An Intrusion Detection System for DDoS Attacks Classification Using Machine Learning

Roushan Kumar[1,] Dr. Jasdeep Singh[2]
[1,2]*Department of Computer Science & Engineering, RIMT University, Punjab, India*

***Abstract*—Distributed Denial of Service (DDoS) attacks are among the most critical threats to modern computer networks, causing service disruption and significant performance degradation. Traditional intrusion detection systems often struggle to identify sophisticated and evolving attack patterns. Machine Learning (ML) techniques provide intelligent and data-driven approaches for detecting malicious network activities. This paper presents a Machine Learning-Based Intrusion Detection System (IDS) for DDoS attack classification using the UNSW-NB15 dataset. Three machine learning algorithms, namely Decision Tree, Random Forest, and XG Boost, were implemented and evaluated. The dataset was preprocessed through categorical feature encoding and stratified train-test splitting. Model performance was assessed using Accuracy, Precision, Recall, F1-Score, Confusion Matrix, Receiver Operating Characteristic (ROC) Curve, Area Under the Curve (AUC), and 5-Fold Cross Validation. Experimental results show that the Random Forest classifier achieved the best overall performance with an accuracy of 95.13%, F1-score of 96.46%, AUC score of 0.990, and a cross-validation accuracy of 95.20%. XG Boost achieved the highest recall of 98.22%, indicating strong attack detection capability. The findings demonstrate that machine learning-based intrusion detection systems can effectively distinguish malicious traffic from legitimate network traffic and provide a reliable solution for DDoS attack classification.**

***Index Terms*—DDoS Attack, Intrusion Detection, Machine Learning, Network Security, Random Forest, UNSW-NB15, XG Boost.**

I. INTRODUCTION

The increasing dependence on internet-based services has significantly expanded the attack surface of modern computer networks. Among various cyber threats, Distributed Denial of Service (DDoS) attacks are considered one of the most severe and disruptive forms of cyber attacks. In a DDoS attack, multiple compromised devices simultaneously generate a large volume of malicious traffic toward a target server or network, resulting in service degradation, resource exhaustion, or complete service unavailability for legitimate users.

Traditional Intrusion Detection Systems (IDS) primarily rely on signature-based and rule-based detection mechanisms. Although these approaches are effective against known attack patterns, they often fail to detect novel and evolving threats. With the rapid growth of network traffic and increasingly sophisticated attack techniques, intelligent and adaptive detection mechanisms have become essential.

Machine Learning (ML) techniques have emerged as promising solutions for intrusion detection because they can learn complex patterns from historical network traffic data and automatically classify normal and malicious activities. By leveraging supervised learning algorithms, intrusion detection systems can achieve higher detection accuracy and improved adaptability compared to traditional approaches.

Working of DDoS Attack

A DDoS attack generally follows a sequence in which an attacker gains control of multiple compromised devices, commonly known as a botnet, and instructs them to send massive amounts of malicious traffic toward a target server. The overwhelming traffic consumes network bandwidth and system resources, preventing legitimate users from accessing the targeted service.

