An Efficient Approach Using Lightweight Machine Learning Models for Detection of DDoS Attacks on IoT Devices

Mamoona Nawaz * and Shireen Tahira

Posted Date: 20 March 2025

doi: 10.20944/preprints202503.1508.v1

Keywords: Machine Learning; Artificial intelligence; Internet of things; DDoS Attacks; Networking; Cyber security

 doi:10.20944/preprints202503.1508.v1

Article

An Efficient Approach Using Lightweight Machine Learning Models for Detection of DDoS Attacks on IoT Devices

Mamoona Nawaz * and Shireen Tahira

Department of Computer Science, IIU

* Correspondence: mamoonanawaz62@gmail.com

Abstract: Advancements in the Internet of Things (IoT) have introduced significant security challenges, with Distributed Denial of Service (DDoS) attacks emerging as one of the most critical threats. These attacks involve botnets controlled by attackers that flood networks with malicious traffic, disrupting legitimate services. As the global DDoS landscape evolves, it has become ever more critical for IoT devices to identify and mitigate these threats rapidly. Machine learning has emerged as a promising method for DDoS detection; however, the field lacks a standardized and efficient framework designed for the resource-constrained nature of IoT devices. Existing solutions often depend on overly complex models, overlooking the chance to utilize lightweight and efficient techniques for real-world deployment. To address these limitations, this research proposes a novel framework that combines feature selection and lightweight machine learning models for efficient DDoS detection in IoT environments. The proposed framework integrates feature selection techniques to identify the most relevant features for enhancing detection efficiency. It influences lightweight machine learning models to ensure compatibility with IoT devices with limited computational resources. Specifically, this study evaluates three machine learning models, Random Forest, Logistic Regression, and Naive Bayes, for binary classification of DDoS attacks, using the NSL-KDD dataset for evaluation. The framework seamlessly integrates feature selection with lightweight models, improving performance, increased efficiency, and lower computational overhead. The results demonstrate that the proposed framework significantly outperforms existing methods, achieving 99.88% detection accuracy with the Random Forest model, 91.61% with Logistic Regression, and 87.62% with Naive Bayes. This research advances IoT security by integrating feature selection with lightweight machine learning, providing practical and effective solutions for wireless applications.

Keywords: Machine Learning; Artificial intelligence; Internet of things; DDoS Attacks; Networking; Cyber security

Introduction

The Internet of Things (IoT) has fundamentally transformed how modern technology operates by changing the way people engage with the physical world and other devices. The term Internet of Things (IoT) encompasses a wide array of physical objects and systems connected via the Internet or other communication and information transfer methods, typically without human involvement (Dachyar, Zagloel, and Saragih 2019). A significant need has arisen for IoT devices in both private and business sectors. This includes a variety of smart home devices, thermostats, refrigerators, and security systems, as well as industrial, medical, and transport systems (Hussein 2019). The IoT transformation brings many benefits, such as increased efficiency, improved automation, and enhanced ease of use in healthcare, agriculture, manufacturing, and urban development. However, with the rise of IoT devices, the risks associated with their widespread use have significantly

 doi:10.20944/preprints202503.1508.v1

increased. These devices are highly vulnerable to attacks due to limitations like insufficient processing capabilities, weak security protocols, and inadequate system configurations (Radouan Ait Mouha 2021). There are several cyber threats to which IoT devices are vulnerable, and among these, DDoS attacks are considered particularly dangerous. A DDoS attack occurs when multiple compromised applications overwhelm a target computer or network with excessive traffic, preventing legitimate users from accessing the site. Many IoT devices carry out critical functions, such as health monitoring, industrial control, and smart city systems, and even a minor attack on these devices can result in catastrophic consequences, including service failure, property damage, or even loss of life (Mu and Antwi-Afari 2024).

The methods employed in DDoS detection are increasingly ineffective in addressing the complexity and dynamism of IoT networks. The primary limitation of signature-based techniques, which depend on identifying previously known attacks, is that these approaches struggle when faced with new, more advanced attack models (Gelgi et al. 2024). Furthermore, while anomaly-based methods excel at detecting unusual behaviors, they often suffer from higher false positive rates and require significant resources. Due to limitations in processing power, memory, and bandwidth in IoT devices, many conventional approaches to detecting DDoS attacks are too computationally intensive for these devices and therefore cannot be executed in real time. Consequently, there is an urgent need to develop lightweight systems capable of efficiently performing DDoS detection with minimal impact on IoT resources (Almadhor et al. 2024). This research focuses on developing an efficient, lightweight ML model for detecting DDoS attacks on IoT devices to address this gap. The proposed method utilizes a machine learning approach to filter out DDoS attacks while maintaining high accuracy with the support of adaptive facilities. In this introduction, the context, problem, objectives, relevance, and scope of the study are described to establish the research need and set expectations for advancing knowledge in the field.

DDoS Attacks

The IoT has transformed how humans interact with technology by enhancing the integration and information exchange among devices. Predictions indicate that IoT devices will increase to 35 billion by 2025; these insights highlight the potential risks associated with these devices (Mahadik, Pawar, and Muthalagu 2023). Many IoT devices are characterized by inadequate security measures, making them all highly susceptible to various types of cyber threats. One of the most significant risks identified is Distributed Denial of Service (DDoS) attacks. With the growing adoption of the Internet of Things in various industries, the safety of these devices becomes crucial. IoT devices offer insights into the performance and safety of healthcare facilities, smart cities, and industrial control systems. They can lead to severe consequences, including financial losses, disruptions to critical services, and threats to human lives (Elgazzar et al. 2022). The combination of numerous networked devices and inadequate security measures creates an ideal environment for malicious actors. These devices often lack robust security mechanisms, making them vulnerable and putting essential infrastructures at risk of threats like DDoS attacks.

In 2017, as expected, an IoT botnet known as IoT Reaper or IoTroop exploited vulnerabilities in IoT devices, thereby creating a functional botnet (Hussain et al. 2020). This malicious botnet primarily targeted household devices such as routers, IP cameras, and Network-Attached Storage systems. The IoT Reaper botnet represents a new level of both volume and complexity in DDoS attacks aimed at IoT devices (Nižetić et al. 2020). This contrasts with previous types of botnets that relied on a single vulnerability in IoT devices, allowing IoT Reaper to create a vast network of compromised devices. These hackers demonstrated that IoT networks lack sufficient security measures, which should prompt more reliable safety protocols in the future. Regarding the purpose of the botnet, its function is still unclear; however, it has the potential to launch large-scale DDoS attacks, which can physically disrupt critical components. Fortunately, security experts have intervened and curtailed its spread by taking control of its server infrastructure. In addition to the healthcare sector, the control systems of smart grids managing the energy infrastructure of entire nations are also at risk of DDoS attacks.

 doi:10.20944/preprints202503.1508.v1

A successful strike could incapacitate a power plant's control systems, resulting in blackouts or even causing destruction (Taherdoost 2023). Transportation, likewise, is not immune to such threats, as connected cars and traffic management systems can be compromised, leading to chaos in city amenities that can result in either an accident or a traffic jam. Figure 1 shows how a DDoS attack can disrupt communication between pacemakers and hospital networks and its implications for healthcare. It depicts the various phases of the attack and the impact on crucial patient information.

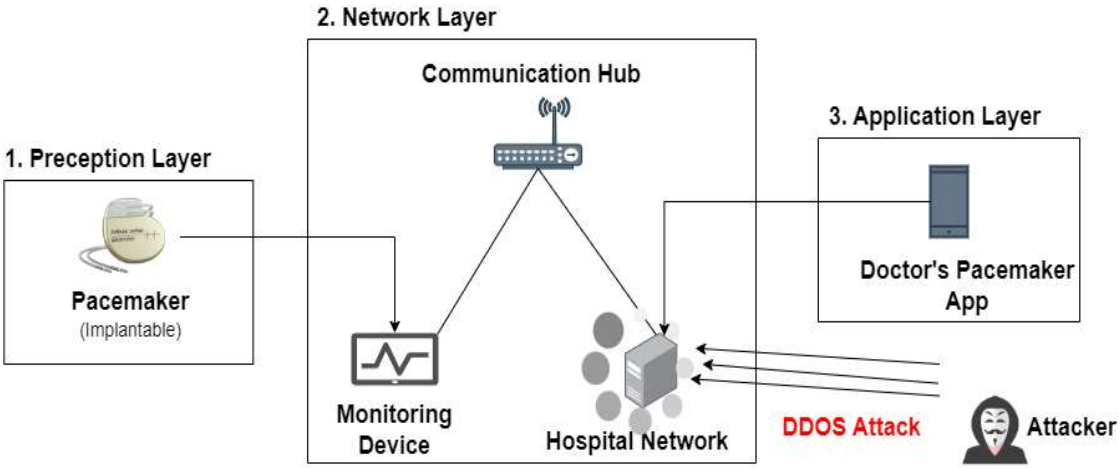


Figure 1. DDoS Attack on Healthcare device.

However, it can easily be demonstrated how a DDoS attack endangers IoT security in our everyday lives, particularly in healthcare, such as with pacemakers. These devices sync data with a hospital's tracking platform to monitor the patient's heartbeat. An attack on the hospital's network can inundate the servers with requests, disrupting effective communication between the pacemaker and the tracking system. This disruption can lead to a serious lack of necessary medical interventions, putting the patient's well-being at risk (Sadek et al. 2022). In the worst-case scenario, such an attack could leave a person in critical condition, necessitating immediate medical attention. The Figure 1 illustrates how a DDoS attack occurs on the pacemaker system.

Related Work

The rising danger of cyberattacks on Internet of Things (IoT) systems has highlighted the limitations of intrusion detection systems, especially when challenged with advanced threats in complex environments. (Jullian et al. 2023) . To address these threats, the authors propose a new distributed framework based on deep learning attack detection techniques. This framework relies on deep learning models that primarily focus on feedforward neural networks and LSTMs to examine network traffic behaviors for detecting illegitimate performance. The proposed solution distributes detection workloads across various network nodes, resulting in improved scalability, more efficient operation, and greater network resilience. The research demonstrates how the framework accurately detects different types of attacks through performance evaluation with real-world testing. Overall, the research significantly enhances IoT system security by presenting an advanced strategy to detect cyber threats more effectively.

