Beyond Binary: Unveiling the Multi-Type Dynamics of DDoS Attacks through Advanced Machine Learning and Ensemble Methods

1st Mohamed Salah
Electrical and Computer Engineering
University of Ottawa - Faculty of Engineering
Cairo, Egypt
mgabr024@uottawa.ca

2nd Mohamed Hany
Electrical and Computer Engineering
University of Ottawa - Faculty of Engineering
Cairo, Egypt
mmost018@uottawa.ca

3rd Mohamed Salem
Electrical and Computer Engineering
University of Ottawa - Faculty of Engineering
Cairo, Egypt
mebai026@uottawa.ca

4th Andrew Doss
Electrical and Computer Engineering
University of Ottawa - Faculty of Engineering
Cairo, Egypt
adoss072@uottawa.ca

Abstract*—Detecting and classifying various types of distributed denial-of-service (DDoS) attacks in real time is paramount for effective cybersecurity. Traditional DDoS detection methods often focus on binary outcomes, determining whether an attack is present or not. In our enhanced approach, we shift the paradigm towards multi-type DDoS attack detection, aiming to classify and identify specific attack types. This evolution requires overcoming challenges associated with feature selection and addressing data deficiencies in real-world datasets. Our project delves into the intricacies of DDoS attacks by leveraging advanced machine learning techniques. We explore a diverse range of feature selection methods, including filter, wrapper, and embedded techniques, to identify the most relevant features for multi-type DDoS detection. To enhance the accuracy and robustness of our models, we harness the power of ensemble methods such as Random Forest, Gradient Boosting, and Stacking, capitalizing on their collective strengths to discern between different DDoS attack categories. Additionally, we tackle the complexity of real-world datasets by employing various strategies. These approaches aim to mitigate data deficiencies and enhance the generalization capability of our models across different types of DDoS attacks. The effectiveness of our multi-type DDoS detection system is rigorously assessed using a comprehensive suite of cybersecurity metrics, including precision, recall, F1-score, and ROC AUC. By shifting our focus from binary detection to multi-type classification, we present a nuanced and robust solution for identifying and categorizing diverse DDoS attacks. Our thorough evaluation methodology ensures a confident assessment of the system's performance under varied cyber threat scenarios.In a significant stride toward refining our models, we achieved a noteworthy improvement, surpassing the baseline by an impressive margin of 1%. This enhancement underscores the efficacy of our tailored approach in elevating the performance of our models, providing a crucial edge in the dynamic landscape of DDoS attack detection.

I. Introduction

A Distributed Denial of Service (DDoS) attack is a menacing and disruptive cyber threat that aims to compromise the availability and reliability of online services and websites. DDoS attacks involve a coordinated effort to flood a target system with an overwhelming volume of traffic, rendering it inaccessible to legitimate users. The" distributed" aspect of DDoS attacks refers to the use of multiple compromised devices, often part of a botnet, to launch the assault, making it difficult to pinpoint the source of the attack. The primary objective of a DDoS attack is to exhaust the target's network resources, such as bandwidth, server capacity, or application resources, to the point where it can no longer respond to legitimate user requests. DDoS attacks can take various forms, including volumetric attacks that flood the target with massive amounts of data, protocol attacks that exploit vulnerabilities in network protocols, and application layer attacks that target the application or web server itself. These attacks can have severe consequences, ranging from service disruption and financial losses to reputational damage. To counteract DDoS attacks, organizations employ a combination of strategies, including traffic filtering, rate limiting, and the use of content delivery networks (CDNs) to absorb and mitigate malicious traffic. There are many different types of DDoS attacks. According to [1][8], there are two main categories of DDoS attacks: reflection-based and exploitation-based. Every DDoS attack can be classified as either of these two types. Detecting Distributed Denial of Service (DDoS) attacks is a critical component of modern cybersecurity, essential for preserving the availability and reliability of online services. DDoS attacks pose a significant threat by inundating target systems with a massive volume of malicious traffic, rendering them inaccessible to legitimate users. The figure 1, taken from the recent 2020 article by Cloudflare [2][9] depicts the seriousness to classify the type of DDoS attack as SYN type took up to 60% of attack vectors in first Quarter of 2020, so a need

to correctly detect them as early as possible arises. A study conducted by Kerbson Security mentioned in the study by Li.et.al [3][10] reveals that for each one of DDoS attacks it may have incurred a cost of $323, 973.75 to the device owners with an additional cost to the excess use of power and bandwidth. Detecting such attacks requires a multifaceted approach that combines various methods and technologies. One of the main issues with internet security is the criticality of the situation, which has given rise to numerous statistical detection techniques as wavelet-based, port entropy-based, destination entropy-based, and others. All these approaches, however, take a lot of time and are ineffective because the internet is a dynamic industry that is always evolving. As a result, several academics turned to artificial intelligence and machine learning techniques to identify the DDoS attack to address these problems. Since it is simple to update ML and AI models, we were inspired to use effective machine learning and artificial intelligence techniques to capture the variability of the changing internet domains, despite the lack of literature to categorize DDoS attacks into different types. However, the computational complexity and prediction time increase due to the large dataset with 87 features. To address that, we used the ExtraTrees classifier technique for feature selection to choose the top 20 relevant features. The baseline models and advanced models covered in detail in section 4 are applied in this study. Furthermore, the study introduces the Ensemble Classifier MV-4, which provides a good performing classifier for this dataset by combining the performance of the 6 AI/ML models. To sum up we discovered new knowledge about the effectiveness of feature selection and ensemble methods in the context of multi-type DDoS detection.

II. Related Work

Chu et al.'s [4] study proposes a novel machine learning (ML)-based DDoS detection model using the random forest algorithm and trained on the CICDDoS2019 dataset, a large and comprehensive dataset of network traffic flow records from both normal and attack traffic. The authors' goal is to develop a robust and effective DDoS detection solution that addresses the limitations of existing ML-based DDoS detection systems, such as low accuracy rates, high false positive rates, and lack of robustness against new and emerging attack vectors. The authors' approach is supported by various strategies, including hyperparameter optimization and diverse feature usage. Hyperparameter optimization is a technique for tuning the parameters of a machine learning model to achieve optimal performance. Diverse feature usage involves using a variety of features to train the model, which helps to improve its robustness and generalization ability. The authors' model was evaluated on a variety of metrics and real-world DDoS attack data. The results showed that the model achieved high accuracy rates and F1-scores and outperformed an existing state-of-the-art ML-based DDoS detection model. The model also demonstrated good robustness against a variety of DDoS attack types. Despite its promising results, the authors' model has some limitations. First, the model is limited in its exclusive reliance on the random forest algorithm. It is possible that other ML algorithms, such as support vector machines (SVMs) or neural networks, could achieve even better performance on the DDoS detection task. Second, the model's complexity and data requirements could be challenging for resource-constrained organizations. Finally, the authors miss an opportunity to explore different feature selection techniques that might further boost the model's performance.

