehicles, drug discovery, etc [6]. Deep learning techniques produce consistent and effective results, which has drawn the attention of several academics.

Here in this study, Kim [7] proposed an IDS model based on Deep Neural Networks (DNN). Here, they preprocessed the data set and used the kdd-CUP'99 data set to train and evaluate the classification model. Their model has 100-layer units and four hidden layers. They achieved an accuracy of almost 98%, and their suggested model also produced relatively low false rate scores.

In this work [8], another IDS model is created using DNN. The CICIDS2017 dataset was utilized to train and test the model that has been employed in this work. The dataset that was used contains actual network traffic information. Label encoding is done at the data preprocessing stage to make sure the model does not show bias for any attack types. Here, the deep neural network is used to help the dataset generate results more quickly and accurately. The newly presented neural network model provides accuracy for binary classification and multi-class classification of 99.13% and 99.29%, respectively.

A Convolutional Neural Network (CNN)-based Intrusion Detection System (IDS) model, proposed by Samson Ho [9]. The suggested IDS paradigm sought to identify intrusions using network traffic in order to increase internet security. In this research, they divided the packet traffic into types that were either benign or malignant. The suggested model was trained and validated using the CICIDS2017 dataset. The presented model's overall accuracy, training costs, attack detection rate, and false alarm rate have all been assessed.

A model for SDN settings that uses GRU-RNN techniques to detect anomalies was introduced by Tang in his paper [10]. The GRU-RNN model demonstrates how historical and contemporary events are related. The model utilized in this study can improve the rate at which abnormalities are found. The NSL-KDD dataset, which has six unprocessed features, was used to test the model, and it showed an accuracy of 89%.

Our study compares the performance of MLP-based IDSs against more conventional ML approaches in order to determine how successful they are at detecting network intrusions. To determine the best configurations for obtaining improved detection accuracy, the research will assess several MLP designs, training methodologies, and feature engineering methods using the UNR-IDD dataset. For our further research study, we propose another approach with the deep learning method CNN. The study will also look at ways to make MLP and CNN models easier to understand and interpret in the context of network intrusion detection.

III. Data Preprocessing

First, the dataset and the model development strategy are provided in detail to assist the development of the proposed framework. We have thoroughly examined the suggested model architecture modeling strategy as well as the training technique addressing the most suitable parameter change.

A. About Dataset

For the purposes of this study, we have used the University of Nevada - Reno Intrusion Detection Dataset (UNR-IDD) [11], which makes use of network port information for fine-grained analysis of intrusions. The UNR-IDD dataset contains 37412 samples and 34 characteristics with five attack types: TCP-SYN flood, Port scan, Flow table overflow, Blackhole, and Diversion. These intrusion types were chosen for this dataset because they are frequent cyber assaults that may occur in any network environment and can be launched on network devices as well as end hosts. UNR-IDD is made up of network port information. These speak about the network's switch/router ports' observed port metrics that are recorded. The collection also contains delta port statistics, which show the magnitude of recorded port statistics that have changed over time. As choices are made at the port level as opposed to the flow level, UNR-IDD may offer a more fine-grained analysis of network flows than flow statistics-based datasets. This allows for the quick detection of probable intrusions.

B. Preprocessing of Data

The data preprocessing pipeline involves loading and splitting the data, performing one-hot encoding for categorical features, handling outliers using the Tukey method, standardizing the numerical features, converting data to TensorFlow tensors, and label encoding the target labels. These preprocessing steps are crucial for preparing the data for training and evaluating the intrusion detection system model. The data is divided into features and labels for each dataset using the **drop()** method.
Categorical features in the training data are encoded using one-hot encoding with **pd.get_dummies()**. Data exploration is conducted using box plots to visualize the distribution of features. A loop iterates through subsets of three features at a time and generates box plots for each subset using Seaborn. To address outliers, the Tukey method is used. A loop iterates through the features, calculating the interquartile range (IQR) for each and identifying outliers based on the IQR. Outliers are printed along with their count. Descriptive statistics of the scaled numerical features are computed using **X_train_numeric.describe()**. Data standardization is performed using StandardScaler from Scikit-learn. The scaled data is then converted to TensorFlow tensors using **tf.convert_to_tensor()** for compatibility with neural network operations as well and label encoding is applied to the target labels using LabelEncoder from Scikit-learn.