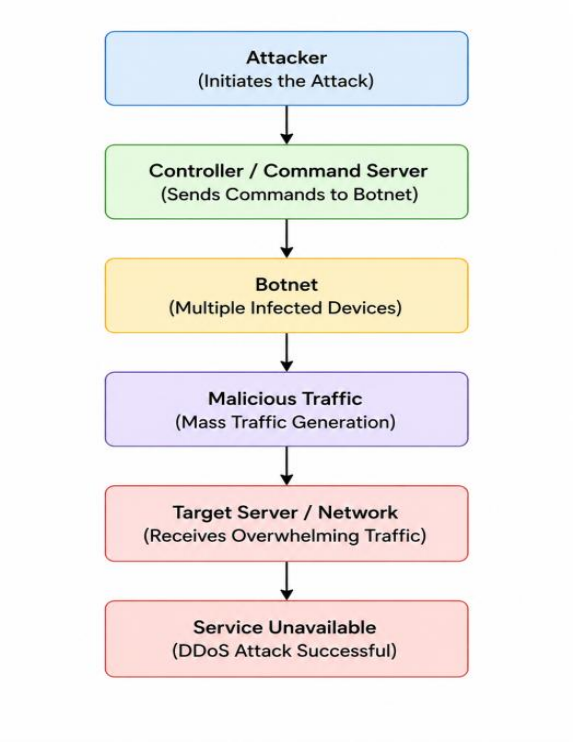

Figure 1: Basic DDoS Attack Flow Diagram

This research focuses on developing a Machine Learning-Based Intrusion Detection System (IDS) for DDoS attack classification using the UNSW-NB15 dataset. Three machine learning algorithms, namely Decision Tree, Random Forest, and XG Boost, are implemented and evaluated using standard performance metrics such as Accuracy, Precision, Recall, F1-Score, Confusion Matrix, ROC Curve, and AUC Score. The objective is to identify the most effective model for accurate and reliable DDoS attack detection.

II. LITERATURE REVIEW

Several researchers have explored machine learning approaches for DDoS attack detection and intrusion detection systems.

S.No.	Authors	Year	Methodology	Dataset	Major Findings
1	Tymoshchuk et al.	2024	ML-based Classification	DDoS Flooding Dataset	Improved DDoS flooding attack detection
2	Ali et al.	2023	Systematic Review	Multiple Datasets	ML effective for DDoS detection in SDN
3	Jewani et al.	2022	ML Classification & Prediction	DDoS Dataset	High detection accuracy with ML techniques
4	Shareena et al.	2021	Deep Learning-based IDS	IoT Botnet Dataset	Deep learning effectively detected IoT botnet attacks with high accuracy
5	Dasari & Devarakonda	2021	Classification Algorithms	Network Traffic Dataset	Successful detection of multiple DDoS attack types
6	Saini et al.	2020	ML Algorithm Comparison	Network Dataset	Compared various ML algorithms for DDoS detection
7	Saranya et al.	2020	IDS Review	Multiple Datasets	Reviewed ML algorithm performance in IDS
8	Roopak et al.	2020	IDS using ML	IoT Dataset	Effective IDS for IoT DDoS attacks
9	Dayanandam et al.	2017	Regression Algorithms	Network Dataset	Efficient attack prediction performance
10	Sharma et al.	2016	ML used in Detection	Multiple Data sets	Summarized strengths and limitations of ML approaches

Recent work by Tymoshchuk et al. (2024) further demonstrated the effectiveness of machine learning

methods for detecting and classifying DDoS flooding attacks.

The literature confirms that machine learning algorithms significantly improve intrusion detection performance. However, comparative analysis of Decision Tree, Random Forest, and XG Boost on the UNSW-NB15 dataset remains valuable for identifying the most suitable classifier.

III. PROBLEM STATEMENT

The major problems addressed in this research are as follows:

1. Traditional Intrusion Detection Systems (IDS) rely mainly on signature-based and rule-based detection techniques, which are effective only for known attack patterns.
2. Existing IDS solutions often fail to detect new and evolving Distributed Denial of Service (DDoS) attacks accurately.
3. Conventional IDS generate a high number of false alarms, reducing their reliability in real-world network environments.
4. The rapid growth in network traffic and increasing attack complexity make it difficult to distinguish legitimate traffic from malicious traffic.
5. There is a need for an intelligent and automated intrusion detection system that can efficiently analyze large-scale network traffic and accurately classify DDoS attacks using machine learning techniques.
6. Although several studies have applied machine learning for intrusion detection, a comparative evaluation of Decision Tree, Random Forest, and XG Boost using the UNSW-NB15 dataset with comprehensive performance metrics is still required.
7. This research aims to address these challenges by identifying the most effective machine learning classifier for accurate and reliable DDoS attack detection.

IV. OBJECTIVES

The main objectives of this research are as follows:

1. To study the concepts of Intrusion Detection Systems (IDS) and Distributed Denial of Service (DDoS) attacks in network security.
2. To preprocess and analyze the UNSW-NB15 dataset for effective machine learning-based attack classification.
3. To develop and implement machine learning models using Decision Tree, Random Forest, and XG Boost algorithms.
4. To evaluate the performance of the implemented models using standard metrics such as Accuracy, Precision, Recall, F1-Score, Confusion Matrix, ROC Curve, AUC, and Cross Validation.
5. To compare the performance of different machine learning algorithms and identify the most effective model for DDoS attack detection and classification.
6. To analyze the importance of network traffic features contributing to attack detection.