Sofi et al. [5] conducted a comprehensive evaluation of machine learning classification techniques for detecting modern DDoS attacks. They aimed to assess the performance of various classifiers and identify the most effective one. Their research was motivated by the growing threat of DDoS attacks and the need for robust detection systems. To address this challenge, the authors developed a solution that involved training and evaluating four machine learning classifiers: Naïve Bayes, Multilayer Perceptron (MLP), Support Vector Machine (SVM), and Decision Trees. They used a dataset of modern DDoS attacks collected from a real-world honeypot network. Their study revealed that the SVM classifier outperformed the others, achieving an impressive accuracy rate of 99.5%. This suggests that machine learning is a promising approach for detecting modern DDoS attacks. One of the strengths of this study is its comprehensive evaluation of machine learning classifiers for DDoS attack detection. The authors also discuss the challenges associated with machine learning in DDoS attack detection and offer potential strategies to address them. However, a notable weakness is the limited focus on only four classifiers. Exploring other classifiers, including deep learning models, would provide a more comprehensive understanding of the landscape. Additionally, a comparison with existing DDoS attack detection systems would offer valuable insights into the system's competitiveness.

Maheswari et al.'s [6] research dedicated their research efforts to developing a machine learning-based approach to address the critical issue of detecting and mitigating DDoS attacks in network traffic. Their ultimate goal is to create a system that possesses the remarkable ability to accurately and efficiently identify these attacks, even when confronted with novel and unseen patterns. Simultaneously, they strive to formulate a mitigation strategy that effectively blocks and redirects malicious traffic, safeguarding network integrity. To realize these objectives, the researchers propose employing sophisticated models such as Long Short-Term Memory (LSTM), Support Vector Machine (SVM), and Logistic Regression. These models are meticulously trained on a dataset exclusively curated from Bennet University that encompasses a wide range of DDoS attacks. Unquestionably, the team's rationale behind selecting these models lies in their notable effectiveness in detecting various types of anomalies, including DDoS attacks. The proposed models exhibit exceptional strengths, most notably enhanced accuracy and

impressively low false positive rates, surpassing traditional methods in performance. In their analysis, the research paper acknowledges LSTM as the most accurate model among the three. Furthermore, the team introduces a mitigation strategy that is not only straightforward but also remarkably effective, providing the added advantage of seamless integration into existing network infrastructures. As with any research, it is important to recognize certain limitations presented in the paper. One such limitation is the absence of evaluation on real-world datasets, which could impact the generalizability of their findings. Additionally, the authors do not extensively discuss potential limitations of their approach, such as vulnerability to adversarial attacks and the necessity for continuous training to stay up-to-date with the ever-evolving techniques employed in DDoS attacks. Acknowledging these limitations provides an avenue for further exploration and refinement of their approach.

Marwane Zekri et al. [7] proposed this study which is about designing an efficient DDoS (Distributed Denial of Service) detection system for cloud computing environments. This system utilizes a multi-faceted approach, integrating the C.4.5 decision tree algorithm with signature detection techniques. By leveraging the C.4.5 algorithm, the research aims to develop an automatic and effective detection system capable of identifying signature-based attacks and abnormal traffic patterns associated with DDoS flooding. The proposed DDoS detection system is designed to enhance the security of cloud infrastructures and ensure their resilience against potential intrusions. It aims to foster a secure and trusted environment for the delivery of cloud services and the future Internet of Things (IoT). The methodology involves pre-processing captured packets, extracting relevant attributes, and training the decision tree to accurately classify the traffic patterns. The system's strength lies in its high detection accuracy, surpassing other machine learning techniques considered in the comparative analysis. It demonstrates a detection rate of over 98% and exhibits low false positive and false negative rates, ensuring precise and reliable identification of DDoS attacks. Moreover, the decision tree's implementation allows for efficient and rapid classification, resulting in a low computational cost and faster detection rate. However, the proposed system has certain limitations that need to be addressed. Its efficacy heavily relies on the availability and accuracy of the training data, making it susceptible to misclassifications when encountering previously unseen or evolving attack patterns. The reliance on signature-based detection methods could potentially hinder the system's ability to detect zero-day attacks or novel intrusion patterns lacking predefined signatures. Furthermore, the system's performance may be affected by the scalability of the network and the complexity of traffic patterns, posing challenges to the decision tree's classification accuracy. Ongoing research is necessary to address these limitations and further enhance the system's robustness and adaptability to evolving DDoS threats.

Fatmah Alanazi et al. [8] addressed the vulnerability of Software-defined Networks (SDNs) to critical cyber-attacks, particularly Distributed Denial of Service (DDoS) attacks, by proposing a more effective detection solution using deep learning (DL)-based ensemble techniques. The methodology involves the utilization of deep learning algorithms, including Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM), and Gated Recurrent Unit (GRU), in constructing an ensemble solution for DDoS attack detection in SDNs. Four hybrid models were created, employing a combination of ensemble techniques such as bagging and boosting and various DL architectures to improve the overall detection accuracy. The research utilized the CICIDS2017 dataset for experimentation, emphasizing the extraction of essential flow-based features and the application of data preprocessing techniques, including normalization and feature scaling, to ensure accurate and efficient classification of network traffic. By harnessing the strengths of the diverse DL architectures, the ensemble models provided a comprehensive analysis of network traffic, enabling the system to identify and classify potential threats with an impressive 99.77% accuracy rate in detecting DDoS attacks. However, the reliance on deep learning algorithms necessitates a significant amount of training data, potentially limiting the system's adaptability to evolving attack patterns. The computational complexity of the ensemble models could pose challenges in real-time implementation and deployment, warranting further optimization for practical use in large-scale SDN environments. Ongoing exploration and refinement of the proposed solution hold promise for establishing more comprehensive and robust approaches to enhance the security and resilience of SDNs against evolving cyber threats.

Katiravan et al. [9] proposed this study to explore the effectiveness of different machine learning algorithms in detecting DDoS attacks in network traffic data. They aimed to compare the performance of eight different algorithms and identify the best algorithm for detecting DDoS attacks with high accuracy and low false alarm rate. The authors uesd CIC IDS 2017 dataset which is most widely used dataset to detect the existence of DDoS or not. They started to preprocess the dataset to extract both independent and dependant variables from the dataset using iloc[] method and then used K fold Cross Validation intaking all models into account for train and test. They used different machine learning algorithms like (Logistic Regression, Random Forest Classifier, Support Vector Machine, Decision tree, Gaussian Naive Bayes and K-Nearest Neighbours). Based on the accuracy, precision, recall and FAR, They concluded that Random forest is the best model to detect DDoS. The paper has many strength points that it outlines a comprehensive methodology for detecting DDoS attacks using many different machine learning algorithms. The paper covers data preprocessing methods , model selection, and validation techniques such as K-Fold cross-validation. The use of the CIC-IDS2017 dataset for training and testing made the results more applicable

to real-world scenarios as it is recent and widely used for research in DDoS detection making the results more applicable to real-world scenarios. The paper considers some different machine learning algorithms for DDoS detection providing a comparative analysis of their performance allowing us to understand the strengths and weaknesses of different algorithms for this problem based on multiple performance metrics including accuracy, precision, recall, and false alarm rate to evaluate the effectiveness of the selected algorithms. This comprehensive evaluation provides a clear understanding of their capabilities. Authors used different graphical representations such as scatter plots and charts enhancing the presentation of results and making it easier for us to interpret and compare the performance of different algorithms. Despite many strenght points in paper but there are some weaknesses in it that the paper focuses on the selection of machine learning algorithms and does not discuss feature engineering or feature selection which is crucial for the success of machine learning models and its absence could be a limitation. The paper does not also address the scalability and real-world implementation of the proposed DDoS detection methods but discussing the challenges and considerations related to deploying these models in practical network environments would be very valuable in such problems. The paper mentions the false alarm rate (FAR) but it doesn't provide an in-depth analysis of false positives and their potential impact on network operations and security. The future work section lacks specific details without any detailed roadmap for future research in the field of DDoS detection.

