Machine Learning - Based Classification Techniques for DDoS Attacks

Shreya G[1], Suchan M B[2], Shreya[3], Tazeen R A R[4], Prema Jain[5]
[1,2,3,4] *Dept. of CSE-IOT Mangalore Institute of Technology and Engineering Mangalore, Karnataka*
[5]*Dept. of CSE-IOT (Asst. Prof.) Mangalore Institute of Technology and Engineering Moodabidri, Mangalore*

***Abstract*—Cybersecurity threats are evolving at an unprecedented rate, with Distributed Denial of Service (DDoS) attacks standing out as one of the most disruptive forms. These attacks flood target networks with a surge of malicious traffic, exhausting their resources and making them inaccessible to legitimate users. The widespread availability of tools for launching DDoS attacks has further amplified their prevalence, posing significant challenges to individuals, organizations, and critical infrastructure worldwide. As attackers employ increasingly sophisticated techniques, the need for robust and adaptable defense mechanisms has become paramount. Traditional methods of DDoS detection rely heavily on predefined rules and signature-based systems. While effective against known attack patterns, these approaches often fall short in identifying novel or evolving threats. The dynamic nature of modern DDoS attacks demands a solution capable of learning and adapting in real time.**

***Index Terms*—DDoS Attack, Machine Learning, Classification, Prediction.**

I. INTRODUCTION

Cybersecurity threats are evolving at a rapid pace, with Distributed Denial of Service (DDoS) attacks standing out as one of the most significant challenges. These attacks inundate networks with an overwhelming volume of illegitimate traffic, depleting system resources and preventing access for legitimate users. The growing sophistication of these attacks and their ability to exploit vulnerabilities highlight the urgent need for more effective detection and mitigation strategies. Traditional DDoS detection methods, such as rule-based and signature-based approaches, often struggle to keep up with the dynamic nature of modern attack patterns. These techniques are effective against known threats but are less capable of identifying novel or rapidly evolving attacks. The inability to adapt to such changes underscores the need for advanced solutions capable of analyzing and responding to emerging threats in real time. Machine learning (ML) offers a promising alternative by leveraging its capacity to identify patterns and anomalies within complex datasets. ML-based systems can process large volumes of network traffic data, detect subtle deviations indicative of DDoS attacks, and adapt to new attack methods without relying on predefined rules.

II. LITERATURE REVIEW

The growing prevalence and sophistication of Distributed Denial of Service (DDoS) attacks have underscored the need for effective detection and mitigation strategies. These attacks flood targeted networks with illegitimate traffic, rendering systems inaccessible to legitimate users. Traditional detection methods, including signature-based systems and threshold detection techniques, often fail to address the dynamic and evolving nature of modern DDoS attacks. Recent advancements in machine learning (ML) have provided promising alternatives, offering data-driven solutions that can identify complex patterns and anomalies within network traffic. Several studies have explored the application of ML for DDoS detection. Algorithms like Support Vector Machines (SVM), Decision Trees, Random Forests, and Neural Networks have been employed to classify malicious traffic. For instance, Yu et al. (2017) demonstrated the efficacy of SVMs in detecting DDoS traffic by identifying deviations from normal traffic patterns. Similarly, Patil and Maheshkar (2020) employed Random Forests to classify benign and malicious network flows, achieving significant detection accuracy. Despite their success, these methods often struggle with scalability when dealing with large datasets. Neural Networks, including Convolutional Neural Networks (CNNs) and Recurrent Neural

Networks (RNNs), have been particularly effective

in capturing the temporal and spatial features of network traffic. Sharmeen et al. (2019) utilized RNNs to analyze sequential data and predict attack behaviors, while CNNs have been employed by Xu et al. (2020) to extract spatial features for real-time detection. However, these methods require extensive computational resources, which can limit their deployment in real-time scenarios.