The limitations of intrusion detection systems in identifying various cyberattack types have prompted exploration into more advanced techniques. Deep learning shows significant promise for enhancing these systems, which is why a new model for multi-attack classification is proposed (Silivery et al. 2023). This model used convolutional neural networks (CNNs) and recurrent neural networks (RNNs) with long short-term memory (LSTM) units to analyze network traffic data for identifying multiple attack types. The model is trained on an extensive dataset, with evaluation based

 doi:10.20944/preprints202503.1508.v1

on performance metrics such as accuracy, precision, recall, and F1-score. The approach aims to improve both the operational effectiveness and predictive accuracy of intrusion detection systems, thereby strengthening cyber defense mechanisms for digital networks.

Traditional techniques struggle to detect and prevent advanced DDoS attacks, prompting the exploration of deep-learning methods (Aktar and Yasin Nur 2023). The authors propose utilizing deep learning approaches to enhance DDoS attack detection, given their ability to better handle complex attack patterns. This research develops a deep learning model through the implementation of neural networks, including recurrent neural networks (RNNs) with long short-term memory (LSTM) units and convolutional neural networks (CNNs), to effectively analyze network traffic data and distinguish between normal and DDoS attack traffic patterns. The model is trained on relevant data and evaluated using performance metrics such as accuracy, precision, recall, and F1-score. By applying deep learning techniques, this research aims to strengthen protection mechanisms against DDoS attacks, ultimately improving the resilience of network infrastructures.

GPU-accelerated machine learning technology is explored in the context of improving botnet attack detection capabilities (Motylinski et al. 2022). Detection methods often struggle with speed and efficiency, leading to the development of a new system that utilizes the parallel processing power of GPUs. The research investigates the performance of various machine learning algorithms, such as support vector machines (SVMs) and deep learning models, when implemented on GPU hardware. Effective feature engineering and thorough evaluations using real-world datasets are central to the methodology. By incorporating GPU acceleration, the proposed system enhances detection accuracy and speed, offering significant improvements in botnet activity identification.

Recognizing and addressing Distributed Denial of Service (DDoS) attacks continues to be a significant challenge, especially as conventional methods fall short against increasingly complex and evolving threats (Ismail et al. 2022). The study establishes a framework that creates models for detecting DDoS attacks by experimenting with various algorithms, including support vector machines (SVMs), XGBoost, Random Forests, and deep learning networks, utilizing network traffic data. These models are trained on suitable datasets and assessed using metrics like precision, recall, accuracy, and F1-score. Similarly, the goal of this research (Ahmad, Wan, and Ahmad 2023) is to harness machine learning to enhance DDoS protection systems, thereby increasing the operational resilience of networks against such attacks.

DDoS attack detection in the rapidly growing Internet of Things (IoT) networks presents a significant challenge due to the limitations of existing methods in resource-constrained environments (Hariprasad 2022). It proposes a hybrid detection solution that combines recurrent neural networks (RNNs) and extreme learning machines (ELMs). RNNs are utilized for their ability to model temporal dependencies, while ELMs contribute fast training and strong generalization capabilities. The model is further optimized through a data point selection mechanism, which identifies the most informative data points for training. The resulting hybrid system offers a more accurate and efficient approach to detecting DDoS attacks, thus improving the security of IoT networks.

Explainable AI (XAI) techniques are integrated into a novel framework proposed (Almadhor et al. 2024). Centralized methods have shown to be limited due to privacy concerns and resource constraints, leading the authors to integrate federated learning with explainable artificial intelligence (XAI). Federated learning enables collaborative model development across IoT devices while maintaining data privacy. Incorporating XAI improves the transparency of the model's decision-making processes, fostering both trust and understanding. This combined approach effectively addresses DDoS attack detection in diverse IoT environments, preserving privacy while providing explainable results for enhanced decision-making.

Fine-tuning Multi-Layer Perceptron (MLP) neural networks was explored in this paper (Sanmorino, Marnisah, and Kesuma 2024) as a method to enhance their detection capabilities for Distributed Denial-of-Service (DDoS) attacks. The authors focus on adapting pre-trained MLP models for specific use in DDoS attack detection, addressing the shortcomings of traditional methods that often fail to accurately identify such attacks. Network traffic data is preprocessed before

 doi:10.20944/preprints202503.1508.v1

evaluating the MLP model's performance using metrics such as accuracy, precision, and recall. This research aims to improve DDoS detection systems by leveraging pre-trained models tailored to strengthen security technologies against these cyber vulnerabilities.

"ML-DDoSnet" is an intrusion detection system developed to combat Denial-of-Service (DDoS) attacks in Internet of Things (IoT) environments, (Revathi, Ramalingam, and Amutha 2021). IoT networks are vulnerable to various attacks, and the researchers apply machine learning technology to analyze network traffic and detect malicious patterns indicative of DDoS attacks. The system explores several machine learning algorithms, including support vector machines (SVMs) and decision trees, to classify network traffic as either normal or malicious. The NSL-KDD dataset is used for testing and validating the performance of ML-DDoSnet through training algorithms within the framework. The development and evaluation of ML-DDoSnet aim to enhance security mechanisms across IoT networks, improving their ability to defend against DDoS attacks.

Table 1. Summary of related work.

Reference	Datasets	Objective	Methodology	Limitations
(Jullian et al. 2023)	NSL KDD	To develop a robust and efficient deep learning-based distributed attack detection framework for IoT networks.	Feedforward neural networks and recurrent neural networks (RNNs)	Deploying and managing a distributed system across a large and diverse IoT network can be complex.
(Silivery et al. 2023)	NSL KDD	To develop a deep learning-based model for classifying multiple cyber-attacks, aiming to improve the accuracy and effectiveness of intrusion detection systems.	Long-Short Term Memory Recurrent Neural Network (LSTM-RNN)	Complex Model High False Alarm Rate
(Aktar and Yasin Nur 2023)	NSL KDD	To investigate the use of a deep learning approach for detecting DDoS attacks, potentially improving the accuracy and effectiveness of	Deep Contractive Autoencoder (DCAE)	The model's performance may be limited by the availability and quality of the training data, potentially leading to inaccurate or biased detection results.

 doi:10.20944/preprints202503.1508.v1

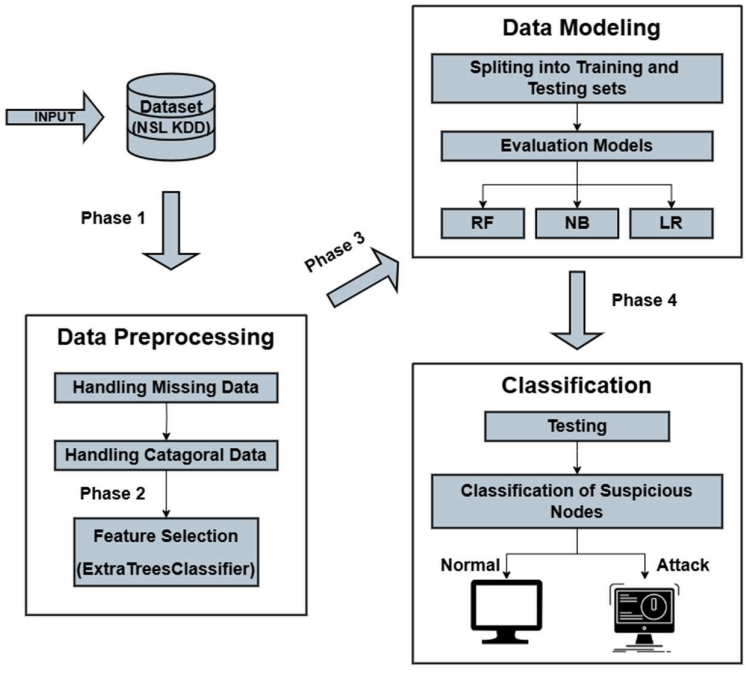
		DDoS detection methods.		
(Motylinski et al. 2022)	NSL KDD	To enhance the speed of detection while upholding a commendable level of accuracy.	SVM, logistic regression, KNN	The use of GPU technology results in decreased training and prediction time.
(Ismail et al. 2022)	NSL KDD	To categorize and predict various types of DDoSattacks through the application of machine learning.	Random forest, XGBoost	Improved accuracy may be achieved using an enhanced suggested model.
(Hariprasad 2022)	NSL KDD	To develop a precise and effective DDoS attack detection system for IoT networks with a hybrid Sample Selected RNN-ELM model.	Recurrent Neural Networks (RNNs) and Extreme Learning Machines (ELMs)	The model's efficiency may hinge on the quality and variety of the training data, together with the particular attributes of the IoT network environment.
(Almadhor et al. 2024)	NSL KDD	To provide a resilient and privacy-conscious DDoS attack detection solution for diverse IoT contexts by integrating federated learning with explainable a50rtificial intelligence approaches.	Explainable Artificial Intelligence (XAI) with Federated Deep Neural Networks (FDNNs)	The efficiency of this methodology may be affected by issues including communication latency, variability in device capabilities, and the intricacy of incorporating XAI algorithms into the federated learning framework.
(Ahmad, Wan, and Ahmad 2023)	NSL KDD	To develop an optimized ensemble framework using big data analytics to effectively	Convolutional Neural Network (CNN) embedded with a Gated Recurrent Unit (GRU)	The model's complexity results in high computational time

 doi:10.20944/preprints202503.1508.v1

		detect DDoS attacks targeting (IoT)		
(Sanmorino, Marnisah, and Kesuma 2024)	NSL KDD	To develop a DDoS attack detection system using fine-tuned Multi-Layer Perceptrons.	fine-tuned Multi-Layer Perceptron models	They are computationally intensive and slow
(Revathi, Ramalingam, and Amutha 2021)	NSL KDD	To develop a system by integrating machine learning techniques with an SDN controller framework.	Support Vector Machines, Decision Trees	The system may need to be continuously updated and adapted to effectively address new and evolving DDoS attack techniques.