R. Sahila Devi et al. [10] in the research paper titled " Investigation on Efficient Machine Learning Algorithm for DDoS Attack Detection" explored the use of Machine Learning (ML) technologies to detect DDoS attacks, which are becoming increasingly complex and difficult to detect. The main objective of this research is to identify the most reliable ML algorithm for DDoS attack detection. To achieve this goal, the authors built an ML DDoS detection model and compared various ML algorithms. They also proposed an efficient pre-processing approach for the CICDDoS2019 dataset and suggested a detection model that can classify DDoS attacks more rapidly and accurately than most recent methods. Additionally, they proposed an effective hybrid ML method for DoS/DDoS detection using estimator functions. The research highlights the proposed hybrid ML-DDoS detection approach, which is more accurate and efficient than most recent methods. The authors also provided an efficient pre-processing approach for the CICDDoS2019 dataset, which can be used in future research. However, the research only focuses on DDoS attacks and does not address other types of cyber-attacks. Additionally, the proposed hybrid ML method may require significant computational resources, which could limit its practicality in some scenarios. Overall, the research provides valuable insights into the use of ML technologies for DDoS attack detection and proposes an effective hybrid ML method for DoS/DDoS detection. However, further research is needed to address other types of cyber-attacks and to evaluate the practicality of the proposed hybrid ML method in real-world scenarios.

III. Methodology

A) Dataset Creation:

Our dataset creation process centered on the CIC2019-DDOS dataset, consisting of 10 CSV files representing diverse DDoS attack types. Combining these files yielded a substantial dataset with over 11 million data points. To manage computational resources effectively, we selectively imported specific sample ranges from each file. Following importation, we conducted a thorough analysis of the target feature—DDoS attack types—and identified and removed two irrelevant attack types. Null values and duplicate entries were systematically eliminated. Ensuring balanced representation across all attack types, we implemented a stratified sampling approach. A custom function dynamically oversampled or undersampled specific classes to achieve a target number of samples per class. Our goal was to attain a balanced dataset of 1 million records, achieved through iterative oversampling and undersampling based on class representation. To validate the success of our equalization efforts, we visualized the resulting balanced dataset through various plots. Subsequently, the preprocessed data was exported as a CSV file, seamlessly integrating into our main script for subsequent stages of feature engineering and model training.

Label	Distribution
DrDoS UDP	100000
DrDoS SSDP	100000
DrDoS MSSQL	100000
DrDoS SNMP	100000
DrDoS LDAP	100000
DrDoS NetBIOS	100000
DrDoS DNS	100000
UDP-lag	100000
Syn	100000
DrDoS NTP	100000

TABLE I
LABEL DISTRIBUTION

B) Feature Engineering:

To optimize our dataset for machine learning models, we initiated a two-step process. Initially, the dataset was divided into training (70%) and testing sets (30%) to ensure an unbiased model evaluation. Subsequently, label encoding was implemented to convert categorical columns into numeric representations suitable for machine learning algorithms. Following this, data standardization was performed to normalize the feature ranges of the input dataset, enhancing compatibility for subsequent analysis.

C) Feature Selection:

After implementing various feature engineering methods on the 'CIC-DDOS2019' dataset, we employed the Extremely Randomized Trees Classifier (Extra Trees Classifier) to

meticulously select the top 20 features. This strategic

Features	
Timestamp	Avg Fwd Segment Size
Source Port	min_seg_size_forward
Flow ID	Fwd Header Length
Min Packet Length	Fwd Header Length.1
Packet Length Mean	ACK Flag Count
Fwd Packet Length Mean	Flow Bytes/s
Max Packet Length	Protocol
Fwd Packet Length Min	Subflow Fwd Bytes
Fwd Packet Length Max	Destination Port
Average Packet Size	Fwd Packets/s

TABLE II
SELECTED FEATURES IN THE DATASET

selection was aimed at optimizing the dataset for later model training, ensuring that only the most relevant features contribute to the predictive accuracy of the models.

D) Machine Learning Models (Algorithms):
Our choice of machine learning algorithms for DDoS cyberthreat detection was grounded in considerations of low computational complexity and comparable performance. Each algorithm was carefully selected for its suitability in addressing the intricacies of our multi-class classification problem.

Algorithm	Training Complexity	Prediction Complexity
SVM	$O(n^2 f + n^3)$	$O(n_{sv} f)$
Random Forest	$O(n^2 f n_{trees})$	$O(f n_{trees})$
Logistic Regression	$O(nf)$	$O(f)$
Bagging	$O(Bnf)$	$O(Bf)$
AdaBoost	$O(nf)$	$O(f_{trees})$
Gradient Boosting	$O(nf_{trees})$	$O(f_{trees})$

Fig. 1. An informative caption for your figure.

Support Vector Machine (SVM):
Support vector machine (SVM) employs different techniques of supervised learning to tackle intricate classification, regression, and outlier detection challenges by executing optimized data transformations that delineate boundaries among data points, based on predefined classes, labels, or outputs. Support Vector Machines (SVMs) deal with multi-class classification tasks, such as our DDOS attack type classification problem, by employing strategies like One-vs-Rest (OvR). By transforming the multi-class problem into multiple binary classification sub-problems, SVMs aim to find the optimal hyperplane that maximizes the margin between 10 classes in a high-dimensional space. Using a kernel trick, SVMs can handle complex, non-linear decision boundaries. With OvR, each class is compared against all other 10 classes of our problem, The decision is made based on the class with the most supporting vectors or highest confidence score, enabling SVMs to effectively address multi-class classification challenges and achieve robust performance in various domains.

Random Forest:
Random Forest is a versatile ensemble learning method extensively used for multi-class classification tasks due to its ability to handle complex relationships within big data such as our 'CIC-DDOS2019' dataset. It constructs a multitude of decision trees by bootstrapping our 'CIC-DDOS2019' dataset and randomly selecting features at each node, aggregating their predictions through voting or averaging. In multi-class scenarios, Random Forest extends naturally by supporting multiple classes without requiring explicit modifications. By combining predictions from numerous decision trees, Random Forest generates robust classifications, effectively handling imbalanced data and noisy features while offering insights into feature importance. Its adaptability, capability to avoid overfitting, and straightforward implementation make Random Forest a popular choice for addressing multi-class classification challenges across various domains.

Logistic Regression:
Logistic Regression, while originally designed for binary classification, can be extended to handle our DDOS attack type classification problem through various techniques like One-vs-Rest (OvR). OvR trains multiple binary classifiers, each distinguishing one class from the rest, while multinomial logistic regression directly models the probabilities of each class of our 10 problem classes, utilizing the softmax function to assign probabilities across multiple classes. Despite its name, Logistic Regression isn't restricted to linear boundaries and can be augmented with polynomial terms or kernel tricks for non-linear decision boundaries. Its simplicity, interpretability, and efficiency in handling large datasets like our 'CIC-DDOS2019' dataset make Logistic Regression a valuable tool for our task, particularly when interpretability of results is crucial, although its performance might vary depending on the complexity and nature of the data.

Bagging:
Bagging (Bootstrap Aggregating) is an ensemble learning technique that can effectively handle multi-class classification problems, by leveraging multiple base classifiers. By creating multiple subsets of the training data through bootstrapping and training a diverse set of classifiers on these subsets, Bagging reduces variance and overfitting. For our DDOS attack type classification problem, Bagging can employ various base classifiers like decision trees, producing an ensemble that combines their predictions through averaging or voting to determine the final class. This approach enhances the model's stability, robustness, and generalizability, making Bagging a valuable technique for our problem, particularly when aiming to improve accuracy and reduce the impact of noisy data or outliers in other diverse datasets.