V. PROPOSED METHODOLOGY

The proposed methodology consists of the following stages:

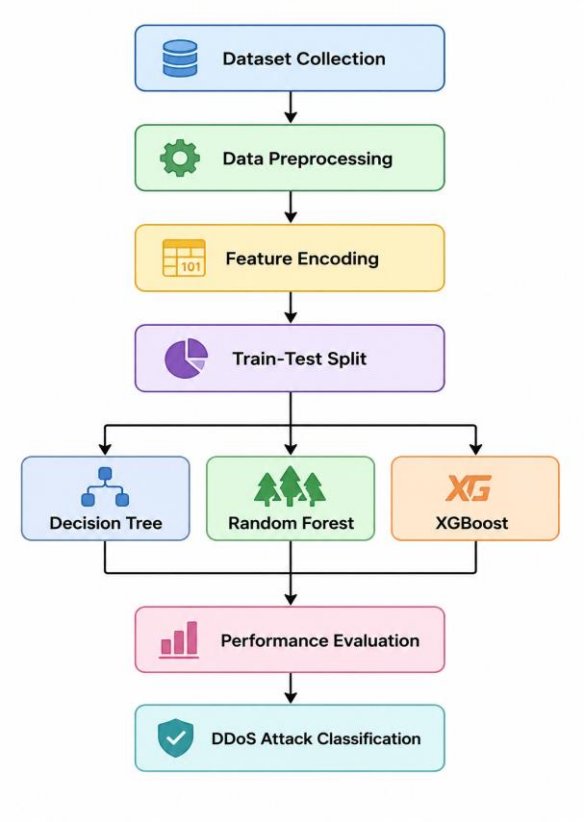

Figure 2: Methodology Flow Diagram

5.1 Dataset Collection

The UNSW-NB15 dataset was selected for experimentation because it contains realistic network traffic records and multiple attack categories. The dataset includes both normal and malicious traffic samples and is widely used in intrusion detection research.

According to Output :

- Attack (1) = 119,341
- Normal (0) = 56,000

Class	Records
Normal (0)	56,000
Attack (1)	119,341
Total	175,341

Table 1: Dataset Label Distribution

5.2 Data Preprocessing

The following preprocessing steps were performed:

- Loading dataset using Pandas.
- Encoding categorical attributes:
  - proto
  - service
  - state
- Removing non-predictive target columns from feature space.
- Splitting dataset into training and testing subsets.

The UNSW-NB15 dataset contains 175,341 network traffic records consisting of both normal and attack traffic. After preprocessing, 34 input features were used for model training and evaluation, along with one target label. For binary classification, the label attribute was used as the target variable, where 0 represents normal traffic and 1 represents attack traffic.

5.3 Train-Test Split

The dataset was divided into training and testing subsets using a 70:30 ratio with stratified sampling to preserve the class distribution across both sets. The training set contained 122,738 records, while the testing set contained 52,603 records. Stratified sampling ensured that both the training and testing datasets maintained a similar proportion of normal and attack instances, thereby reducing sampling bias. This split provided sufficient data for model training while reserving an independent test set for reliable performance evaluation and generalization of the machine learning models.

5.4 Machine Learning Models

Decision Tree

Decision Tree is a supervised machine learning algorithm used for classification tasks. It creates a hierarchical tree structure by splitting the dataset based on feature values and decision rules. The model classifies network traffic by traversing decision nodes from the root to leaf nodes, making it suitable for intrusion detection applications due to its simplicity and interpretability.

Random Forest

Random Forest is an ensemble learning algorithm that combines multiple decision trees to improve classification performance. Each tree is trained on a random subset of the data, and the final prediction is obtained through majority voting. This approach reduces over fitting, improves generalization capability, and provides robust performance for DDoS attack detection.

XG Boost

XG Boost (Extreme Gradient Boosting) is an advanced boosting algorithm that constructs decision trees sequentially, where each new tree corrects the errors of previous trees. It incorporates gradient optimization, regularization, and efficient computation techniques to achieve high prediction accuracy. Due to its strong learning capability, XG Boost is widely used in intrusion detection and cyber security applications.

