Effective Prediction of DDOS Attack Using Deep Learning Classifiers

Anisha L[1], J. Caroline Misbha[2]
[1]*Department of Computer science and engineering, Arunachala College of Engineering for Women, Kanyakumari, Tamilnadu, India*
[2]*Assistant Professor, Department of Computer science and engineering, Arunachala College of Engineering for Women, Kanyakumari, India*

Abstract-Distributed Denial of Service (DDoS) assaults are a frequent moniker for distributed network attacks. These attacks take use of certain restrictions that apply to each asset of the arrangement, such as the design of the website for the allowed organisation. In this research, a deep learning method for anticipating DDoS attacks is proposed. The techniques of deep learning were created for this project's classification of DDOS assaults. The deep learning methodology includes the classification algorithms Multilayer Perceptron (MLP) and Long Short-Term Memory Networks (LSTM). The datasets are pre-processed using Standard Scaler. To enable the identification and categorization of DDOS assaults, deep learning methods are deployed. An artificial neural network feed-forward model called MLP converts input sets into output sets. In order to diagnose defects in that area, the LSTM classifier is built to categorize errors according to their nature. This suggested project generated a confusion matrix in order to evaluate the model's performance. Python software is used to implement this simulation.

***Keywords*-DDOS, LSTM, MLP, DL, Confusion matrix.**

I. INTRODUCTION

Distributed Denial of Service (DDoS) assaults are the most common name for distributed network attacks. These attacks take use of certain restrictions that are applicable to every arrangement asset, such the design of the website for the authorized organization. In order to overwhelm the target website's capacity to handle many requests at once and prevent it from functioning properly and efficiently for even authorized users of the network, a DDoS attack sends varied requests to the target web assets. Web applications and commercial websites are frequently the targets of various DDoS assaults, and the attacker may have numerous objectives [1, 2].

The Internet of Things (IoT) refers to a network of linked, web-connected things that may exchange information automatically across faraway organizations [3]. The Things might be anything with sensors that can gather and transfer information inside the organization, including related clinical equipment, bio-chip transponders, solar panels, and associated automobiles with sensors that can alert the driver of a variety of possible issues. A little gadget called artificial intelligence converts information into data. Information has affected consumers' security and privacy during the past 50 years, roughly. The amount of information is little, with the exception of the potential for exploring it and discovering the instances concealed therein. This effort will attempt to identify key hidden instances in some way. Artificial intelligence technology is often used to find important secret examples in complicated material. Unknown instances and information about a situation may be utilized to make predictions about the future and engage in a variety of complicated dynamics. For the categorization and prevention of DDoS attacks, many strategies were put forth [4, 5]. Deep learning algorithms for intrusion detection are put out in [6]. The models used were Convention neural network CNN and RNN, and the performance of the model as a whole was excellent. The proposal was proven to work well with CNN. For intrusion detection, authors of study [7] suggested a hybrid deep learning model. For the categorization of CNN and LSTM from the RNN model, they integrated two deep learning techniques. To our understanding, DDoS assaults involve a variety of deep learning models [8–10].

In this research, a deep learning method for anticipating DDoS attacks is proposed. The rest of this essay is structured as follows. We introduced the suggested system in Section II. We offer the findings and debates of the suggested technique in Section III. In Section IV, we finally bring the essay to a close.

II. PROPOSED SYSTEM

The detection method uses a discriminative deep neural network technique to predict the DDOS attack as shown in figure 1. Preprocessing, data analysis, classification, and projected performance matrix are the four phases that make up the general solution block diagram shown in Figure 1.

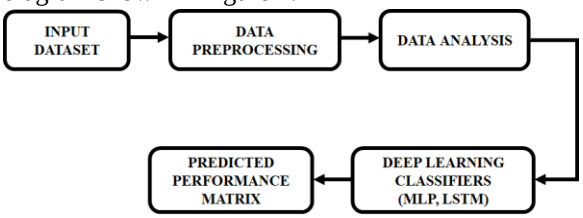

Figure 1. Block diagram for proposed system

The suggested study employs a deep learning approach to forecast various DDoS attack types. This project makes use of the SDN Dataset. A study of the incoming dataset takes place during the first step of data pre-processing. Standard Scaler is used to pre-process the datasets. Data pre-processing procedures are used to deal with the unnecessary data in the dataset. Researching the observed data is part of the data analysis stage after data pre-processing. The following deep learning classifier method is acceptable for the data. MLP and LSTM are used in the deep learning classifier approach. The MLP network is trained via training, and after training, it produces rapid predictions. The DDOS assaults are categorized using the Long Short-term Memory Networks Algorithm (LSTM) classifier in order to find issues in that area. The data are then assessed to produce a forecast result.