Proposed Technique

The proposed framework adopts a structured approach, as shown in Figure 2. It starts with the NSL-KDD dataset. Preprocessing techniques address missing values, duplication, and normalization to guarantee data consistency. Feature selection is conducted using an Extra Trees classifier to pinpoint the most relevant attributes, improving detection efficiency while minimizing computational overhead. The refined dataset is subsequently employed to train three machine learning models: Random Forest, Logistic Regression, and Naïve Bayes, for DDoS attack classification. Model performance is assessed using accuracy, precision, recall, and F1-score. This comprehensive method enhances DDoS detection in IoT environments by combining effective preprocessing and lightweight classifiers.



 doi:10.20944/preprints202503.1508.v1

Figure 2. Architectural Diagram of proposed technique.

Motivation

The increasing complexity and scale of IoT networks necessitate effective intrusion detection systems (IDS) to guard against advancing threats. Conventional IDS frequently struggle with new attacks, which drives the adoption of machine learning (ML) to enhance IoT threat detection (Alve et al. 2025). Lightweight ML models maintain an effective balance between accuracy and speed, which is essential for IoT devices with limited resources. ML-based solutions are capable of adapting to evolving security threats, providing a more flexible defense than traditional methods. Research on ML-driven DDoS detection enhances the development of intelligent security solutions, strengthening the IoT environment against cyberattacks.

Dataset

NSL-KDD ("Intrusion Detection Systems: NSL-KDD | Saylor Academy," n.d.) is used for our research. This dataset has been derived from the KDD Cup 1999 dataset and has undergone specific modifications to address the impact of duplicate records on the outputs of intrusion detection systems. The dataset includes 41 features spread across 125,973 training records and 22,544 testing records. These features are categorized into four groups: basic features, content features, time-based features, and host-based features, which together provide a comprehensive understanding of network behaviour. The NSL-KDD dataset is utilized as it resolves the redundancy issues present in the original KDD'99 dataset, offering a more balanced and dependable benchmark for intrusion detection. It helps evaluate machine learning models effectively by offering a range of attack patterns and realistic network traffic scenarios.

The methodology is divided into four distinct phases:

- Phase 1: Data Preprocessing
- Phase 2: Feature Selection
- Phase 3: Data Modeling
- Phase 4: Classification

Data Preprocessing

The successful training of machine learning models requires data preprocessing as a crucial first step to prepare the dataset. The data cleaning process combines with data transformation to ready the NSL-KDD raw data for analysis. Missing data preprocessing begins with a strategy that employs imputation or deletion techniques to manage incomplete records and prevent result distortion. Categorical attack types and protocols are converted into numeric datasets for compatibility with machine learning algorithms by applying one-hot encoding or label encoding functions. Certain conditions allow for the use of normalization and scaling techniques to achieve standardized features that prevent any single variable from dominating learning outcomes. The data preprocessing stages conclude by creating a standardized dataset prepared for model training, which includes variables formatted appropriately for both feature selection and classification processes.

Feature Selection

By selecting the most relevant features from high-dimensional data, the Extra Trees Classifier serves as an effective technique for feature selection. Rather than reducing dimensionality through transformation, Extra Trees identifies the most informative features based on their importance scores. In this study, the ExtraTreesClassifier from scikit-learn was used to rank features and retain the top 18 most significant attributes for DDoS detection. The model was trained on the dataset, and feature importance scores were calculated using the feature_importances_ attribute. The least contributing features were removed to enhance classification performance while minimizing computational

 doi:10.20944/preprints202503.1508.v1

overhead. By concentrating on the most relevant features, the Extra Trees-based selection improves detection efficiency for DDoS attacks in IoT networks while preserving essential data characteristics. This approach optimizes model performance, reduces processing costs, and advances IoT security by enabling more effective threat identification.

The ExtraTreesClassifier evaluates datasets by constructing multiple decision trees from various data subsets to evaluate feature importance based on successful node splits within each tree structure [48]. The algorithm determines the amount of impurity reduction that occurs during the decision phase for each selected feature. A greater impurity reduction indicates stronger feature importance, as these characteristics enhance the efficiency of the decision tree in segregating analytical datasets. Figure 3 shows the most relevant features that are selected by ExtraTreeClassifier.

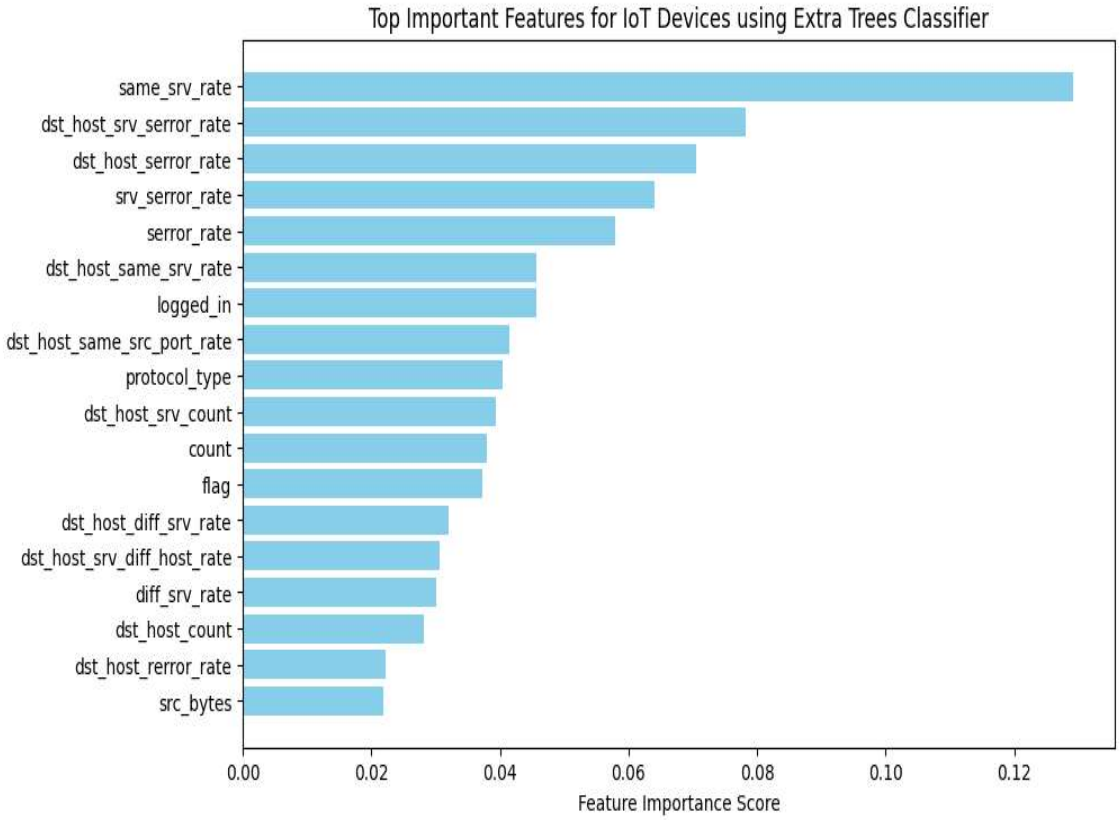


Figure 3. Top 18 Selected features.

Models Selection

We have chosen three supervised learning classifiers—Random Forest, Logistic Regression, and Naïve Bayes—for DDoS attack detection in IoT environments. Random Forest was selected for its robustness, scalability, and ability to handle high-dimensional data, which makes it well-suited for detecting complex attack patterns. Logistic Regression was chosen for its probabilistic approach, estimating the likelihood of an attack and providing interpretable decision boundaries. Naïve Bayes was included due to its efficiency in handling categorical data and its ability to classify attacks based on probabilistic assumptions of feature independence. These models were selected to balance accuracy, computational efficiency, and interpretability, ensuring an effective and lightweight solution for IoT security.

Classification

 doi:10.20944/preprints202503.1508.v1

The final stage of the methodology involves deploying trained models to carry out binary classification, identifying network connections as either normal traffic or DDoS attacks. The evaluation process identifies the most effective models for predicting class labels of unknown network traffic instances. This classification depends on features extracted and refined in earlier stages, where data cleaning, preprocessing, and feature selection improved relevance assessment. Using Random Forest, Naïve Bayes, and Logistic Regression, the testing dataset is classified to detect potential DDoS attack signals targeting IoT devices. Model predictions are validated against ground truth labels to differentiate between normal and malicious traffic.

Performance evaluation emphasizes accuracy, precision, recall, and F1-score, offering insights into detection effectiveness. Precision indicates the accuracy of attack identification, recall gauges the model's ability to identify attack instances, and the F1-score harmonizes both metrics. Moreover, false positives (normal traffic incorrectly classified as attacks) and false negatives (attacks wrongly classified as normal) are examined to evaluate model reliability. This phase guarantees that the chosen models provide a fast, accurate, and efficient solution for real-world IoT environments that require robust DDoS attack detection.

Results and Discussion

To evaluate the effectiveness of our approach, we utilize Detection Accuracy, Precision, Recall, F1-score, and Computational Time as performance metrics. The assessed metrics correspond with those found in the existing research, thereby promoting consistent performance comparisons among various models and techniques.

A comparative analysis of the classifiers used in the methodology appears in its initial section. The description of metrics focuses on evaluating the performance of each classifier based on these criteria. Random Forest, Naive Bayes, and Logistic Regression were assessed using the feature-selected dataset. Each model is evaluated through performance analysis of attack detection accuracy, divergence rate, and generational capabilities with unknown data samples. The study compares the results of the classifiers with those documented in the base paper to demonstrate the effectiveness of the proposed methodology.

Evaluation Metrics

A set of evaluation metrics measures both the performance and effectiveness of the proposed method throughout this study. These metrics, commonly used in machine learning research, enable a quantitative assessment of classification model success. The formulas for these performance assessment metrics are derived from standard methodologies. Our experimental results demonstrate an improvement over the baseline, highlighting the effectiveness of our proposed technique for detecting DDoS attacks on IoT devices.

