Machine Learning Based Intrusion Detection System In SDN Environment

Hamza Safwan
Department of computer science
University of Engineering and Technology
Taxila, Pakistan
Hamza.ciit135@gmail.com

Zeshan Iqbal
Department of computer science
University of Engineering and Technology
Taxila, Pakistan
Zeshan.iqbal@uettaxila.edu.pk

***Abstract*— Software Defined Networking (SDN) is a new technology in the networking field. SDN has planes, namely data, control, and infrastructure plane. All planes are decoupled from one another. The Control plane is the brain of the SDN which includes a controller and the logic related to routing or QOS, which is concentrated in the control plane. SDN provides several benefits such as programmability, scalability, and centralized management. This makes it suitable for today's networks. Despite all these advantages, there is one major disadvantage of SDN, which is single point of failure, which is controller. If the controller gets compromised, then the whole network will be compromised. To protect network from intrusion attacks, Intrusion Detection Systems(IDS) is used. IDS detects any kind of malicious activity in thenetwork. Machine learning techniques are widely used in makingIDS. In this paper, we use machine learning techniques to detect DDoS attacks in the SDN network. Besides, the Pearson correlationcoefficient feature selection technique is used for the optimal feature selection method. The main goal here is to select the machine learning algorithm with the highest accuracy and less false positive rate.Optimal feature selection is also one of the goals. The proposed algorithm is compared against other machine learning algorithms. (*Abstract*)**

Keywords—SDN, machine learning, IDS, DDoS.

I. INTRODUCTION

SDN has achieved a lot of importance in modern days due to centralized management and programmability. SDN seperates data plane from control plane. In SDN, planes communicate with each other by using a predefined application programming interface (API). In SDN, Northbound and Southbound API is present. In SDN, there is a single point of failure, which is the controller.SDN is prone to several security threats like DoS, DDoS, unauthorized access, and modification of data. DoS and DDoS is the most common and most dangerous attacks in the networking domain. Due to DoS and DDoS legitimate users are unable to access the legitimate resources in the network. These attacks create congestion in the network by sending lots of traffic to a server in a very short amount of time. A large number of packets which are being sent to the server create congestion in the network [1]. Man in the middle attack is also a serious and challenging attack. Due to this attack the attacker captures the packets in the network and falsify the network management information. Therefore, it is necessary to stop or prevent these type of attacks in the network.

Intrusion Detection System (IDS) is used to detect anomalies in the network. Mainly two types of IDS are in security domain host-based IDS and network-based IDS. Host-based IDS is present on the host machines, or computers, and Network-based IDS is present in the network architecture. Signature-based IDS depends upon the predefined rules. The rules are already defined, and all the attacks are known in advance. It is not suitable for new or zero-day attacks. In anomaly-based IDS, the anomaly in the traffic is observed if the traffic deviates from the normal pattern, then an alert is generated to warn the natwork administrator. Machine Learning is also used in this domain to detect the anomaly in the networks.. Machine learning algorithms that are used for anomaly detection are support vector machine (SVM), Naïve Bayes (NB), Logistic Regression, K-nearest neighbor (KNN), and Decision Tree. Unsupervised or reinforcement learning is also used when the data is unlabeled. Machine learning and deep learning techniques improve security to a very greater extent.

Machine learning and deep learning techniques are used widely in the cyber security domain. Several deep learning techniques like CNN, RNN, and LSTM are used. Autoencoders are also usedfor intrusion detection purposes, as described in [2] and [3]. Autoencoder is an unsupervised learning technique that extracts high-level features and then do prediction on data. While using deep learning models, it is necessary to deal withthe issue of overfitting by adding the regularization function.Machine learning and deep learning techniques provide a promising solution in the IDS domain. Progression inaccuracy, reduced false alarm rates, reduced training time, and a suitable flow-based dataset are still the main issues and can be improved. In this research, our contribution is as follows:

- A machine learning model based on PCC-RF is proposed.
- Relevant features are selected based on the feature selection technique.
- Evaluate the proposed model based on accuracy andtraining time.

- Comparison of different machine learning algorithms on the basis of accuracy.

In this research, four machine learning algorithms are trained and tested—random forest. KNN, Naïve Bayes and Logistic Regression. The feature selection technique is used for optimal feature selection. High accuracy is achieved by using the Random Forest model.