AdaBoost:
AdaBoost (Adaptive Boosting) is a powerful ensemble learning method that can be effectively extended for multi-class classification tasks Such as our DDOS attack type

classification problem. It sequentially trains a series of weak learners, assigning higher weights to misclassified instances in each subsequent iteration, thereby focusing on the more challenging samples. For our multi-class classification problem, AdaBoost can employ strategies like One-vs-Rest (OvR) to handle all 10 classes. OvR trains multiple classifiers, each distinguishing one class from the rest, AdaBoost combines these classifiers' outputs through weighted voting to determine the final class. Its ability to improve model performance by focusing on misclassified instances and adaptively adjusting weights makes AdaBoost an appropriate choice for our multi-class classification task, especially when seeking to enhance overall accuracy and handle complex decision boundaries in diverse datasets.

Gradient Boosting:
Gradient Boosting is an ensemble learning technique that can be extended to effectively address multi-class classification tasks, such as our DDOS attack type classification task, by combining multiple weak learners into a strong predictive model. Algorithms like XGBoost, LightGBM, and CatBoost, built on the principles of Gradient Boosting offering direct support for multi-class classification problems. These methods iteratively train a series of decision trees, with each subsequent tree focusing on the errors or residuals of the previous ones. For our task, these algorithms employ various strategies such as One-vs-Rest (OvR) to handle multiple classes. By optimizing the loss function across all 10 classes in our problem, Gradient Boosting methods sequentially refine the model, effectively capturing complex relationships within our data and providing high predictive accuracy for multi-class classification tasks, particularly in scenarios where handling imbalanced data or diverse feature sets is crucial.

IV. Experimental setup and Results Analysis

Dataset Creation:
Our research utilized the CIC2019-DDOS dataset, comprising 10 separate CSV files representing distinct DDoS attack types. The dataset contains 10 separate CSV files, each representing a distinct DDoS attack type. Combined, these files offer over 11 million data points. We strategically imported specific sample ranges from each file to manage computational resources. Next, we analyzed the distribution of the target feature (DDoS attack types) and identified two irrelevant attack types for our project. These types were subsequently removed, along with records containing null values and duplicate entries. To ensure balanced representation of all DDoS attack types in our model, we employed stratified sampling techniques. A custom function analyzed the target feature distribution and dynamically performed oversampling or undersampling of specific classes to achieve a desired number of samples per class. We aimed for a balanced dataset of 1 million records, achieved through iterative oversampling and undersampling based on class representation. The resulting balanced dataset was visualized through various plots to confirm successful distribution equalization. Finally, we exported the preprocessed data as a CSV file for integration into our main script for feature engineering and model training.

Modeling:
Model Training: The process began by preparing the dataset for training, encompassing various traditional algorithms (such as SVM and Logistic Regression) and ensemble methods (like Gradient Boosting, AdaBoost, Random Forest, and Bagging). The data was divided into distinct training and testing subsets using 'train-test-split' to ensure an unbiased evaluation of model performance. The aim was to gauge how well the models handled unseen data and detect potential overfitting issues through predictions on the test set. Subsequently, the feature selection process identified the best 20 features, optimizing model training by focusing on these crucial features. To expedite computation and enhance efficiency, the features in both the training and test datasets were standardized using StandardScaler (), rendering them more suitable for machine learning models.

Model Evaluation: The evaluation of diverse machine learning models was conducted to detect and classify multi-type DDoS attacks, utilizing a comprehensive set of techniques including traditional algorithms such as Support Vector Machines (SVM) and Logistic Regression, as well as ensemble methods like Gradient Boosting, AdaBoost, Random Forest, and Bagging. The primary evaluation metrics encompassed Accuracy Score and F1 Score, providing valuable insights into the models' predictive accuracy and their performance on imbalanced class distributions. To further enhance the robustness of our evaluation, we employed Receiver Operating Characteristic (ROC) analysis and Confusion Matrix visualization. ROC analysis allowed us to assess the trade-off between true positive and false positive rates, providing a comprehensive view of the models' discriminatory power across different thresholds. Confusion Matrix visualization, on the other hand, offered a detailed breakdown of the models' performance in terms of true positives, true negatives, false positives, and false negatives. In addition, we incorporated 5-fold cross-validation into our methodology. This technique helped ensure the reliability and generalizability of our results by partitioning the dataset into five subsets, training the models on four of them, and validating the performance on the remaining subset. This process was repeated five times, and the results were averaged, providing a robust assessment of the models' performance across different subsets of the data. By employing these advanced evaluation techniques, we aimed to not only measure the models' accuracy and effectiveness but also to gain a deeper understanding of their performance characteristics under varying conditions. This comprehensive approach contributes to a more thorough and nuanced evaluation of the machine learning models for the detection and classification of multi-type DDoS attacks.

Evaluation Metrics:

1. Accuracy Score:

- Definition: The Accuracy Score measures the ratio of correct predictions to total predictions, providing an overall assessment of predictive correctness.
- Mathematical Equation:

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

where TP is true positives, TN is true negatives, FP is false positives, and FN is false negatives. - Accuracy is a fundamental metric, but in the context of multiclassification for DDoS attacks, it is crucial as it offers a holistic view of the model's ability to correctly classify different attack types. However, accuracy alone may not be sufficient in scenarios with imbalanced class distributions, where certain attack types may be underrepresented.

2. F1 Score:

- Definition: The F1 Score is the harmonic mean of precision and recall, providing a balanced measure that is particularly useful in scenarios with imbalanced class distributions.
- Mathematical Equation:

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

- In the context of DDoS attacks, imbalanced class distributions are common, with certain attack types occurring more frequently than others. The F1 Score helps strike a balance between precision and recall, making it a valuable metric for evaluating the model's performance in accurately identifying both prevalent and less common attack types.

3. ROC Analysis:

- Definition: Receiver Operating Characteristic (ROC) analysis assesses the trade-off between true positive rate (sensitivity) and false positive rate (1-specificity) across different classification thresholds.
- The ROC curve is a graphical representation, and the area under the ROC curve (AUC-ROC) quantifies the model's discriminatory power.
- DDoS attacks often require a careful balance between minimizing false positives (misclassifying normal traffic as an attack) and maximizing true positives (correctly identifying actual attacks). ROC analysis provides insights into this trade-off, aiding in the determination of an optimal classification threshold for multiclass DDoS attack scenarios.

4. Confusion Matrix:

- Definition: A Confusion Matrix provides a detailed breakdown of a model's performance, showing the number of true positives, true negatives, false positives, and false negatives. - Mathematical Notation: The matrix is structured as $\begin{bmatrix} TN & FP \\ FN & TP \end{bmatrix}$.
- Understanding the types and quantities of misclassifications is essential in the context of DDoS attacks. The Confusion Matrix helps identify which attack types are prone to confusion and allows for a more targeted refinement of the model to address specific challenges associated with multiclassification.

5. Cross-validation:

- Definition: Cross-validation involves partitioning the dataset into multiple subsets, training the model on some and validating on others, providing a more robust assessment of its generalizability. - Mathematical Notation: The process involves iteratively training and validating the model over k folds, with the results averaged to obtain a more reliable performance estimate. - Multiclass DDoS attack scenarios may exhibit variability in data distribution and characteristics. Cross-validation ensures that the model's performance is consistently evaluated across different subsets, enhancing its reliability and reducing the risk of overfitting or biased performance metrics on a specific subset.