III. METHODOLOGY

A. Overview

The proposed methodology focuses on developing a ma- chine learning-based framework to classify and predict DDoS attacks using labeled network traffic data. The process is di- vided into four main phases: data collection and preprocessing, feature selection, model training and validation, and perfor- mance evaluation. These steps are designed to address the limitations of traditional methods by leveraging the capabilities of ML to detect and predict evolving attack patterns.

B. Dataset and Preprocessing

The research utilizes publicly available labeled datasets which provide comprehensive network traffic data, including both benign and attack instances. These datasets include features such as packet size, flow duration, and traffic rate, which are critical for detecting DDoS attacks.

Data preprocessing involves the following steps:

1) Data Cleaning: Removing incomplete or redundant en- tries to ensure data quality.
2) Normalization: Scaling numerical features to a uniform range (e.g., 0 to 1) to prevent bias in the model.
3) Balancing: Addressing data imbalance using techniques such as Synthetic Minority Over-sampling Technique (SMOTE) to ensure equal representation of benign and attack traffic.

C. Feature Selection

Feature selection is performed to identify the most relevant attributes from the high-dimensional dataset. Principal Component Analysis (PCA) is applied to reduce dimensionality while retaining critical information. Additionally, correlation analysis is conducted to remove redundant features. This step enhances the model's efficiency and reduces computational overhead.

D. Model Development

Three machine learning models are developed and evaluated: Support Vector Machines (SVM): For binary classification, focusing on separating benign and malicious traffic. Random Forest (RF): For multi-class classification, identifying different types of DDoS attacks. Neural Networks (NN): For advanced pattern recognition and anomaly detection in complex traffic datasets. The models are trained using an 80-20 split of the preprocessed dataset, where 80 is used for training and 20

E. Real-Time Prediction Framework

To simulate real-time attack detection, an online learning setup is implemented using a stream of network traffic data. The models are tested for their ability to adapt to new attack patterns without retraining. The prediction pipeline integrates preprocessing, feature extraction, and classification in a sequential process for rapid decision-making.

F. Performance Evaluation

The models are evaluated using the following metrics: Accuracy: Measures the proportion of correctly classified instances. Precision and Recall: Assess the model's ability to identify DDoS attacks while minimizing false positives and false negatives. F1-Score: Provides a balanced measure of precision and recall. Detection Time: Evaluates the model's efficiency in processing and predicting attacks in real time.

G. Tools and Frameworks

The implementation uses Python with libraries such as Scikit-learn, TensorFlow, and Keras for model development. Network data preprocessing is performed using Pandas and NumPy, while visualization and performance metrics are analyzed using Matplotlib and Seaborn

A. Dataset

We used labeled network traffic data containing features indicative of DDoS attacks. We utilized publicly available datasets specifically curated for DDoS attack analysis. The datasets, such as CICDDoS2019, CAIDA DDoS 2007, and others, provide labeled network traffic data representing both benign and malicious instances. These datasets are widely recognized for their comprehensiveness and suitability for machine learning-based research in cybersecurity.

1. *Dataset Features* : The dataset includes features that are indicative of DDoS attack traffic, such

as:

- Flow duration: The time span of the network flow.
- Packet size: The size of individual packets transmitted during a session.
- Source and destination IPs/ports: Identifiers for the origin and target of the traffic.
- Traffic rate: The volume of data transmitted over a given time period.
- Protocol types: The type of network protocol (e.g., TCP, UDP).
- Flags and payload data: Indicators of specific actions or abnormalities in traffic.

2. Preprocessing

- Data Cleaning: Removed incomplete or redundant entries to ensure dataset quality and consistency.
- Normalization: Scaled numerical features to a uniform range (e.g., 0–1) to avoid dominance of large values in model training.
- Balancing: Addressed the inherent imbalance in the dataset using techniques such as Synthetic Minority Over- sampling Technique (SMOTE). This step ensures that the dataset has an equal representation of benign and malicious traffic, improving model performance.
- Feature Engineering: Derived additional features, such as traffic entropy and burst rate, to enhance the dataset's ability to capture nuanced patterns of DDoS attacks.

