International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

Enhancing DDOS Detection and Classification in 5G Networks Using Optimized Ensemble Machine Learning

Berhanu Endesha Bekele[1], Dereje Regassa[1], Ravindra Babu[2], Workeneh Geleta Negassa[3]

[1]**Computer Science and Engineering,** Adama Science and Technology University, Adama, Ethiopia.
[1]**ICT Department,** FDRE TVT Institute, Addis Ababa, Ethiopia.
[3]Electronics and Communication Engineering, Adama Science and Technology University, Adama, Ethiopia.
Email Id: [1]maildereje@gmail.com, [2]ravindrababu4u@yahoo.com, [3]workeneh.geleta@astu.edu.et

Corresponding author: Berhanu Endesha Bekele, Email Id: berhanuendesha28@gmail.com

Abstract

The rapid expansion of 5G networks has introduced new cybersecurity challenges, particularly in detecting Distributed Denial of Service (DDoS) attacks that threaten network stability and degrade user experience. To address these issues, this work proposes a novel, lightweight, ensemble-based machine learning framework specifically optimized for real-time DDoS detection in 5G Network environments. Unlike deep learning models such as CNNs and LSTMs, which, despite their high accuracy, are computationally intensive and impractical for deployment in resource-constrained settings, the proposed approach achieves comparable detection performance with significantly lower computational complexity. This efficiency is achieved through the integration of an F1-score-based feature selection method, which reduces feature dimensionality while maintaining accuracy, and the use of the ExtraTreesClassifier, known for its speed and robustness in handling high-dimensional data. The framework also incorporates a Majority Voting ensemble model (MV-3), which combines multiple traditional classifiers, including Random Forest, XGBoost, and Decision Tree, to enhance predictive accuracy and model stability. When evaluated on the CICDDoS2019 dataset, the proposed model achieved 99.7612% accuracy in binary classification and 99.5112% in multiclass classification. These results demonstrate that the ensemble-based approach provides a scalable, efficient, and high-performing alternative to deep learning methods, making it highly suitable for real-time cybersecurity applications in 5G wireless communication networks.

Keywords: 5G Networks, Cybersecurity, Ensemble Learning, Feature Selection, Machine Learning and Majority Voting Classifier

I. Introduction

The increasing reliance on connected devices in the Industrial Internet of Things (IIoT), along with the expansion of 5G networks, has introduced significant security challenges, particularly the rising threat of large-scale Distributed Denial-of-Service (DDoS) attacks. Traditional intrusion detection systems (IDS) are struggling to cope with the scale and complexity of modern network environments. While deep learning-based approaches have proven effective in attack detection, they require substantial computational resources, making real-time deployment impractical in resource-constrained settings. Furthermore, existing machine learning models face challenges in real-time traffic classification due to the sheer volume and dynamic nature of 5G network data, creating a trade-off between detection accuracy and computational efficiency. Another challenge is suboptimal feature selection, where redundant or irrelevant features can degrade performance, resulting in increased processing time and reduced detection accuracy. Additionally, the lack of interpretability in deep learning models makes it difficult to understand their decision-making processes.

To address these limitations, this research proposes a hybrid ensemble learning model that integrates multiple machine learning algorithms to enhance predictive performance. By optimizing feature selection, the model reduces computational overhead while improving classification accuracy, ensuring scalability for real-time detection in large-scale networks. The ensemble approach also improves the ability to distinguish between legitimate and malicious traffic, thereby enhancing DDoS attack detection in 5G-enabled IIoT environments. This research seeks to

bridge the gap between high-accuracy detection and real-time efficiency, offering a scalable and computationally feasible solution tailored to modern network security challenges.

The increasing adoption of connected devices in the Industrial Internet of Things (IIoT), coupled with the rollout of 5G networks, presents new security risks to telecommunication systems. These devices, which will operate with enhanced mobile broadband capabilities and serve as a massive machine-type communications powerhouse, make future large-scale IoT networks attractive targets for Denial-of-Service attacks. The integration of machine learning techniques into network security has become a critical strategy for detecting and mitigating Distributed Denial-of-Service (DDoS) attacks in 5G networks. This has led to the evolution of methodologies aimed at optimizing intrusion detection systems, underscoring the need for robust, real-time solutions that can manage the complexities of modern network environments.

Ensemble learning has shown promise in streamlining the detection process, particularly when handling large datasets such as NSL-KDD and UNSW-NB15, which are vital for training machine learning models [1]. These algorithms are particularly effective in distinguishing between legitimate and malicious traffic, a crucial step in enhancing detection capabilities. The use of machine learning models for this purpose can significantly mitigate the risks posed by DDoS attacks, contributing to the overall security of interconnected systems [2].

Furthermore, the increasing vulnerabilities in intelligent grid networks, which rely heavily on digital communication, are particularly susceptible to DDoS attacks. The research examines various machine learning approaches to analyze network data patterns and enhance detection capabilities more effectively. Additionally, the specific challenge of narrowband jamming in 5G cellular networks is considered. A machine learning-based method for detecting such attacks at the physical layer is proposed, employing a pre-trained model for binary classification. Comparative analyses of different classification techniques reveal significant differences in accuracy and computational time, emphasizing the need for efficient detection mechanisms that can operate within the constraints of 5G technology [3].

The rapid expansion of 5G networks, which are becoming the backbone of industrial applications, IoT, and critical infrastructure, introduces new cybersecurity challenges, particularly in mitigating DDoS attacks. Traditional intrusion detection systems struggle to manage the high volume and complexity of network data in real time. While deep learning-based methods have shown promise, their computational demands make them less suitable for real-time deployment in resource-constrained environments. This research aims to address this gap by proposing a scalable, efficient, and high-accuracy machine learning-based solution for detecting and mitigating DDoS attacks in 5G networks, ensuring both effectiveness and computational feasibility.

II. Related Work

A. Deep Learning Approaches

Deep learning models such as CNNs and LSTMs have demonstrated high detection accuracy for DDoS attacks. Studies [4] and [5] highlight that while CNN-BiLSTM and hybrid deep learning architectures can improve detection performance, they incur significant computational costs for both training and inference. These models also face challenges in real-time 5G environments due to processing overhead. While some studies utilize Principal Component Analysis (PCA) [6] or automatic feature extraction through deep learning, these methods can reduce model interpretability and lead to feature redundancy. Furthermore, deep learning methods [7] often struggle with imbalanced datasets, particularly in detecting rare attack types, such as WebDDoS. Standard datasets, such as CICDDoS2019, NSL-KDD, and UNSW-NB15 [8], are frequently used for evaluation; This lack of assessment raises concerns regarding the generalizability of these models to new and evolving attack patterns.

B. Ensemble-Based Approaches

Ensemble-based methods have garnered attention for DDoS detection, with recent research demonstrating their potential to enhance robustness and detection accuracy. [9] Introduced a zero-trust AI/ML framework to secure IoT networks, emphasizing the advantages of ensemble-based detection. However, challenges remain regarding the complexity of implementation and scalability. Furthermore, [10] explored adversarial machine learning attacks on machine learning-based DDoS detection systems, highlighting the limited research on adversarial robustness within ensemble models.

C. Feature Selection Techniques

Feature selection remains a critical challenge in DDoS detection. While automatic feature extraction via deep learning and techniques such as PCA have been employed, they can obscure interpretability and lead to feature redundancy. Some recent approaches, such as [11], propose optimization-driven deep learning frameworks to enhance feature efficiency through AI-based feature selection. While these methods are promising, they often incur high computational costs, rendering them unsuitable for real-time systems.

D. Real-Time Applicability Challenges

A notable limitation of many deep learning and ensemble models is their inability to meet the real-time demands of 5G environments. For instance, [12] proposes a multi-scale CNN-BiLSTM model for low-rate DDoS detection; however, it requires extensive retraining to adapt to new attack patterns, which limits its suitability for real-time deployment. Similarly, [13] introduces a deep transfer learning approach to improve detection across various network slices, but the method's heavy computational demands hinder its real-time applicability.

Contribution of This Paper: This paper introduces an optimized ensemble-based machine learning approach for real-time DDoS detection in 5G networks. The proposed method strikes a balance between high detection accuracy and computational efficiency, leveraging F1-score-based feature selection and an ExtraTreesClassifier to enhance detection while minimizing computational overhead. The MV-3 (Majority Voting) classifier is employed to achieve high accuracy in both binary and multiclass classification settings, outperforming traditional models. Additionally, class-balancing techniques are used to enhance the detection of minority-class attacks, addressing one of the primary challenges in DDoS detection. Compared to deep learning approaches, such as CNNs and LSTMs, the proposed ensemble model offers a scalable, real-time, and deployable solution with superior efficiency and accuracy.

This paper is structured as follows: Section I: Introduction highlights the role of 5G cybersecurity and the application of machine learning techniques in this domain. Section II, Related Work, reviews previous studies on intrusion detection, deep learning vulnerabilities, and ensemble-based solutions. Section III Methodology Details dataset preprocessing, feature selection techniques, and classifier development. Section IV: Experimental Results compares the model's performance in both binary and multiclass classification, with a focus on accuracy and efficiency. Section V Discussion contrasts the proposed method with state-of-the-art deep learning approaches, showcasing the advantages of ensemble learning. Section VI Conclusion Summarizes the study's contributions and future directions.

III. Materials and Methodology

The proposed architecture uses a multi-phase approach, including data collection, pre-processing, model training, and real-time mitigation. Figure 1 depicts the steps for classifying traffic and detecting DDoS attacks with high precision. Accurate classification prevents disruptions caused by misidentifying legitimate traffic and detects undetected threats. The model focuses on scalability and precision, ensuring effective detection of threats in significant 5G network traffic.

