SvedbergOpen
DISSEMINATION OF KNOWLEDGE

International Journal of Data Science and Big Data Analytics

Publisher's Home Page: https://www.svedbergopen.com/

Research Paper Open Access

Binary and Multi-Class Prediction of DDoS Attack Using Deep Learning Models

Tapu Biswas[1], Farhan Sadik Ferdous[2] and Akinul Islam Jony[3*]

[1]Department of Computer Science, American International University-Bangladesh (AIUB), Dhaka 1229, Bangladesh. E-mail: tapubiswas731@gmail.com
[2]Department of Computer Science, American International University-Bangladesh (AIUB), Dhaka 1229, Bangladesh. E-mail: farhansferdous@gmail.com
[3]Department of Computer Science, American International University-Bangladesh (AIUB), Dhaka 1229, Bangladesh. E-mail: akinul@gmail.com

Article Info

Volume 4, Issue 2, November 2024
Received : 23 June 2024
Accepted : 11 October 2024
Published : 05 November 2024
doi: 10.51483/IJDSBDA.4.2.2024.49-58

Abstract

Dealing with network security has always been challenging work, especially due to the prevalence of Distributed Denial of Service attacks. A DDoS attack occurs when a hacker takes control of several computers, turning them into bots, and then sends a large number of requests simultaneously to specific servers on the internet. This causes the targeted server to become too busy to provide normal services to legitimate users, those who need to use that particular server. Various Deep-learning algorithms have been used to identify DDoS attacks in this research. To study and analyse DDoS attacks, researchers have used the CIC-DDoS 2019 dataset. In this paper, the primary goal is to make a comparison of the performance of various DL algorithms for both binary and multi-class prediction of detect DDoS attacks accurately, such as Convolutional Neural Network, Deep Neural Network, Long Short-Term Memory Network, Recurrent Neural Network, Feedforward Neural Network, Radial Basis Function Network, and Multilayer Perceptron. Along with that, the experimenter demonstrated that DDoS attacks can be better identified if they are stored in the dataset in a binary way.

Keywords: *DDoS attack, Deep learning, DL algorithms, CIC-DDoS 2019 dataset, Cyber security*

1. Introduction

A Distributed Denial of Service (DDoS) attack is a cyber-attack that targets a particular website to make it inactive. With the rising demand for software, the number of DDoS attacks is also increasing. DDoS attacks degrade the performance of software so that it cannot respond to the consumers on time. These attacks are widespread due to their ease of design and execution, but they are difficult to detect and control (Jony and

* *Corresponding author: Akinul Islam Jony, Department of Computer Science, American International University-Bangladesh (AIUB), Dhaka 1229, Bangladesh. E-mail: akinul@gmail.com*

Hamim, 2023). In recent days, deep learning (DL) has become a reliable method in networking systems to detect DDoS attacks. DL is an integral branch of Machine Learning (ML) owing to its remarkable ability to abstract and generalize information across a wide range of domains (Novaes *et al.*, 2021). In a DDoS attack, a single bot master or hacker creates an army of zombies to attack a network so that it cannot receive genuine requests from consumers on time and eventually fails to respond. The bot master initiates the attack on the central server point (Al-Shareeda *et al.*, 2023) and quickly starts to send numerous requests to the server which results in ultimate chaos.

The frequency of DDoS attacks in the field of cybersecurity is increasing significantly. This persistent issue is concerning for both servers and users. Deep learning algorithms offer a potential solution to this problem. If properly detected, this type of attack can be identified and avoided. Therefore, based on researchers' suggestions, this paper aims to identify the attack and demonstrate the accuracy, recall, precision, and F1 score of the identification.

The research utilized eight distinct supervised and unsupervised DL models, including Convolutional Neural Network (CNN), Deep Neural Network (DNN), Long Short-Term Memory Network (LSTM), Recurrent Neural Network (RNN), Feedforward Neural Network (FNN), Radial Basis Function Network (RBFN), Multilayer Perceptron (MLP) and Deep Belief Network (DBN). Each method considered various dataset features and provided accurate data classifications. The main objective of this research is to create a new dataset and identify the most effective ensemble framework for supervised and unsupervised models to detect and mitigate DDoS scenarios.

The remainder of the paper is structured as follows: In section 2, delve into previous work in this field. Section 3 provides a comprehensive discussion of the dataset, detailing the data pre-processing and the application of DL algorithms and evaluation metrics. Section 4 elucidates the table and chart, offering a visual representation of the data. Finally, in the conclusion section, concluding remarks have been presented.

2. Literature Review

DDoS attacks have become a common phenomenon in the cybersecurity world. Figure 1 presents a scenario of a DDoS attack occurring and capturing a server.