5.5 Evaluation Metrics

The performance of the proposed intrusion detection system was evaluated using several standard classification metrics.

Accuracy:

Accuracy measures the overall proportion of correctly classified instances among all observations. It indicates the general effectiveness of the classification model.

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN}$$

Precision:

Precision measures the proportion of correctly identified attack instances among all instances predicted as attacks.

$$\text{Precision} = \frac{TP}{TP+FP}$$

Recall:

Recall, also known as sensitivity, measures the proportion of actual attack instances that were correctly detected by the model.

$$\text{Recall} = \frac{TP}{TP+FN}$$

F1-Score:

F1-Score is the harmonic mean of Precision and Recall, providing a balanced measure of classification performance.

$$\text{F1} = \frac{2*Precision*Recall}{Precision+Recall}$$

Confusion Matrix:

A Confusion Matrix provides a detailed summary of classification results by presenting True Positives (TP), True Negatives (TN), False Positives (FP), and False Negatives (FN).

- TP (True Positive): Attack traffic correctly classified as attack.
- TN (True Negative): Normal traffic correctly classified as normal.
- FP (False Positive): Normal traffic incorrectly classified as attack.
- FN (False Negative): Attack traffic incorrectly classified as normal.

Classification Report:

The Classification Report summarizes Precision, Recall, F1-Score, and support values for each class, providing a comprehensive performance evaluation.

ROC Curve (Receiver Operating Characteristic Curve):

The ROC Curve illustrates the relationship between the True Positive Rate (TPR) and False Positive Rate (FPR) at different classification thresholds.

AUC Score (Area Under the Curve):

The AUC score measures the overall ability of a model to distinguish between attack and normal traffic. A higher AUC value indicates better classification performance.

5.6 Feature Importance Analysis

Feature importance analysis was conducted using the Random Forest classifier to determine the contribution of individual network traffic features toward DDoS attack classification. The most influential features were identified based on their importance scores.

5.7 Cross Validation

A 5-Fold Cross Validation technique was applied to evaluate the stability and generalization capability of the best-performing model. The dataset was divided into five folds, and the model was trained and tested iteratively on different partitions.

Feature importance analysis was conducted using the Random Forest classifier to determine the contribution of individual network traffic features toward DDoS attack classification. The most influential features were identified based on their importance scores.

VI EXPERIMENTAL RESULTS AND DISCUSSION

6.1 Model Performance Comparison

Algorithm	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Decision Tree	94.06	95.58	95.70	95.64
Random Forest	95.13	95.46	97.47	96.46
XGBoost	94.58	94.08	98.22	96.10

Table 2: Model Performance Comparison

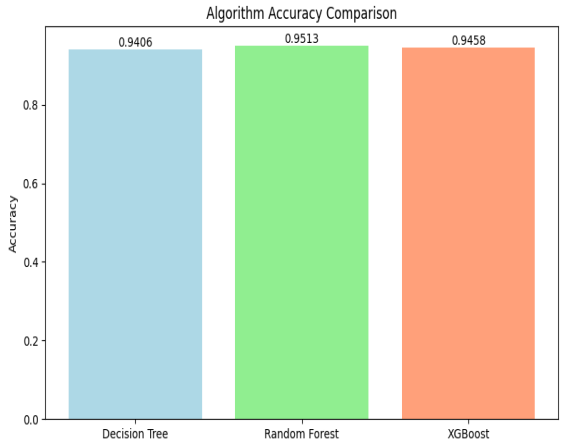

Figure 3. Accuracy Comparison of Decision Tree, Random Forest, and XG Boost Models

Discussion

The experimental results indicate that all three machine learning algorithms achieved high classification performance on the UNSW-NB15 dataset. Random Forest achieved the highest accuracy (95.13%) and F1-score (96.46%), demonstrating the most balanced classification performance. XG Boost achieved the highest recall (98.22%) and the lowest false negative count,

indicating superior capability in detecting DDoS attacks. Therefore, Random Forest is considered the best overall model, while XG Boost is particularly effective for attack detection scenarios where minimizing missed attacks is critical.