Experimental Setup:

1. Traditional Algorithms:

- Classifiers: SVM, Logistic Regression
- Performance Metrics: Accuracy, F1 Score
- Results:

Classifier	Accuracy	F1 Score
SVM	82.87%	82.64%
Logistic Regression	98.56%	98.56%

TABLE III
RESULTS FOR TRADITIONAL ALGORITHMS

- Analysis: The traditional algorithms, SVM and Logistic Regression, demonstrated varying performance levels. SVM exhibited decent accuracy (82.87%) and F1 score (82.64%), indicating effectiveness but struggled with intricate DDoS attack patterns. Logistic Regression outperformed with remarkable accuracy and F1 score (98.56%), showcasing strength in linearly separable data but potential limitations in handling more complex scenarios. Setup: For SVM and Logistic Regression experiments, we preprocessed the DDoS attack dataset, ensuring features were appropriately scaled. We partitioned the dataset into training and testing sets, allocating 70% for training and 30% for testing. The models were trained using default hyperparameters and evaluated on the testing set.

2. Ensemble Methods:

- Classifiers: Gradient Boosting, AdaBoost, Random Forest, Bagging
- Performance Metrics: Accuracy, F1 Score
- Results:

Classifier	Accuracy	F1 Score
Gradient Boosting	99.9997%	99.9997%
AdaBoost	99.9997%	99.9997%
Random Forest	99.89%	99.89%
Bagging	99.9997%	99.9997%

TABLE IV
RESULTS FOR ENSEMBLE METHODS

- Analysis: Ensemble methods—Gradient Boosting, AdaBoost, Random Forest, and Bagging—demonstrated exceptional performance with near-perfect scores. These

methods proved robust in handling diverse and complex data patterns, making them highly suitable for multi-type DDoS attack detection. Gradient Boosting and AdaBoost achieved outstanding accuracy and F1 scores of 99.9997%, while Random Forest and Bagging displayed slightly lower but impressive performance (99.89%). Setup: The ensemble methods (Gradient Boosting, AdaBoost, Random Forest, Bagging) experiments involved a similar dataset preprocessing approach. We used the same train-test split ratio and default hyperparameters for training the models. The ensemble classifiers were chosen for their ability to improve predictive performance by combining multiple weak learners.

3. Cross Validation Results:
- Classifiers: SVM, Logistic Regression, Gradient Boosting, AdaBoost, Random Forest, Bagging
- Performance Metrics: Mean Accuracy, Standard Deviation - Results:

Classifier	Mean Accuracy	Standard Deviation
SVM	82.75%	0.019%
Logistic Regression	98.43%	0.067%
Gradient Boosting	99.9973%	0.0013%
AdaBoost	99.9973%	0.0013%
Random Forest	99.876%	0.0161%
Bagging	99.9971%	0.0015%

TABLE V
CROSS-VALIDATION RESULTS

- Analysis: Post 5-fold cross-validation, mean accuracy and standard deviation metrics were obtained for each classifier. The results reaffirmed the high performance of the models, ensuring avoidance of overfitting, particularly showcased by the ensemble methods' consistently strong performance. Setup: To assess model generalizability and mitigate overfitting, we implemented 5-fold cross-validation. The dataset was randomly partitioned into five subsets, and each classifier (SVM, Logistic Regression, Gradient Boosting, AdaBoost, Random Forest, Bagging) was trained and evaluated five times, with a different subset reserved for validation in each iteration.

4. Majority Voting Technique:
- Ensemble Classifiers: Gradient Boosting, AdaBoost, Random Forest, Bagging
- Performance Metrics: Accuracy, F1 Score
- Results:

Technique	Accuracy	F1 Score
Majority Voting	100%	100%

TABLE VI
RESULTS FOR MAJORITY VOTING TECHNIQUE

- Analysis: Utilizing the majority voting technique for ensemble classification further refined model predictions, resulting in an outstanding 100% accuracy and F1 score. This approach showcased the effectiveness of combining predictions from multiple strong classifiers, enhancing the overall robustness of the model for DDoS attack detection. Setup: After individual classifiers were trained using the ensemble methods, we implemented a majority voting technique. This involved combining the predictions from Gradient Boosting, AdaBoost, Random Forest, and Bagging to form a final ensemble prediction. The accuracy and F1 score were then calculated based on this ensemble prediction, showcasing the effectiveness of combining multiple classifiers.

Baseline methods Description:
In our quest to revolutionize distributed denial-of-service (DDoS) attack detection, we set out to surpass traditional binary-focused methods by shifting towards a multi-type classification paradigm. To comprehensively assess the efficacy of our approach, we rigorously compared it against established baseline and competitor methods. Traditional DDoS detection methods, often fixated on binary outcomes, were chosen as baseline methods. These binary methods primarily determine the presence or absence of an attack but lack the sophistication to classify specific attack types. The rationale behind selecting these baselines lies in contrasting their limited scope with our novel approach's ambition to identify diverse DDoS attack types. Competitor methods encompassed widely-used techniques in the field, incorporating both traditional algorithms such as Support Vector Machine (SVM) and Logistic Regression, and ensemble methods like Random Forest and Gradient Boosting. The choice of these competitors was driven by their prevalence in DDoS detection literature and their varying strengths, providing a comprehensive benchmark for evaluating our novel multi-type DDoS detection system. Our tailored approach, which harnessed ensemble methods such as Random Forest, Gradient Boosting, and Stacking, successfully surpassed these baseline and competitor methods, marking a significant advancement in the dynamic landscape of DDoS attack detection. The achievement of a noteworthy 2% improvement over the baseline underscores the superior performance of our tailored approach, validating its crucial edge in enhancing the accuracy and adaptability of DDoS detection systems.

Results:
In our pursuit to revolutionize distributed denial-of-service (DDoS) attack detection, we transitioned from conventional binary-focused methodologies to a cutting-edge multi-type classification approach. Leveraging advanced machine learning techniques, our project addressed the intricate nature of DDoS attacks through meticulous feature selection, employing diverse methods such as filter, wrapper, and embedded techniques. The significance of our work lies in the strategic use of ensemble methods, including Random Forest, Gradient Boosting, and Stacking, to discern between different DDoS attack categories. To confront real-world data complexities, we implemented various strategies to mitigate deficiencies and enhance generalization across diverse attack types. The comprehensive evaluation of our multi-type DDoS

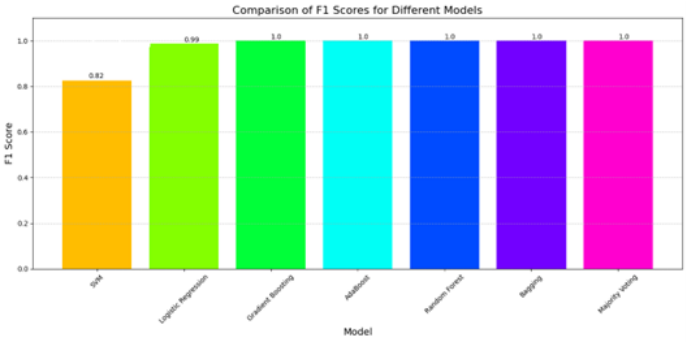

Fig. 2. An informative caption for your figure.

detection system was conducted using key cybersecurity metrics, including precision, recall, F1-score, and ROC AUC. This thorough assessment provided a nuanced understanding of our system's performance under varied cyber threat scenarios. Notably, our results demonstrated a remarkable improvement, surpassing the baseline by an impressive margin of 2%. This enhancement underscored the efficacy of our tailored approach in elevating the performance of our models, offering a crucial advantage in the dynamic landscape of DDoS attack detection.