II. RELATED WORK

In [4], the intrusion is detected in computer networks. In work, a novel hybrid methodology is proposed. Efficient selection of features is selected through a technique called CAPER. Two state-of-the-art machine learning datasets are used NSL-KDD and UNSW. Optimal results are obtained in this research. In [5], a novel technique is introduced to detect intrusion in the network. This novel technique consists of five modules which are preprocessing modules then auto encoder module. After the autoencoder module, there is a database module and at last, a classification module. CICIDS2017 dataset is used in this research. Optimal accuracy is achieved in this study. Intrusion is detected in the SDN environment in [6]. Deep Learning techniques are used. In this work, a hybrid Deep Learning model is proposed based on CNN and LSTM to extract some extra features from the data. CICIDS2017 dataset is used, and 98.67% accuracy is achieved. In [7], advanced SVM is used to detect intrusion in SDN environment. In this research, training and testing time is reduced by using two feature types which are asymmetric and volumetric features. 97% accuracy is achieved in this research.

In [8] conceptual model for SDN with respect to security is proposed. This model is an abstraction of the application, data, and control layer. Three machine learning algorithms are used SVM, J48, and Naïve Bayes. Feature selection techniques are also used. Higher accuracy is achieved in this research. In [9] CICIDS 2017 dataset is used. Twelve features are used along with machine learning algorithms. 99% accuracyis achieved in this research. In [10], NSL-KDD and CICIDS 2017 datasets are used. Several machine learning algorithmsare used for training purposes. A decision tree, along withenhanced data quality, is used. In this research, overall 99% accuracy is achieved on the NSL-KDD dataset and 98% accuracyachieved on CICIDS 2017 dataset. In [11] DDoS attack is detected by using machine learning. In this research semisupervised clustering method is introduced. K-means algorithm is used in this research. DDOS 1.0 dataset is used. In [12], a new technique called DDoSNet is proposed, which detects an anomaly in the SDN environment. This framework is based on Deep Learning techniques along with RNN and autoencoder. CICIDS 2019 dataset is used in work. Higher and optimal accuracy is achieved in this research. In a similar manner, a broad learningsystem (BLS) [13] is used for fault detection in a network.

III. METHODOLOGY

An intrusion Detection System is a software application that monitors the network traffic and decides whether the traffic is malicious or normal based on captured packet features. Machine learning techniques are utilized for training and testing themodel. The proposed model prediction is illustrated in Figure2.

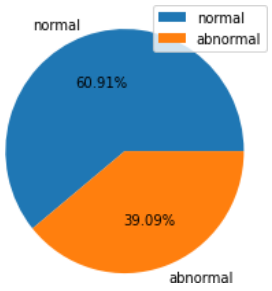

Figure.1. Dataset Distribution

A. Data Collection

For intrusion detection purpose SDN dataset is used, which includes 1,04,345 records. The dataset contains 23 features extracted from real-time traffic in an SDN environment. Three types of attacks are present in the dataset, which are TCP syn, UDP Flood, and ICMP attacks. Extracted features includepacket count, byte count, durations received on the switch port. Benign traffic is labeled as 0 and malicious as 1.

This dataset is created in an SDN environment and is specifically used for DDoS attack detection in an SDN environment. This dataset is used in machinelearning and Deep Learning research, used in [14].

There is nearly 61 percent of normal records in the dataset, whereas 31 percent are attacked traffic presentin the dataset. The attack is a DDoS attack in the dataset.

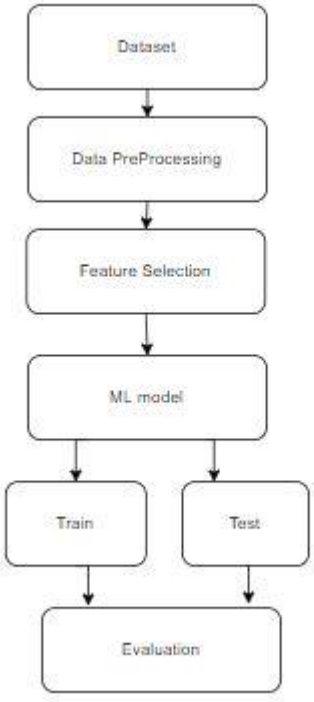

Figure 2:Proposed model architecture

B. Data Preprocessing:

Data preprocessing is a very important step in machine learning processes. In data preprocessing, all the missing values are removed or transformed

all the standardization of data and encoding is done. We preprocess raw data to a standard format.

1). Identify categorical features:

All the categorical features in the dataset need to be identified and converted to numerical format. Machine learning only works well with numerical data, so we need to convert categorical columns to numerical format. It is necessary to convert categorical features to numerical in machine learning domain.