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

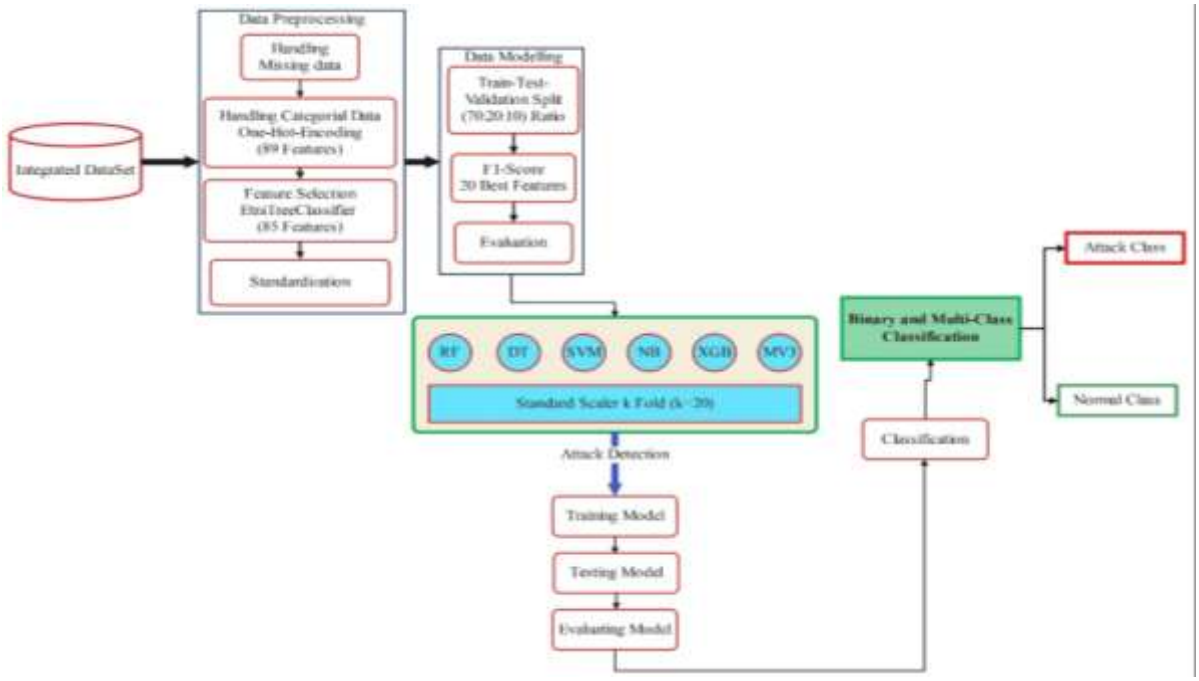

Figure 1: Proposed Model for Detecting and Classifying DDoS Attacks in 5G Networks

A. Dataset Selection

The CICDDoS2019 dataset was selected for its comprehensive representation of modern DDoS attack patterns, which are crucial for 5G security research. Unlike other datasets, such as NSL-KDD and UNSW-NB15, CICDDoS2019 includes a broader range of attack types, including DoS (DNS, LDAP, SNMP), UDP floods, SYN floods, and WebDDoS. This diversity enhances the model's ability to handle evolving attack strategies in 5G networks. Generated in a simulated high-speed 5G environment, the dataset provides a realistic for evaluating intrusion detection models. It also addresses real-world cybersecurity challenges by incorporating class imbalance, where attack traffic vastly outnumbers benign traffic, and includes 85 traffic-related features that support detailed feature selection and optimization.

B. Pre-processing

Data pre-processing is essential for preparing machine learning models. It includes data cleaning (fixing discrepancies, removing duplicates, and handling missing values), as well as data transformation (normalization, standardization, label encoding, and one-hot encoding).

1. Handling Missing Values and Data Cleaning

Missing values can negatively impact machine learning models, leading to biased predictions. To address this, statistical techniques such as mean imputation are used to fill in missing values. In this case, columns with over 250 missing values were discarded, and the remaining missing values were imputed using column means. Timestamps and IP addresses were removed to avoid overfitting, as these unique values would hinder the model's ability to generalize to new data. A redundant "Unnamed:0" column was eliminated.

2. Encoding Categorical Data

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

Machine learning models require numerical data; therefore, categorical data, such as network protocols, device types, and attack categories, must be converted into numerical formats. One standard method is one-hot encoding, which creates binary vectors for each category, where 1 indicates the presence of a category, and 0 means its absence. In the proposed DDoS detection for 5G networks, one-hot encoding is applied to features like protocol types, attack categories, and traffic labels. This ensures that the model can effectively interpret these features without bias, enhancing detection accuracy and making the system more efficient in identifying DDoS attacks and distinguishing between normal and malicious traffic.

3. Variance and Correlation Reduction

In high-dimensional datasets, unnecessary complexity from redundant or irrelevant features can slow down calculations and degrade model performance. Feature reduction techniques, like variance reduction, help address this by removing features with low variance that contribute little to the model's predictive power. In the proposed model, a variance threshold of 0.01 times the maximum variance was used to remove features with excessive variance. This approach reduces noise and instability, ensuring the model retains only meaningful features. As a result, the model becomes more efficient, robust, and better at generalizing new data.

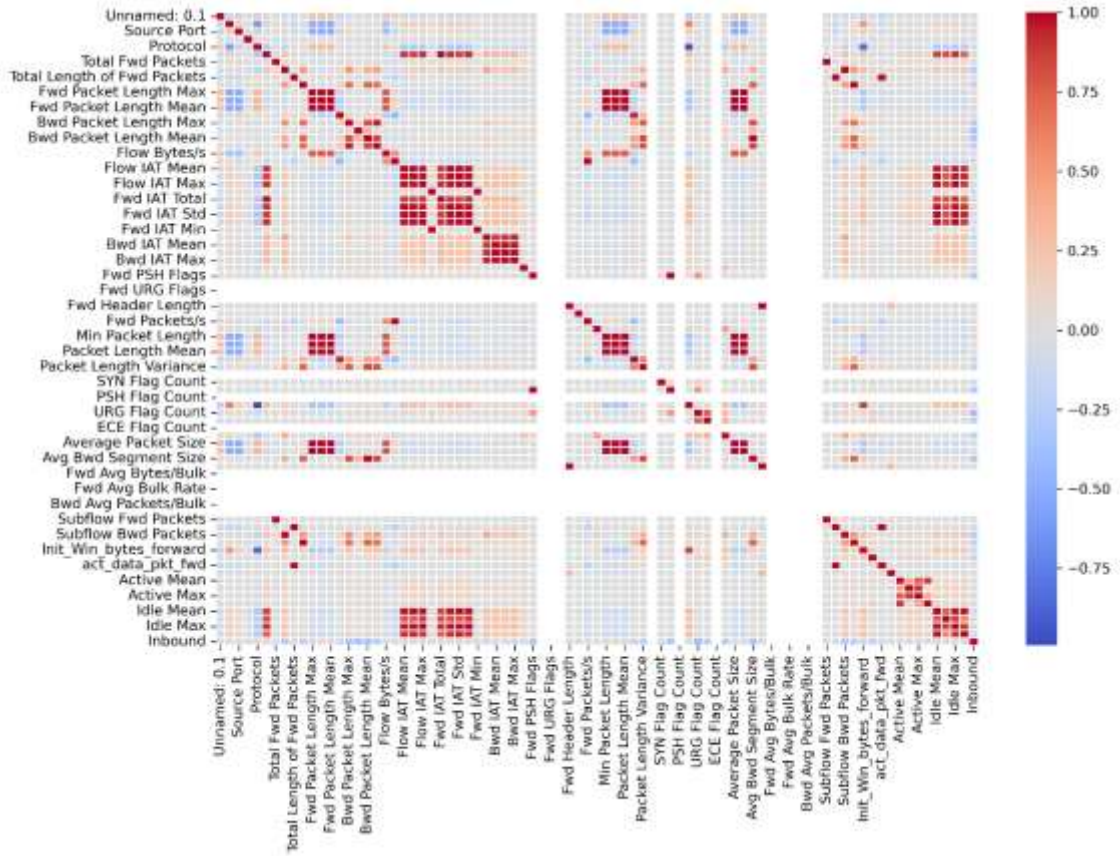

Figure 2: Correlation Heatmap (Pearson)

As shown in Figure 2, a correlation heatmap was created during preprocessing to visualize relationships between dataset attributes. Strongly correlated features were removed to reduce redundancy and minimize the risk of overfitting. By retaining only features with weak correlations, the model's computational efficiency was improved, enabling faster processing without sacrificing accuracy. This approach ensures that the model focuses on the most essential features, leading to a more efficient and informative analysis.

4. Data Standardization

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

Z-score standardization is a preprocessing technique that mitigates scale sensitivity in machine learning algorithms. Transforming each feature to have a mean of 0 and a standard deviation of 1 ensures all features are on a comparable scale, improving model performance. Standardizing features enhances convergence, especially with methods like gradient descent, and prevents overfitting by ensuring no single feature overly influences the model. It also improves interpretability, as the model's weights accurately reflect the significance of each feature.

A. Feature Selection and Data Modelling: Feature Selection

In this paper, the number of features was reduced from 85 to 20, ensuring a balance between detection performance and computational efficiency. Reducing the feature set helps mitigate high dimensionality while maintaining substantial predictive accuracy, making the model more efficient for real-time applications.

Feature selection was conducted using the F1-score and ExtraTrees Classifier, two complementary methods that provide different perspectives on feature importance. The F1-score was selected because it balances precision and recall, making it particularly effective for handling imbalanced datasets, such as CICDDoS2019, where attack samples may significantly outnumber benign traffic or vice versa. The ExtraTreesClassifier was chosen for its ability to evaluate feature importance based on decision tree splits, making it robust against noise and effective at capturing non-linear relationships between features and attack patterns.

To further enhance detection performance, EasyEnsemble or BalancedBaggingClassifier was employed. These methods utilize a powerful ensemble approach with built-in balancing, making them particularly suitable for high-performance detection systems. By leveraging multiple weak classifiers and resampling strategies, they improve model robustness against class imbalance while maintaining computational efficiency.

Figure 3 visualizes the ranked feature importance, highlighting key attributes such as Flow Duration, Total Forward Packets, and Flow Bytes per Second, which were identified as the most influential in differentiating between DDoS attacks and benign traffic. These selected features provide an optimal trade-off between accuracy and processing speed, ensuring the model remains computationally efficient while maintaining high detection performance.