IV. Methodology

Our main goal is to create an Intrusion Detection System (IDS) model by employing Multilayer Perceptron (MLP) neural networks. To improve the reliability and accuracy of our IDS, our method includes a thorough investigation of many machine learning models and deep learning architectures. We put many conventional machine learning models into practice and benchmark them in order to assess the efficacy of our MLP-based IDS. Additionally, in order to further our study and make use of convolutional neural networks (CNNs) importance, we included a CNN model for IDS and evaluated its effectiveness in comparison to the MLP-based model. The general architecture of the IDS model is shown in Fig 1. With the use of this comprehensive approach, we are able to develop an effective IDS based on MLPs while also examining the possibilities for developing intrusion detection methods utilizing alternate deep learning architectures, such as CNNs.

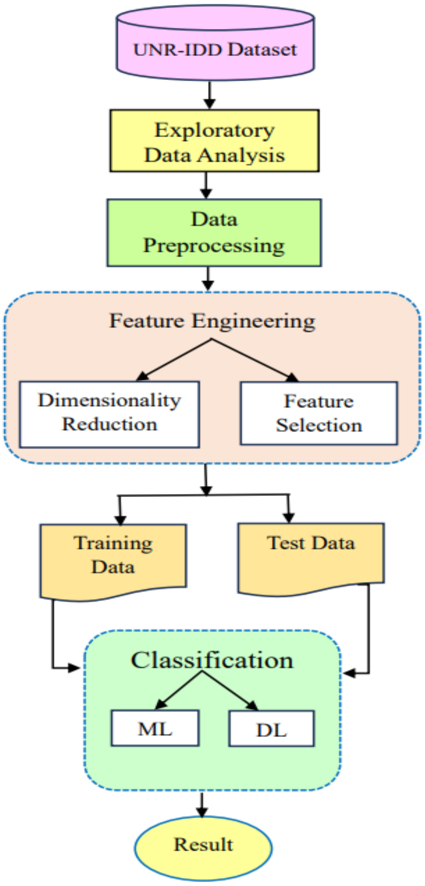

Fig. 1. General Architecture of The IDS Model

A. Feature Selection Phase

In the feature selection phase of our research work, we employed dimensionality reduction techniques and feature selection methods to enhance the efficiency of our Intrusion Detection System (IDS) model. We incorporated Principal Component Analysis (PCA) as a dimensionality reduction technique [12], utilizing a range of components to determine the optimal number that maximizes testing accuracy. Through comprehensive experimentation, we evaluated the effect of PCA on our IDS model by observing how the number of components influences accuracy. Subsequently, we employed feature selection techniques, namely Analysis of Variance (ANOVA) [13] and Mutual Information [14], to determine the most relevant features for the model. We conducted a comparative analysis of the testing accuracies achieved with both techniques and observed that ANOVA outperformed Mutual Information in terms of accuracy. The best number of features was selected based on the technique that provided the highest validation accuracy shown in Fig 2. These explorations led us to choose ANOVA as the preferred method for feature selection, significantly contributing to the optimization of our IDS model's performance.