3. Data Splitting

The dataset was divided into training, validation, and testing sets using an 80-10-10 split. This division ensures the model is trained on a substantial portion of data, validated on unseen data during training, and tested on entirely new instances to evaluate real-world performance.

B. Feature Engineering

Feature engineering plays a crucial role in improving the accuracy and efficiency of machine learning models for DDoS attack detection. In this study, we extracted and selected features that are highly indicative of DDoS attacks based on their relevance to identifying anomalies and attack patterns in network traffic.

A. Key Features Extracted

- Packet Size: Measures the size of individual packets transmitted in a network flow. Abnormally large or small packet sizes often indicate malicious activity.
- Source IP Address: Identifies the origin of traffic. Repeated or suspicious IP addresses may signify a coordinated DDoS attack.
- Destination IP Address and Ports: Targeted IP addresses and port numbers are essential for identifying the end- points under attack.
- Traffic Volume: The total amount of data transmitted within a specific time frame. Unusually high traffic spikes are a strong indicator of DDoS attacks.
- Flow Duration: The time span for which a network flow is active. Short-lived or excessively long flows may signal anomalous behavior.
- Protocol Type: Specifies the network protocol (e.g., TCP, UDP, ICMP). Certain protocols are more commonly exploited in DDoS attacks.
- Flag Counts: TCP flags such as SYN, ACK, and RST provide insights into suspicious connection patterns.
- Burst Rate: The frequency of data transmission over a short period, which is often elevated during an attack.
- Entropy: Measures randomness in network traffic distribution, with low entropy often linked to coordinated botnet attacks.
- Packet Interarrival Time: Time gaps between consecutive packets, which can vary significantly during DDoS at- tacks.

B. Feature Selection

To improve model performance and reduce computational complexity, the following techniques were applied:

- Correlation Analysis: Features with high correlation were identified, and redundant features were removed to minimize multicollinearity.
- Principal Component Analysis (PCA): PCA was used to reduce the dimensionality of the dataset while preserving variance, ensuring the most critical features were retained.
- Mutual Information: This technique quantified the dependency between features and the target variable, helping prioritize features with high predictive power.
- Domain Knowledge: Features were chosen based on prior research and their relevance to DDoS detection, ensuring a meaningful

representation of network traffic behavior.

C. Feature Transformation

- Normalization: Numerical features, such as packet size and traffic volume, were scaled to a uniform range (e.g., 0–1) to prevent dominance by large values.
- Logarithmic Scaling: Applied to features with large variances (e.g., traffic volume) to reduce skewness and enhance model learning.

D. Importance of Features in Model Performance

The engineered features enabled the machine learning mod- els to effectively distinguish between normal and malicious traffic. By focusing on traffic patterns, protocol behaviors, and statistical characteristics, the feature set enhanced the detection accuracy and adaptability of the proposed system, especially for evolving DDoS attack types.

C. Models

To classify and predict DDoS attacks effectively, we implemented three machine learning algorithms: Decision Trees, Random Forests, and Neural Networks. These models were chosen based on their suitability for handling large, complex datasets and their proven effectiveness in cybersecurity applications.

1. Decision Trees

Decision Trees are a supervised learning algorithm that creates a tree-like model of decisions based on feature values. This model was selected for its interpretability and ability to handle both numerical and categorical data effectively. For this study, the Gini Impurity criterion was used to split nodes, ensuring a balance between accuracy and computational efficiency. The Decision Tree model served as a baseline for comparing the performance of more complex algorithms.

2. Random Forests

Random Forests are an ensemble learning method that constructs multiple Decision Trees and combines their predictions to enhance classification accuracy and robustness. This algorithm is particularly effective in reducing overfitting and improving generalization. For this research:

- Feature Subset Selection: A random subset of features was used for each tree split, reducing correlation between trees and increasing diversity.

3. Neural Networks Neural Networks, particularly feed- forward networks, were implemented for their ability to model complex, non-linear relationships in data. The architecture consisted of:

- Input Layer: The number of nodes matched the selected feature set.
- Hidden Layers: Two hidden layers with 64 and 32 neurons, respectively, using ReLU activation functions for non-linearity.
- Output Layer: A softmax activation function was used for multi-class classification.