In the equations presented below, various parameters are defined: TP, TN, FP, FN, L, and M. Specifically, TP stands for true positives (correctly predicted normal class), TN stands for true negatives (correctly predicted attack class), FP signifies false positives (incorrectly predicted normal class), and FN indicates false negatives (incorrectly predicted attack class). L and M are the actual and predicted class labels, respectively. These metrics are expressed by the following formulas:

Detection Accuracy: Accuracy measures the percentage of correctly identified instances, encompassing both normal and attack instances, within a dataset. This metric is defined as the ratio of correctly classified instances to the total number of instances, as shown in Eq. (1). High accuracy signifies that the model is performing effectively, closely aligning its predictions with actual observations. It is essential to consider accuracy in cases where the dataset may be imbalanced to prevent an overrepresentation of false positives (FP) or false negatives (FN).

$$Accuracy = \frac{TP+T}{TP+TN+FP+FN} \quad (1)$$

Precision: Precision calculates the model's ability to accurately identify positive instances, particularly in differentiating attacks from irrelevant data. As shown in Eq. (2), precision is the ratio

 doi:10.20944/preprints202503.1508.v1

of True Positive Rate (TPR) to the sum of True Positive Rate (TPR) and False Positive Rate (FPR). A higher precision indicates that the model is accurate in its positive predictions and reduces the occurrence of false positives. The presence of false positives significantly affects the diagnostic accuracy of DDoS attack detection, potentially resulting in unnecessary alerts or actions.

$$Precision = \frac{TPR}{TPR+FPR} \quad (2)$$

Recall: Recall evaluates the efficacy of the model in accurately identifying all genuine attacks, with a priority on minimizing the number of missed true positives. According to Equation (3), recall is defined as the ratio of the True Positive Rate (TPR) to the total of the True Positive Rate (TPR) and the False Negative Rate (FNR). Recall underscores the model's proficiency in detecting attacks with precision, specifically emphasizing the reduction of false negatives. While precision quantifies the accurate positive predictions, recall signifies the fraction of positive instances that have been successfully identified. A diminished recall may suggest instances of undetected attacks, potentially undermining the overall effectiveness of the attack detection system.

$$Recall = \frac{TPR}{TPR+FNR} \quad (3)$$

F1-Score: The F1-Score is a metric that combines both precision and recall into a single value, emphasizing their symmetry in Eq. (4). It is the harmonic mean of precision and recall, providing a balanced measure of a model's performance. The F1-Score takes into account both false positives and false negatives, offering a more comprehensive evaluation than relying solely on precision or recall. It is computed using the formula below:

$$F1\ Score = 2 * \frac{Precision * Recall}{Precision + Recall} \quad (4)$$

Computational Time: Computational time refers to the total time required for a machine learning model to process data and produce results. It is an important metric for evaluating the efficiency and speed of the model, especially in real-time applications. The average computational time is calculated as the total processing time, representing the overall time taken to complete all necessary computations for a given task.

$$\text{Average Computational Time} = Total\ Processing\ Time$$

Several classifiers support the proposed technique. Specifically, this method employs three classifiers, Random Forest, Naive Bayes, and Logistic Regression, which have been meticulously selected for their efficacy in distinguishing normal traffic patterns from those indicative of Distributed Denial of Service (DDoS) attack data. The verification of each algorithm was conducted through a comprehensive performance analysis encompassing a range of metrics, including accuracy, true positive rate (TPR), false positive rate (FPR), true negative rate (TNR), false negative rate (FNR), as well as computational time.

The comparative performance analysis evaluates these algorithms across seven distinct evaluation metrics. The objective of this research is to ascertain which classifier yields the highest accuracy in the context of DDoS attack detection. Table 4 delineates the performance attributes, thereby providing readers with a succinct overview of the assessment results detailed in Table 3. This analytical framework serves to assist in identifying the most appropriate classifier for safeguarding Internet of Things (IoT) networks against DDoS attacks.

Table 2. Performance measures of selected lightweight Machine learning models.

Evaluation Metrics	Random Forest (%)	Logistic Regression (%)	Naive Bayes (%)
Detection Accuracy	99.88	91.61	87.62
Precision	99.93	92.53	83.57
Recall	99.81	91.61	89.30
F1 Score	99.87	90.89	87.40

 doi:10.20944/preprints202503.1508.v1

The findings indicate that the Random Forest algorithm surpasses both Logistic Regression and Naive Bayes in all four key evaluation metrics: Accuracy, Precision, Recall, and F1-score, as showed in Figure 4. Notably, it achieves the highest classification accuracy of 99.88%, establishing Random Forest as the most effective model for identifying normal attack combinations. The Random Forest attains maximum precision with a score of 99.93%, reflecting an optimal balance between true attack detection and minimal false alarm rates. According to the Recall measurement, Random Forest's capability to detect actual attacks is recorded at 91.81%. Furthermore, Random Forest exhibits the leading F1-score of 99.87%, which underscores its proficiency in maintaining a favourable relationship between precision and recall rates. In contrast, Logistic Regression yields satisfactory results, with an Accuracy of 91.61% and an F1-score of 90.89%; however, its Precision of 92.53% and Recall of 89.3% fall short when compared to those of the Random Forest model. The F1-score of 87.4% for Naive Bayes highlights its insufficient performance metrics across all evaluation criteria in the detection of DDoS attacks relative to the other classifiers analyzed. Therefore, Random Forest emerges as the most viable model for detecting DDoS attacks within IoT networks.

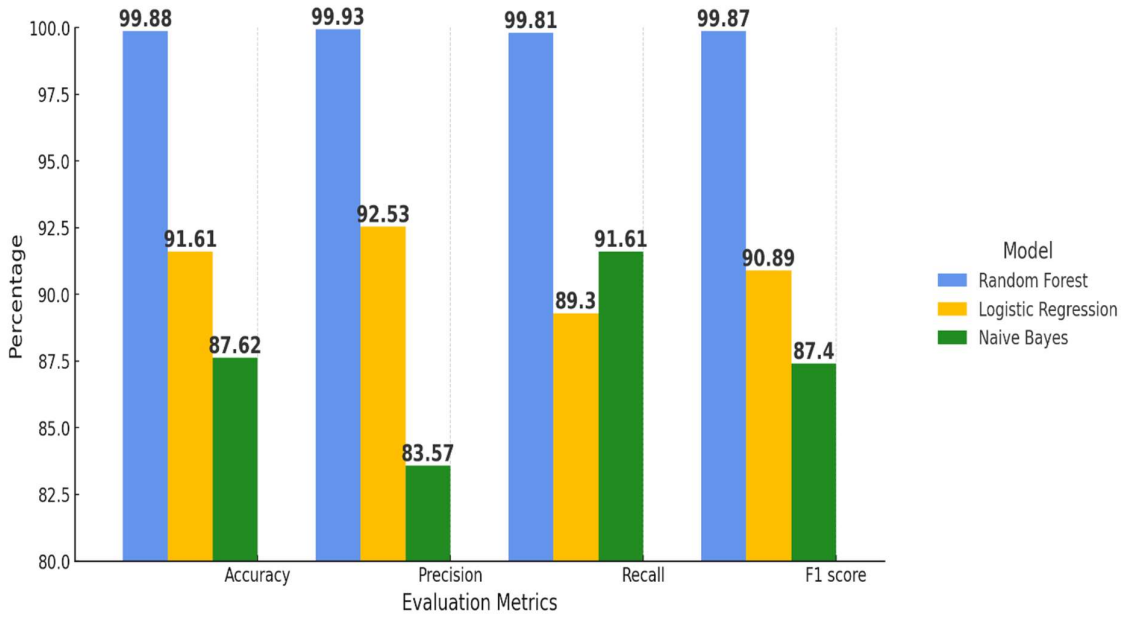


Figure 4. Performance measure chart of selected Machine learning models.

The comparative data evaluation of Random Forest (RF), Logistic Regression (LR), Naive Bayes (NB), and the CNN-GRU_SMA architecture reveals considerable advancements in model performance in Figure 5. The analysis indicates that the Random Forest model achieves the highest performance across all evaluation metrics, with an accuracy rate of 99.88%, followed by CNN-GRU_SMA, Logistic Regression, and Naive Bayes. This finding is further emphasized by the corresponding precision, recall, and F1 score values. Random Forest ranks highest in precision, F1 score, and recall, followed by CNN-GRU, Logistic Regression, and Naive Bayes, in that order.

 doi:10.20944/preprints202503.1508.v1

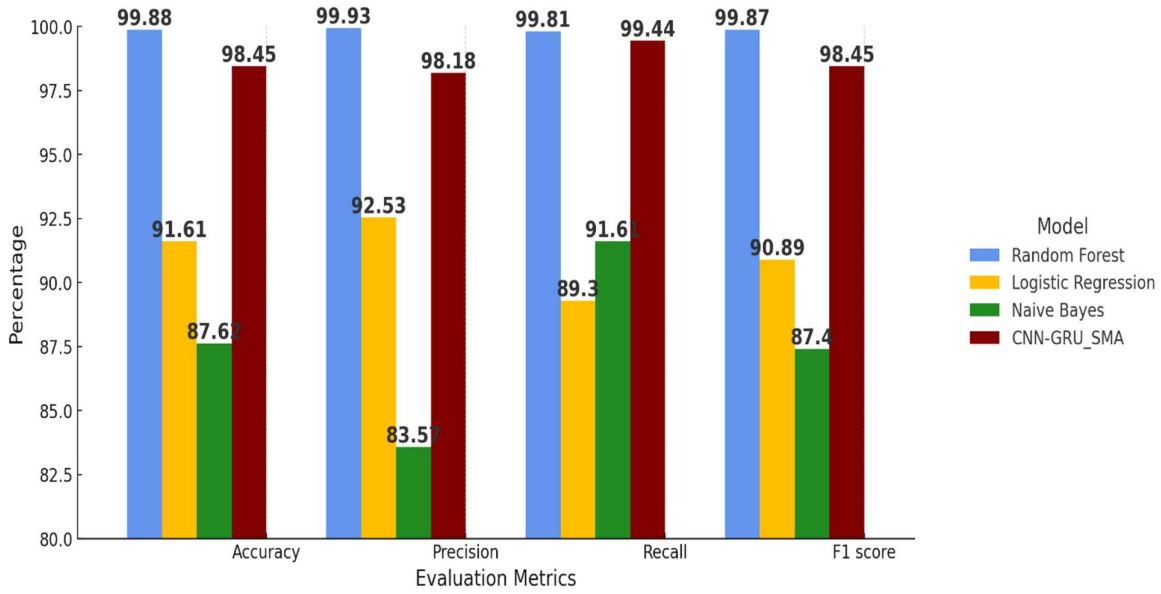


Figure 5. Performance measure with base paper.