2). One hot encoding:

One hot encoding is used to convert categorical features to numerical. All the features in the dataset are converted into binary vectors.Firstly, categorical value is mapped to an integer value, and then this integer value is represented in a binary vector. One hot encoding is necessary because machine learning don't work on categorical data. Machine learning model only works on binary or numerical data so all the categorical features needs to be converted to numerical before training phase.

3). Splitting dataset:

After one hot encoding, data is in a standard format. We need to do a split for training andtesting purposes. For this purpose, 70:30 splitting of data is performed. Seventy percent of data is used for training, and 30 percent is used for testing purpose.

4). Feature Selection:

Feature Selection is one of the most important techniques in machine learning. Not all the features in the dataset are utilized for training purposes. If all the features are included in the dataset, then this might affect the accuracy or performance of the proposed model. Only relevant features are selected for training and testing purposes. Several feature selection techniques are present like Chi-Square, RFE etc. we used Pearson Correlation Coefficient technique for training purpose.

A). Pearson Correlation Coefficient:

This feature selection technique based on the correlation among the features present in the dataset. It measures the statistical relationship between the features in the dataset it mainly based on the method of covariance. The value of the coefficient ranges between -1 and +1. Thefeatures which have high correlation are selected, and low correlated features are removed.

This technique selects only those features which are highly correlated with each other. Sometimes in our dataset we have features which have same correlation or positively correlated features then we remove those features which have same correlation value because they are same and produce the same result when getting trained in our model.

B). Selected Features:

Only four features are selected after feature selection techniques.These features provide the highest accuracy while using machine learning algorithms. Also, the training and testing time is reduced. Compute resources are also used very little while using reduced features. The selected features are as follows. Dt, flows, byte count, and packet count. These are the features that are selected based on the feature selection technique.

IV. CLASSIFICATION

In machine learning, classification is used to classify data or objects based on features and similarities. In our experimentation, we used four machine learning algorithms. Random Forest, KNN, SVM and Naïve Bayes.

A. Random Forest

Random Forest is one of the most important algorithms used in machine learning. It is used for both Regression and classification. It is made up of several decision trees. It forms several decision trees, and from these Decision trees, classification is done. Among all the decision trees the class which has the highest votes is considered as the final prediction.Its prediction is based on majority votes. It searches for thebest features whenever it splits each node. It always searches for the best features.

B. Logistic Regression (LR)

Logistic Regression is one of the most important algorithms in machine learning. It is a linear classifier that is used for classification. This algorithm is fast and convenient for classification problems. It works on the basis of the sigmoid function.

C. K-Nearest Neighbour(KNN)

K-Nearest Neighbor is a machine learning algorithm. It worksbased on distance. It calculates the distance from each of thedata points in the dataset, and the final decision is made based onthe distance. The value of k is of utmost importance in KNN.The value of k determines the final decision. KNN is a lazy learner algorithm because it saves instances during the training period.

D. Naïve Bayes:

Naïve Bayes algorithm works based on probability. It is mostly used in probability problems where the final prediction isbased on probability.

V. Performance Evaluation:

Prediction is performed on the dataset by using machine learningalgorithms. There are two types of label classes in our datasetone is normal traffic which is represented by 0, and attack traffic which is represented by 1. The attack traffic is DDoS.It is a binary classification problem that is evaluated by using a confusion matrix. In the confusion matrix, we have True Positive, True Negative, False Positive, and False Negative values present.

Table.1. Confusion matrix

True Positive(TP)	False Negative(FN)
False Positive(FP)	True Negative(TN)

In table 1, true positive are those records that are predicted correctly by the machine learning model. true negative are those records when the model accurately predicts the negative

Class. In the false-negative model the incorrect predicts the negative class and in the false-positive model incorrectly predictsthe positive class.

IV Experimental Result

Several experiments are performed on the dataset by using machine learning techniques. Only two types of classes are determined one is attacked, and the other is normal traffic. Random forest gives us optimal accuracy because it is an ensemble classifier. It is composed of various decision trees. For binaryclassification, the RoC curve and confusion matrix is used for evaluation purpose.

A. Confusion Matrix.

Our proposed model is trained on the dataset using selected features. The confusion matrix obtained from experiments is depicted below.