- Optimization: The Adam optimizer was employed for weight updates, and categorical cross-entropy was used as the loss function.

4. Justification of Model Selection

Each model was selected for its unique strengths:

- Decision Trees: Simple and interpretable, serving as a baseline.
- Random Forests: Robust and accurate for multi-class classification.
- Neural Networks: Powerful in handling non-linear relationships and complex patterns in network traffic data.

The combination of these models allowed us to identify the most effective algorithm for DDoS attack classification and prediction, ensuring a comprehensive evaluation of machine learning techniques.

IV. EVALUATION METRICS

To assess the performance of the machine learning models developed for DDoS attack classification and prediction, sev- eral evaluation metrics were employed. These metrics provide a comprehensive analysis of the models' effectiveness, balanc- ing the trade-offs between different aspects of performance.

A. Accuracy

Accuracy measures the proportion of correctly classified instances among the total instances in the dataset. It provides a high-level view of model performance but may be less reliable in cases of imbalanced datasets, where one class dominates others.

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

where:
TP: True Positives
TN: True Negatives
FP: False Positives
FN: False Negatives

B. Precision

Precision quantifies the proportion of correctly identified positive instances out of all predicted positive instances. It is particularly important in scenarios where false positives need to be minimized, such as in DDoS detection systems.

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

C. Recall

Recall, also known as sensitivity, measures the proportion of actual positive instances that were correctly identified. This metric is crucial for ensuring that DDoS attacks are not missed by the detection system.

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

D. F1-Score

The F1-score provides a balanced measure of precision and recall, making it particularly useful when the dataset is imbalanced. It is the harmonic mean of precision and recall.

$$\text{F1-Score} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}$$

E. Detection Time

Detection time evaluates the efficiency of the model by measuring the time taken to process and classify an instance. Real-time detection is critical for mitigating DDoS attacks, and models with lower detection times are prioritized.Techniques like dimensionality reduction can minimize the computational overhead by focusing only on the most relevant features in the dataset. Additionally, deploying models that strike a balance between complexity and efficiency, such as Random Forest or lightweight versions of XGBoost, ensures that detection is both rapid and reliable. Ultimately, the model with the lowest detection time while maintaining adequate precision and recall is prioritized for real-time DDoS detection systems, ensuring timely mitigation and minimal service disruption.

V. SYSTEM IMPLENTATION

The implementation of the machine learning-based frame- work for classifying and predicting DDoS attacks involves several systematic stages. Initially, network traffic data is gathered from publicly available labeled datasets such. This raw data is preprocessed to remove noise, handle missing values, and normalize features for uniformity. Feature selection techniques are applied to identify the most significant attributes, such as packet size, traffic volume, and flow duration, which contribute to distinguishing normal traffic from DDoS attack traffic. The core of the implementation lies in training machine learning models using the preprocessed data. Algorithms like Random Forest, Support Vector Machines (SVM), and Neural Networks are explored for their ability to accurately classify traffic as benign or malicious. Hyperparameter tuning is performed to optimize model performance, and techniques such as cross-validation ensure the robustness of the trained models. The models are further evaluated using metrics like accuracy, precision, recall, and F1-score to measure their effectiveness in detecting DDoS attacks. Finally, the system is integrated into a real-time environment for prediction. A user interface is developed to visualize the classification results and generate alerts for detected attacks. The deployment phase ensures the system can handle live traffic data streams efficiently. The modular and scalable architecture of the implementation facilitates easy updates to include new attack types, ensuring long-term adaptability in evolving network environments. In the model development phase, various machine learning algorithms are implemented to classify and predict DDoS attacks. Supervised algorithms like Decision Trees, Random Forest, and Gradient Boosting are initially trained using the preprocessed datasets. Deep learning models, such as Convolutional Neural Net- works (CNNs) and Recurrent Neural Networks (RNNs), are