The precision capabilities of Random Forest outperform the CNN-GRU_SMA architecture, with Random Forest achieving precision levels of 99.93%. CNN-GRU_SMA, on the other hand, exhibits enhanced performance but still falls slightly behind Random Forest. Logistic Regression and Naive Bayes show satisfactory results, but they produce significantly lower values in comparison to the other models, with Naive Bayes reaching a precision of 83.57% and Logistic Regression exhibiting relatively lower recall values. The F1-score attained by Random Forest, at 99.87%, surpasses CNN-GRU_SMA's score of 98.45%, as well as the scores of the other models assessed, indicating a high standard of precision and recall in the context of DDoS attack detection. This study states that while CNN-GRU_SMA provides a promising methodology for the detection of DDoS attacks, Random Forest remains the highest-performing model across all evaluated metrics.

Computational time tests show that CNN-GRU_SMA requires the longest runtime, despite its impressive classification accuracy. As shown in Figure 6, the Random Forest model achieves the best classification accuracy, but it operates with a computational time of 32.0 seconds, which is significantly faster than CNN-GRU_SMA's 70.3 seconds. The longer processing time for CNN-GRU_SMA is due to its complex model structure and advanced architectural design. Although CNN-GRU_SMA provides excellent classification accuracy, Random Forest delivers comparable precision with a substantial speed advantage. The fastest model in the comparison is Naive Bayes, completing execution in just 8.0 seconds, demonstrating its adaptability for less complex applications or lower-data volume scenarios. Logistic Regression, with a runtime of 92.0 seconds, is the most time-consuming approach among the four models. The analysis of processing times highlights the need for a balance between computational performance and model accuracy, particularly in time-sensitive DDoS detection systems. While CNN-GRU_SMA requires longer processing times, it offers strong accuracy, but Random Forest stands out with both high accuracy and faster processing times. Naive Bayes excels in speed, making it suitable for simpler applications.

 doi:10.20944/preprints202503.1508.v1

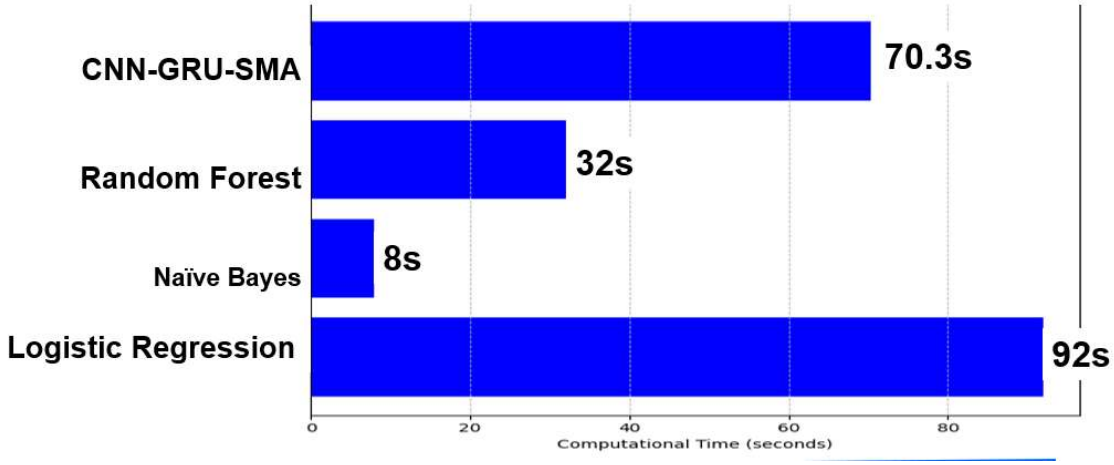


Figure 6. Computational time comparison.

Each classifier was trained using the designated training set and subsequently evaluated on the corresponding testing set to ascertain their accuracy, precision, recall, and F1 score in detecting Distributed Denial of Service (DDoS) attacks. A confusion matrix serves as a valuable tool in assessing the effectiveness of a machine learning-based detection system for identifying DDoS attacks, particularly in Internet of Things (IoT) devices. Figures 7, 8, and 9 present the confusion matrices for the selected lightweight machine learning models.

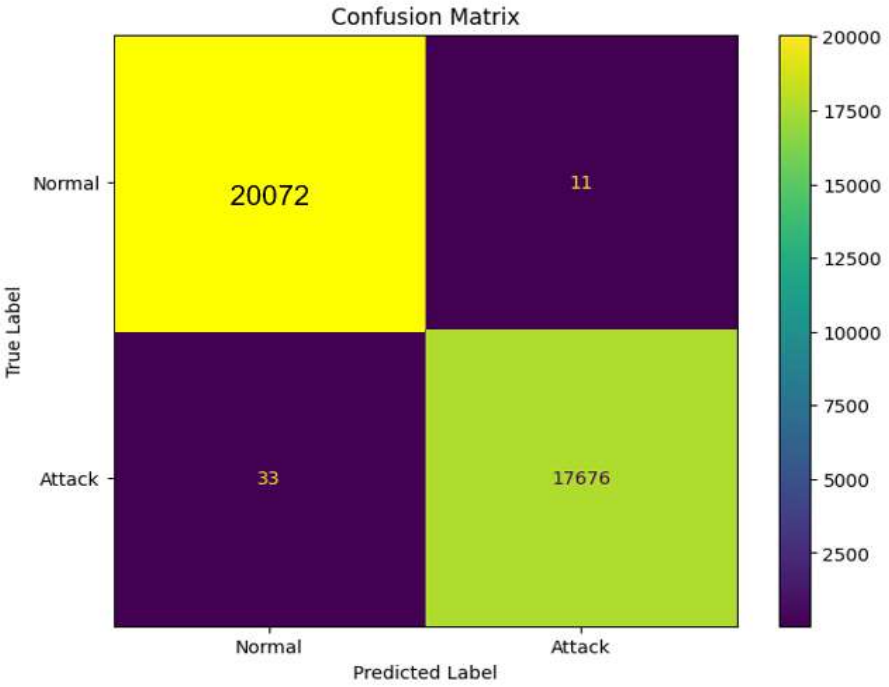
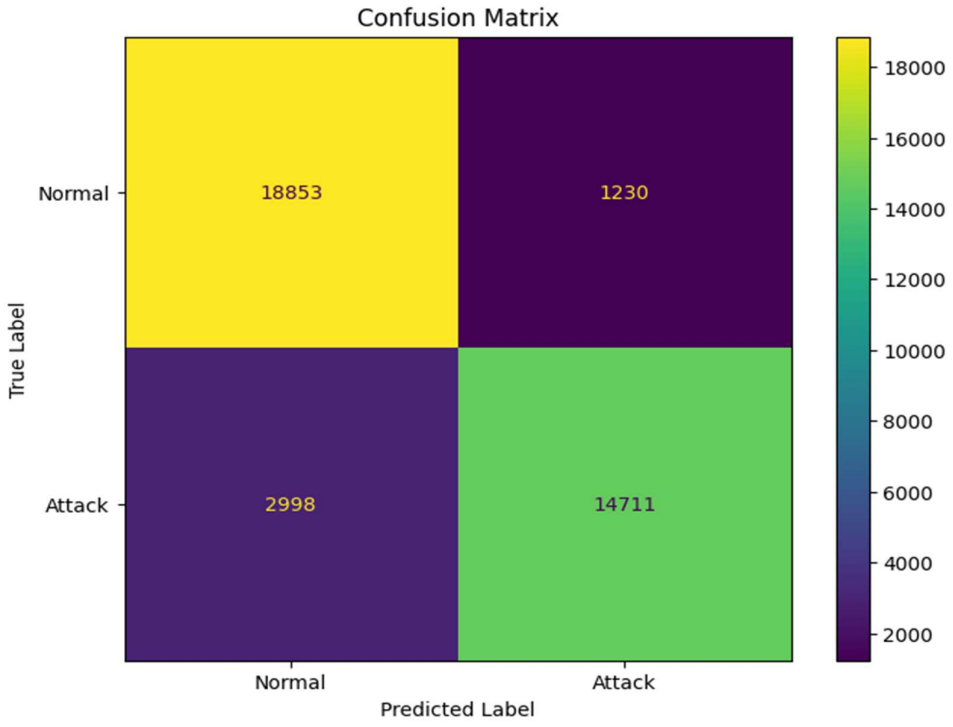


Figure 7. Confusion matrix of Random Forest.

 doi:10.20944/preprints202503.1508.v1



S

Figure 8. Confusion matrix of Logistics Regression.