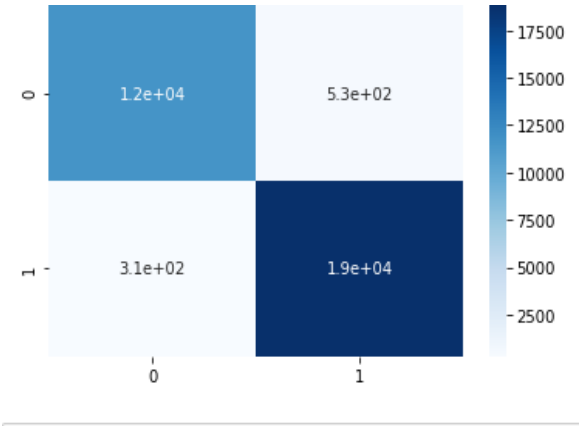

Figure.3.KNN Confusion matrix

The accuracy which is achieved through KNN is 97%. From the confusion matrix, it is evident that the performance of the KNN model is better by using relevant features selected based on the feature selection technique.

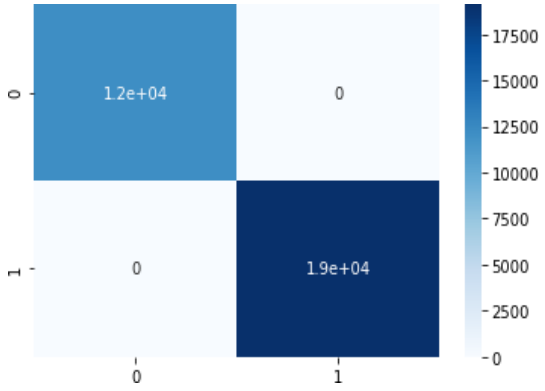

Figure.4.Random Forest confusion matrix

The accuracy achieved by the random forest model is nearly 100%. It is evident from the confusion matrix that the number of false positives and false negatives are zero. The random forest model works well in determining the intrusion in the system. All the attacks are classified accurately by using a random forest model.

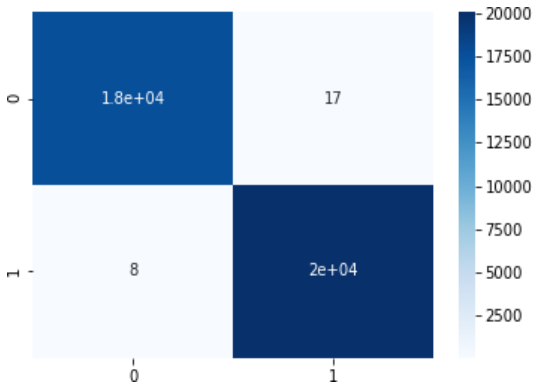

Figure.5. Naïve Bayes confusion matrix

Naïve Bayes achieves an accuracy of 42%. This model performs well when dealing with probability conditions.
The Roc curve measures the area between the true positive and false positive rate. It provides us area under the curve. It is also a very strong performance measure used in binary classification problems.

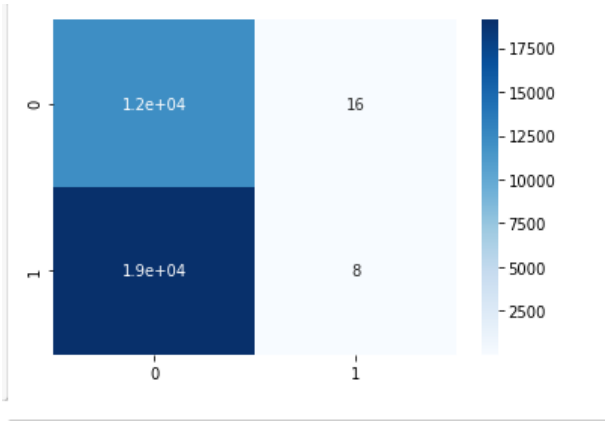

Figure.6.Logistic Regression confusion matrix

Logistic Regression performs very badly in terms of accuracy.It achieves an accuracy of 38% with very high false-positiverates.

B. Roc curves.

The results obtained from Roc curves aredepicted below.