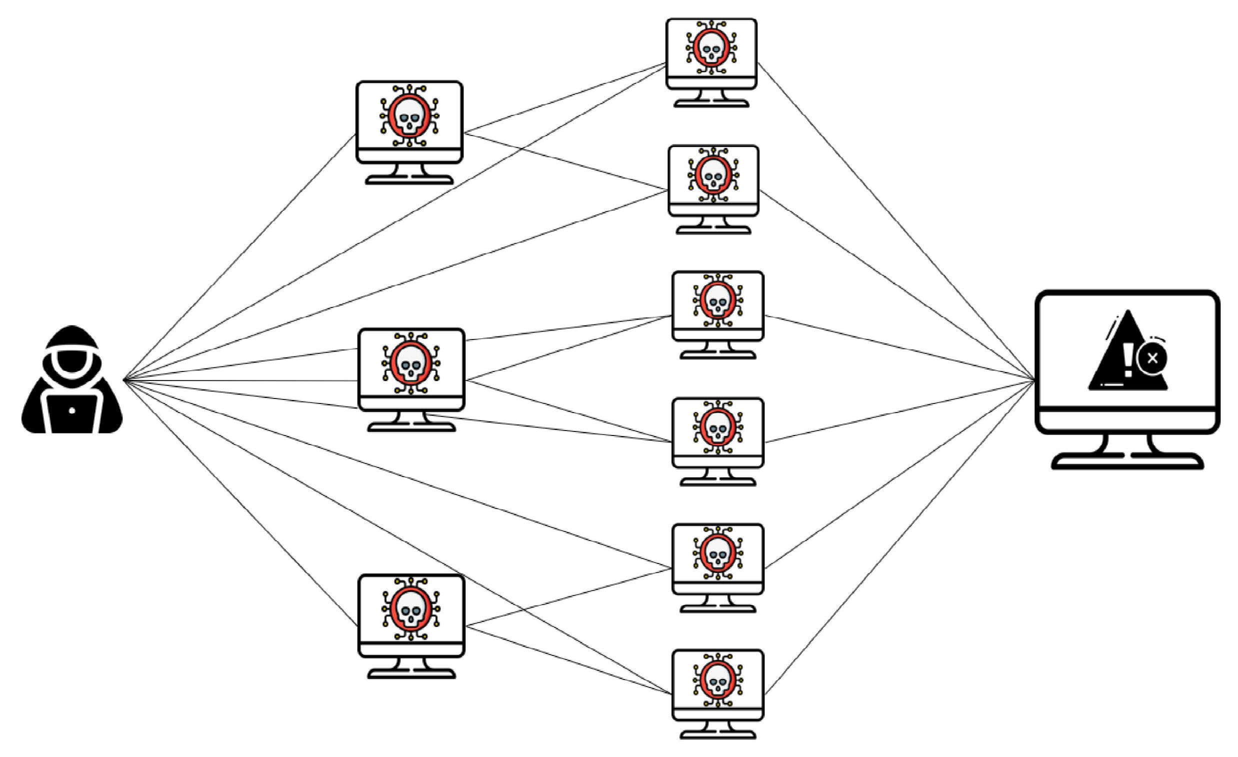

Figure 1: Visualization of DDoS Attack

Al-Shareeda *et al.* (2023) discussed several ML and DL techniques to make a study that analysed important differences between ML and DL techniques. The author wanted to find out when one of these techniques can be useful.

Shaaban *et al.* (2019) used a technique that uses CNN to detect and classify DDoS traffic with an accuracy of 99%. The technique is tested on two different datasets, namely the MCC network by Wireshark and a predefined open-source dataset. The outcomes are in contrast with other classification algorithms, such as decision trees, support vector machines (SVM), K-nearest neighbor, and neural networks.

Wang *et al.* (2020) proposed a framework that is composed of an SD-IoT controller, SD-IoT switches that are integrated with an IoT gateway, and IoT devices. Also proposed a DL detection algorithm utilizes the presented SD-IoT framework which is based on time series analysis that has shown good results.

He *et al.* (2020) showcased a paper that is based on deep transfer learning that works on small sample DDoS attack detection. Several neural networks are trained through DL that is used to transfer in DDoS attacks with sufficient samples.

Thapanarath Khempetch and Pongpisit Wuttidittachotti (Khempetch and Wuttidittachotti, 2021) have introduced a system for detecting DDoS attacks that uses a DNN and LSTM algorithm. Their research has shown that the system can accurately detect all three types of DDoS attacks with 99.9% accuracy.

Imamverdiyev and Abdullayeva (2018) proposed an analysis of the accuracy of the proposed method using Bernoulli-Bernoulli RBM, Gaussian–Bernoulli RBM, DBN on the NSL-KDD data set for detecting DoS attack.

Hussain *et al.* (2020) propose a framework using CNNs and real network data, for early detection of DDoS attacks that control malicious devices organized by a botnet. The author implemented a puppet device to carry out a coordinated DDoS attack on a cellular network that could disrupt the operations of CPSs. The attack involved silent calls, signalling, SMS spamming, or a combination of these techniques targeting voice, internet, SMS, or a combination of these services. The proposed framework was able to accurately detect normal and under-attack cells with over 91% accuracy.