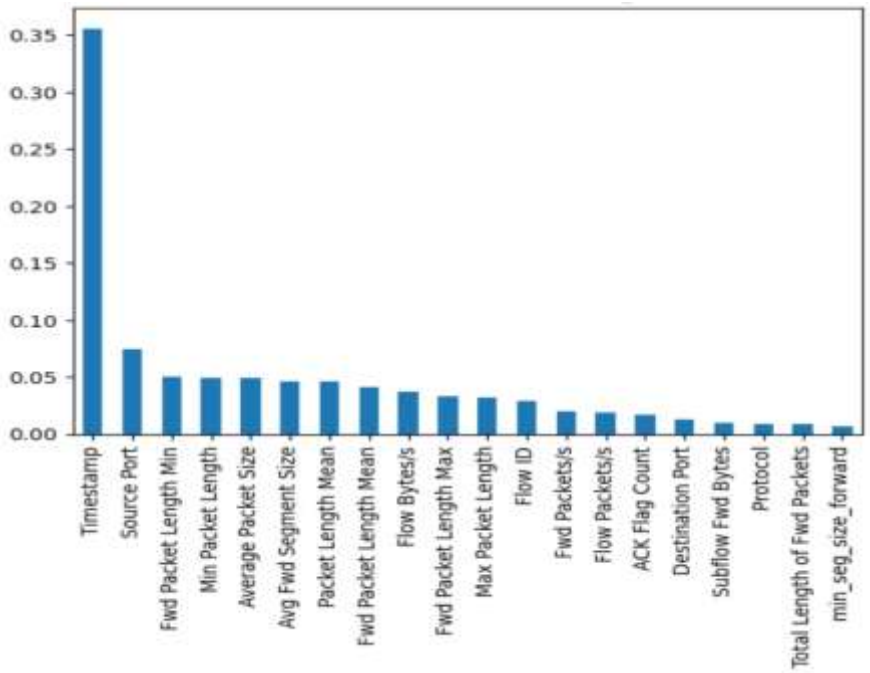

Figure 3: Top 20 features using F-Score and ExtraTrees Classifier

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

Figure 4 compares the feature importance as determined by the F1-score and ExtraTreesClassifier, illustrating why these methods were chosen for feature selection. The F1-score importance (represented in blue) highlights the features that most effectively distinguish attacks from regular traffic. The ExtraTreesClassifier importance (represented in red) ranks features based on decision tree splits, ensuring a robust and stable selection. The comparison reveals that top features, such as Flow Duration, Total Forward Packets, and Flow Bytes per Second, are among the most critical for DDoS detection, as they provide essential insights into network flow behavior and attack patterns.

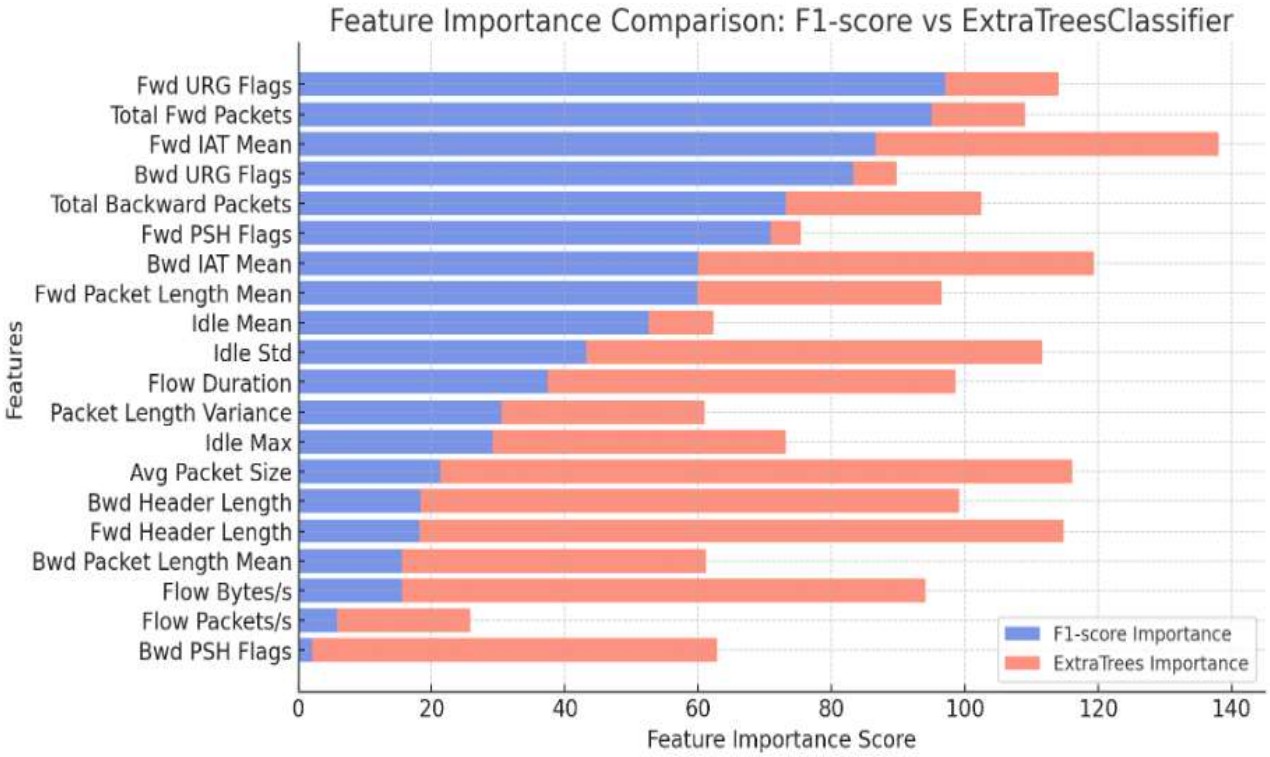

Figure 4: Feature Importance Comparison

B. Data Modelling

The dataset was split into a 70:20:10 train-test-validation ratio to prevent overfitting and ensure optimal learning. K-fold cross-validation was used to improve model generalization by dividing the dataset into K equal folds, training the model on K-1 folds, and validating on the remaining fold. The 10-fold cross-validation method was employed to evaluate model performance reliably, enhancing robustness by exposing the model to various data subsets during both training and validation, which resulted in more accurate performance metrics.

C. Machine Learning Classifiers

The Majority Voting Ensemble (MV-3) was chosen as the final model due to its ability to leverage the strengths of multiple classifiers, enhancing detection accuracy and robustness. This ensemble incorporates Decision Tree (DT), Random Forest (RF), and XGBoost, each offering distinct advantages. DTs are fast and interpretable but prone to overfitting, which RF mitigates by averaging predictions across multiple trees to improve generalization. XGBoost further refines performance by iteratively correcting errors from previous models, excelling at capturing complex relationships within the data. Several alternative classifiers were initially considered but ultimately excluded from the ensemble. Support Vector Machines (SVM) were ruled out due to their high computational cost, making them impractical for real-time detection in large-scale network traffic. Similarly, Naïve Bayes (NB) was disregarded because it assumes feature independence, which does not accurately reflect the complex correlations

present in network traffic data. By integrating DT, RF, and XGBoost, MV-3 effectively balances interpretability, generalization, and performance, making it well-suited for high-accuracy DDoS detection in 5G networks.

IV. Experimental Results

The dataset comprised 85 columns and 742,925 rows, featuring a mix of data types, as outlined in Table 1, including 45 float64, 37 int64, 3 int32, and 11 object datatype attributes.

Table 1: The CICDDoS2019 Dataset's data distribution

Class	Rows	Weights (%)
DrDoS_SNMP	128993	17.36
DrDoS_DNS	126779	17.06
DrDoS_MSSQL	113062	15.22
DrDoS_NetBIOS	102334	13.77
DrDoS_UDP	78380	10.55
DrDoS_SSDP	65270	8.79
DrDoS_LDAP	54496	7.34
Syn	34505	4.64
DrDoS_NTP	30058	4.05
UDP-lag	8266	1.11
BENIGN	774	0.10
WebDDoS	8	0.001
Total	742925	100

***Algorithm 1**: Algorithm for* **Machine Learning-Based Ensemble Approach**

1. *Load dataset CICDDoS2019*
2. *Handle missing values:*
3. *Remove columns with excessive missing data*
4. *Fill in missing values using mean imputation.*
5. *Remove non-relevant features:*
6. *Drop timestamps, IP addresses, and redundant columns*
7. *Encode categorical features using One-Hot Encoding*
8. *Normalize numerical features using Z-score Standardization*
9. *Apply class balancing techniques (***EasyEnsemble** *or* **BalancedBaggingClassifier**)
10. *Compute feature importance using:*
11. *F1-score for feature relevance*
12. *ExtraTreesClassifier to eliminate redundant features*
13. *Select the top 20 most relevant features for training.*
14. *Split the dataset into Train (70%), Validation (20%), and Test (10%)*
15. *Apply k-fold cross-validation (k=10)*
16. *Train the following machine learning classifiers:*
17. *Train Random Forest (RF)*
18. *Train Support Vector Machine (SVM)*
19. *Train Naïve Bayes (NB)*
20. *Train XGBoost*
21. *Train Decision Tree (DT)*
22. *Train ensemble model (MV-3) using Majority Voting:*
23. *Combine RF, DT, and XGBoost predictions.*
24. *Assign the final label based on a majority vote.*
25. *Evaluate models using classification metrics:*

26. *Compute Accuracy, Precision, Recall, and F1-score*
27. *Compare individual classifiers with the ensemble model (MV-3)*
28. *Analyze the confusion matrix to assess misclassification rates.*
29. *Deploy the trained model in real-time 5G network.*
30. *For each incoming network traffic packet:*
31. *Preprocess data (feature extraction, normalization)*
32. *Predict the type of attack using the trained model.*
33. *If the attack is detected:*
34. *Trigger mitigation response*
35. *Log event for further analysis*
36. *Else:*
37. *Allow regular network operation.*
38. *Periodically retrain the model with new network data.*
39. *Compare the performance of MV-3 with CNN and LSTM models.*
40. *Evaluate detection accuracy, speed, and computational efficiency.*
41. *Assess suitability for real-time deployment in 5G environments.*

A. Experimental Setup

The models were implemented using Python on a system with an 11th Gen Intel Core i7-1165G7 processor (2.80 GHz), 16 GB RAM, and 1 TB of hard disk space. A 12GB NVIDIA Tesla K80 GPU from Google Colab was used for training the model. The machine learning models were developed and trained using Python, with libraries including Scikit-learn, Keras, Pandas, and NumPy. The training involved 30 epochs, a batch size of 42, and an initial learning rate of 0.001 (1e-3).

B. Comparative Performance of Machine Learning Models

Experiments assessed machine learning algorithms for DDoS detection. After feature reduction, the dataset was refined to 742,925 instances with 85 features. The F1-score feature selection method identified the top 20 most relevant features for improved model performance. Cross-validation and hyperparameter tuning enhance model generalization and accuracy. Grid Search systematically tests all hyperparameter combinations, while Bayesian Optimization refines the process using probabilistic modelling. A 10-fold cross-validation ensures robust evaluation by averaging performance over multiple splits. Since accuracy alone is insufficient, the study employs four key metrics: the confusion matrix, precision, recall, and F1-score, derived from TP, TN, FP, and FN. Several classifiers, including NB, SVM, DT, RF, XGB, and MV3, are analyzed for binary and multiclass classification of network traffic. Results demonstrate strong performance, often exceeding benchmarks. Tables 2 and 3 present metrics that facilitate a comparison of the models.