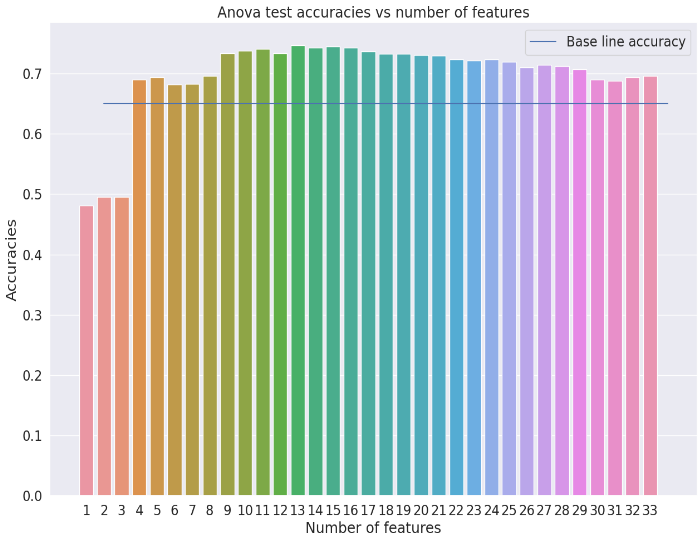

Fig. 2. Best Feature Selection Using Anova

B. Classification Phase

Our research's classification phase included a thorough investigation of intrusion detection utilizing a variety of machine-learning models. The Multi-Layer Perceptron (MLP), Convolutional Neural Network (CNN), and numerous other well-known models were essential to this research. The use of the Anova feature selection approach, which precisely determined the most relevant features from the input dataset, was very significant. Through this procedure, it was hoped to make the models more effective at identifying important patterns by reducing dimensionality and noise.

The MLP was able to learn complex associations since the chosen characteristics were successively fed into layers of neurons. The systematic arrangement of hidden layers, neuron counts, and activation functions demonstrated the architecture's versatility. As a result, the MLP was able to recognize intricate patterns in the dataset and get insightful knowledge from the chosen features. Similar to how the CNN was successful in using the chosen attributes. The CNN identified significant features from the input data in a hierarchical manner by using convolutional and pooling layers. This skill was crucial for identifying temporal trends in network traffic information, which improved the model's ability to distinguish between typical and invasive activity.

Chosen features helped the models generalize successfully to new, unexplored situations by serving as condensed representations of the original dataset. The increased predictive performance and resilience of the models were highlighted by this optimization procedure, which was directed by the Anova feature selection. As a result, the classification of network traffic data using MLP, CNN, and other machine learning models showed exceptional accuracy, allowing the detection of intrusions within regular activities.

V. Experimental Evaluation

In the course of our study's experimental evaluation phase, intrusion detection was thoroughly examined using a wide variety of machine learning models as well as the Multi-Layer Perceptron (MLP) and Convolutional Neural Network (CNN), among others. By locating relevant features in the input dataset, feature selection techniques, notably Anova, were essential in improving model performance.

A. Tuning of the hyper-parameters

To improve intrusion detection models, many variables are routinely adjusted throughout the hyperparameter tuning process. Various batch sizes, hidden layers, neurons, optimization techniques, and activation functions are all used throughout the experiment. The batch size of 64, the four hidden layers with 40 neurons each, the AdamW optimizer with a learning rate of 0.01, and the ”Leaky relu” activation function are found to be the best parameters for MLP. The models' ability to distinguish between benign and malicious network activity is improved by this approach.

B. Result

This section shows the results and analysis of machine learning models which were conducted as a part of our research evaluation.

TABLE I
Evaluation Results on ML Algorithms

ML Algorithms	Accuracy	Precision	Recall	F1-score
Decision Tree	0.71	0.73	0.75	0.70
Support Vector Machine	0.69	0.73	0.68	0.69
Naive Bayes	0.61	0.68	0.61	0.62
KNN	0.67	0.69	0.65	0.67

Table II shows the comparative result of the models that have used in this research work.

TABLE II
COMPARATIVE RESULTS OF THE MODELS

Methods	Accuracy
Decision Tree	71%
SVM	69%
Naïve Bayes	61%
KNN	67%
MLP	83%
CNN	85.7%

VI. EPILOGUE & FUTURE WORK

Security concerns have become a major problem as a result of the massive growth of digital information, system automation, and the Internet. IDS is quite effective in finding network intrusions. The major goal of this research project is to develop an intrusion detection system (IDS) model to identify intrusions using network port data when approaches like firewalls are unable to identify all of these assaults.

In conclusion, this study suggested a strategy for using the UNR-IDD dataset to work with MLP and CNN to build an enhanced IDS system. Our suggested techniques outperformed conventional machine learning (ML) models in terms of accuracy after rigorous testing and review.