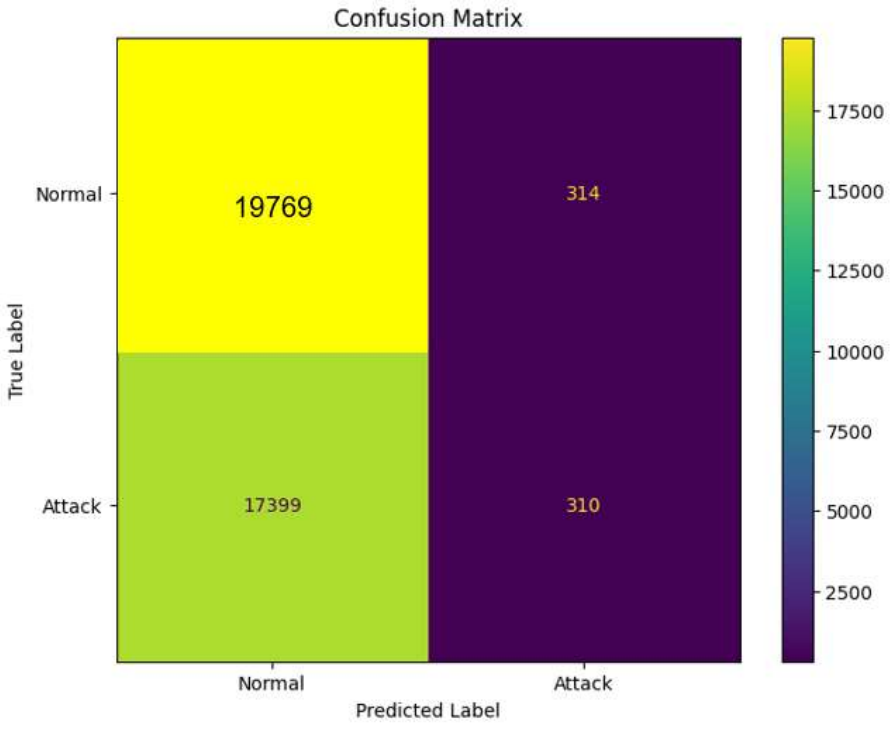


Figure 9. Confusion matrix of Naïve bayes.

The implementation of Random Forest, complemented by enhanced feature selection methodologies such as Error-Tree Correction (ETC) and Principal Component Analysis (PCA), yielded superior outcomes compared to the initial models delineated in the foundational paper.

 doi:10.20944/preprints202503.1508.v1

Specifically, the Random Forest model leveraging ETC achieved remarkable performance metrics with an Accuracy of 99.88%, Precision of 99.93%, and Recall of 99.81%, culminating in an F1-score of 99.87%. Additionally, when PCA was employed for feature extraction, the Random Forest model sustained commendable performance, achieving an Accuracy of 99.87%, Precision of 99.79%, Recall of 99.94%, and an F1-score of 99.86%. The findings of this research clearly found that the Random Forest methodology, in conjunction with ETC-based feature extraction, offers enhanced accuracy in the detection of DDoS attacks when compared with the detection systems detailed in the foundational study.

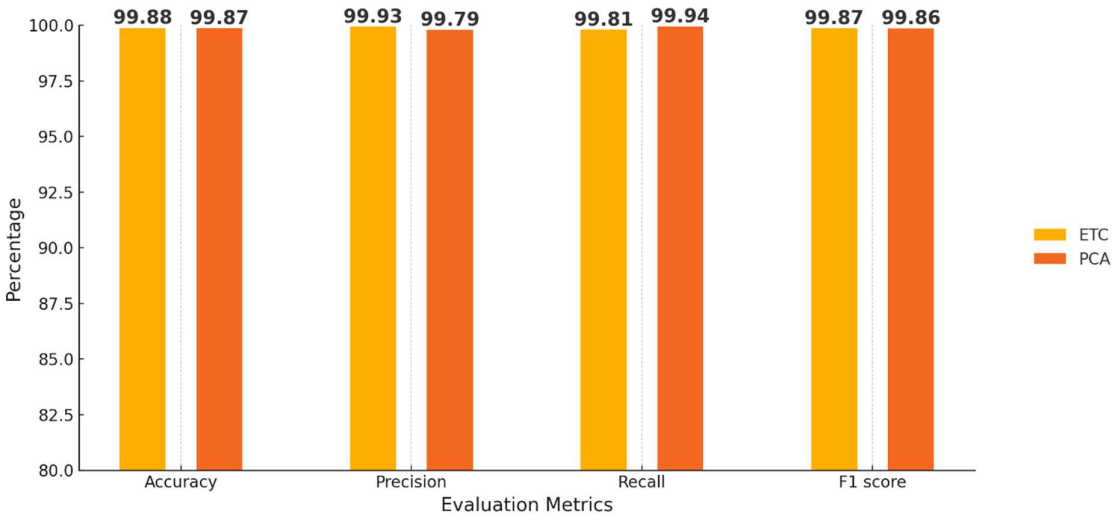


Figure 10. Performance measure of Random Forest.

The comparative analysis of Logistic Regression employing two feature selection methodologies, namely Embedded Tree Classifier (ETC) and Principal Component Analysis (PCA), elucidates the significant influence of these techniques on the model's overall performance. The findings indicate that ETC consistently outperforms PCA across all evaluative metrics: Accuracy, Precision, Recall, and F1-score. Specifically, ETC facilitates Logistic Regression in achieving an impressive Accuracy of 91.61%, accompanied by 92.53% Precision, 89.3% Recall, and an F1-score of 90.89%. Conversely, the PCA technique results in a comparatively lower performance output when applied to the sample dataset. The resultant metrics comprising Accuracy at 90.09%, Precision at 90.41%, Recall at 88.61%, and an F1-score at 89.51% reflect this disparity.

In Figure 11, the results substantiate that ETC surpasses the efficiency of PCA, optimizing both Precision and Accuracy metrics for Logistic Regression models, despite PCA exhibiting an acceptable level of effectiveness in model construction. The selected feature selection strategy, namely ETC, demonstrates superior attributes that empower Logistic Regression to achieve heightened detection capabilities concerning DDoS attacks on Internet of Things (IoT) devices. Comprehensive analysis indicates that both ETC and PCA contribute significantly to performance enhancements for Logistic Regression models, thereby underlining the importance of feature selection methodologies in model optimization.

 doi:10.20944/preprints202503.1508.v1

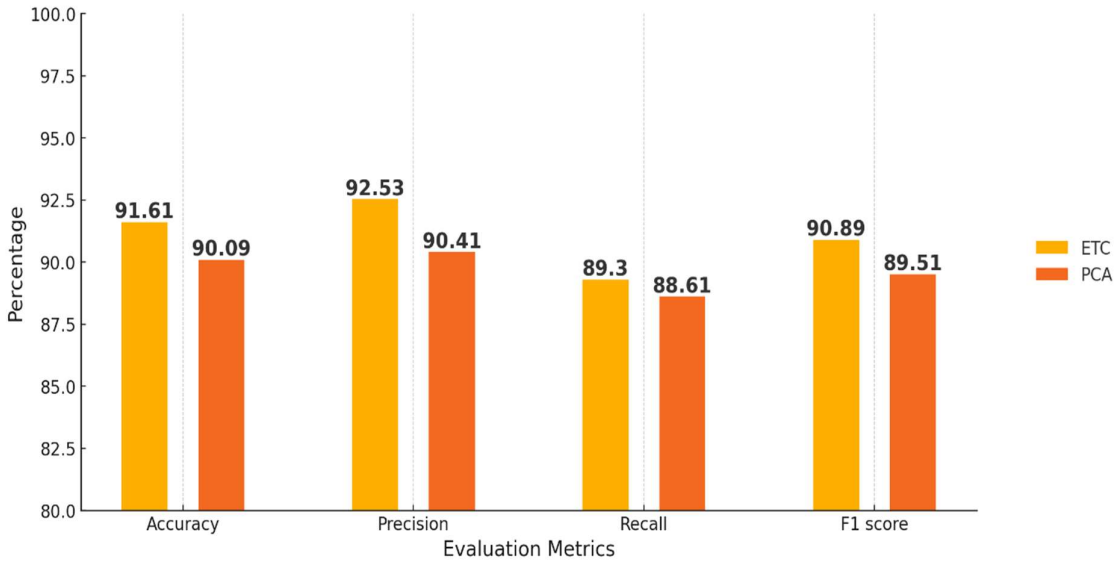


Figure 11. Performance measure of Logistics Regression.

The comparative analysis of the Naive Bayes classifier reveals several significant performance discrepancies, as demonstrated in Figure 12. The Enhanced Tree Classifier (ETC) consistently yields superior results across all evaluated metrics: Accuracy, Precision, Recall, and F1-score. Specifically, when utilizing ETC, Naive Bayes attains an Accuracy of 87.62%, Precision of 83.57%, Recall of 91.61%, and an F1-score of 87.4%. Conversely, the application of Principal Component Analysis (PCA) for feature selection results in marginally lower performance metrics, with Accuracy recorded at 87.14%, Precision at 80.11%, Recall at 91.29%, and an F1-score of 85.34%.