A. INPUT DATASET

To guarantee the precision of intrusion detection systems, the dataset that was utilised must be evaluated. Strong network resilience is required due to the exponential growth of today's networks and applications. By choosing the appropriate learning and testing datasets, this is achieved.

B. DATA PREPROCESSING

Data preprocessing is a phase in the data mining and data analysis process that converts raw data into a format that computers and machine learning algorithms can understand and analyse. Text, photos, video, and other types of unprocessed, real-world data are disorganised. In addition to the possibility of faults and inconsistencies, it is frequently lacking and lacks a regular, consistent design.

C. DATA ANALYSIS

Although many individuals, companies, and professionals approach data analysis in various ways, most of them may be summed up in a single, all-encompassing definition. Data analysis is the act of converting, evaluating, and cleaning up raw data to provide useful, pertinent information that helps organisations make informed decisions. By providing pertinent information and data, which are typically presented as charts, graphics, tables, and graphs, the strategy lowers the risks connected with decision-making.

D. LONG SHORT TERM MEMORY (LSTM)

Although formally learned using supervised learning techniques—known as self-supervised—LSTM is an unsupervised learning approach. Many recurrent neural networks (RNNs) are able to learn long-term dependencies, particularly in tasks involving sequence prediction. Time series forecasting models may anticipate future values based on prior, sequential data by utilising LSTM. As a consequence, demand forecasters can make predictions more accurately, which helps the firm make better decisions.

E. MLP

An ANN model with a feed-forward architecture that iteratively maps sets of input data onto sets of desired outputs. Each layer in an MLP is completely linked to the layer above it. There are three levels in an MLP: an input layer, one or more hidden layers, and an output layer.This feed-forward artificial neural network model converts input sets into appropriate sets for output. Multiple layers that are coupled to one another make form a multilayer perceptron (MLP). All nodes, except the input nodes, are processing components or neurons with a nonlinear activation function. To train the network, back propagation, a method of supervised learning, is used.

III. RESULT AND DISCUSSION

Python software is used in the execution of this project. You may construct environments for several Python and package versions with the anaconda programme.

	dt	switch	src	dst	pktcount	bytecount	dur	dur_nsec	tot_dur	flows
0	11425	1	10.0.0.1	10.0.0.8	45304	48294064	100	716000000	1.010000e+11	3
1	11605	1	10.0.0.1	10.0.0.8	126395	134737070	280	734000000	2.810000e+11	2
2	11425	1	10.0.0.2	10.0.0.8	90333	96294978	200	744000000	2.010000e+11	3
3	11425	1	10.0.0.2	10.0.0.8	90333	96294978	200	744000000	2.010000e+11	3
4	11425	1	10.0.0.2	10.0.0.8	90333	96294978	200	744000000	2.010000e+11	3
5	11425	1	10.0.0.2	10.0.0.8	90333	96294978	200	744000000	2.010000e+11	3
6	11425	1	10.0.0.1	10.0.0.8	45304	48294064	100	716000000	1.010000e+11	3
7	11425	1	10.0.0.1	10.0.0.8	45304	48294064	100	716000000	1.010000e+11	3
8	11425	1	10.0.0.1	10.0.0.8	45304	48294064	100	716000000	1.010000e+11	3
9	11425	1	10.0.0.2	10.0.0.8	90333	96294978	200	744000000	2.010000e+11	3

pktrate	Pairflow	Protocol	port_no	tx_bytes	rx_bytes	tx_kbps	rx_kbps	tot_kbps	label
451	0	UDP	3	143928631	3917	0	0.0	0.0	0
451	0	UDP	4	3842	3520	0	0.0	0.0	0
451	0	UDP	1	3795	1242	0	0.0	0.0	0
451	0	UDP	2	3688	1492	0	0.0	0.0	0
451	0	UDP	3	3413	3665	0	0.0	0.0	0
451	0	UDP	1	3795	1402	0	0.0	0.0	0
451	0	UDP	4	3665	3413	0	0.0	0.0	0
451	0	UDP	1	3775	1492	0	0.0	0.0	0
451	0	UDP	2	3845	1402	0	0.0	0.0	0
451	0	UDP	4	354583059	4295	16578	0.0	16578.0	0