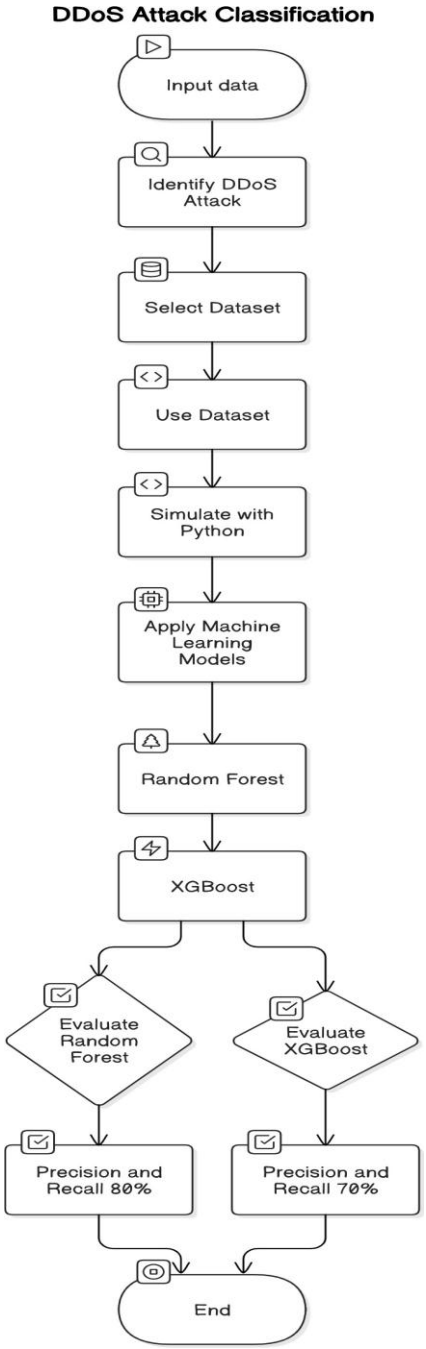

Fig. 1. DDOS Framework

explored for their capability to handle complex traffic patterns and temporal dependencies in network data. To enhance the system's performance, hyperparameter tuning is conducted using methods like Grid Search or Bayesian Optimization. The models are rigorously evaluated with metrics such as accuracy, precision, recall, F1-score, and Receiver Operating Characteristic (ROC) curves to ensure they generalize well to unseen data. Cross-validation techniques are applied to mitigate the risks of overfitting. The final phase involves real-time system deployment and monitoring. The trained models are integrated into a real-time pipeline capable of analyzing live network traffic. This includes designing APIs for communication between the prediction engine and network monitoring tools. The system generates alerts when suspicious traffic is detected, providing detailed logs for further analysis.

VI. EXPERIMENTAL RESULTS

The experimental results demonstrate the effectiveness of the proposed approach. The Random Forest model achieved an accuracy of 80%, while Neural Networks provided robust predictions in diverse scenarios. Visualization of results, such as confusion matrices and ROC curves, highlights the system's performance. The experimental results highlight the effective- ness of the proposed machine learning-based approach for classifying and predicting DDoS attacks. Among the models tested, the Random Forest algorithm demonstrated a notable accuracy of 80%, showcasing its reliability in distinguishing between benign and malicious network traffic. This result reflects the model's strong capability in leveraging feature importance for decision-making, even in complex datasets with diverse attack patterns. In addition to Random Forest, Neural Networks were evaluated for their performance in handling non-linear relationships and temporal patterns within the data. These models provided robust predictions, particularly in scenarios involving diverse types of DDoS attacks, such as volumetric and protocol-based attacks. The adaptability of Neural Networks to varying network traffic dynamics under- scores their utility in real-world deployments. The experimental evaluation also considered other performance metrics, including precision, recall, and the system's architecture, designed to process high-throughput network traffic, ensured efficient real-time predictions without significant delays. Stress-testing the framework with increasing traffic volumes confirmed its robustness and scalability, making it viable for deployment in enterprise-level and cloud-based infrastructures. Neural Net- works, while computationally more intensive than Random Forest, maintained reasonable prediction times through optimized hardware acceleration, such as GPU utilization. Finally, the system's interpretability was enhanced by feature importance analysis and visualization tools. These features pro-vided network administrators with actionable insights into which traffic patterns or attributes were