6.2 Confusion Matrix Analysis

Decision Tree

[[15215 1585]
 [1538 34265]]

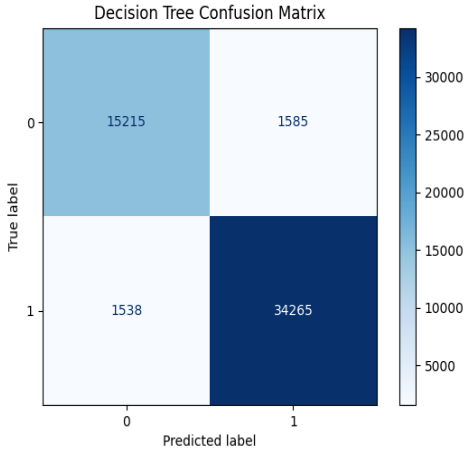

Figure 4. Decision Tree Confusion Matrix

Random Forest

[[15141 1659]
 [905 34898]]

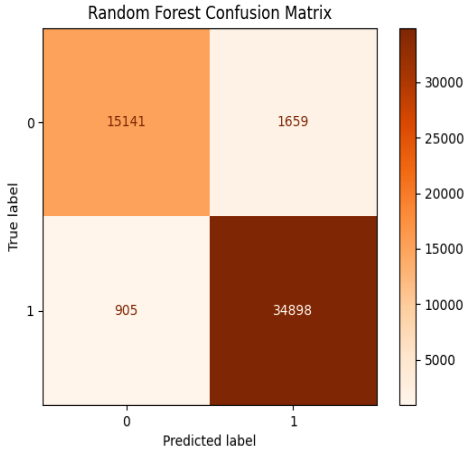

Figure 5. Random Forest Tree Confusion Matrix

XG Boost

[[14587 2213]
 [638 35165]]

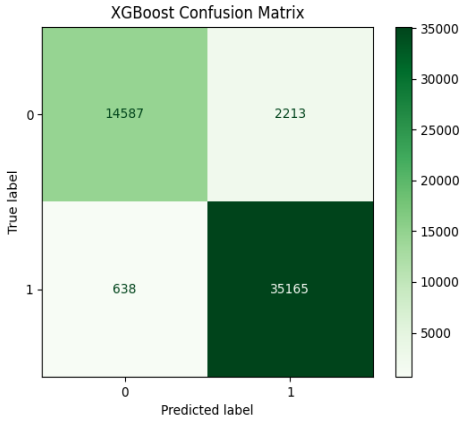

Figure 6. XGBoost Confusion Matrix

The XG Boost model produced the lowest number of false negatives (638), indicating superior attack detection capability. Since false negatives represent undetected attacks, minimizing them is important for intrusion detection systems. Random Forest maintained a better balance between false positives and false negatives, resulting in the highest overall classification performance.

6.3 ROC Curve and AUC Analysis

Algorithm	AUC Score
Decision Tree	0.939
Random Forest	0.990
XGBoost	0.990

Table 3: AUC Scores of Machine Learning Models

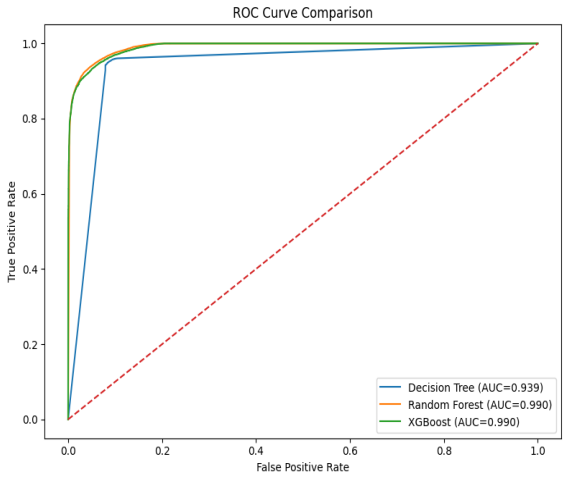

Figure 7. ROC Curve Comparison of Decision Tree, Random Forest, and XG Boost

Random Forest and XG Boost achieved near-perfect AUC values, indicating excellent capability in distinguishing malicious traffic from normal traffic. Their ROC curves remained close to the upper-left corner, representing high true positive rates and low false positive rates.

6.4 Feature Importance Analysis

Feature importance was extracted using the Random Forest classifier.