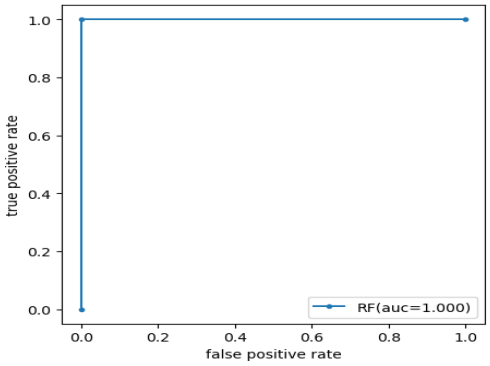

Figure.7. Random Forest Roc curve

The Roc curve of the random forest model is depicted in the figure above. It is evident from the figure that the area under the curve of the model is 1. The optimal area under the curve for the good model is 1.

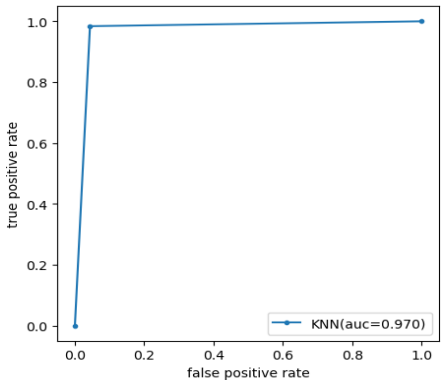

Figure.8. KNN Roc curve

The Roc curve of the KNN model is depicted in the figure above. Itis evident from the figure that the area under the curve of the model is 0.97, which is optimal.

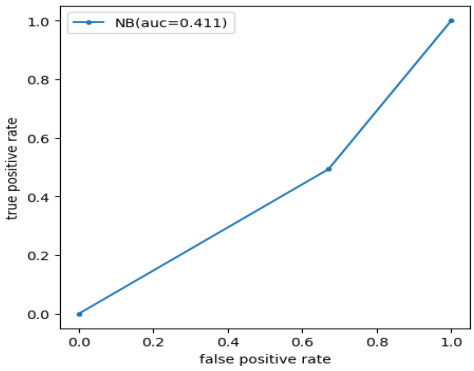

Figure.9. Naïve Bayes Roc curve

The Roc curve of the NB model is depicted in the figure above. It isevident from the figure that the area under the curve of the modelis 0.411, which is very low for the classification rate.

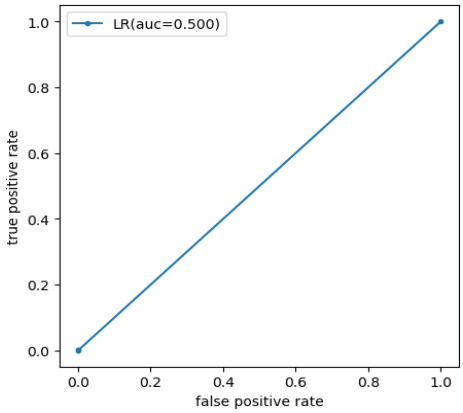

Figure.10.Logistic Regression Roc curve

C. Accuracy Graph and table.

The accuracy obtained from different models is depicted below. Random forest achieves the highest accuracy while logistic Regression obtained very less accuracy.

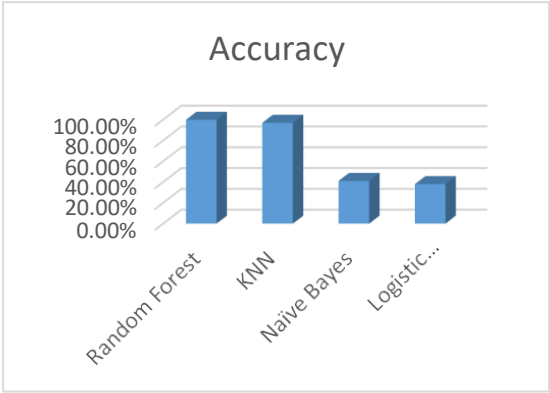

Figure.11.Accuracy graph

From the above figure it is depicted that the random forest performs well in detecting the intrusion in the network. The random forest comprises several decision trees, thus makingit effective for prediction tasks. Logistic Regression does not perform well.

Table.2.Accuracy table

Algorithm	Accuracy	Train time	Test time
Random Forest	99.9%	2.38ms	2.51ms
KNN	97%	263ms	920ms
Logistic Regression	38%	12ms	6.9ms
Naïve Bayes	41.1%	10ms	7.98ms

From table 2 it is evident that the accuracy of the random forest model is greater than other algorithms. The training and testing time of the randomforest algorithm is also less as compared to other algorithms, which makes it best for determining intrusion in the SDN environment. Testing time is critical in real-time systems because delay is not tolerated in such kinds of systems. So random forest is a good candidate for intrusion detection.