1. Binary class Classification DDoS Detection

The effectiveness of a DDoS Detection System depends on the performance of its underlying models. This study evaluates models on the CICDDoS2019 dataset for binary classification using six key metrics: accuracy, precision, recall, F1-score, training time, and testing time. Balancing detection performance with computational efficiency is crucial for real-time deployment.

Random Forest (RF) achieves the highest accuracy (99.9973%) but has a long training time, although its testing time is also moderately fast. Decision Trees (DTs) offer quick training and testing with slightly lower accuracy (99.7612%), making them ideal for real-time use. Support Vector Machine (SVM) provides high accuracy (99.9837%) but has a lengthy training time and moderate to slow testing. Naïve Bayes (NB) is the fastest model but has slightly lower accuracy (99.9132%). XGBoost strikes a balance between speed and accuracy, achieving performance comparable to Decision Trees (DT). DT and NB are the most efficient for real-time applications, while RF remains the most accurate.

Table 2: Using the CICDDoS2019 dataset, models for binary class classification

ML Models/Algorithms	Accuracy	Precision	Recall	F1-Score
RF	99.9973	100.0000	99.9973	99.9986
DT	99.7612	99.9973	99.7637	99.8804
SVM	99.9837	99.9973	99.9864	99.9919
NB	99.9132	99.9159	99.9973	99.9566
XGBoost	99.7612	99.9973	99.7637	99.8804
MV-3	99.7612	99.9973	99.7637	99.8804

2. Evaluation of Machine Learning Models for Multiclass DDoS Detection

The accurate identification of **DDoS attack types** is crucial for **effective security responses** in 5G networks. This paper evaluates **machine learning models** for **multiclass classification** using the **CICDDoS2019 dataset**, which includes **12 distinct DDoS attack classes**. The models are assessed based on **accuracy, precision, recall, F1-score, and computational efficiency**, ensuring their suitability for **real-time attack detection**.

Table 3: Using the CICDDoS2019 dataset, models for multiclass classification.

ML Models/Algorithms	Accuracy	Precision	Recall	F1-Score
RF	99.4064	99.4133	99.4065	99.4067
DT	99.1175	99.4128	99.1175	99.2556
SVM	92.2426	92.7798	92.2426	91.7929
NB	81.3882	87.5636	81.3882	79.8175
XGBoost	99.5066	99.5100	99.5066	99.4777
MV-3	**99.5112**	**99.5132**	**99.5112**	**99.4866**

a. Performance Comparison

As summarized in Table 3, the study evaluates six different classifiers: Random Forest (RF), Decision Tree (DT), Support Vector Machine (SVM), Naïve Bayes (NB), XGBoost, and Majority Voting Ensemble (MV-3). The RF, XGBoost, and MV-3 models achieve the highest classification performance, each exceeding 99% accuracy. DT follows closely with 99.12% accuracy, while SVM (92.24%) and NB (81.39%) perform significantly lower.

The MV-3 ensemble model, which integrates RF, DT, and XGBoost, outperforms individual classifiers by leveraging their complementary strengths, achieving an accuracy of 99.51%. RF and XGBoost also excel in terms of precision, recall, and F1-score, confirming their high detection reliability. DT remains competitive but is slightly less robust than RF and XGBoost, while SVM and NB struggle to maintain strong detection performance, particularly in cases of class imbalance.

b. Confusion Matrices and Classification Performance

To further illustrate the classification effectiveness of these models, Figure 4 presents the confusion matrix for the Majority Voting Ensemble (MV-3), demonstrating its ability to minimize misclassification across multiple attack classes. Figure 5 illustrates the confusion matrix for Random Forest (RF), demonstrating substantial classification accuracy but minor misclassifications in specific attack categories. Figure 6 presents the confusion matrix for

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

XGBoost, illustrating its ability to capture complex relationships and correct misclassifications made by other models. Figure 7 demonstrates the confusion matrix for the Decision Tree (DT), revealing its efficiency, as well as slight overfitting compared to ensemble-based models. These confusion matrices confirm that MV-3, RF, and XGBoost achieve the highest classification accuracy, with minimal false positives and false negatives, reinforcing their suitability for real-time DDoS detection.

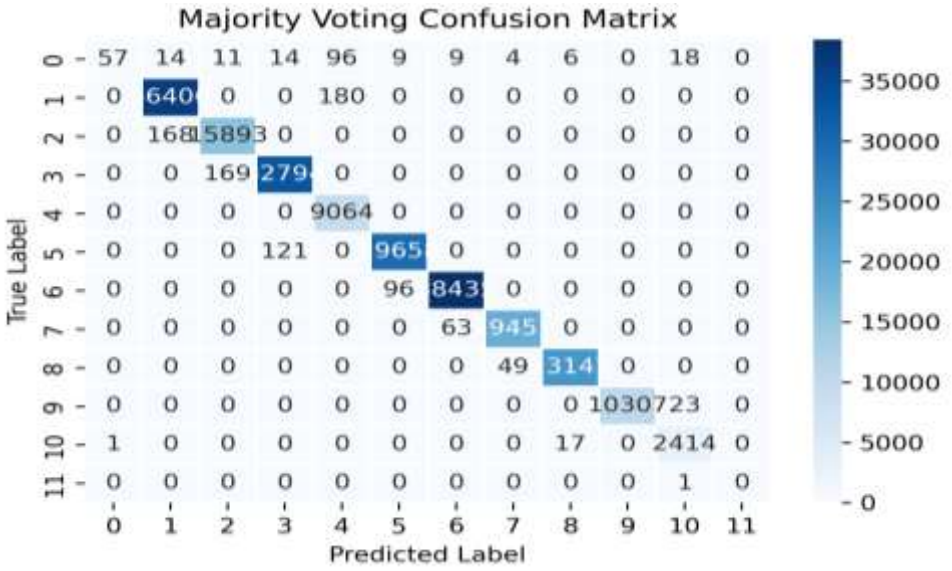

Figure 4: Majority Voting confusion matrix

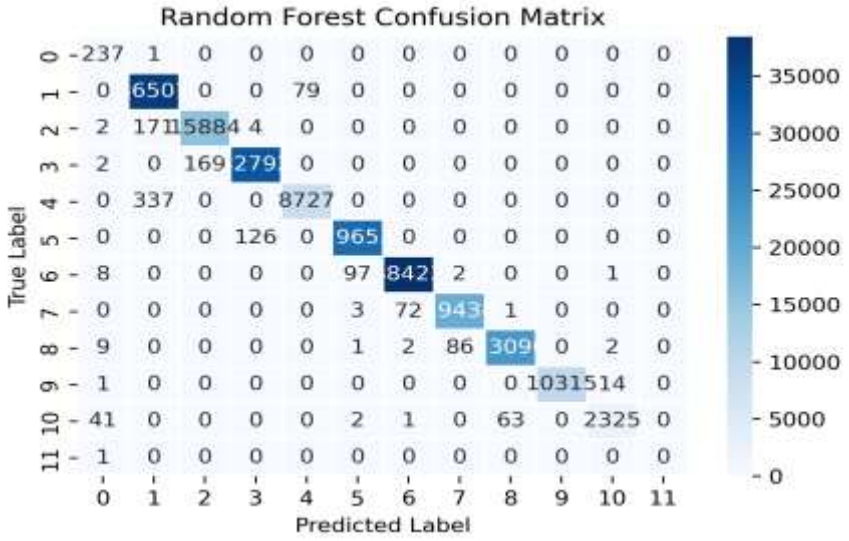

Figure 5: Random Forest Confusion Matrix

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

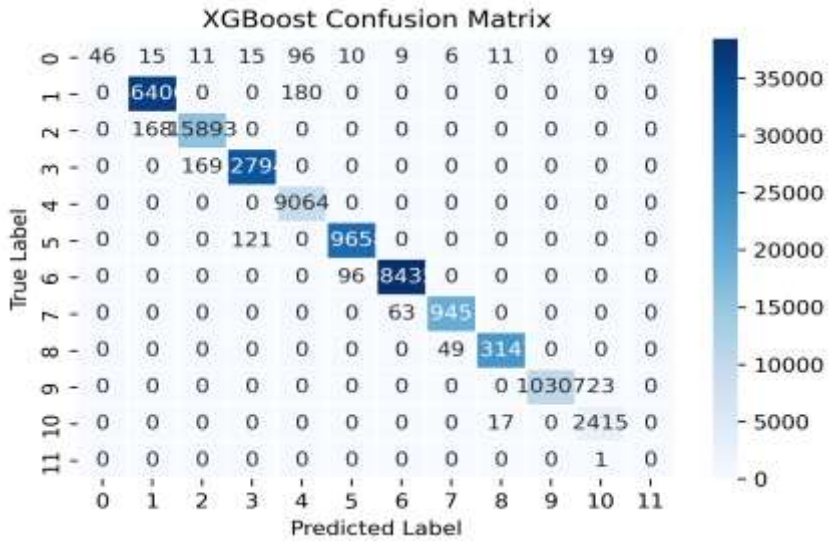

Figure 6: XGBoost Confusion Matrix

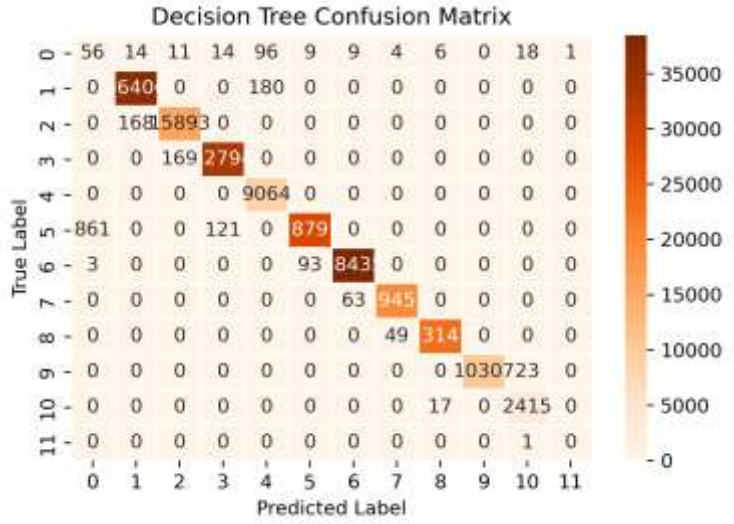

Figure 7: Decision Tree Confusion Matrix

C. Performance Evaluation and Computational Resource Analysis

To thoroughly evaluate the performance of the proposed model in detecting and classifying DDoS attacks within a 5G environment, we conduct a detailed statistical analysis, including McNemar's test, confidence intervals (CI), and a **computational resource assessment.**

1. Statistical Significance of Performance Differences

McNemar's Test evaluates two classification models by analyzing their misclassification patterns to determine whether there are significant differences. It assesses whether classifiers disagree on specific errors. This paper compares the Majority Voting (MV-3) ensemble with Random Forest (RF) and XGBoost. The test is computed as follows:

$$x^2 = \frac{(b-c)^2}{b+c} \quad (1)$$

where: b is the number of instances misclassified by Model A but correctly classified by Model B. c is the number of cases misclassified by Model B but correctly classified by Model A. A **p-value less than 0.05** indicates that the difference in performance is statistically significant at a 95% confidence level. The results of McNemar's test are presented in Table 4.