Table 4: Top 10 Important Features

Feature	Importance
dload	0.102865
synack	0.083800
rate	0.075995
ackdat	0.071376
sload	0.071133
dmean	0.066284
dur	0.055314
tcprtt	0.049673
sbytes	0.043666
sinpkt	0.042297

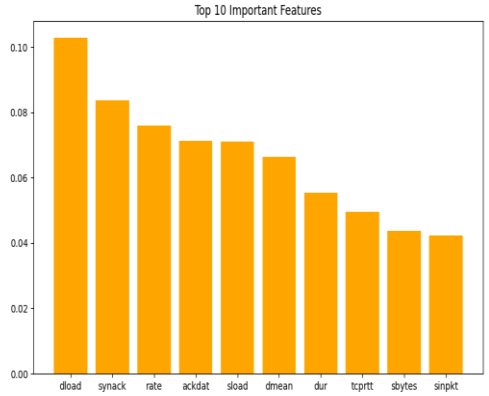

Figure 8. Top 10 Important Features Identified by the Random Forest Classifier

The feature dload was identified as the most influential feature, indicating that destination traffic load plays a significant role in DDoS attack detection.

6.5 Cross Validation Analysis

Table 5: Fold Cross Validation Results

Metric	Value
Mean Accuracy	95.20%
Standard Deviation	0.0011

To evaluate model stability and generalization capability, 5-fold cross-validation was performed on the Random Forest classifier. The model achieved a mean accuracy of 95.20% with a standard deviation of 0.0011, indicating consistent and reliable performance across different data partitions.

6.6 Best Model Selection

Based on the experimental results, Random Forest was identified as the best-performing model. It achieved the highest accuracy (95.13%), highest F1-score (96.46%), and an AUC score of 0.990. Furthermore, the cross-validation accuracy of 95.20% demonstrates the model's robustness and generalization capability. Therefore, Random Forest was selected as the final model for DDoS attack classification.

VII. CONCLUSION

This research presented a Machine Learning-Based Intrusion Detection System (IDS) for DDoS attack classification using the UNSW-NB15 dataset. The proposed system employed three machine learning algorithms, namely Decision Tree, Random Forest, and XG Boost, to distinguish malicious network traffic from normal traffic. The dataset was preprocessed through categorical feature encoding and stratified train-test splitting before model training and evaluation.

Experimental results demonstrated that all three models achieved high classification performance. Among them, the Random Forest classifier achieved the best overall results with an accuracy of 95.13%, an F1-score of 96.46%, and an AUC score of 0.990. The XG Boost model achieved the highest recall value of 98.22%, indicating strong attack detection capability with the lowest number of false negatives. Feature importance analysis revealed that attributes such as dload, synack, rate, and ackdat play a significant role in DDoS attack detection. Furthermore, 5-Fold Cross Validation produced a

mean accuracy of 95.20%, confirming the stability and reliability of the proposed approach.

Based on the obtained results, Random Forest was identified as the most suitable classifier for the proposed intrusion detection system due to its balanced performance, high accuracy, and strong generalization capability. The study demonstrates that machine learning techniques can effectively enhance network security by providing accurate and efficient DDoS attack classification.

VIII. FUTURE WORK

Future enhancements of this research may include:

1. In future we implement Deep Learning techniques such as CNN, LSTM, and Hybrid Neural Networks for improved attack detection.
2. We will evaluate of the proposed system on recent cyber security datasets such as CICIDS2017 and CIC-DDoS2019 to validate its performance and generalization capability.
3. We will develop a real-time intrusion detection framework for live network traffic monitoring.
4. We will investigate advanced feature selection and optimization techniques to further improve detection accuracy and reduce computational complexity.
5. Extension of the system to multi-class attack classification for identifying different categories of network attacks.

REFERENCES

[1] V. K. Jewani et al., "Machine Learning Classification and Prediction Techniques to Detect DDoS Attack," IEEE Access, vol. 10, pp. 21443–21454, 2022.

[2] T. E. Ali, Y.-W. Chong, and S. Manickam, "Machine Learning Techniques to Detect a DDoS Attack in SDN: A Systematic Review," Applied Sciences, vol. 13, no. 5, p. 3183, 2023.