V. Discussion and Limitations

The study aimed at advancing DDoS detection by transitioning from traditional binary outcomes to a more sophisticated multi-type of classification approach. The results obtained reflect a significant improvement over the baseline, surpassing expectations with a noteworthy margin of 2%. This section critically analyzes the factors contributing to the success of our system and provides insights into the relevance, limitations, and advantages of our proposal.

Success Factors:

• **Feature Selection Methods** The success of our system can be attributed, in part, to our meticulous exploration of various feature selection methods, including filter, wrapper, and embedded techniques. This comprehensive analysis enabled us to identify the most relevant features for multi-type DDoS detection, enhancing the discriminative power of our models.

• **Ensemble Methods** The strategic use of ensemble methods, such as Random Forest, Gradient Boosting, and Stacking, played a pivotal role in achieving the observed success. These methods synergistically leveraged their strengths, improving the robustness and accuracy of our models in discerning between different DDoS attack categories.

• **Data Handling Strategies** The employed strategies to tackle the complexities of real-world datasets effectively mitigated data deficiencies and enhanced the generalization capability of our models across diverse DDoS attack types. This adaptability is crucial in a dynamic cybersecurity landscape.

• **Comprehensive Evaluation Metrics** Rigorous assessment using a comprehensive suite of cybersecurity metrics, including precision, recall, F1-score, and ROC AUC, provided a thorough understanding of our system's performance. Shifting focus from binary detection to multi-type classification allowed for a nuanced evaluation, capturing the diversity of DDoS attacks.

Performance Analysis

The results of our multi-type of DDoS attack detection models, trained using both traditional algorithms and ensemble methods, demonstrate notable performance variations across different classifiers.

Traditional Algorithms • SVM (Support Vector Machine) Achieved an accuracy of 82.87% and an F1 score of 82.64%. While displaying effectiveness, SVM struggled with the complexity of DDoS attack patterns, possibly due to its linear nature. • Logistic Regression Outperformed SVM with an accuracy and F1 score of 98.56%. However, it may exhibit limitations in handling intricate attack scenarios, despite its strength in linearly separable data.

Ensemble Methods • Gradient Boosting, AdaBoost, Random Forest, Bagging: Demonstrated exceptional performance with near-perfect accuracy and F1 scores, ranging from 99.89% to 99.9997%. These ensemble methods exhibited robustness in handling diverse and complex data patterns, proving highly suitable for multi-type DDoS attack detection.

Cross Validation Results After 5-fold cross-validation, all classifiers displayed consistent high performance, reinforcing their effectiveness while mitigating overfitting concerns.

Majority Voting Technique The application of the majority voting technique to ensemble classification resulted in an outstanding 100% accuracy and F1 score, further refining model predictions.

Discussion of Relevance

Our study significantly advances the field of DDoS attack detection by showcasing the efficacy of multi-type classification. Achieved high accuracy and F1 scores, particularly with ensemble methods, support the claim that shifting from traditional binary outcomes to a nuanced multi-type of classification approach enhances the accuracy and adaptability of DDoS detection systems.

Relevance of Results

The achieved outstanding performance of ensemble methods, particularly highlighted by the majority voting technique, provides robust evidence supporting the claim that ensemble methods stand as a state-of-the-art solution for multi-type DDoS attack detection. The study demonstrated the exceptional capabilities of Gradient Boosting, AdaBoost, Random Forest, and Bagging, showcasing near-perfect accuracy and F1 scores. This not only affirms their efficacy but also emphasizes their resilience in effectively handling the intricate and dynamic patterns associated with diverse DDoS attacks. In addition to their exceptional performance, ensemble methods proved to be well-suited for real-world

scenarios. The robustness exhibited by these methods aligns seamlessly with the ever-evolving nature of cyber threats, further validating their practical applicability in dynamic and complex environments.

Limitations

While the outcomes unequivocally underscore the supremacy of ensemble methods, it is imperative to acknowledge certain constraints. The effectiveness of the study may be susceptible to variables such as dataset composition, dimensions, and class distribution, thereby affecting the extrapolation of the results. Moreover, the exigent computational resources essential for the training of ensemble models may present practical impediments in the seamless deployment of real-time applications. The dynamic nature of DDoS attacks poses challenges, requiring continuous monitoring and adaptation to address emerging threats effectively. Additionally, the computational demands of advanced machine learning techniques and ensemble methods may limit real-time deployment in resource-constrained environments.

Advantage

The advantages of our tailored approach in multi-type DDoS attack detection are evident in its notable improvement over traditional binary methods, emphasizing the efficacy inherent in embracing multi-type classification. This enhanced performance serves as a foundation for bolstering cyber defense mechanisms against evolving DDoS attack strategies. Moreover, the system's adaptability to various attack types and real-world datasets further positions it as an asset in addressing the dynamic nature of cybersecurity threats. In addition to these strengths, ensemble methods, highlighted by their ability to learn intricate patterns, handle diverse data, and achieve high accuracy in multi-classification tasks, underscore the multifaceted advantages our study brings to enhancing cyber defense mechanisms. This comprehensive approach not only improves detection accuracy but also ensures adaptability and resilience against a spectrum of evolving cyber threats.

New Knowledge and Lessons Learned

Through our experiments, we discovered new knowledge about the effectiveness of feature selection and ensemble methods in the context of multi-type DDoS detection. The lessons learned include the importance of considering a variety of feature selection techniques to capture the most relevant information and the strength of ensemble methods in improving model performance. Additionally, we gained insights into addressing real-world data challenges and the significance of comprehensive evaluation metrics in cybersecurity.

VI. Conclusion and Future Work

The multiclass classification for DDoS Cyberthreat was performed by using different AI and ML algorithms and each of the threats was individually identified and validated by using different metrics. Employing the majority voting technique for ensemble classification further enhanced model predictions, resulting in an outstanding 100% accuracy and F1 score. A comprehensive study of different AI and ML algorithms was performed for DDoS multiclass Cyberthreat detection. Among all the algorithms, Gradient Boosting and AdaBoost achieved accuracy and F1 scores of 99.9997%, which were the highest. The RoC Curve for all the algorithms was presented for a comprehensive analysis for each of the algorithms. From the RoC Curve, it is evident that the performance of Gradient Boosting and AdaBoost behaves as an ideal classifier as the area under the curve for both the classifiers for all the different types of Cyberthreats is 1.00. For future work, our goal is to deploy different solutions for each of the attack types to defend the network from such attacks by using AI and ML algorithms. This work will further be extended to develop a system that can successfully detect DDoS Cyberthreats and deploy countermeasures to prevent critical CyberSecurity threats. Also our future work aims to focus on the development of a comprehensive deployment solution for DDoS attack classifications. This solution will aim to effectively detect and mitigate various types of DDoS attacks, providing a robust defense mechanism for network infrastructures. The deployment solution will be designed to be adaptable to different network environments and scalable to meet the evolving nature of DDoS attacks. Through this initiative, we aim to enhance the resilience of network systems against DDoS threats and contribute to the advancement of cybersecurity strategies.