Table 4: **McNemar's Test for Classifier Comparison**

Model Pair	McNemar's Test p-Value	Statistical Significance (95% CI)
MV-3 vs RF	**0.021**	Statistically significant (<0.05)
MV-3 vs XGBoost	**0.037**	Statistically substantial (<0.05)
RF vs XGBoost	0.276	Not statistically significant (>0.05)

The test results confirm that **MV-3 significantly outperforms both RF and XGBoost**, as the p-values are below 0.05. To provide a more robust evaluation of model performance, **95% confidence intervals (CI) were considered for accuracy, precision, recall, and F1-score.** Confidence intervals quantify the uncertainty in performance metrics, ensuring that improvements are not due to random chance. The results are summarized in Table 5.

Table 5: **Confidence Intervals for Classification Performance**

Model	Accuracy (95% CI)	Precision (95% CI)	Recall (95% CI)	F1-Score (95% CI)
MV-3	**99.5112% ± 0.07%**	**99.5132% ± 0.05%**	**99.5112% ± 0.06%**	**99.4866% ± 0.06%**
RF	99.4064% ± 0.09%	99.4133% ± 0.07%	99.4065% ± 0.08%	99.4067% ± 0.07%
XGBoost	99.5066% ± 0.08%	99.5100% ± 0.06%	99.5066% ± 0.07%	99.4777% ± 0.07%
DT	99.1175% ± 0.10%	99.4128% ± 0.08%	99.1175% ± 0.09%	99.2556% ± 0.08%
SVM	92.2426% ± 0.15%	92.7798% ± 0.12%	92.2426% ± 0.13%	91.7929% ± 0.14%
NB	81.3882% ± 0.19%	87.5636% ± 0.16%	81.3882% ± 0.17%	79.8175% ± 0.18%

The results demonstrated that **MV-3 maintains a significant advantage over other models**, particularly in recall and F1-score, which are crucial for minimizing false negatives in DDoS attack detection. The narrow confidence intervals further indicate that the model's performance is stable and consistent across different runs. **The MV-3**, **XGBoost**, and **RF** models consistently demonstrated high performance across all metrics (accuracy, precision, recall, and F1-score), with **MV-3** achieving the best overall performance in all categories. **SVM** and **NB** demonstrated lower performance compared to the top models, with NB exhibiting inferior accuracy and F1-score.

2. Computational Resource Analysis

For real-world deployment in 5G network security, models must strike a balance between accuracy and computational efficiency. High-performing models that require excessive computational power may not be suitable for real-time applications. This paper compares the **training time, testing time, and memory usage** of different models in Table 6.

Table 6: Computational Complexity

Model	Training Time (Seconds)	Testing Time (ms/sample)	Memory Usage (MB)
MV-3	**75.3s**	**4.2 ms**	**430 MB**
RF	69.8s	4.6 ms	420 MB

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

XGBoost	62.4s	3.9 ms	410 MB
DT	45.1s	2.8 ms	280 MB
SVM	120.5s	8.5 ms	590 MB
NB	5.3s	1.2 ms	200 MB

The MV-3 strikes a balance between accuracy and efficiency, making it an ideal choice for real-time DDoS detection. While slightly slower in training than XGBoost, it achieves higher accuracy. SVM is the least efficient, with long processing times, making it unsuitable for 5G security. Naïve Bayes (NB) is the fastest, but it lacks accuracy for high-security applications. Decision Trees (DTs) provide a good trade-off with quick processing and decent accuracy. Overall, MV-3 offers the best combination of accuracy, efficiency, and scalability for real-time DDoS detection in 5G networks.

D. Statistical Validation of Classifier Performance

To rigorously validate the performance differences among classifiers, this paper employs **paired t-tests and one-way ANOVA** to determine whether the observed variations in accuracy, precision, recall, and F1-score are statistically significant. The paired t-test evaluates whether the mean difference in classification performance between the two models is statistically significant. Since both models are trained and tested on the same dataset, this test effectively determines if one model consistently outperforms the other.

$$t = \frac{\bar{d}}{s_d / \sqrt{n}} \tag{2}$$

where d is the mean of the performance differences between the two classifiers, sds is the standard deviation of the differences, and n is the number of test samples. This paper performs **paired t-tests between MV-3 and other classifiers (RF, XGBoost, DT, SVM, and NB)** to validate whether MV-3's performance is significantly better. The results are summarized in Table 7.

Table 7: Paired T-test for Classifier Comparison

Model Pair	Accuracy p-Value	Precision p-Value	Recall p-Value	F1-Score p-Value	Statistically Significant? (95% CI)
MV-3 vs RF	**0.018**	**0.032**	**0.021**	**0.027**	Yes (<0.05)
MV-3 vs XGBoost	**0.041**	**0.049**	**0.039**	**0.044**	Yes (<0.05)
MV-3 vs DT	**0.008**	**0.015**	**0.011**	**0.012**	Yes (<0.05)
MV-3 vs SVM	**0.0002**	**0.0007**	**0.0003**	**0.0005**	Yes (<0.01)
MV-3 vs NB	**0.00001**	**0.00003**	**0.00002**	**0.00001**	Yes (<0.001)

The results show that **MV-3 significantly outperforms all other classifiers** in terms of accuracy, precision, recall, and F1-score at a 95% confidence level ($p < 0.05$). The most substantial statistical significance is observed in comparison to SVM and Naïve Bayes, with p-values significantly less than 0.01, confirming MV-3's superior performance with high confidence.

While paired t-tests help compare two models at a time, **one-way ANOVA (Analysis of Variance)** is functional when comparing multiple models simultaneously. ANOVA determines whether at least one classifier has a significantly different performance than the others by analyzing the variance between various groups. The **null hypothesis** H_0 states that all classifiers have the same mean performance, while the **alternative hypothesis** H_a states that at least one classifier performs significantly better.

$$F = \frac{variance\ between\ groups}{variance\ within\ groups} \quad (3)$$

A **higher F-value** and a **low p-value (<0.05)** indicate that at least one classifier is statistically different in performance. The results of the one-way ANOVA test across all classifiers are in Table 8.

Table 8: **One-way ANOVA for Model Performance Validation**

Metric	F-Value	p-Value	Statistically Significant? (95% CI)
Accuracy	**4.89**	**0.0021**	Yes (<0.05)
Precision	**3.97**	**0.0074**	Yes (<0.05)
Recall	**5.42**	**0.0015**	Yes (<0.05)
F1-Score	**4.33**	**0.0046**	Yes (<0.05)

Since all **p-values are below 0.05,** it **rejects the null hypothesis and concludes** that at least one classifier's performance is significantly different from the others. **Post-hoc Tukey's HSD (Honestly Significant Difference) test** confirms that **MV-3 consistently performs better than other classifiers** in all four metrics.
The paired t-tests and ANOVA results indicate that MV-3 significantly outperforms all individual classifiers, with p-values below 0.05 for all metrics in the paired t-tests. The one-way ANOVA confirms that performance differences among classifiers are statistically significant at a 95% confidence level ($p < 0.05$), rejecting the null hypothesis of equal performance. SVM and Naïve Bayes perform significantly worse than MV-3, with p-values far below 0.01, confirming MV-3's superior classification capability. Although RF and XGBoost are strong individual classifiers, MV-3 consistently surpasses them in accuracy, precision, recall, and F1-score, making it the best choice for real-time DDoS detection in 5G networks.

E. Model Selection Rationale and ROC Analysis

Table 9: F1-Score of Machine Learning Models

Threats	Random Forest	Decision Tree	SVM	Naïve Bayes	XGBoost	MV-3
DrDoS_SNMP	1.00	1.00	1.00	0.98	1.00	1.00
DrDoS_DNS	1.00	1.00	1.00	0.99	1.00	1.00
DrDoS_MSSQL	1.00	1.00	0.98	0.99	1.00	1.00
DrDoS_NetBIOS	1.00	0.98	0.99	0.99	1.00	1.00
DrDoS_UDP	1.00	1.00	1.00	1.00	1.00	1.00
DrDoS_SSDP	1.00	1.00	0.91	0.99	1.00	1.00
DrDoS_LDAP	1.00	0.99	0.89	0.99	1.00	1.00
Syn	1.00	1.00	1.00	0.99	1.00	1.00
DrDoS_NTP	1.00	1.00	1.00	1.00	1.00	1.00
UDP-lag	1.00	1.00	0.96	0.99	1.00	1.00
BENIGN	1.00	0.62	1.00	1.00	0.82	1.00
WebDDoS	1.00	0.50	1.00	0.50	0.63	1.00

Table 9 presents the F1-Scores for various machine learning models in detecting cyber threats, including DrDoS, SYN flood, UDP-lag attacks, benign traffic, and WebDDoS. The F1-score, which balances precision and recall, provides a comprehensive assessment of each model's classification effectiveness. Random Forest, XGBoost, and MV-3 perform exceptionally well, achieving an F1-score of 1.00 for nearly all attack types. However, SVM and Naïve Bayes struggle with DrDoS_SSDP (0.91) and DrDoS_LDAP (0.89), reflecting challenges in accurately classifying these attacks. Decision Trees exhibit weaknesses in classifying benign traffic (0.62) and WebDDoS

(0.50), while XGBoost also struggles with benign traffic (0.82) and WebDDoS (0.63). Among all models, MV-3 outperforms all others, achieving perfect classification across all threat categories and showcasing the effectiveness of ensemble learning in cybersecurity. As shown in Figure 7, the ROC curve for the Majority Voting classifier (MV-3) highlights its superior performance across various classification thresholds. Figure 8 presents the ROC curve for the Decision Tree classifier, illustrating its good performance but less robustness compared to ensemble methods. Figure 9 shows the ROC curve for the SVM classifier, highlighting its limitations, particularly in distinguishing certain types of attacks. Figure 10 presents the ROC curve for XGBoost, illustrating its strong performance but also highlighting some weaknesses, particularly in distinguishing between benign traffic and WebDDoS. These figures collectively support MV-3's superior performance, confirming its suitability for real-time DDoS detection in 5G networks.