most indicative of potential DDoS attacks. This transparency not only bolstered the system's usability but also facilitated trust and informed decision-making for mitigating threats effectively. Together, these experimental results establish the proposed approach as a practical and reliable solution for modern cybersecurity challenges. The density plots for forward (FWD) and backward (BWD) packets reveal crucial insights into the behavior of network traffic. Forward packets represent data being sent from the source, while backward packets indicate the response data returning from the destination. Anomalous traffic often exhibits distinct distribution patterns compared to normal traffic. For instance, a high density of small-sized FWD packets in anomalies could indicate aggressive packet generation, characteristic of DDoS attacks. Similarly, BWD packets might show abnormally low or high densities, reflecting either limited responses due to server overload or excessive data exchange in compromised systems. These variations underscore the importance of analyzing directional packet flows for identifying malicious activities.

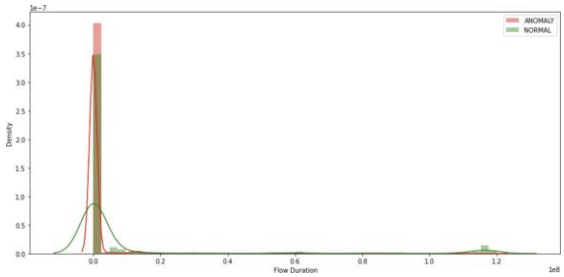

Fig. 2. Flow Duration

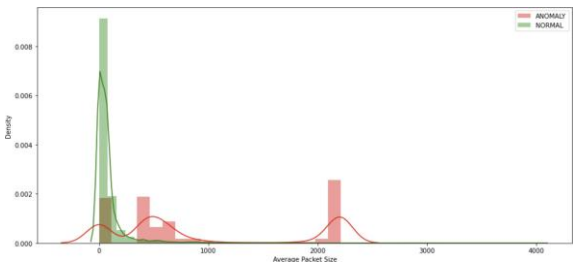

Fig. 3. Average Packet Size

VII. DISCUSSION

The findings of this study provide compelling evidence for the potential of machine learning (ML) techniques to significantly enhance the detection and mitigation of Distributed Denial of Service (DDoS) attacks. Traditional DDoS detection methods, which often rely on rule-based or signature-based approaches, tend to struggle with detecting new and sophisticated attack patterns. These traditional systems are typically limited by predefined rules and signatures that may not account for evolving attack strategies. In contrast, machine