Li *et al.* (2018) presented a model for detecting and preventing DDoS attacks in a Software-Defined Network (SDN) environment using DL. This model helps in cleaning the DDoS attack traffic effectively in the SDN and reduces the dependence on the environment. The paper also showcased the simplified way of the real-time update of the detection system and reduced the difficulty of upgrading or changing the detection strategy.

Agarwal *et al.* (2022) introduced a novel method, FS-WOA-DNN, to effectively prevent DDoS attacks. The paper involves pre-processing the input dataset, feature selection using FS-WOA, and classification using a DNN. The model ensures security by employing homomorphic encryption and cloud storage. Tested using MATLAB, the algorithm achieved 95.35% accuracy in detecting DDoS attacks.

Yuan *et al.* (2017) designed a DNN to understand patterns in network traffic sequences to effectively track and combat network attacks. This experiment reduces the error rate from 7.517% to 2.103% in the larger data set compared with the conventional ML method.

Nugraha and Murthy (2020) propose utilizing a hybrid Convolutional Neural Network-Long Short-Term Memory (CNN-LSTM) model for the detection of slow DDoS attacks in SDN-based networks. This hybrid CNN-LSTM model demonstrates superior performance compared to other DL models such as MLP and standard ML models like 1-Class (SVM).

This recent research executes various DL algorithms to capture all the DDoS attacks presented in the dataset CIC-DDoS 2019. The dataset created in this paper was utilized to analyse the accuracy of various DL algorithms. However, only random data from each attack was chosen to construct an idealized dataset. This research study strongly emphasizes the impact on accuracy when the target variables are modified. Additionally, the paper effectively showcases the accuracy, recall, precision, and F1 score achieved by various DL techniques using the CIC-DDoS 2019 dataset.

3. Materials and Methods

This research paper meticulously followed a sequential methodology to acquire the dataset and carry out the entire research. The overall methodological approach has been presented in Figure 2.

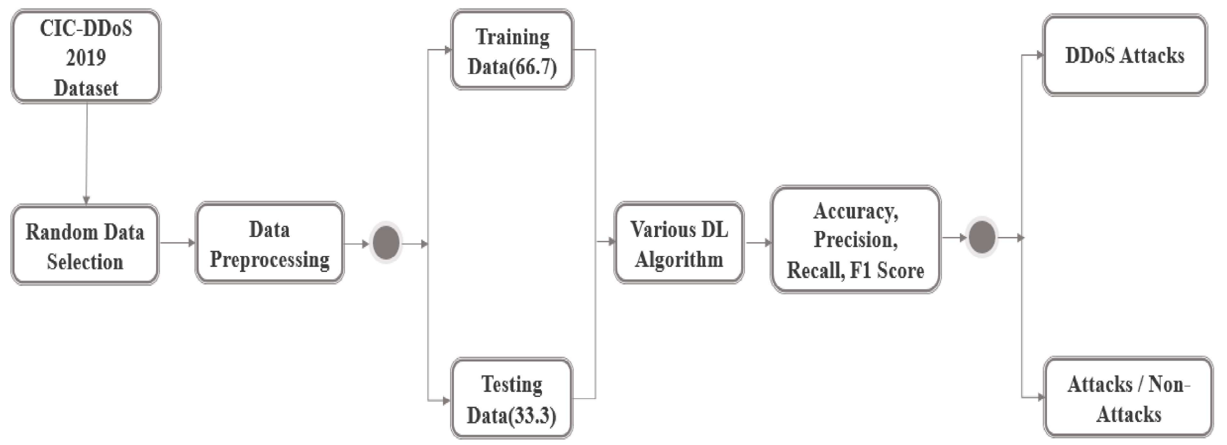

Figure 2: Methodological Approach

3.1. Dataset

The dataset is related to DDoS attacks (University of New Brunswick, 2019), which pose a significant threat to network security that attacks inundate the target network with malicious traffic, rendering it inaccessible to users. The dataset used in this paper was obtained from the Canadian Institute for Cybersecurity (University of New Brunswick, 2019). The dataset consists of 87 feature columns and 1 target column, totalling 88 columns. The target column encompasses 14 different variables, including NTP, DNS, LDAP, MSSQL, NetBIOS, SNMP, SSDP, UDP, UDP-Lag, WebDDoS, SYN, TFTP, Portmap, and BENIGN (representing non-attack variables). The Canadian Institute for Cybersecurity has provided two datasets-one for training and one for testing (Sharafaldin *et al.*, 2019). The training dataset covers the period from January 12th, starting at 10:30 AM and ending at 5:15 PM. This dataset includes 12 types of DDoS attacks, such as NTP, DNS, LDAP, MSSQL, NetBIOS, SNMP, SSDP, UDP, UDP-Lag, WebDDoS, SYN, and TFTP. The testing dataset covers the period from March 11th, starting at 9:40 AM and ending at 5:35 PM. It includes 7 types of attacks, such as Portmap, NetBIOS, LDAP, MSSQL, UDP, UDP-Lag, and SYN.