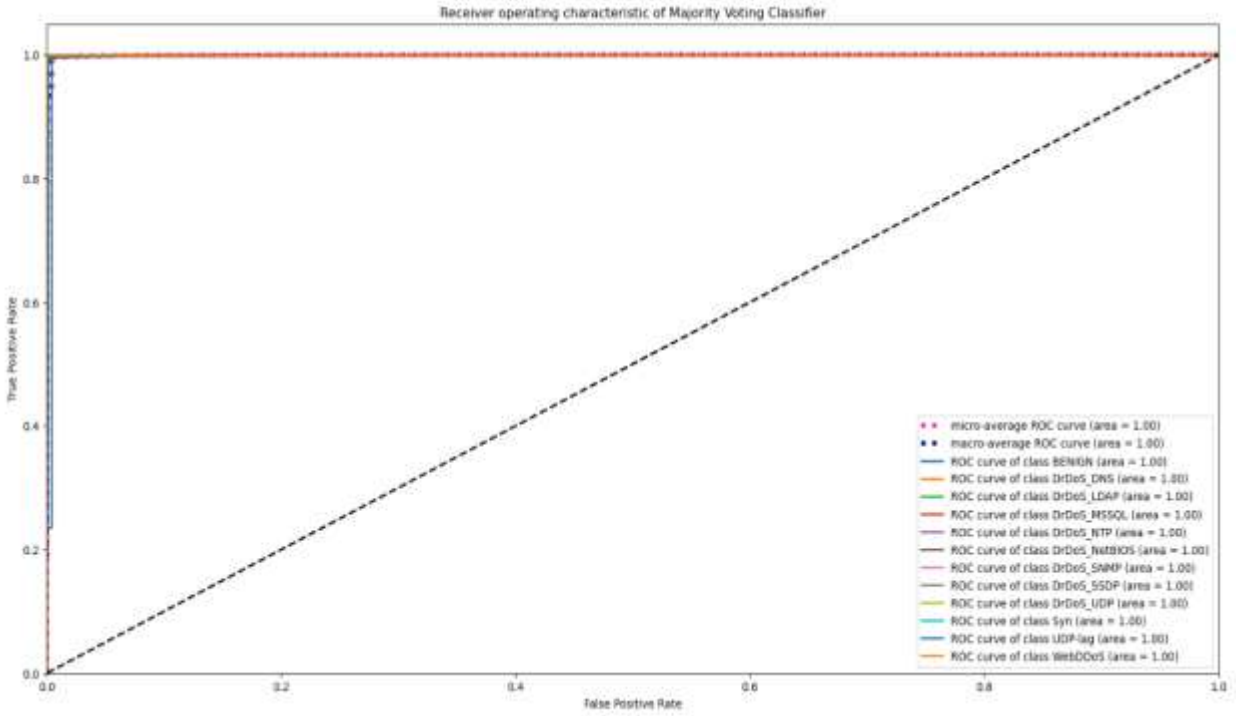

Figure 7: ROC of majority voting classifier

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

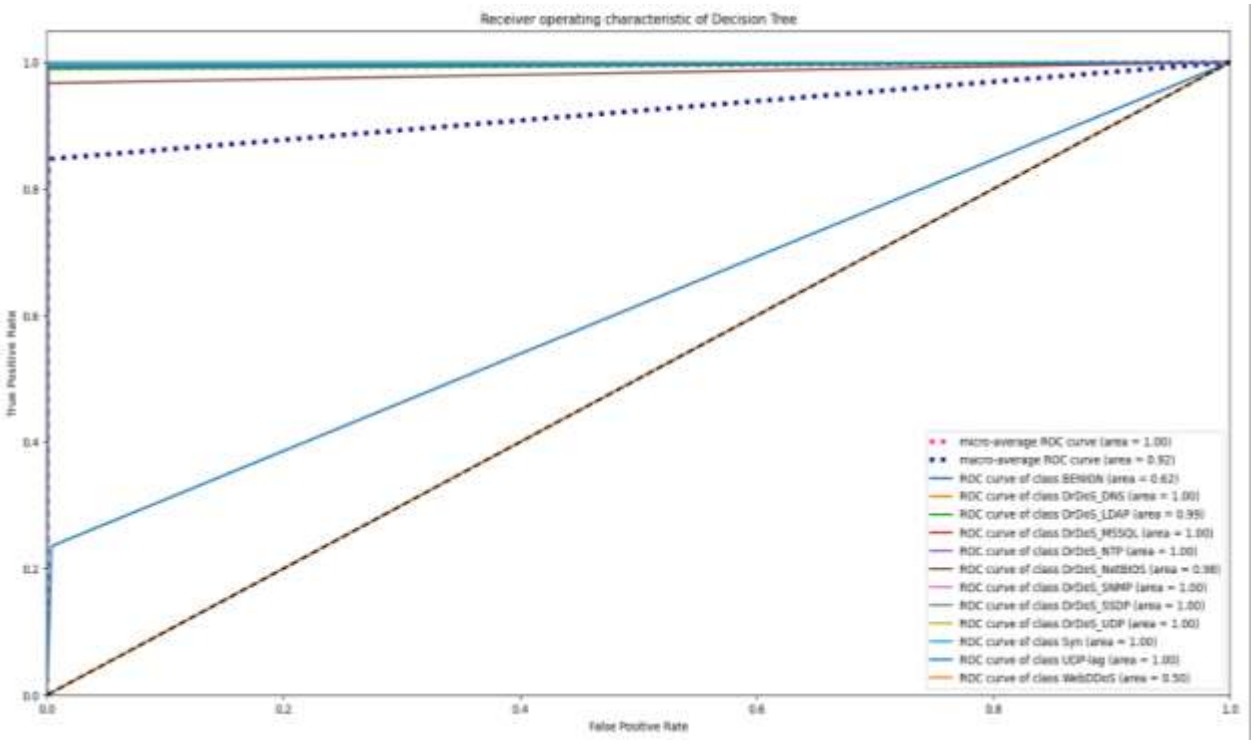

Figure 8: ROC of Decision Tree classifier

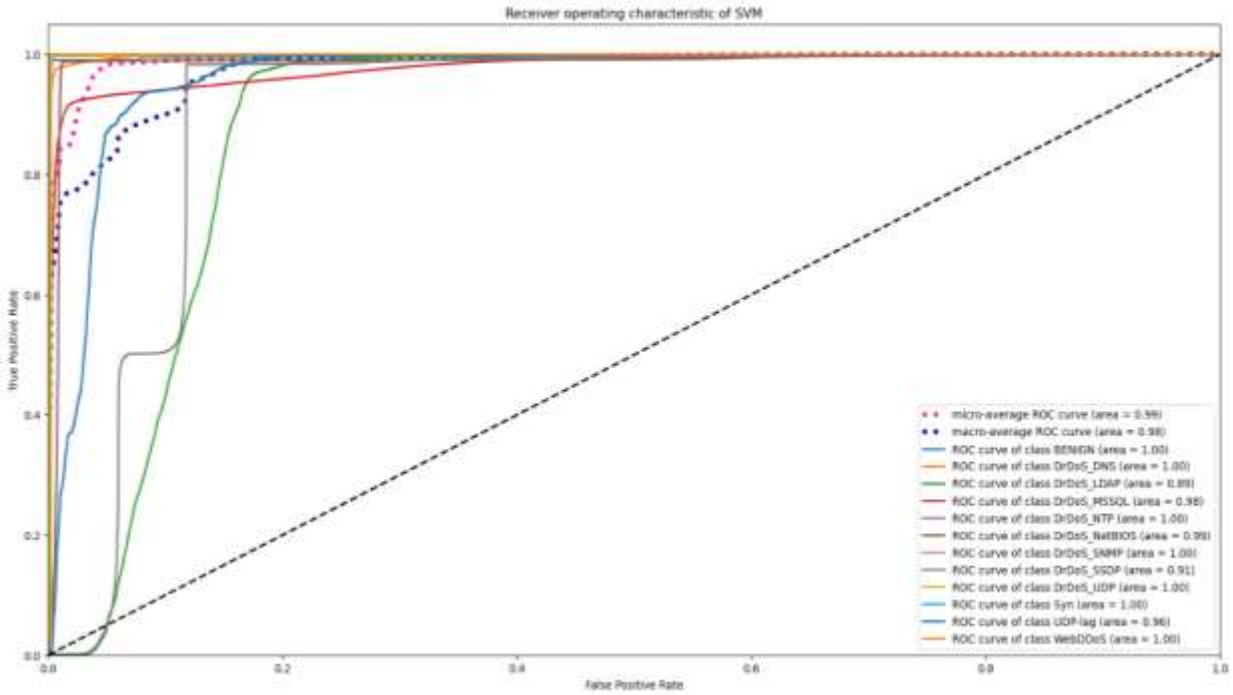

Figure 9: ROC of SVM classifier

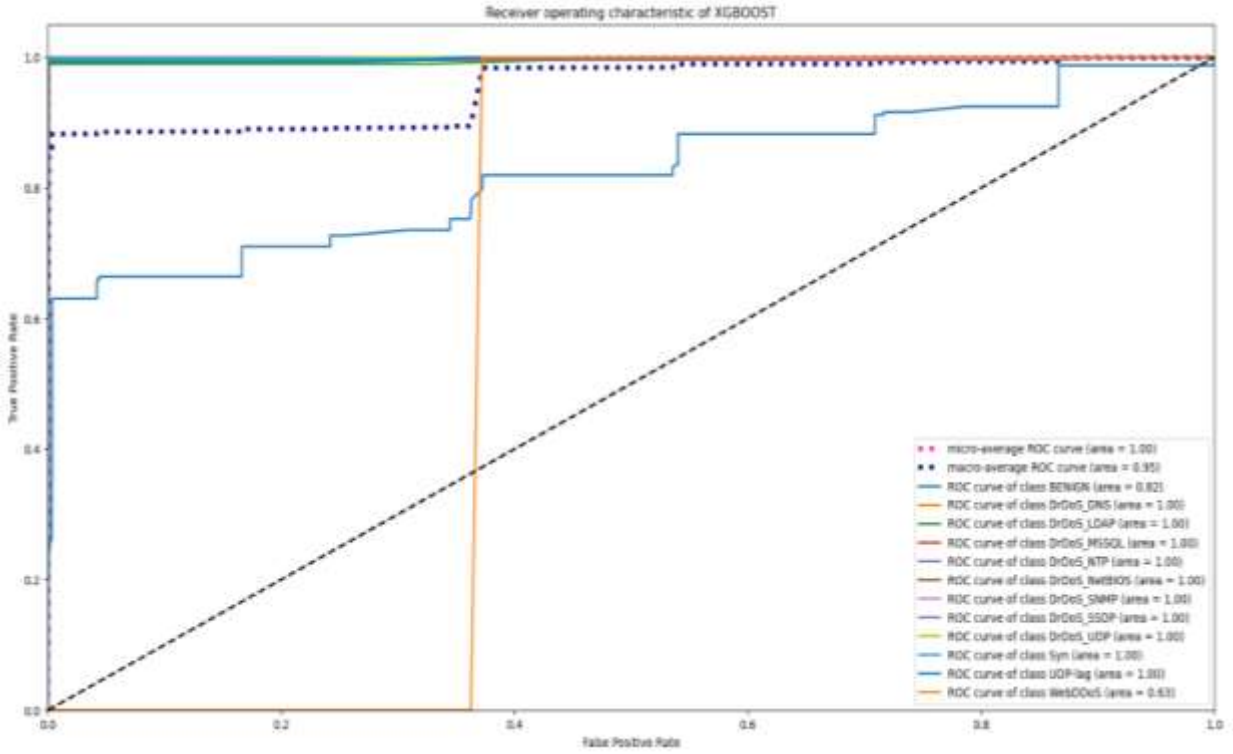

Figure 10: ROC of XGBoost classifier

F. Comparison with Existing Approaches

Table 10 compares existing data processing techniques with a proposed approach, showcasing improvements in key areas. Traditional feature selection methods, such as PCA and Mutual Information, reduce dimensionality, whereas the proposed approach retains only the most relevant features using an F1-score-based selection method. For handling imbalanced data, conventional techniques such as ROS and SMOTE are replaced by an advanced ensemble balancing method, enhancing minority class detection. Unlike Min-Max Scaling or Z-score standardization, the proposed approach dynamically adapts normalization based on dataset characteristics. Data augmentation shifts from synthetic data generation to real-time augmentation for better model generalization. Noise reduction, typically handled with Gaussian or Median filters, is enhanced through advanced denoising techniques that utilize feature correlation and anomaly detection. The proposed method significantly enhances computational efficiency by reducing overhead through optimized feature selection and lightweight processing. It also improves scalability, efficiently handling large datasets by optimizing memory management. Unlike PCA, which can cause information loss, the proposed approach selects key features based on statistical relevance, ensuring accuracy and adaptability in data preprocessing.

Table 10: Comparison Table of Current Data Processing Methods and Proposed Approaches

Features	Existing Data Processing Techniques	Proposed Procedure	References
Feature Selection	Traditional methods, such as Principal Component Analysis (PCA) and Mutual Information, are used for dimensionality reduction.	It uses F1-score-based feature selection, ensuring only the most relevant features are retained.	[14]

Handling Imbalanced Data	Uses Random Over-Sampling (ROS) and Synthetic Minority Over-Sampling Technique (SMOTE) to balance datasets.	Employs an advanced ensemble balancing approach to maintain data integrity and improve minority class detection.	[15]
Data Normalization	Applies Min-Max Scaling or Standardization (Z-score) to normalize numerical features.	It employs an adaptive normalization technique that adjusts according to dataset characteristics.	[16]
Data Augmentation	Primarily limited to synthetic data generation for minority class expansion.	Integrates real-time augmentation techniques to improve model generalization.	[17]
Noise Reduction	Utilizes standard filtering techniques, such as Gaussian or Median filters.	Implements an advanced denoising method based on feature correlation and anomaly detection.	[18]
Computational Efficiency	Computationally expensive for large-scale data due to high-dimensional feature space.	Optimized feature selection and lightweight processing reduce computational overhead.	[19]
Scalability	Often struggles with large datasets, requiring extensive preprocessing.	Efficient handling of large-scale network traffic data with optimized memory management.	[11]
Performance Impact	Some preprocessing steps, such as Principal Component Analysis (PCA), may result in information loss, which can affect model accuracy.	Ensures minimal information loss by selecting key features based on statistical relevance.	[20]

The proposed approach, utilizing the MV-3 ensemble model, achieved a remarkable accuracy of 99.9973% for binary classification and over 99.75% for multiclass detection. The Random Forest (RF) classifier also demonstrated strong performance, achieving an accuracy of 99.9973%, which proves its effectiveness in detecting DDoS attacks in 5G environments. Compared to deep learning models like CNNs and LSTMs, which typically achieve around 99.5% accuracy but require high computational resources, the proposed method offers competitive or superior performance with greater efficiency.

MV-3 outperformed deep learning-based models in precision, recall, and F1-score, particularly across different attack types, achieving perfect F1-scores (1.00) in most cases. While CNNs and LSTMs are effective, their computational intensity and scalability limitations hinder real-time deployment. Unlike deep learning models that rely on automatic feature extraction, MV-3 employs an F1-score-based feature selection method, enabling faster training and more efficient data handling. For real-world deployment, the models in this study are well-suited for real-time DDoS detection in 5G networks due to their efficiency and scalability. While deep learning models may excel in specialized settings, their resource-intensive nature limits their practical implementation. The proposed approach stands out for its balance of high performance, adaptability, and computational efficiency, making it ideal for real-world cybersecurity applications.

Table 11: Comparison with the State-of-the-art models

Characteristic	This Paper	State-of-the-Art
Performance Metrics	MV-3 (Majority Voting) achieves the highest accuracy, with 99.7612% for binary classification and 99.5112% for multiclass classification. The RF classifier also reaches 99.9973% accuracy.	Recent models report 99.5% accuracy with CNNs and LSTMs [21]. Deep learning models are more computationally intensive [4].