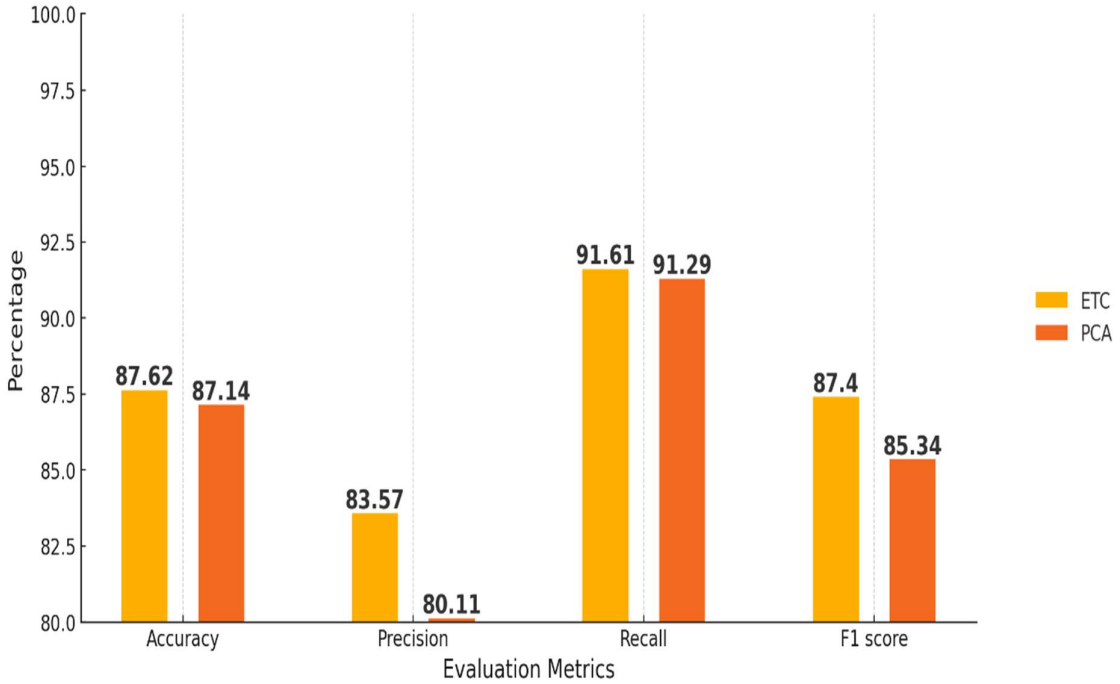


Figure 12. Performance measure of Naïve bayes.

 doi:10.20944/preprints202503.1508.v1

The ETC methodology consistently outperforms PCA in terms of Precision and F1-score, while PCA exhibits a slight advantage in Recall. However, the reduction in Precision associated with PCA underscores the inherent trade-offs involved in employing various feature selection techniques. When juxtaposed with the findings documented in the foundational paper, Naive Bayes utilizing the ETC validates a pronounced enhancement in Precision and F1-score, thus establishing it as a more dependable model for the detection of Distributed Denial-of-Service (DDoS) attacks, although it is still less proficient than more sophisticated models such as Random Forest. These results indicate that the ETC constitutes a more effective feature selection strategy for Naive Bayes, significantly augmenting its capacity to identify attacks without detracting from its accuracy.

An analysis of the performance of the Random Forest model, both with and without the implementation of the Extra Trees Classifier (ETC) for feature selection purposes, shown in Figure 13. The findings reveal a substantial improvement in the model's performance upon the application of feature selection through ETC. Specifically, the accuracy exhibits a marked enhancement from 91.39% in the absence of feature selection to 99.88% with feature selection implemented. Precision demonstrates a significant increase from 87.03% to 99.93% following the inclusion of ETC. In a similar vein, recall escalates from 91.34% to 99.81%, and the F1 score also reflects an advancement from 87.65% to 99.87%. These results indicate that the utilization of ETC for feature selection markedly elevates the performance of the Random Forest model across all assessed metrics, thereby emphasizing the effectiveness of ETC in enhancing model accuracy, precision, recall, and F1 score.

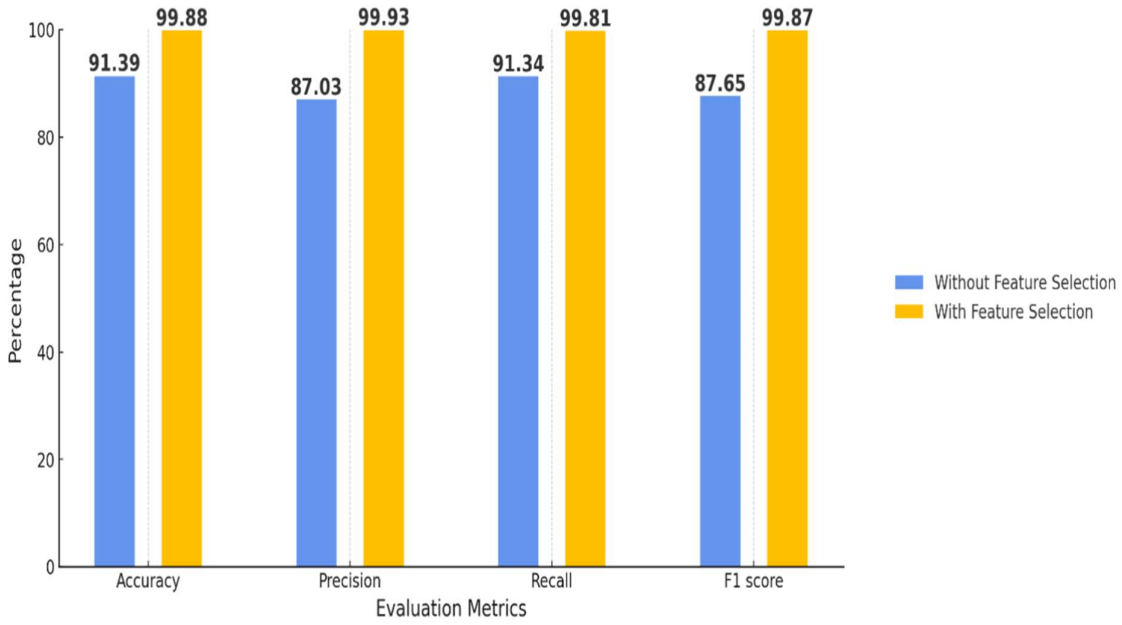


Figure 13. Comparison of RF performance with and without feature selection.

The performance comparison of the Logistic Regression (LR) model, both with and without the Extra Trees Classifier (ETC) for feature selection, evaluated across four key metrics: Accuracy, Precision, Recall, and F1 Score. With feature selection, the model exhibits a significant rise in Accuracy, increasing from 74.53% without feature selection to 91.61% with it. Precision shows in Figure 14 a notable increase as well, climbing from 62.65% to 92.53%. Recall similarly improves from 74.43% to 91.61%, and the F1 Score experiences a considerable enhancement from 66.5% to 90.89%. These findings indicate that utilizing ETC for feature selection greatly enhances the performance of the Logistic Regression model, boosting all essential metrics.

 doi:10.20944/preprints202503.1508.v1

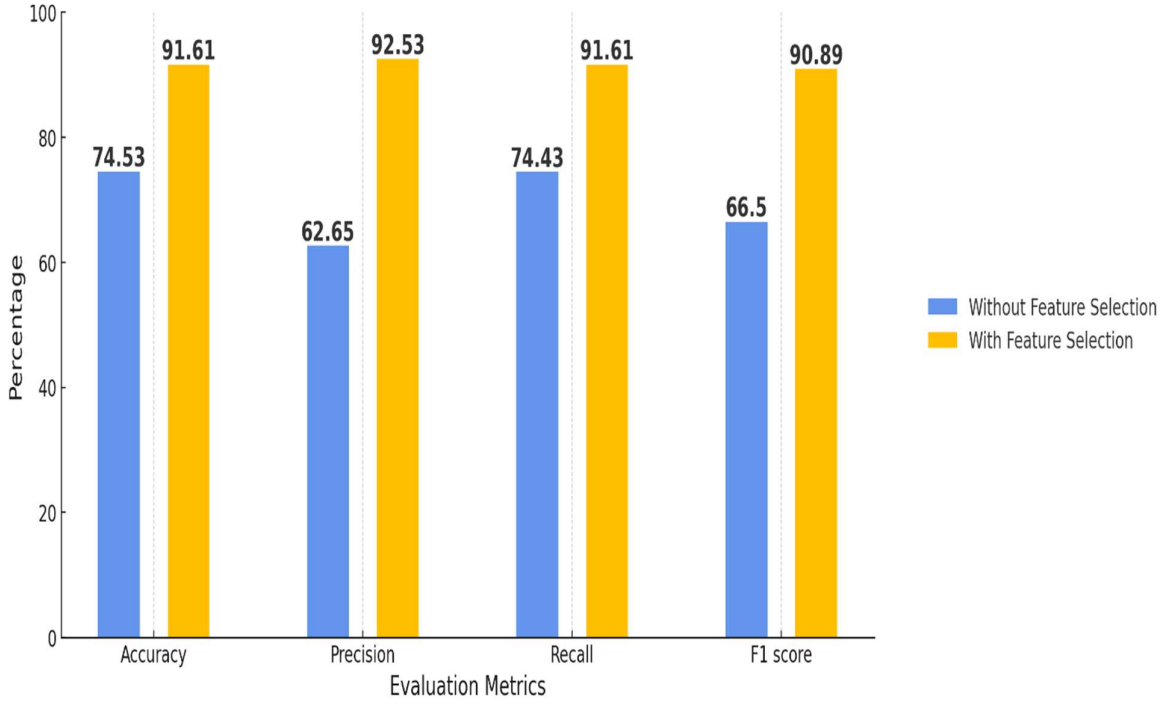
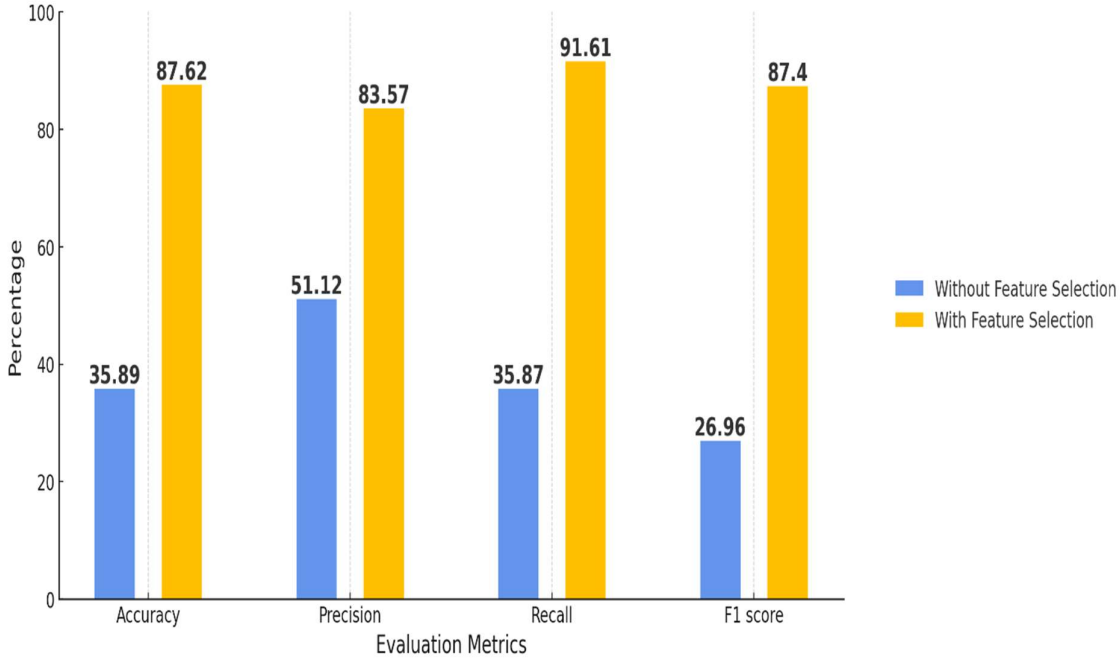


Figure 14. Comparison of LR performance with and without feature selection.