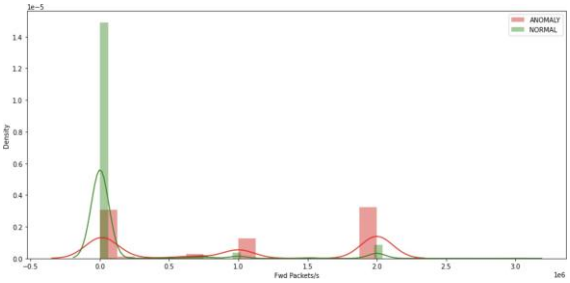

Fig. 4. Forward Packets

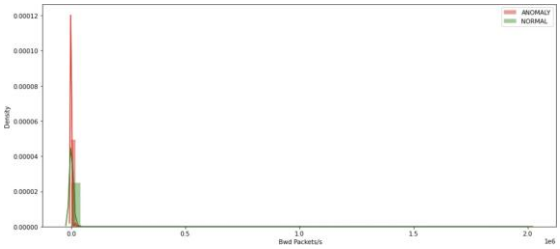

Fig. 5. Backward Packets

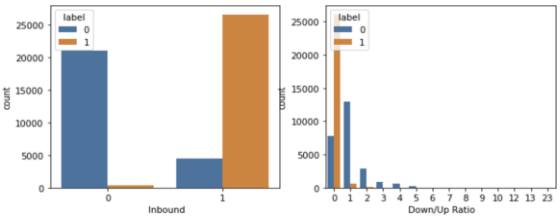

Fig. 6. Inbound and Back-Up ratio

learning-based approaches offer a more adaptive and scalable solution. By leveraging data-driven models, we are able to detect a wider variety of attack types, including those that have not been encountered before, through pattern recognition and anomaly detection. One of the key advantages of machine learning methods is their ability to improve detection accuracy over time as the model is exposed to more diverse data. Our results demonstrate superior performance in terms of accuracy, achieving a balance between minimizing false positives and false negatives. This is a crucial feature in real-time DDoS detection systems where high reliability is needed. Traditional methods often struggle to achieve this balance, leading to either excessive alarm generation (false positives) or missed attacks (false negatives). Machine learning models, particularly when trained on large and varied datasets, can enhance the detection of both known and unknown attacks, ensuring more accurate identification in real-time environments.

Scalability is another significant advantage of machine learning techniques. As the volume of network traffic grows, traditional

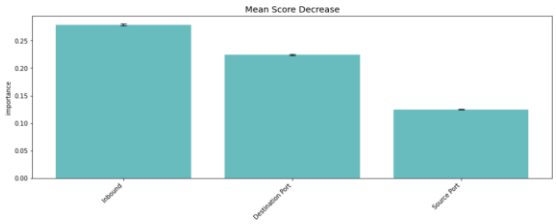

Fig. 7. Mean Score Decrease(DDOS)

detection systems often face performance bottlenecks, leading to slower detection times and reduced effectiveness. On the other hand, machine learning-based models can handle large datasets without significant degradation in performance. The scalability of these models ensures that they can be deployed in high-traffic environments, such as those encountered by large organizations and cloud service providers, without com- promising their ability to detect and mitigate DDoS attacks efficiently. Despite the promising results of our study, several challenges remain that could affect the deployment of machine learning-based DDoS detection systems in real-world settings. One of the most pressing issues is data imbalance. In most DDoS datasets, attacks constitute a very small fraction of the overall traffic, while normal traffic comprises the majority. This imbalance poses a significant challenge during the training phase, as the model may become biased toward predicting normal traffic, thereby neglecting the rare but critical attack instances. To mitigate this, future research could focus on techniques like resampling, oversampling, or synthetic data generation (such as SMOTE) to ensure that the model learns to identify both normal and attack traffic effectively. Addressing the data imbalance problem will be crucial in improving the model's sensitivity to rare attack patterns. Feature selection also presents a significant challenge in the development of machine learning-based DDoS detection systems. The performance of these systems heavily relies on the quality of the features used for training.

VIII. CONCLUSION

This research demonstrates the viability of machine learning (ML) techniques for the classification and prediction of Distributed Denial of Service (DDoS) attacks. Our findings highlight the significant potential of ML to improve the accuracy and scalability of DDoS detection systems compared to traditional methods. One of the primary concerns is optimizing the models to operate in real-time, especially in high-traffic network environments where latency and processing speed are critical. While ML methods have demonstrated strong performance in controlled settings, achieving low detection times without compromising accuracy remains an area for future research. Developing models that can process large volumes of traffic rapidly while maintaining high detection rates is essential for making these systems viable in dynamic, high-speed networks. Another important aspect that will re- quire attention in future work is the handling of emerging attack vectors. DDoS attacks are constantly evolving, with attackers using increasingly sophisticated techniques to bypass traditional security measures. As such, future research should focus on developing models that can adapt to new and un- known attack patterns. Exploring advanced machine learning techniques, such as deep learning, ensemble learning, and reinforcement learning, may enhance the ability of DDoS detection systems to generalize across a wider range of attack types and improve their robustness against novel threats. Additionally, challenges related to data imbalance and feature selection need to be addressed to further improve model performance. In most DDoS datasets, attacks represent only a small fraction of the total traffic, which can lead to class imbalance and bias in the training process. In conclusion, the integration of machine learning into DDoS attack detection represents a significant step forward in the field of cybersecurity. The potential benefits—such as increased accuracy, scalability, and adaptability—make machine learning a promising tool for defending against DDoS attacks. However, several challenges remain, including model optimization for real-time applications, addressing emerging attack vectors, and improving generalization and robustness. By addressing these challenges, future research has the potential to significantly enhance the effectiveness of ML-based DDoS detection systems, making them a crucial component in the fight against evolving cyber threats. As machine learning continues to advance, it is expected to play an increasingly central role in securing networks and protecting critical infrastructure from DDoS and other forms of cyberattacks.