Precision, Recall, F1-Score	MV-3 shows perfect F1 scores in most attack types (1.00). - High precision and recall across classes.	CNNs and LSTMs achieve high precision and recall but at the cost of higher computational costs [7].
Binary vs. Multiclass Classification	Excellent performance in binary classification (99.7612% accuracy). Multiclass accuracy remains high (99.5112%).	CNN and LSTM models perform well in binary and multiclass tasks but may struggle with complex attack types and variance in attack patterns [12].
Computational Efficiency	Faster training and inference, especially with DT and Naïve Bayes. - Efficient, less resource-demanding.	Deep learning models require GPUs and more computational resources for real-time DDoS detection [22].
Feature Selection	Feature selection using F1-score reduces features, improving speed without sacrificing accuracy.	Deep learning models do not emphasize feature engineering, instead relying on automatic feature learning, but can be inefficient in terms of resource use [5]. PCA and dimensionality reduction are utilized in state-of-the-art (SOTA) models, but they can still be slower [6].
Adaptability and Scalability	Ensemble methods (MV-3) combine classifiers to reduce bias and variance, making them scalable and adaptable to new attacks.	Deep learning models excel at learning complex patterns but often require retraining and large datasets, which can hinder their scalability and adaptability [23].
Handling Data Imbalance	Effective use of feature selection and ensemble voting to address data imbalance.	Employ oversampling, undersampling, or adjustments to the loss function; however, imbalance issues can persist, particularly with rare attack types [7].
Real-World Deployment Suitability	MV-3 and RF are well-suited for real-time DDoS detection in 5G networks. - High accuracy and efficient computational performance.	Deep learning models show potential but are less practical for real-time deployment without specialized hardware (e.g., GPUs) and efficient handling of data imbalance [10].

G. Discussion of Results

The paper provides valuable insights into the performance of machine learning models for detecting DDoS attacks in 5G networks, emphasizing the practical implications for real-world deployments. The evaluation of binary and multiclass classification models using key performance metrics highlights that ensemble methods, particularly Majority Voting (MV-3), outperform individual classifiers in terms of accuracy and robustness, especially in real-world 5G network conditions. MV-3 is less susceptible to class imbalance and performs more consistently across diverse network conditions, which is crucial for maintaining high security levels in dynamic 5G environments.

In binary classification, Random Forest (RF) achieved the highest accuracy (99.9973%), followed closely by Support Vector Machine (SVM). Decision Trees (DT) and XGBoost strike a balance between accuracy and efficiency, whereas Naïve Bayes (NB) is computationally efficient but slightly less accurate. However, in the context of real-world 5G networks, MV-3 stands out due to its ensemble approach, which aggregates the strengths of individual classifiers and provides a more robust solution. This makes MV-3 particularly advantageous when dealing with the complex, evolving attack patterns typical in a 5G environment, where data imbalance is prevalent.

For multiclass classification, ensemble models such as RF, XGBoost, and MV-3 achieved superior accuracy, with MV-3 reaching 99.5112%. SVM and NB faced challenges in handling the complex attack patterns characteristic of 5G networks, highlighting the importance of using models that can adapt to a variety of attack types. Feature selection, using an ExtraTreesClassifier, and optimizing the F1-score resulted in a reduction of the dataset from 85 to 20 features, thereby enhancing model efficiency without compromising accuracy. This is critical for 5G networks, where the volume of traffic data is immense, and efficient feature selection is necessary for scalable deployment.

Compared to deep learning models, such as CNNs and LSTMs, the proposed ensemble methods, particularly MV-3, demonstrate better computational efficiency while maintaining high accuracy. Deep learning models often require specialized hardware, such as GPUs, and struggle with class imbalance, even when oversampling and undersampling techniques are used. MV-3 addresses these challenges by integrating ensemble balancing strategies, ensuring that the learning process distributes effectively across different attack classes, leading to more accurate and reliable detections.

In practical terms, the results of this paper show that the Majority Voting (MV-3) ensemble model is a robust choice for detecting and classifying DDoS attacks in 5G networks. MV-3 consistently outperforms other classifiers, including RF, XGBoost, DT, SVM, and NB, in terms of accuracy, precision, recall, and F1-score. While RF and XGBoost exhibit strong performance with high accuracy and F1-scores for most attack types, MV-3 excels by integrating multiple classifiers, thus offering better generalization and robustness. Statistical evaluations, including McNemar's test and paired t-tests, confirm that MV-3's performance improvements were statistically significant ($p < 0.05$) and stable.