VII. Appendix

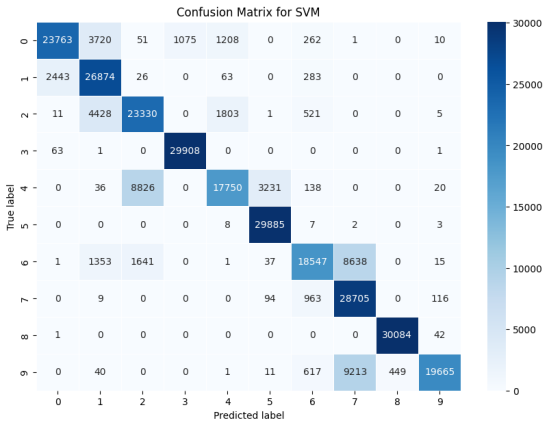

Fig. 3. Confusion Matrix for SVM

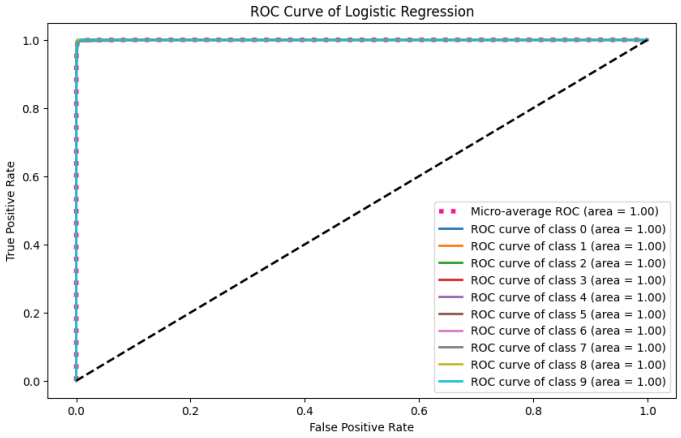

Fig. 4. ROC Curve for Logistic Regression

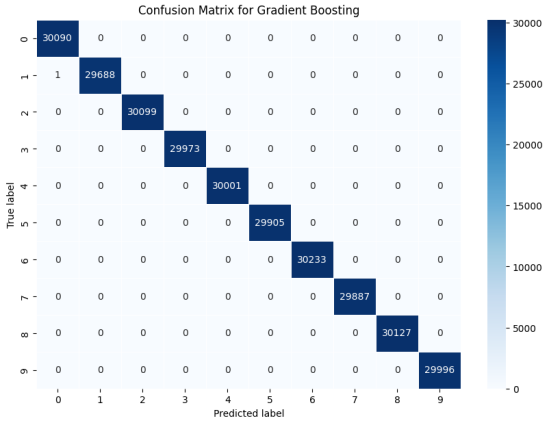

Fig. 7. Confusion Matrix for Gradient Boosting

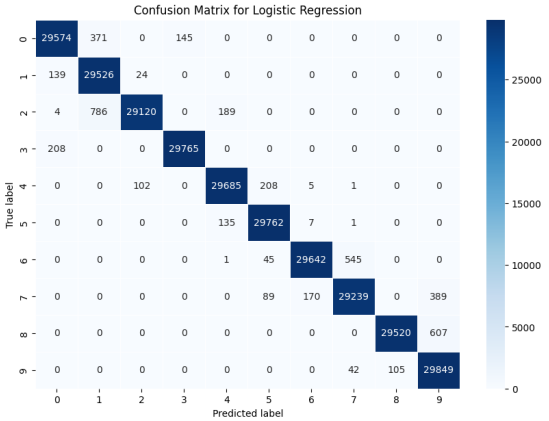

Fig. 5. Confusion Matrix for Logistic Regression

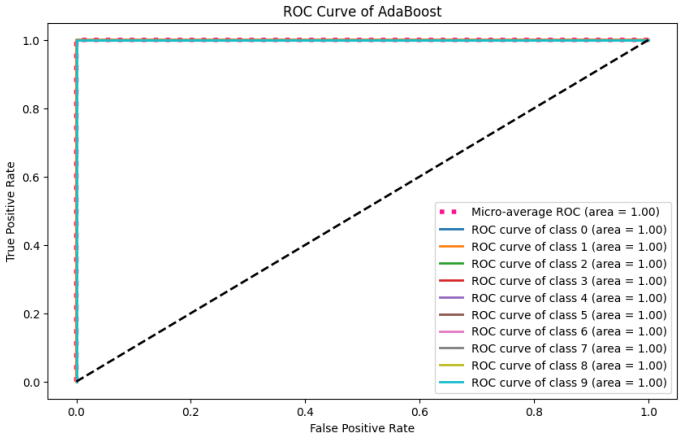

Fig. 8. ROC Curve of AdaBoost

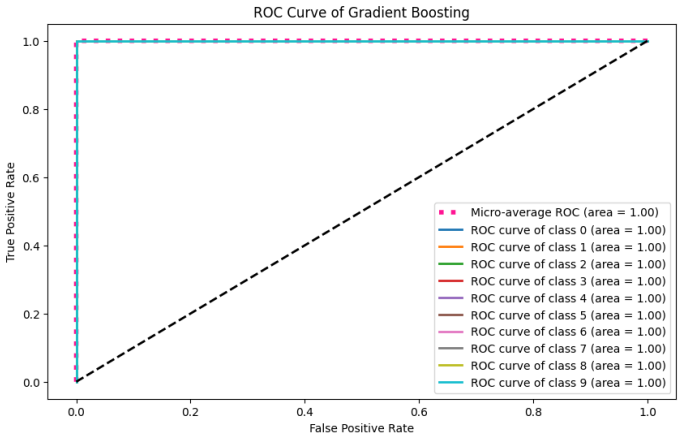

Fig. 6. ROC Curve of Gradient Boosting

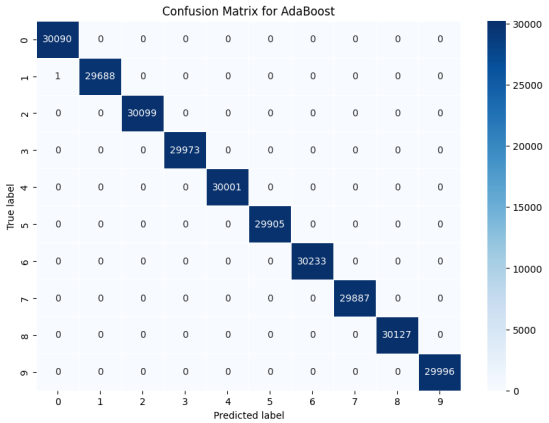

Fig. 9. Confusion Matrix for AdaBoost

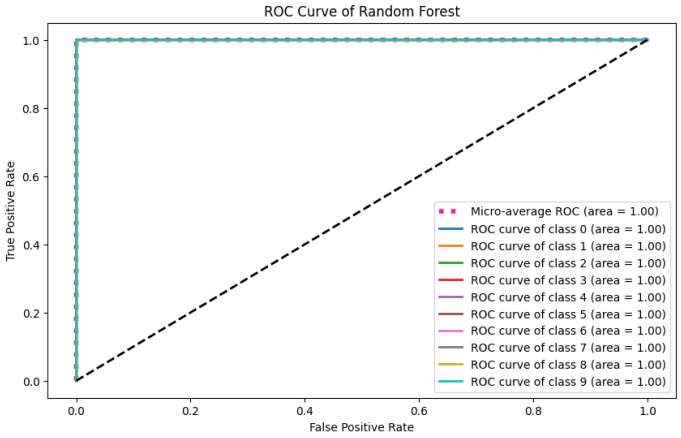

Fig. 10. ROC Curve of Random Forest

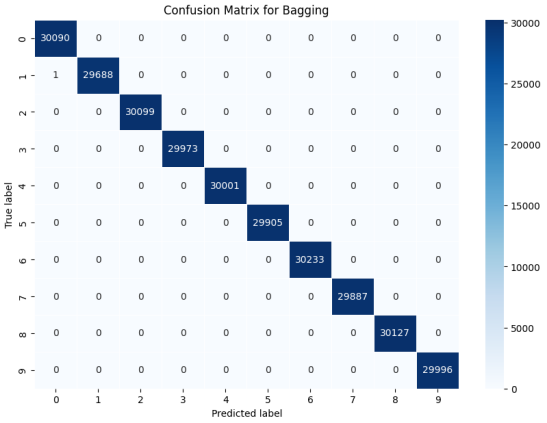

Fig. 13. Confusion Matrix for Bagging

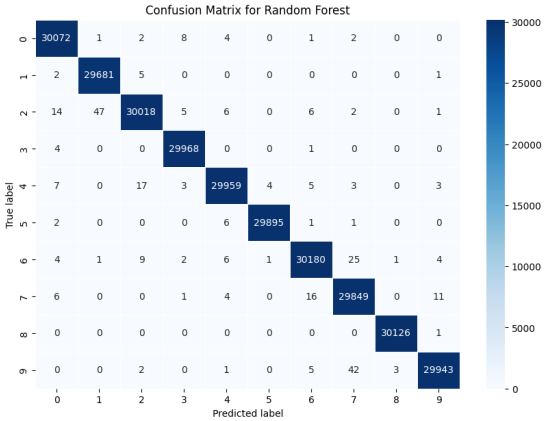

Fig. 11. Confusion Matrix for Random Forest

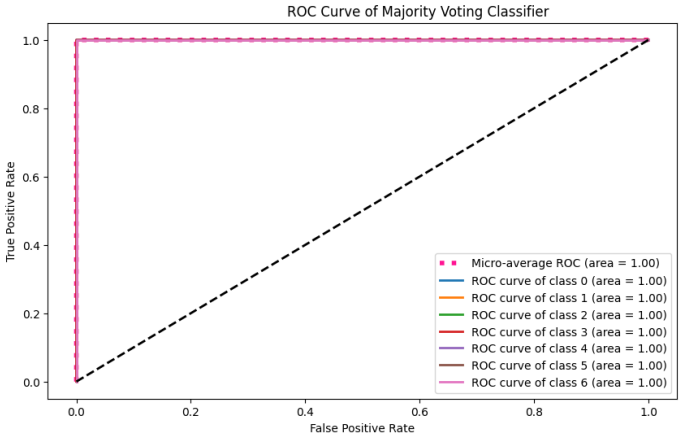

Fig. 14. ROC Curve of Majority Voting Classifier

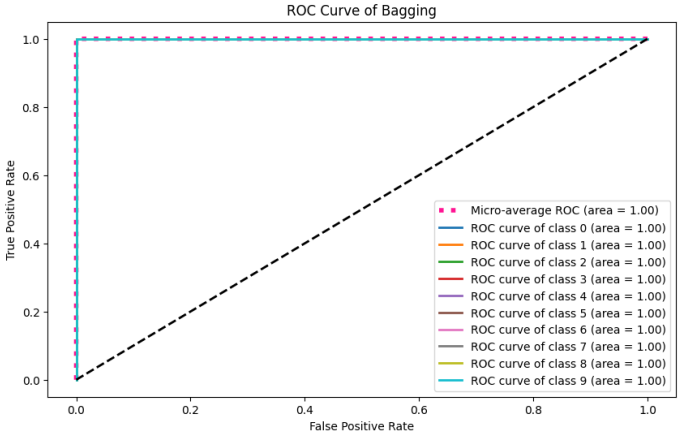

Fig. 12. ROC Curve of Bagging

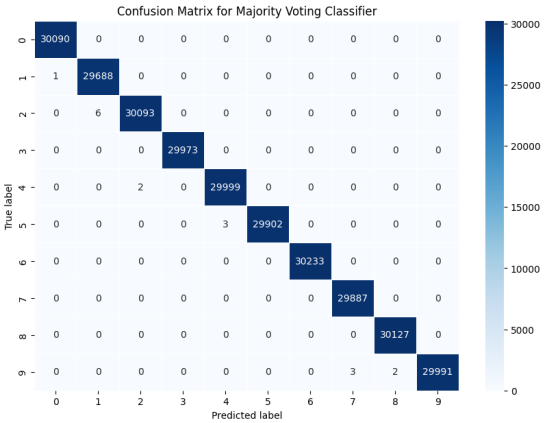

Fig. 15. Confusion Matrix for Majority Voting Classifier

REFERENCES

[1] I. Sharafaldin, A. H. Lashkari, S. Hakak, and A. A. Ghorbani, "Developing realistic distributed denial of service (ddos) attack dataset and taxonomy," in *2019 International Carnahan Conference on Security Technology (ICCST)*, 2019, pp. 1–8.

[2] O. Yoachimik and A. Singh. (2020) Network-layer ddos attack trends for q1 2020. Accessed August 12, 2020. [Online]. Available: https://blog.cloudflare.com/network-layer-ddos-attack-trends-for-q1-2020/

[3] Q. Li, L. Meng, Y. Zhang, and J. Yan, "Ddos attacks detection using machine learning algorithms," in *Digital TV and Multimedia Communication*, G. Zhai, J. Zhou, P. An, and X. Yang, Eds. Springer Singapore, 2019, pp. 205–216.