3.2. Dataset Preprocessing

To create our dataset, both the training and testing datasets were used. Here data were randomly selected 50,000 data for each type of attack (NTP, DNS, LDAP, MSSQL, NetBIOS, SNMP, SSDP, UDP, UDP-Lag, SYN, and TFTP) from the training dataset, including all BENIGN data. Additionally, 50,000 Portmap attack data were also randomly collected, including all benign data from the testing dataset. WebDDoS data was removed from the dataset since there was the minimum account of data available for WebDDoS. After merging all datasets, a new dataset was created that contained 661597 records. The new dataset has 87 feature columns, 1 target column with 13 target variables.

After removing the object datatype column during data cleaning, the dataset was left with a total of 82 columns. After replacing the infinity values with NaN, the corresponding rows are removed from the dataset. The final dataset contains 638455 records. The target variable in the final dataset was renamed from its original names (DrDoS_DNS, DrDoS_LDAP, etc.) to more concise names (DNS, LDAP, etc.).

After applying recursive feature elimination to the dataset, the dataset was narrowed down to 70 columns from the original set. Subsequently, the dataset has assessed the performance of various models in terms of accuracy, precision, recall, and F1 score.

3.3. Deep Learning Algorithms

In this comparative study, eight DL algorithms have been categorized as presented in Figure 3.

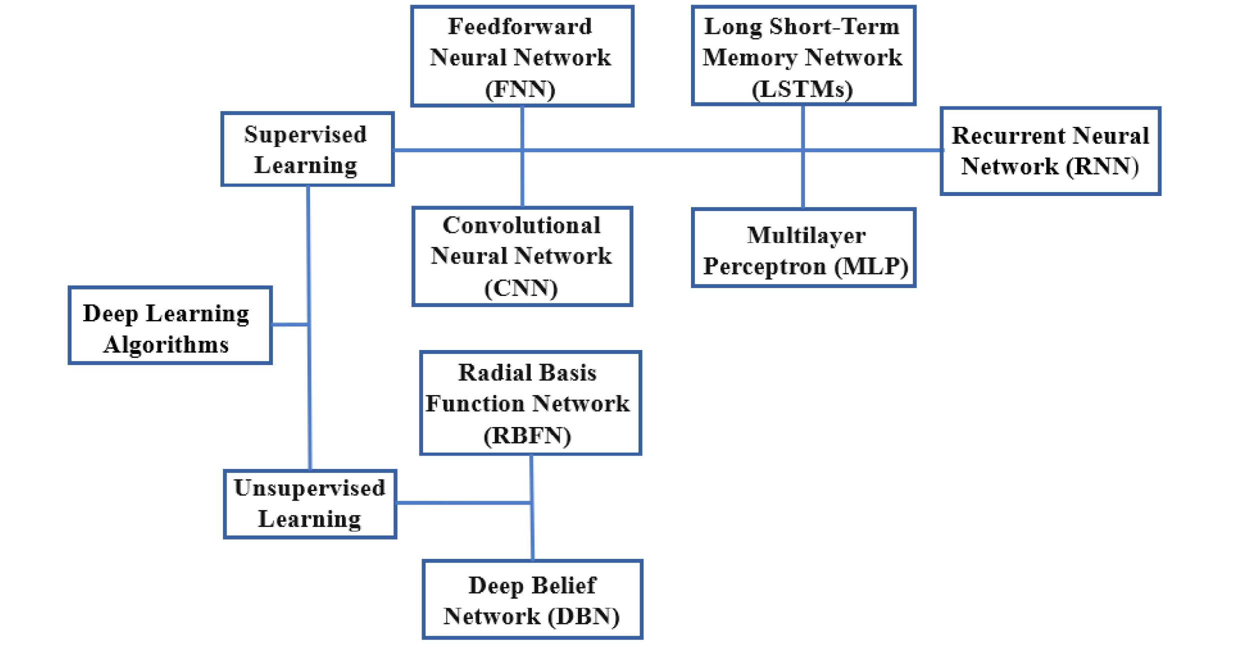
Feedforward Neural Network (FNN)
Long Short-Term Memory Network (LSTMs)
Supervised Learning
Recurrent Neural Network (RNN)
Convolutional Neural Network (CNN)
Multilayer Perceptron (MLP)
Deep Learning Algorithms
Radial Basis Function Network (RBFN)
Unsupervised Learning
Deep Belief Network (DBN)

Figure 3: DL Algorithms

3.3.1. CNN

The CNN is a crucial artificial neural network extensively utilized in DL, particularly in the realm of computer vision. It can achieve (Alashhab *et al.*, 2022) high performance by automatically extracting raw data features and finding correlations through model training. CNN architecture is decisively inspired by the organization of the animal visual cortex.

3.3.2. FNN

In FNN, each neuron is connected to all other neurons in the preceding and following layers. FNN does not make any assumptions about the input data and introduces a versatile solution for classification problems (Arnob and Jony, 2024).