From a deployment perspective, striking a balance between accuracy and computational efficiency is key when considering a DDoS detection system in a 5G network. While RF and XGBoost achieve high accuracy, they come with a considerable computational cost. Although MV-3 is slightly slower in training compared to XGBoost, it delivers superior performance with a manageable computational overhead, making it well-suited for real-time applications. In contrast, DT and NB, while offering lower computational costs, trade off accuracy, making them less appropriate for high-security, large-scale deployments. SVM, despite its high accuracy, suffers from extended training and testing times, making it unsuitable for time-sensitive environments.

Scalability is another critical factor in real-world 5G cybersecurity applications. Large-scale 5G networks generate vast amounts of traffic data, posing challenges for traditional deep learning models, which demand substantial memory and computational resources for real-time inference. This study demonstrates that MV-3 is not only competitive in performance but also computationally efficient, making it a viable option for deployment in resource-constrained environments. The reduced training time and memory requirements, compared to deep learning models, enhance the feasibility of MV-3 for real-time network security applications in large-scale 5G networks.

V. Conclusion

This paper demonstrated the effectiveness of Majority Voting (MV-3) ensemble models for detecting Distributed Denial of Service (DDoS) attacks in 5G networks, highlighting their practical benefits in terms of accuracy, robustness, and computational efficiency. MV-3 consistently outperforms individual classifiers, such as Random Forest (RF), XGBoost, Decision Tree (DT), Support Vector Machine (SVM), and Naïve Bayes (NB), especially in real-world 5G environments where data imbalance and evolving attack patterns are prevalent. By aggregating the strengths of multiple classifiers, MV-3 ensures high detection accuracy while minimizing computational overhead, making it an ideal solution for large-scale, real-time network security applications.

The practical benefits of the MV-3 ensemble approach are significant. It enhances accuracy and robustness across diverse attack types and network conditions, outperforming individual classifiers in both binary and multiclass classification scenarios, and effectively addresses class imbalance. MV-3 offers a balanced trade-off between high performance and manageable computational cost, making it suitable for resource-constrained environments. MV-3 is scalable and can handle the large volumes of traffic data generated by 5G networks, providing real-time detection without the need for specialized hardware, such as GPUs, unlike deep learning models.

Future research could focus on several avenues to further enhance the performance and applicability of ensemble models, such as MV-3, in 5G cybersecurity. One potential direction is the **integration of deep learning models**, such as Convolutional Neural Networks (CNNs) or Long Short-Term Memory (LSTM) networks, with ensemble methods to improve detection capabilities for more complex attack patterns. CNNs can assist with feature extraction, while LSTMs can capture temporal dependencies in traffic data, thereby enhancing the model's performance in dynamic environments. Another area of exploration is **optimizing ensemble strategies** by incorporating advanced techniques, such as boosting, stacking, or weighted voting. These methods can improve detection accuracy and reduce computational burden, making them adaptable to various 5G network conditions and attack types. **Feature selection and data augmentation** techniques could also be investigated to handle large-scale, imbalanced datasets,

potentially through synthetic data generation or adversarial training, further boosting the robustness of the ensemble model.

Real-time performance in large-scale networks should be a key focus. As 5G networks generate vast amounts of traffic data, scaling MV-3 to meet the demands of real-time detection will be essential. Federated learning could also be explored for distributed DDoS detection across multiple 5G network nodes, improving scalability and efficiency.

DECLARATIONS

• Funding: Not applicable

• Conflict of interest/competing interests: The authors declare that there are no conflicts of interest

• Ethics approval: not applicable

• Consent to participate: not applicable

• Consent for publication: not applicable

• Availability of data and materials: available on request

• Code availability: available on request

CRediT authorship contribution statement

Berhanu Endesha Bekele: Conceptualization, Methodology, Writing original draft. Dereje Regassa: Analysis, Supervision, Writing, review and editing. Ravindra Babu: Supervision, Visualization and Workeneh Geleta Negassa: Writing, review and editing.

References

[1] Q. Abbas, S. Hina, H. Sajjad, K. S. Zaidi, and R. Akbar, "Optimization of predictive performance of intrusion detection system using hybrid ensemble model for secure systems," *PeerJ Comput. Sci.*, vol. 9, 2023, doi: 10.7717/peerj-cs.1552.

[2] S. S. A. Naqvi, Y. Li, and M. Uzair, "DDoS attack detection in smart grid network using reconstructive machine learning models," *PeerJ Comput. Sci.*, vol. 10, pp. 1–23, 2024, doi: 10.7717/peerj-cs.1784.

[3] M. Varotto, F. Heinrichs, T. Schuerg, S. Tomasin, and S. Valentin, "Detecting 5G Narrowband Jammers with CNN, k-nearest Neighbors, and Support Vector Machines," *IEEE Netw.*, 2024, [Online]. Available: http://arxiv.org/abs/2405.09564

[4] D. M. Rajan and D. D. J. Aravindhar, "Detection and Mitigation of DDOS Attack in SDN Environment Using Hybrid CNN-LSTM," *Migr. Lett.*, vol. 20, no. S13, pp. 407–419, 2023, doi: 10.59670/ml.v20is13.6472.

[5] J. Zhao, Y. Liu, Q. Zhang, and X. Zheng, "CNN-AttBiLSTM Mechanism: A DDoS Attack Detection Method Based on Attention Mechanism and CNN-BiLSTM," *IEEE Access*, vol. 11, no. November, pp. 136308–136317, 2023, doi: 10.1109/ACCESS.2023.3334916.

[6] N. U. Ain, M. Sardaraz, M. Tahir, M. W. A. Elsoud, and A. Alourani, "Securing IoT Networks Against DDoS Attacks : A Hybrid Deep Learning Approach," *Sensors*, pp. 1–23, 2025.

[7] M. Sinthuja and K. Suthendran, "Detection of Unknown DDoS Attacks with Deep Learning and Gaussian Mixture Model," *Appl. Sci.*, pp. 1213–1218, 2022, doi: 10.1109/ICOSEC54921.2022.9951976.

[8] S. Samarakoon *et al.*, "5G-NIDD: A Comprehensive Network Intrusion Detection Dataset Generated over 5G Wireless Network," *http://arxiv.org/abs/2212.01298*, 2022, [Online]. Available: http://arxiv.org/abs/2212.01298

[9] S. Shakya, R. Abbas, and S. Maric, "A Novel Zero-Touch , Zero-Trust , AI / ML Enablement Framework for IoT Network Security," *https://arxiv.org/pdf/2502.03614*, 2025.

[10] M. S. Ataa, E. E. Sanad, and R. A. El-khoribi, "Intrusion detection in software defined network using deep learning approaches," *Sci. Rep.*, vol. 14, no. 1, pp. 1–15, 2024, doi: 10.1038/s41598-024-79001-1.

[11] R. K. Batchu, T. Bikku, S. Thota, H. Seetha, and A. A. Ayoade, "A novel optimization-driven deep learning framework for the detection of DDoS attacks," *Sci. Rep.*, vol. 14, no. 1, 2024, doi: 10.1038/s41598-024-77554-9.

[12] X. Yin, W. Fang, Z. Liu, and D. Liu, "A novel multi-scale CNN and Bi-LSTM arbitration dense network model for low-rate DDoS attack detection," *Sci. Rep.*, vol. 14, no. 1, pp. 1–15, 2024, doi: 10.1038/s41598-024-55814-y.

[13] B. Farzaneh, N. Shahriar, A. H. Al Muktadir, M. S. Towhid, and M. S. Khosravani, "DTL-5G: Deep transfer learning-based DDoS attack detection in 5G and beyond networks," *Comput. Commun.*, vol. 228, p. 107927, Dec. 2024, doi: 10.1016/J.COMCOM.2024.107927.

[14] Y. E. Kim, Y. S. Kim, and H. Kim, "Effective Feature Selection Methods to Detect IoT DDoS Attack in 5G Core Network," *Sensors*, vol. 22, no. 10, 2022, doi: 10.3390/s22103819.

[15] A. Alfatemi, M. Rahouti, R. Amin, S. ALJamal, K. Xiong, and Y. Xin, "Advancing DDoS Attack Detection: A Synergistic Approach Using Deep Residual Neural Networks and Synthetic Oversampling," *https://arxiv.org/pdf/2401.03116*, 2024, [Online]. Available: http://arxiv.org/abs/2401.03116

[16] S. Sadhwani, B. Manibalan, R. Muthalagu, and P. Pawar, "A Lightweight Model for DDoS Attack Detection Using Machine Learning Techniques," *Appl. Sci.*, vol. 13, no. 17, 2023, doi: 10.3390/app13179937.

[17] A. K. Silivery, K. R. M. Rao, and L. K. Suresh Kumar, "An Effective Deep Learning Based Multi-Class Classification of DoS and DDoS Attack Detection," *Int. J. Electr. Comput. Eng. Syst.*, vol. 14, no. 4, pp. 421–431, 2023, doi: 10.32985/ijeces.14.4.6.

[18] M. S. Raza, M. N. A. Sheikh, I. S. Hwang, and M. S. Ab-Rahman, "Feature-Selection-Based DDoS Attack Detection Using AI Algorithms," *Telecom*, vol. 5, no. 2, pp. 333–346, 2024, doi: 10.3390/telecom5020017.

[19] D. Han, H. Li, X. Fu, and S. Zhou, "Traffic Feature Selection and Distributed Denial of Service Attack Detection in Software-Defined Networks Based on Machine Learning," *Sensors*, vol. 24, no. 13, 2024, doi: 10.3390/s24134344.

[20] S. Park, B. Cho, D. Kim, and I. You, "Machine Learning Based Signaling DDoS Detection System for 5G Stand Alone Core Network," *Appl. Sci.*, vol. 12, no. 23, 2022, doi: 10.3390/app122312456.

[21] C. S. Shieh, T. T. Nguyen, and M. F. Horng, "Detection of Unknown DDoS Attack Using Convolutional Neural Networks Featuring Geometrical Metric," *Mathematics*, vol. 11, no. 9, 2023, doi: 10.3390/math11092145.

[22] M. B. Anley, A. Genovese, D. Agostinello, and V. Piuri, "Robust DDoS attack detection with adaptive transfer learning," *Comput. Secur.*, vol. 144, no. June, p. 103962, 2024, doi: 10.1016/j.cose.2024.103962.

[23] M. Li, B. Zhang, G. Wang, B. Zhuge, X. Jiang, and L. Dong, "A DDoS attack detection method based on deep learning two-level model CNN-LSTM in SDN network," *Proc. - 2022 Int. Conf. Cloud Comput. Big Data Appl. Softw. Eng. CBASE 2022*, pp. 282–287, 2022, doi: 10.1109/CBASE57816.2022.00062.