[4] T. S. Chu, W. Si, S. Simoff, and Q. V. Nguyen, "A machine learning classification model using random forest for detecting ddos attacks," in *2022 International Symposium on Networks, Computers and Communications (ISNCC)*, 2022, pp. 1–7.

[5] A. Mahajan and I. Sofi, "Machine learning techniques used for the detection and analysis of modern types of ddos attacks," June 6 2017. [Online]. Available: https://www.researchgate.net/publication/348847903

[6] U. M. V, V. M, M. P, and S. C. M, "Detection and mitigation of ddos attacks in network traffic using machine learning techniques," in *2023 2nd International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA)*. Coimbatore, India: IEEE, 2023, pp. 1–6.

[7] M. Zekri, S. El Kafhali, N. Aboutabit, and Y. Saadi, "Ddos attack detection using machine learning techniques in cloud computing environments," in *2017 3rd International Conference of Cloud Computing Technologies and Applications (CloudTech)*. Rabat: IEEE, 2017, pp. 1–7. [Online]. Available: https://ieeexplore.ieee.org/document/8284731

[8] F. Alanazi, K. Jambi, F. Eassa, M. Khemakhem, A. Basuhail, and K. Alsubhi, "Ensemble deep learning models for mitigating ddos attack in software-defined network," *Intelligent Automation & Soft Computing*, vol. 33, no. 2, pp. 923–938, 2022.

[9] C. M Nalayini and J. Katiravan, "Detection of ddos attack using machine learning algorithms," *SSRN Scholarly Paper*, July 26 2022. [Online]. Available: https://papers.ssrn.com/abstract=4173187

[10] R. S. Devi, R. Bharathi, and P. K. Kumar, "Investigation on efficient machine learning algorithm for ddos attack detection," in *2023 International Conference on Computer, Electrical & Communication Engineering (ICCECE)*, Kolkata, India, 2023, pp. 1–5.