3.3.3. RNN

Each neuron in the RNN sends output to neurons in the previous layer, making the design complex and expensive from a development perspective. The design of RNN is complex and costly due to each neuron sending output to neurons in the previous layer (Arnob and Jony, 2024).

3.3.4. LSTM

LSTM represents a significant advancement in addressing the problem of long-term dependencies. The LSTM architecture comprises an input gate layer and a tan*h* layer, which determine the information to be obtained from the cell state and the new information to be added to the cell state (Jony and Arnob, 2024a).

3.3.5. MLP

The MLP stands as a robust feed-forward artificial neural network that leverages interconnected neurons with weighted links. MLP consists of three crucial components: input layer, hidden layer, and output layer. The input layer adeptly handles external input data and conveys it to the initial hidden layer, which systematically refines the data until it ultimately reaches the output layer (Widiasari and Nugroho, 2017).

3.3.6. RBFN

RBFN uses radial basis functions as activation functions within a three-layer architecture consisting of input, hidden, and output layers. Input neurons receive features, hidden neurons compute radial basis functions based on input distances to prototypes, and output neurons aggregate the outputs from the hidden layer (Thandar and Khine, 2012).

3.3.7. DNN

DNN enable the hierarchical extraction of abstract knowledge from raw network data (Novaes *et al.*, 2021). This allows for more accurate and efficient data processing, prediction, and classification in applications like image recognition, natural language processing, and autonomous driving.

3.3.8. DBN

DBN is a sophisticated form of DL model comprising multiple layers of stochastic, generative neural networks, typically Restricted Boltzmann Machin. DBNs are characterized by a hierarchical architecture, where each layer progressively learns more abstract representations of the input data. These networks undergo training through unsupervised learning, followed by supervised learning fine-tuning (Voulodimos *et al.*, 2018).

3.4. Evaluation Metrics

Performance evaluation of the dataset prediction employs four crucial metrics: precision, recall, accuracy, and F1-measure, mainly used for model evaluation in research work (e.g., Jony and Arnob, 2024b; Shurman *et al.*, 2020; Jony and Arnob, 2024c; Salmi and Oughdir, 2023; Ferdous *et al.*, 2024).

Accuracy, in particular, denotes the ratio of correctly classified DDoS attack instances or benign instances out of all instances in the dataset. This metric effectively showcases the proportion of correct predictions about all samples. Equation 1 is used *t* calculate the accuracy of the models where True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN) constitute the equation.

$$Accuracy = \frac{TP}{TP + FN + TN + FP} \qquad ...(1)$$

Precision represents the proportion of correctly identified attacks out of all packets classified as attacks.

$$Precision = \frac{TP}{TP + FP} \qquad ...(2)$$

Recall indicates the proportion of accurately classified attacks out of all generated flows.

$$Recall = \frac{TP}{TP + FN} \qquad ...(3)$$

The F1-Score is a combined measure of precision and recall, providing a single value to assess both.

$$F1 - Score = \frac{TN + TP}{2TP + FN + FP} \qquad ...(4)$$

4. Results and Findings

In this research paper, experiments were conducted using the CIC-DDoS 2019 dataset. This research paper study tested 8 DL models to forecast their accuracy, precision, recall, and F1 score. The models used in this paper include CNN, DNN, LSTM, RNN, FNN, RBFN, MLP, and DBN classifiers.

Table 1 displays the accuracy, precision, recall, and F1 scores of 8 classifiers when the target column is classified into 13 types of attacks. The table shows that the RBFN classifier has the lowest accuracy, precision, recall, and F1 score, while the DBN classifier performs exceptionally well with high scores across all metrics. The performances of CNN, DNN, LSTM, FNN, and MLP classifiers are very similar to RF classifiers. Figure 4, showcases the result of Table 1.

Table 2 presents the accuracy, precision, recall, and F1 scores of 8 classifiers when the target column is classified as attacks and non-attacks. In this context, the target variable represents the classification of attacks as "ATTACK" and non-attacks as "BENIGN". The results reveal that the CNN classifier achieves nearly 100% accuracy, precision, recall, and F1 score, outperforming the DNN, LSTM, RNN, and FNN classifiers, which also demonstrate exceptional performance across all metrics. Furthermore, the RBFN, MLP, and DBN classifiers also exhibit commendable performance. Figure 5, represents the result of Table 2.