[3] K. B. Dasari and N. Devarakonda, "Detection of Different DDoS Attacks Using Machine Learning Classification Algorithms," Ingénierie des Systèmes d'Information, vol. 26, no. 5, pp. 461–468, 2021.

[4] J. Shareena, A. Ramdas, and H. A. P., "Intrusion Detection System for IoT Botnet Attacks Using Deep Learning," SN Computer Science, vol. 2, no. 3, p. 205, 2021.

[5] G. Dayanandam, E. S. Reddy, and D. B. Babu, "Regression Algorithms for Efficient Detection and Prediction of DDoS Attacks," in Proceedings of the 3rd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), IEEE, 2017.

[6] N. Sharma, A. Mahajan, and V. Mansotra, "Machine Learning Techniques Used in Detection of DoS Attacks: A Literature Review," International Journal of Advance Research in Computer Science and Software Engineering, vol. 6, no. 3, pp. 100–105, 2016.

[7] D. Tymoshchuk et al., "Detection and Classification of DDoS Flooding Attacks by Machine Learning Method," arXiv:2412.18990, 2024.

[8] M. Roopak, G. Y. Tian, and J. Chambers, "An Intrusion Detection System Against DDoS Attacks in IoT Networks," in 10th Annual Computing and Communication Workshop and Conference (CCWC), IEEE, 2020.

[9] P. S. Saini, S. Behal, and S. Bhatia, "Detection of DDoS Attacks Using Machine Learning Algorithms," in 7th International Conference on Computing for Sustainable Global Development (INDIACom), IEEE, 2020.

[10] T. Saranya et al., "Performance Analysis of Machine Learning Algorithms in Intrusion Detection System: A Review," Procedia Computer Science, vol. 171, pp. 1251–1260, 2020.

[11] K. Lee, J. Kim, K. H. Kwon, Y. Han, and S. Kim, "DDoS Attack Detection Method Using Cluster Analysis," Expert Systems with Applications, vol. 34, no. 3, pp. 1659–1665, 2008.

[12] O. Ussatova et al., "Comprehensive DDoS Attack Classification Using Machine Learning Algorithms," Computers, Materials & Continua, vol. 73, no. 1, 2022.

[13] Y. W. Chen et al., "Design and Implementation of IoT DDoS Attacks Detection System Based on Machine Learning," in Proc. European Conference on Networks and Communications (EuCNC), IEEE, 2020.

[14] T. Aytaç, M. A. Aydın, and A. H. Zaim, "Detection DDoS Attacks Using Machine

Learning Methods," Electrica, vol. 20, no. 2, pp. 159–167, 2020.

[15] S. Mohammed, "A Machine Learning-Based Intrusion Detection of DDoS Attack on IoT Devices," International Journal, vol. 10, 2021.

[16] R. Patgiri et al., "An Investigation on Intrusion Detection System Using Machine Learning," in Proc. IEEE Symposium Series on Computational Intelligence (SSCI), IEEE, 2018.

[17] M. ElKashlan, H. Aslan, and M. A. Azer, "DDoS Attack Detection in IoT Using Machine Learning Based Intrusion Detection System (IDS)," in Proc. 18th International Computer Engineering Conference (ICENCO), IEEE, 2022.

[18] A. K. Silivery, K. R. M. Rao, and L. K. Kumar, "An Effective Deep Learning Based Multi-Class Classification of DoS and DDoS Attack Detection," International Journal of Electrical and Computer Engineering Systems, vol. 14, no. 4, pp. 421–431, 2023.

[19] F. S. Lima Filho et al., "Smart Detection: An Online Approach for DoS/DDoS Attack Detection Using Machine Learning," Security and Communication Networks, vol. 2019, Article ID 1574749, 2019.

[20] K. V. V. N. L. S. Kiran et al., "Building an Intrusion Detection System for IoT Environment Using Machine Learning Techniques," Procedia Computer Science, vol. 171, pp. 2372–2379, 2020.

[21] K. Park, Y. Song, and Y. G. Cheong, "Classification of Attack Types for Intrusion Detection Systems Using a Machine Learning Algorithm," in Proc. IEEE International Conference on Big Data Computing Service and Applications (BigDataService), IEEE, 2018.