Figure 2. Input Dataset

The SDN dataset contains a variety of DoS attack methods that may be initiated at various OSI model layers. A number of DDoS attack scenarios, including TCP-SYN flood, UDP flood, and ICMP flood assaults, are also included in the SDN dataset. The input dataset is shown in figure 2.

```
dt                0
switch            0
src               0
dst               0
pktcount          0
bytecount         0
dur               0
dur_nsec          0
tot_dur           0
flows             0
packetins         0
pktperflow        0
byteperflow       0
pktrate           0
Pairflow          0
Protocol          0
port_no           0
tx_bytes          0
rx_bytes          0
tx_kbps           0
rx_kbps         506
tot_kbps        506
label             0
dtype: int64
```

Figure 3. Null Dataset

The null values are displayed in Figure 3. Any sort of processing done on raw data to get it ready for another data processing operation is referred to as data pre-processing, which is a part of data preparation. Pre-processing is necessary to raise the data's quality. The machine is trained appropriately during pre-processing using the obtained SDN datasets as input. Figure 4 displays the distribution of labels by class.

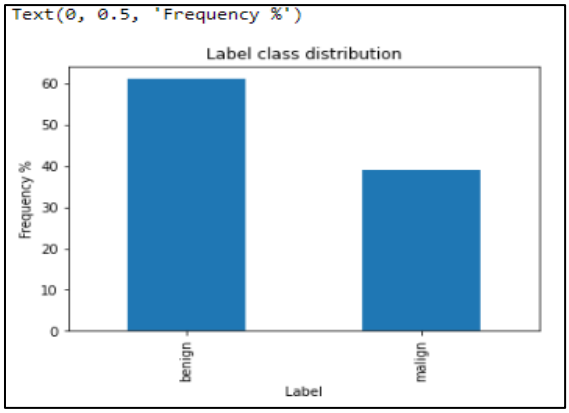

Figure 4. Label Class Distribution

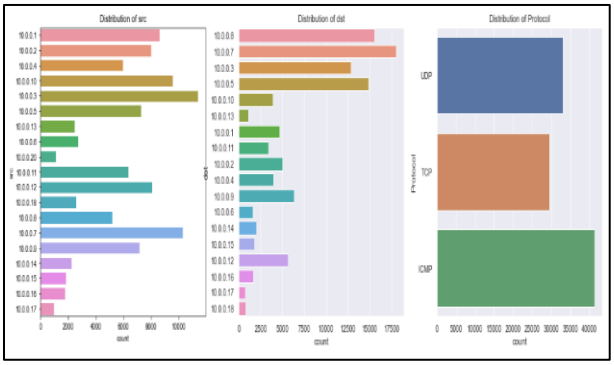

Figure 5. Distributions of SRC, DST and Protocol

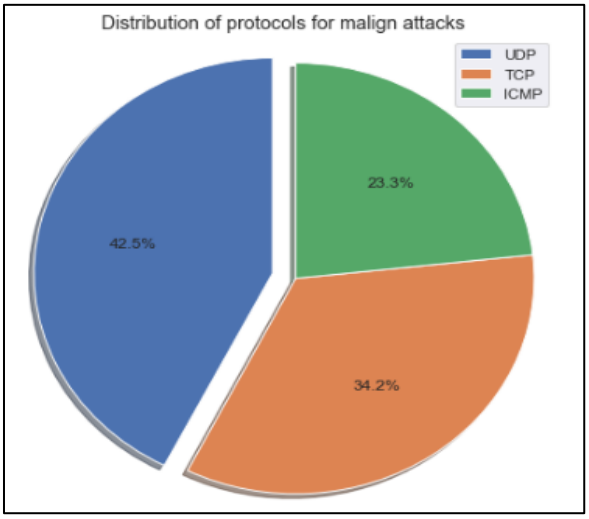

Figure 6. Distribution of protocol for Malign attacks

Figure 5 shows the distributions of SRC, DST, and Protocol. The spatial distribution of the protocol for malicious assaults is shown in Figure 6.

```
Accuracy: 98.49%
Recall: 99.19%
Precision: 96.98%
F1-Score: 98.07%
time to train: 34.74 s
time to predict: 3.80 s
total: 38.54 s
```

Figure 7. Performance of MLP

A directed graph, in which the signal route via the nodes is only one direction, is what a multilayer perceptron is: a neural network linking many layers. Every node has a nonlinear activation function, with the exception of the input nodes. The performance of MLP is shown by this number. The performance of MLP is displayed in Figure 7.