Table 1: Outcome of DDoS Attacks Detection (13 Types of Attacks)

Prediction Model	Accuracy	Precision	Recall	F1 Score
CNN	0.74	0.78	0.74	0.70
DNN	0.73	0.75	0.73	0.71
LSTM	0.75	0.77	0.75	0.71
RNN	0.71	0.76	0.71	0.66
FNN	0.74	0.77	0.74	0.70
RBFN	0.66	0.66	0.66	0.64
MLP	0.73	0.74	0.73	0.68
DBN	0.74	0.78	0.74	0.72

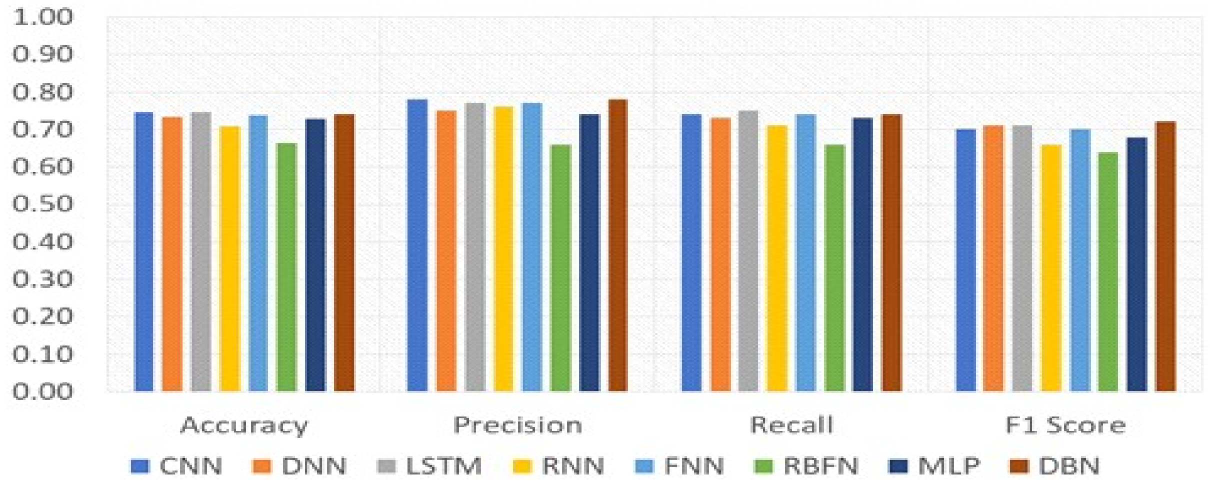

Figure 4: Result Comparison for DL Algorithms (13 Types of Attacks)

Table 2: Outcome of DDoS Attacks Detection (Attack/Non-Attack)

Prediction Model	Accuracy	Precision	Recall	F1 Score
CNN	1.00	1.00	1.00	1.00
DNN	0.99	1.00	1.00	1.00
LSTM	0.99	1.00	1.00	1.00
RNN	0.99	1.00	1.00	1.00
FNN	0.99	1.00	1.00	1.00
RBFN	0.99	1.00	1.00	1.00
MLP	0.99	1.00	1.00	1.00
DBN	0.99	1.00	1.00	1.00

On the other hand, when attacks are categorized into 13 different names, the accuracy seems to be lower when they are categorized into 2 categories which presented in Figure 7.

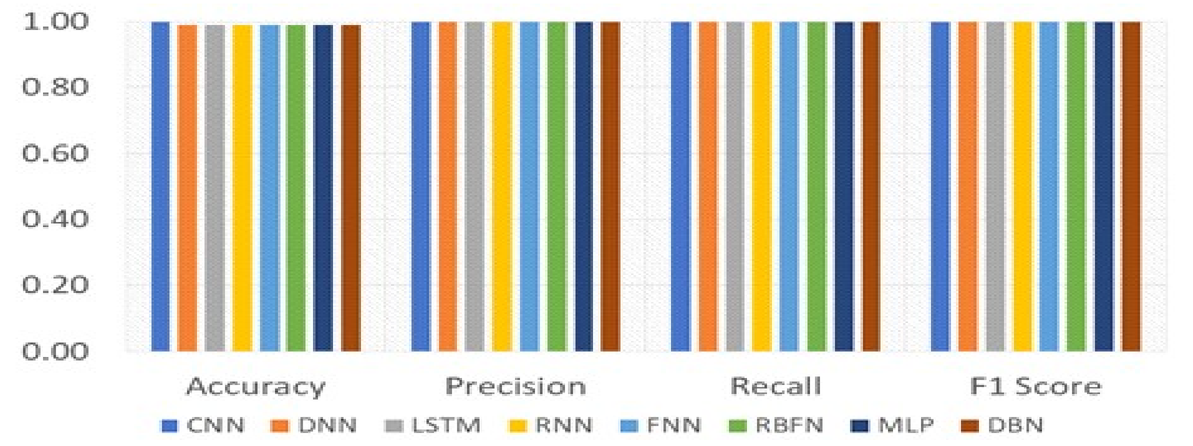

Figure 5: Result Comparison for DL Algorithms (Attack/Non-Attack)