The MLP and CNN outperformed the ML models and attained better accuracy because it was able to recognize intricate patterns and correlations in the dataset. This result demonstrates the potency of MLP and deep learning methods, particularly CNN, in overcoming the difficulties posed by the UNR-IDD dataset.

Despite the positive outcomes of this study, there are still several directions in which intrusion detection research might go. First, investigating more sophisticated neural network topologies, including recurrent networks and transformer models, might enhance detection precision. It may also be possible to improve the models' capacity to recognize new assaults by looking at the inclusion of ensemble methods and anomaly detection algorithms. Additionally, constant model retraining and adaptation are essential for real-time intrusion detection due to the dynamic nature of network threats. Last but not least, investigating the incorporation of explicable AI techniques would provide insights into the model's decision-making process, improving its transparency and making it easier for security specialists to understand. This study paves the way for future developments in intrusion detection with the goal of building stronger and more reliable cybersecurity solutions.

REFERENCES

[1] Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; emerging trends and recent developments," *Energy Reports*, vol. 7, pp. 8176–8186, 2021.

[2] W. H. Hassan *et al.*, "Current research on internet of things (iot) security: A survey," *Computer networks*, vol. 148, pp. 283–294, 2019.

[3] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, "A survey of machine and deep learning methods for internet of things (iot) security," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1646–1685, 2020.

[4] S. Meftah, T. Rachidi, and N. Assem, "Network based intrusion detection using the unsw-nb15 dataset," *International Journal of Computing and Digital Systems*, vol. 8, no. 5, pp. 478–487, 2019.

[5] H. Om and A. Kundu, "A hybrid system for reducing the false alarm rate of anomaly intrusion detection system," in *2012 1st international conference on recent advances in information technology (RAIT)*. IEEE, 2012, pp. 131–136.

[6] J. Ahmad, H. Farman, and Z. Jan, "Deep learning methods and applications," in *Deep learning: convergence to big data analytics*. Springer, 2019, pp. 31–42.

[7] J. Kim, N. Shin, S. Y. Jo, and S. H. Kim, "Method of intrusion detection using deep neural network," in *2017 IEEE international conference on big data and smart computing (BigComp)*. IEEE, 2017, pp. 313–316.

[8] K. Farhana, M. Rahman, M. Ahmed *et al.*, "An intrusion detection system for packet and flow based networks using deep neural network approach." *International Journal of Electrical & Computer Engineering (2088-8708)*, vol. 10, no. 5, 2020.

[9] S. Ho, S. Al Jufout, K. Dajani, and M. Mozumdar, "A novel intrusion detection model for detecting known and innovative cyberattacks using convolutional neural network," *IEEE Open Journal of the Computer Society*, vol. 2, pp. 14–25, 2021.

[10] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho, "Deep recurrent neural network for intrusion detection in sdn-based networks," in *2018 4th IEEE Conference on Network Softwarization and Workshops (NetSoft)*. IEEE, 2018, pp. 202–206.

[11] T. Das, O. A. Hamdan, R. M. Shukla, S. Sengupta, and E. Arslan, "Unr-idd: Intrusion detection dataset using network port statistics," in *2023 IEEE 20th Consumer Communications & Networking Conference (CCNC)*. IEEE, 2023, pp. 497–500.

[12] R. Abdulhammed, H. Musafer, A. Alessa, M. Faezipour, and A. Abuzneid, "Features dimensionality reduction approaches for machine learning based network intrusion detection," *Electronics*, vol. 8, no. 3, p. 322, 2019.

[13] S. Shakeela, N. S. Shankar, P. M. Reddy, T. K. Tulasi, and M. M. Koneru, "Optimal ensemble learning based on distinctive feature selection by univariate anova-f statistics for ids," *International Journal of Electronics and Telecommunications*, pp. 267–275, 2021.

[14] F. Amiri, M. R. Yousefi, C. Lucas, A. Shakery, and N. Yazdani, "Mutual information-based feature selection for intrusion detection systems," *Journal of Network and Computer Applications*, vol. 34, no. 4, pp. 1184–1199, 2011.