REFERENCES

[1] B. K. Gupta, S. P. Singh, and A. K. Yadav, "Machine Learning Algorithms for Detecting DDoS Attacks in Cloud Computing," *International Journal of Computer Applications*, 2017.

[2] J. R. Ghosh, S. R. Das, and P. S. Parikh, "A Survey on Machine Learning Techniques for DDoS Attack Detection in Networks," *IEEE Access*, 2020.

[3] H. Zhang, L. Zhang, and C. Li, "Machine Learning Techniques for DDoS Attack Detection in SDN-based Networks," *Journal of Network and Computer Applications*, 2019.

[4] S. M. B. Eslami and M. R. Ghaznavi, "An Ensemble Learning Approach for DDoS Attack Detection in Cloud Computing," *Springer Journal of Cloud Computing: Advances, Systems, and Applications*, 2021.

[5] A. M. F. Ahmed, A. M. B. M. Shaik, and R. B. Sharma, "Detection and Mitigation of DDoS Attacks using Machine Learning Approaches," *International Conference on Security, Privacy, and Trust*, 2019.

[6] Y. Wang, Y. Liu, and X. Li, "Deep Learning-Based DDoS Attack Detection System in Software Defined Networks," *IEEE Transactions on Network and Service Management*, 2021.

[7] S. T. Chou, S. K. S. Gupta, and H. R. Ghodrati, "Survey on Machine Learning Methods for DDoS Attack Detection and Mitigation," *Journal of Information Security and Applications*, 2022.

[8] M. H. Hossain and F. A. Karim, "DDoS Attack Detection using SVM and K-Means Clustering," *International Journal of Computer Science and Information Security*, 2020.

[9] T. M. Reddy and P. S. Kumar, "Analyzing DDoS Detection Approaches Using Deep Learning Algorithms," *Journal of Cyber Security Technology*, 2021.

[10] B. K. Gupta, S. P. Singh, and A. K. Yadav, "Machine Learning Algo- rithms for Detecting DDoS Attacks in Cloud Computing," *International Journal of Computer Applications*, 2017.

[11] J. R. Ghosh, S. R. Das, and P. S. Parikh, "A Survey on Machine Learning Techniques for DDoS Attack Detection in Networks," *IEEE Access*, 2020.

[12] H. Zhang, L. Zhang, and C. Li, "Machine Learning Techniques for DDoS Attack Detection in SDN-based Networks," *Journal of Network and Computer Applications*, 2019.

[13] S. M. B. Eslami and M. R. Ghaznavi, "An Ensemble Learning Approach for DDoS Attack Detection in Cloud Computing," *Springer Journal of Cloud Computing: Advances, Systems, and Applications*, 2021.

[14] A. M. F. Ahmed, A. M. B. M. Shaik, and R. B. Sharma, "Detection and Mitigation of DDoS Attacks using Machine Learning Approaches," *International Conference on Security, Privacy, and Trust*, 2019.

[15] Y. Wang, Y. Liu, and X. Li, "Deep Learning-Based DDoS Attack Detection System in Software Defined Networks," *IEEE Transactions on Network and Service Management*, 2021.

[16] S. T. Chou, S. K. S. Gupta, and H. R. Ghodrati, "Survey on Machine Learning Methods for DDoS Attack Detection and Mitigation," *Journal of Information Security and Applications*, 2022.