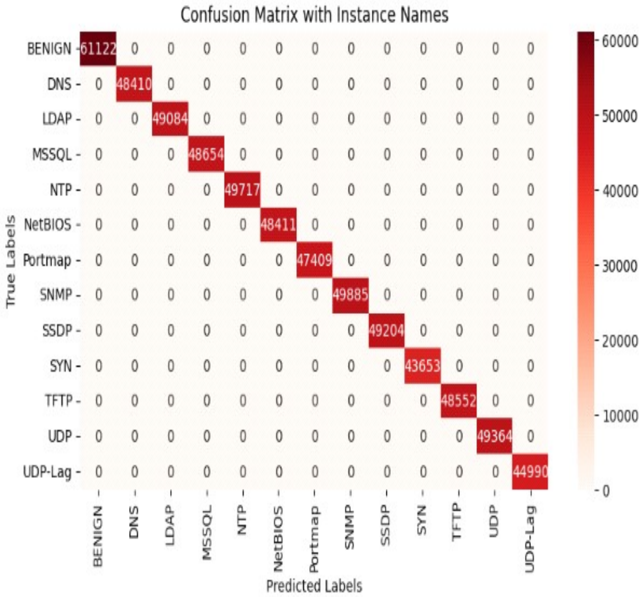

Figure 6: Confusion Matrix (13 Types of Attacks)

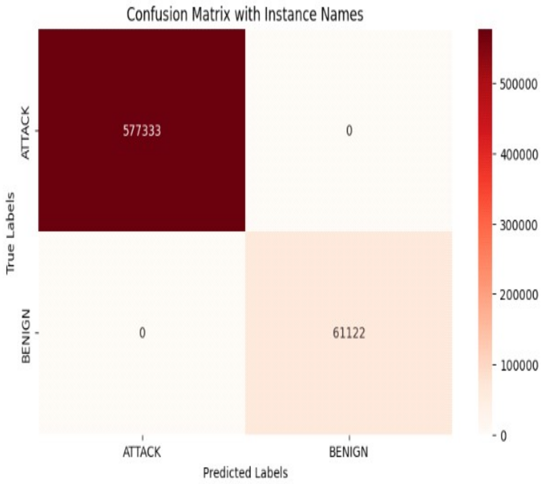

Figure 7: Confusion Matrix (Attack/Non-Attack)

5. Conclusion

In the last few years, notifiable efforts have been researched or developed with the help of DL models to counter DDoS threats (Malliga *et al.*, 2022). DL plays a significant part in the advancement of attack detection solutions. The research in this paper began by examining and analysing the relationship between the timestamps of the instances in the CIC-DDoS 2019 dataset. The paper also aimed to analyse the different DDoS attack methods and provide a comprehensive analysis of their occurrence. A specific amount of data was carefully selected for the experiment. The selection was made using a random function to ensure unbiased data selection. Various DL models were introduced to detect DDoS attacks. Feature selection methods were also introduced to choose features for further analysis. The results indicate that the proposed method is not only feasible but also demonstrates superior performance compared to various recent and relevant approaches documented in the literature.

The current model prioritizes limiting damage over preventing it, with predictions being identified by DL algorithms. However, the research does not introduce a new method for detecting DDoS attacks. Our future goal is to conduct a comprehensive analysis using the Large Language Model (LLM) to explore effective methods for preventing cyber-attacks. Our future research aims to develop new techniques and efficient algorithms to effectively halt DDoS attacks.

References

Agarwal, M., Khari, M. and Singh, R. (2022). Detection of DDOS Attack Using Deep Learning Model in Cloud Storage Application. *Wireless Personal Communications*, 1-21.

Alashhab, A., Zahid, M.S.M., Muneer, A. and Abdullahi, M. (2022). Low-Rate DDoS Attack Detection Using Deep Learning for SDN-Enabled IoT Networks. *International Journal of Advanced Computer Science and Applications*, 13(11).

Al-Shareeda, M.A., Manickam, S. and Ali, M. (2023). DDoS Attacks Detection Using Machine Learning and Deep Learning Techniques: Analysis and Comparison. *Bulletin of Electrical Engineering and Informatics*, 12(2), 930-939.

Arnob, A.K.B. and Jony, A.I. (2024). Enhancing IoT Security: A Deep Learning Approach with Feedforward Neural Network for Detecting Cyber Attacks in IoT. *Malaysian Journal of Science and Advanced Technology*, 4(4), 413-420.

Ferdous, F.S., Biswas, T. and Jony, A.I. (2024). Enhancing Cybersecurity: Machine Learning Approaches for Predicting DDoS Attack. *Malaysian Journal of Science and Advanced Technology*, 4(3), 249-255.

He, J., Tan, Y., Guo, W. and Xian, M. (2020). A Small Sample DDoS Attack Detection Method Based on Deep Transfer Learning. *In 2020 International Conference on Computer Communication and Network Security (CCNS)*, 47-50, Guilin, China.

Hussain, Q., Du, B., Sun, B. and Han, Z. (2020). Deep Learning-Based DDoS-Attack Detection for Cyber-Physical System Over 5G Network. *IEEE Transactions on Industrial Informatics*, 17(2), 860-870.

Imamverdiyev, Y. and Abdullayeva, F. (2018). Deep Learning Method for Denial of Service Attack Detection Based on Restricted Boltzmann Machine. *Big Data*, 6(2), 159-169.