[22] O. Rahman, M. A. G. Quraishi, and C. H. Lung, "DDoS Attacks Detection and Mitigation in SDN Using Machine Learning," in Proc. IEEE World Congress on Services (SERVICES), IEEE, 2019.

[23] S. Aktar and A. Y. Nur, "Towards DDoS Attack Detection Using Deep Learning Approach," Computers & Security, vol. 129, 2023.

[24] S. Peneti and E. Hemalatha, "DDoS Attack Identification Using Machine Learning Techniques," in Proc. International Conference on Computer Communication and Informatics (ICCCI), IEEE, 2021.

[25] A. Agarwal et al., "Classification Model for Accuracy and Intrusion Detection Using Machine Learning Approach," PeerJ Computer Science, vol. 7, e437, 2021.

[26] G. Logeswari, S. Bose, and T. J. I. A. Anitha, "An Intrusion Detection System for SDN Using Machine Learning," Intelligent Automation & Soft Computing, vol. 35, no. 1, pp. 867–880, 2023.

[27] A. Maslan, K. M. B. Mohamad, and F. B. M. Foozy, "Feature Selection for DDoS Detection Using Classification Machine Learning Techniques," IAES International Journal of Artificial Intelligence, vol. 9, no. 1, p. 137, 2020.

[28] C. Bagyalakshmi and E. S. Samundeeswari, "DDoS Attack Classification on Cloud Environment Using Machine Learning Techniques with Different Feature Selection Methods," International Journal, vol. 9, no. 5, 2020.

[29] J. Ashraf and S. Latif, "Handling Intrusion and DDoS Attacks in Software Defined Networks Using Machine Learning Techniques," in Proc. National Software Engineering Conference, IEEE, 2014.

[30] A. Amouri, V. T. Alaparthy, and S. D. Morgera, "A Machine Learning Based Intrusion Detection System for Mobile Internet of Things," Sensors, vol. 20, no. 2, p. 461, 2020.

[31] R. Santos et al., "Machine Learning Algorithms to Detect DDoS Attacks in SDN," Concurrency and Computation: Practice and Experience, vol. 32, no. 16, e5402, 2020.

[32] M. J. Awan et al., "Real-Time DDoS Attack Detection System Using Big Data Approach," Sustainability, vol. 13, no. 19, p. 10743, 2021.

[33] M. Almseidin et al., "Evaluation of Machine Learning Algorithms for Intrusion Detection System," in Proc. IEEE 15th International Symposium on Intelligent Systems and Informatics (SISY), IEEE, 2017.

[34] R. J. Alzahrani and A. Alzahrani, "Security Analysis of DDoS Attacks Using Machine Learning Algorithms in Network Traffic," Electronics, vol. 10, no. 23, p. 2919, 2021.

[35] E. E. Abdallah and A. F. Otoom, "Intrusion Detection Systems Using Supervised Machine Learning Techniques: A Survey," Procedia Computer Science, vol. 201, pp. 205–212, 2022.

[36] V. Gaur and R. Kumar, "Analysis of Machine Learning Classifiers for Early Detection of DDoS Attacks on IoT Devices," Arabian Journal for Science and Engineering, vol. 47, no. 2, pp. 1353–1374, 2022.

[37] I. Sofi, A. Mahajan, and V. Mansotra, "Machine Learning Techniques Used for the Detection and Analysis of Modern Types of DDoS Attacks," International Research Journal of Engineering and Technology, vol. 4, no. 6, pp. 1085–1092, 2017.

[38] I. Hidayat, M. Z. Ali, and A. Arshad, "Machine Learning-Based Intrusion Detection System: An Experimental Comparison," Journal of Computational and Cognitive Engineering, vol. 2, no. 2, pp. 88–97, 2023.

[39] R. R. R. Robinson and C. Thomas, "Ranking of Machine Learning Algorithms Based on the Performance in Classifying DDoS Attacks," in Proc. IEEE Recent Advances in Intelligent Computational Systems (RAICS), IEEE, 2015.

[40] Z. Ahmad, A. Shahid Khan, C. W. Shiang, J. Abdullah, and F. Ahmad, "Network Intrusion Detection System: A Systematic Study of Machine Learning and Deep Learning Approaches," Transactions on Emerging Telecommunications Technologies, vol. 32, no. 1, e4150, 2021.