V. CONCLUSION

In this research, attack and normal traffic is classified in SDN environment using machine learning.SDN specific dataset is used in this research which is composed of TCP, UDP and ICMP traffic.Dataset contains statistical features like byte count, flow count, and packet rate. Pearson correlation coefficient technique is used to select most important features from the dataset. After feature selection four features are selected from 22features. different machine learning algorithms are used for classification.

Random Forest, KNN, Naïve Bayes, and Logistic Regression. Results show that the accuracy of random forest is maximum with zero false-positive rate and nearly 100% accuracy.

References

[1] N. Z. Bawany, J. A. Shamsi, and K. Salah, "Attack Detection and Mitigation Using SDN: Methods, Practices, and Solutions," *Arab. J. Sci. Eng.*, vol. 42, no. 2, pp. 425–441,2017, doi: 10.1007/s13369-017-2414-5.

[2] Q. Niyaz, W. Sun, A. Y. Javaid, and M. Alam, "A deep learning approach for network intrusion detection system," *EAI Int. Conf. Bio-inspired Inf. Commun.Technol.*, 2015, doi: 10.4108/eai.3-12-2015.2262516.

[3] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, "A Deep Learning Approach to Network Intrusion Detection,"*IEEE Trans. Emerg. Top. Comput. Intell.*, vol. 2, no. 1, pp. 41–50, 2018, doi: 10.1109/TETCI.2017.2772792.

[4] T. Rincy N and R. Gupta, "Design and Development of an Efficient Network Intrusion Detection System Using Machine Learning Techniques," *Wirel. Commun. Mob. Comput.*, vol. 2021, no. 1, 2021, doi: 10.1155/2021/9974270.

[5] C. Zhang *et al.*, "A Novel Framework Design of Network Intrusion Detection Based on Machine Learning Techniques," *Secur. Commun. Networks*, vol. 2021, 2021, doi: 10.1155/2021/6610675.

[6] P. Sun *et al.*, "DL-IDS: Extracting features using CNN-LSTM hybrid network for intrusion detection system," *Secur. Commun. Networks*, vol. 2020, 2020, doi: 10.1155/2020/8890306.

[7] M. Myint Oo, S. Kamolphiwong, T. Kamolphiwong, and S. Vasupongayya, "Advanced Support Vector Machine-(ASVM-) based detection for Distributed Denial of Service (DDoS) attack on Software Defined Networking (SDN)," *J. Comput. Networks Commun.*, vol. 2019, 2019, doi: 10.1155/2019/8012568.

.

[8] A. A. Ahmad, P. S. Boukari, A. M. Bello, and M. A. Muhammad, "Solution Model forIntrusion Detection in Software Defined Networking (SDN) Using Machine Learning," vol. 7, no. 8, pp. 40–47, 2021.

[9] E. M. Zeleke, H. M. Melaku, and F. G. Mengistu, "Efficient Intrusion Detection System for SDN Orchestrated Internet of Things," *J. Comput. Networks Commun.*, vol. 2021, pp. 1–14, 2021, doi: 10.1155/2021/5593214.

[10] A. Guezzaz, S. Benkirane, M. Azrour, and S. Khurram,"A Reliable Network Intrusion Detection Approach Using Decision Tree with Enhanced Data Quality," *Secur. Commun. Networks*, vol. 2021, 2021, doi: 10.1155/2021/1230593.

[11] Y. Gu, Y. Wang, Z. Yang, F. Xiong, and Y. Gao, "Multiple-Features-Based Semisupervised Clustering DDoS Detection Method," *Math. Probl. Eng.*, vol. 2017, 2017, doi: 10.1155/2017/5202836.

[12] M. S. Elsayed, N. A. Le-Khac, S. Dev, and A. D. Jurcut, "DDoSNet: A Deep-Learning Model for Detecting Network Attacks," *Proc. - 21st IEEE Int. Symp. a World Wireless, Mob. Multimed. Networks, WoWMoM 2020*, pp. 391–396, 2020, doi: 10.1109/WoWMoM49955.2020.00072.

[13] Adegoke, Muideen, Hiu Tung Wong, and Chi Sing Leung. "A Fault Aware Broad Learning System for Concurrent Network Failure Situations." *IEEE Access*, vol. 9, no.5, 2021, doi46129-46142.

[14] Ahuja, N.; Singal, G.; Mukhopadhyay, D. "DDOS S attack SDN Dataset", Mendeley Data, V1; BennettUniversity: Greater Noida, India, 2020.