Jony, A.I. and Arnob, A.K.B. (2024a). A Long Short-Term Memory Based Approach for Detecting Cyber Attacks in IoT Using CIC-IoT2023 Dataset. *Journal of Edge Computing*, 3(1), 28-42.

Jony, A.I. and Arnob, A.K.B. (2024b). Deep Learning Paradigms for Breast Cancer Diagnosis: A Comparative Study on Wisconsin Diagnostic Dataset. *Malaysian Journal of Science and Advanced Technology*, 4(2), 109-117.

Jony, A.I. and Arnob, A.K.B. (2024c). Securing the Internet of Things: Evaluating Machine Learning Algorithms for Detecting IoT Cyberattacks Using CIC-IoT2023 Dataset. *International Journal of Information Technology and Computer Science*, 16(4), 56-65.

Jony, A.I. and Hamim, S.A. (2023). Navigating the Cyber Threat Landscape: A Comprehensive Analysis of Attacks and Security in the Digital Age. *Journal of Information Technology and Cyber Security*, 1(2), 53-67.

Khempetch, T. and Wuttidittachotti, P. (2021). DDoS Attack Detection Using Deep Learning. *IAES International Journal of Artificial Intelligence*, 10(2), 382-390.

Li, X. *et al.* (2018). Detection and Defense of DDoS Attack-Based on Deep Learning in Open Flow Based SDN. *International Journal of Communication Systems*, 31(5), e3497.

Malliga, S., Nandhini, P.S. and Kogilavani, S.V. (2022). A Comprehensive Review of Deep Learning Techniques for the Detection of (Distributed) Denial of Service Attacks. *Information Technology and Control*, 51(1), 180-215.

Novaes, M.P., Carvalho, L.F., Lloret, J. and Proença, M.L. (2021). Adversarial Deep Learning Approach Detection and Defense Against DDoS Attacks in SDN Environments. *Future Generation Computer Systems*, 125, 156-167.

Nugraha, B. and Murthy, R.N. (2020). Deep Learning-Based Slow DDoS Attack Detection in SDN-Based Networks. *In 2020 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN),* 51-56, Madrid, Spain.

Salmi, S. and Oughdir, L. (2023). Performance Evaluation of Deep Learning Techniques for DoS Attacks Detection in Wireless Sensor Network. *Journal of Big Data*, 10(1), 17.

Shaaban, R., Abd-Elwanis, E. and Hussein, M. (2019). DDoS Attack Detection and Classification via Convolutional Neural Network (CNN). *In 2019 9th International Conference on Intelligent Computing and Information Systems (ICICIS),* 233-238, Cairo, Egypt.

Sharafaldin, I., Lashkari, A.H., Hakak, S. and Ghorbani, A.A. (2019). Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy. *In 2019 International Carnahan Conference on Security Technology (ICCST),* 1-8, Chennai, India.

Shurman, M., Khrais, R. and Yateem, A. (2020). DoS and DDoS Attack Detection Using Deep Learning and IDS. *International Arab Journal of Information Technology*, 17(4A), 655-661.

Thandar, M. and Khine, M.K. (2012). Radial Basis Function (RBF) Neural Network Classification Based on Consistency Evaluation Measure. *International Journal of Computer Applications*, 54(15).

University of New Brunswick. (2019). Canadian Institute for Cybersecurity DDoS Attack Dataset. Retrieved from https://www.unb.ca/cic/datasets/ddos-2019.html

Voulodimos, A., Doulamis, N., Doulamis, A. and Protopapadakis, E. (2018). Deep Learning for Computer Vision: A Brief Review. *Computational Intelligence and Neuroscience*, 2018, Article 7068349.

Wang, J., Liu, Y., Su, W. and Feng, H. (2020). A DDoS Attack Detection Based on Deep Learning in Software-Defined Internet of Things. *In 2020 IEEE 92nd Vehicular Technology Conference (VTC2020-Fall),* 1-5, Victoria, BC, Canada.

Widiasari, R. and Nugroho, L.E. (2017). Deep Learning Multilayer Perceptron (MLP) for Flood Prediction Model Using Wireless Sensor Network-Based Hydrology Time Series Data Mining. *In 2017 International Conference on Innovative and Creative Information Technology (ICITech),* 1-5, Salatiga, Indonesia.

Yuan, X., Li, C. and Li, X. (2017). DeepDefense: Identifying DDoS Attack via Deep Learning. *In 2017 IEEE International Conference on Smart Computing (SMARTCOMP),* 1-8, Hong Kong.

Cite this article as: Tapu Biswas, Farhan Sadik Ferdous and Akinul Islam Jony (2024). Binary and Multi-Class Prediction of DDoS Attack Using Deep Learning Models. *International Journal of Data Science and Big Data Analytics,* 4(2), 49-58. doi: 10.51483/IJDSBDA.4.2.2024.49-58.