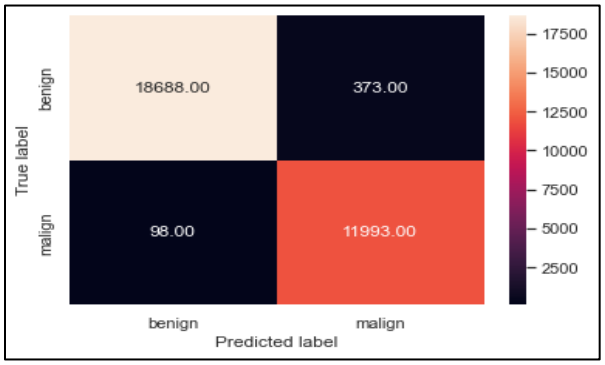

Figure 8. Confusion matrix for MLP

For MLP, this confusion matrix is shown in Figure 8. This graph displays the value for benign and malignant growths. It is frequently used to assess how well categorization models work. These models try to predict a category label for each input event.

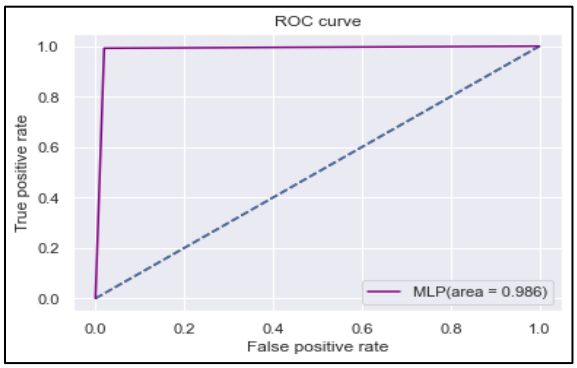

Figure 9. ROC Curve for MLP

The MLP ROC curve is seen in this figure. False positive rate on the y axis and true positive rate on the x axis. With the use of MLP, accuracy, recall precision, and F1-score are discovered.

```
Accuracy: 98.80%
Recall: 98.81%
Precision: 98.11%
F1-Score: 98.46%
time to train: 109.38 s
time to predict: 6.87 s
total: 116.25 s
```

Figure 10. Performance of LSTM

Because the programme uses a framework built on short-term memory processes to build longer-term memory, the unit is known as a long short-term memory block. Examples of applications for these systems include natural language processing. This graph shows how well the LSTM performed.

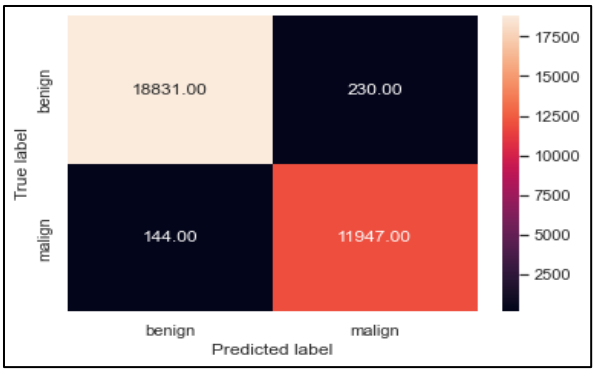

Figure 11. Confusion Matrix for LSTM

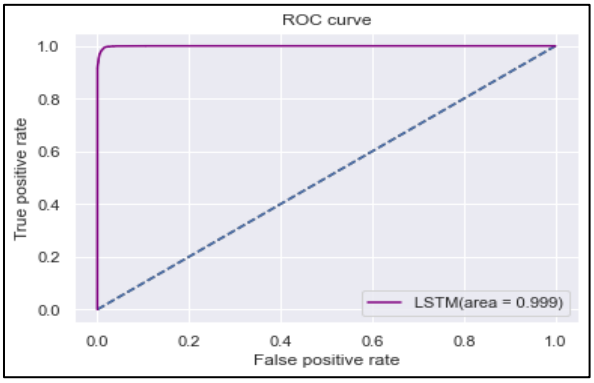

Figure 12. Roc Curve for LSTM

For LSTM, such confusion matrix is shown in Figure 11. A particular kind of neural network utilised in deep learning is the LSTM. The ROC curve for LSTM is shown in Figure 12. False positive rate on the y axis and true positive rate on the x axis. With the use of LSTM, accuracy, recall precision, and F1-score are discovered.

	Accuracy	Recall	Precision	F1-Score	time to train	time to predict	total time
MLP	98.49%	99.19%	96.98%	98.07%	34.7	3.8	38.5
LSTM	98.80%	98.81%	98.11%	98.46%	109.4	6.9	116.3

Figure 13. Comparison of Classification

Figure 13 illustrates how the MLP and LSTM accurately predicted accuracy, recall, precision, F1-score, time to train, time to predict, and total time.

IV. CONCLUSION

Distributed denial of service (DDoS) assaults are one of the serious and increasingly complicated security threats to computer networks. This project offers a thorough simulation of a deep learning method to anticipate various DDoS attacks. The classification methods Multilayer Perceptron (MLP) and Long Short-Term Memory Networks (LSTM) are included in the deep learning methodology. Standard Scaler is used to pre-process the datasets. The detection and classification of distributed denial-of-service (DDOS) attacks is aided by deep learning algorithms. MLP is a feed-forward artificial neural network model that associates input sets with output sets. For fault diagnosis in that area, the LSTM classifier is designed to categorize problems depending on their nature. A confusion matrix was produced as part of the recommended project to evaluate the model's effectiveness.

REFERENCE

[1] J. Bhayo, S. Hameed and S. A. Shah, "An Efficient Counter-Based DDoS Attack Detection Framework Leveraging Software Defined IoT (SD-IoT)," in IEEE Access, vol. 8, pp. 221612-221631, 2020.

[2] Y. Jia, F. Zhong, A. Alrawais, B. Gong and X. Cheng, "Flow Guard: An Intelligent Edge Defense Mechanism Against IoT DDoS Attacks," in IEEE Internet of Things Journal, vol. 7, no. 10, pp. 9552-9562, Oct. 2020.

[3] D. Yin, L. Zhang and K. Yang, "A DDoS Attack Detection and Mitigation with Software-Defined Internet of Things Framework," in IEEE Access, vol. 6, pp. 24694-24705, 2018.

[4] J. Li, M. Liu, Z. Xue, X. Fan and X. He, "RTVD: A Real-Time Volumetric Detection Scheme for DDoS in the Internet of Things," in IEEE Access, vol. 8, pp. 36191-36201, 2020.

[5] R. Abubakar et al., "An Effective Mechanism to Mitigate Real-Time DDoS Attack," in IEEE Access, vol. 8, pp. 126215-126227, 2020.

[6] R. Doriguzzi-Corin, S. Millar, S. Scott-Hayward, J. Martínez-del-Rincón and D. Siracusa, "Lucid: A Practical, Lightweight Deep Learning Solution for DDoS Attack Detection," in IEEE Transactions on Network and Service Management, vol. 17, no. 2, pp. 876-889, June 2020.

[7] S. Haider et al., "A Deep CNN Ensemble Framework for Efficient DDoS Attack Detection in Software Defined Networks," in IEEE Access, vol. 8, pp. 53972-53983, 2020.

[8] B. I. Hairab, M. Said Elsayed, A. D. Jurcut and M. A. Azer, "Anomaly Detection Based on CNN and Regularization Techniques Against Zero-Day Attacks in IoT Networks," in IEEE Access, vol. 10, pp. 98427-98440, 2022.

[9] W. Sun, Y. Li and S. Guan, "An Improved Method of DDoS Attack Detection for Controller of SDN," 2019 IEEE 2nd International Conference on Computer and Communication Engineering Technology (CCET), pp. 249-253, 2019.

[10] M. P. Novaes, L. F. Carvalho, J. Lloret and M. L. Proença, "Long Short-Term Memory and Fuzzy Logic for Anomaly Detection and Mitigation in Software-Defined Network Environment," in IEEE Access, vol. 8, pp. 83765-83781, 2020.