Naive Bayes (NB) model's performance with and without feature selection via the Extra Trees Classifier (ETC), evaluated across four metrics: Accuracy, Precision, Recall, and F1 Score, shown in Figure 15. Implementing feature selection leads to a marked enhancement in Accuracy, which increases from 35.89% (without feature selection) to 87.62% (with feature selection). Precision also grows significantly, from 51.12% to 83.57% post feature selection. Recall sees a rise from 35.87% to 91.61%, and the F1 Score shows impressive growth from 26.96% to 87.4%. These findings indicate that utilizing ETC for feature selection significantly boosts the Naive Bayes model's performance, notably enhancing all primary metrics, particularly Recall and F1 Score.



 doi:10.20944/preprints202503.1508.v1

Figure 15. Comparison of NB performance with and without feature selection.

A visual comparison known as the ROC (Receiver Operating Characteristic) curve illustrates the detection accuracy of DDoS attacks by examining Gaussian Naive Bayes alongside Logistic Regression and Random Forest classifiers, as shown in Figure 13. AUC values accompany each model to provide a numerical assessment of performance metrics. Random Forest proves to be superior to both Logistic Regression and Gaussian Naive Bayes in balancing the True Positive Rate, achieving an area under the curve (AUC) of 0.92 according to the ROC curve analysis. Random Forest shows the strongest ability to distinguish between attack and normal traffic, indicated by its position utmost from the random guessing diagonal line. The performance metrics for Logistic Regression and Naive Bayes yield lower results, although Logistic Regression maintains a slight advantage by attaining a better AUC than Naive Bayes.

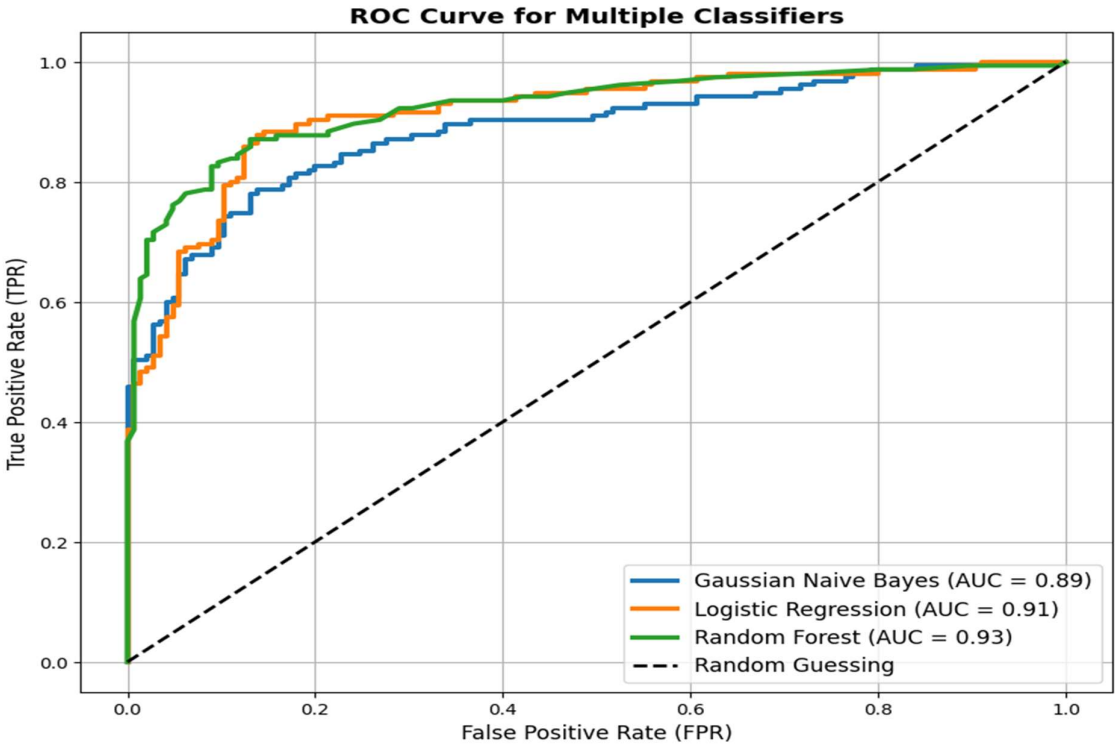


Figure 16. Comparative performance measure of machine learning models.

The overall results illustrate that the application of the Extra Trees classifier for feature selection significantly enhances the detection of Distributed Denial of Service (DDoS) attacks targeting Internet of Things (IoT) devices. This approach not only optimizes feature representation but also leads to improved performance metrics of machine learning classifiers. Our study utilized the NSL KDD dataset, which is crucial for analyzing patterns associated with DDoS attacks.

Among the classifiers examined, the Random Forest model emerged as the most effective, outperforming Logistic Regression and Naive Bayes in terms of accuracy, precision, recall, and F1-score. Random Forest exhibited superior overall performance, characterized by reduced training and prediction durations, thereby affirming its suitability for real-time DDoS detection applications. Additionally, feature selection utilizing the Extra Trees methodology demonstrated enhanced efficiency compared to outdated techniques like the Pearson correlation coefficient, resulting in a decreased computational burden while maintaining high levels of accuracy.

Conclusion and Future Work

 doi:10.20944/preprints202503.1508.v1

The detection of Distributed Denial of Service (DDoS) attacks targeting Internet of Things (IoT) devices represents a pivotal challenge in safeguarding the security and reliability of contemporary networks. This investigation sought to implement binary classification methodologies for the identification of DDoS attacks on IoT devices utilizing Random Forest, Logistic Regression, and Naive Bayes models. The findings indicated that all three models exhibited capabilities in detecting DDoS traffic. Notably, the Random Forest model demonstrated superior performance with the highest accuracy score of 99.88% and F1-scores, surpassing the comparative efficacy of the other models. Furthermore, the integration of the Extra Trees classifier for feature selection significantly advanced the efficiency and effectiveness of the detection procedure by omitting unnecessary features while maintaining critical attributes. This refined approach ensures scalability and adaptability within IoT environments, which commonly operate under the constraints of limited resources. Ultimately, this study contributes to the enhancement of security frameworks for IoT devices in the face of emerging cybersecurity threats through the application of machine learning models and the implementation of robust feature selection strategies.

Future Work

Future research in this domain should prioritize several critical areas aimed at enhancing the detection of DDoS (Distributed Denial of Service) attacks targeting Internet of Things (IoT) devices. It is imperative to broaden the scope of the study to encompass a diverse array of attack vectors and configurations of IoT devices, as this will be vital for the development of a more robust detection framework. Additionally, assessing the scalability and real-time performance of the proposed models across various network environments is essential for determining their effectiveness under a range of conditions.

The application of similar machine learning techniques to other IoT-specific datasets will not only bolster the validation of existing methodologies. It may also reveal new insights that could further optimize detection accuracy. Furthermore, the creation of an intuitive front-end application capable of detecting attacks on various IoT devices would facilitate effective implementation and enhance user engagement with security protocols. Collectively, these initiatives are poised to significantly improve DDoS detection in IoT networks, offering stronger defenses against the evolving landscape of cyber threats.

References

Ahmad, Ijaz, Zhong Wan, and Ashfaq Ahmad. 2023. “A Big Data Analytics for DDOS Attack Detection Using Optimized Ensemble Framework in Internet of Things.” *Internet of Things* 23 (October):100825. https://doi.org/10.1016/j.iot.2023.100825.

Aktar, Sharmin, and Abdullah Yasin Nur. 2023. “Towards DDoS Attack Detection Using Deep Learning Approach.” *Computers & Security* 129 (June):103251. https://doi.org/10.1016/j.cose.2023.103251.

Almadhor, Ahmad, Ali Altalbe, Imen Bouazzi, Abdullah Al Hejaili, and Natalia Kryvinska. 2024. “Strengthening Network DDOS Attack Detection in Heterogeneous IoT Environment with Federated XAI Learning Approach.” *Scientific Reports* 14 (1): 24322. https://doi.org/10.1038/s41598-024-76016-6.

Alve, Shahran Rahman, Muhammad Zawad Mahmud, Samiha Islam, Md Asaduzzaman Chowdhury, and Jahirul Islam. 2025. “Smart IoT Security: Lightweight Machine Learning Techniques for Multi-Class Attack Detection in IoT Networks.” arXiv. https://doi.org/10.48550/arXiv.2502.04057.

Dachyar, M., Teuku Yuri M. Zagloel, and L. Ranjaliba Saragih. 2019. “Knowledge Growth and Development: Internet of Things (IoT) Research, 2006–2018.” *Heliyon* 5 (8): e02264. https://doi.org/10.1016/j.heliyon.2019.e02264.

Elgazzar, Khalid, Haytham Khalil, Taghreed Alghamdi, Ahmed Badr, Ghadeer Abdelkader, Abdelrahman Elewah, and Rajkumar Buyya. 2022. “Revisiting the Internet of Things: New Trends, Opportunities and Grand Challenges.” *Frontiers in the Internet of Things* 1 (November):1073780. https://doi.org/10.3389/friot.2022.1073780.

 doi:10.20944/preprints202503.1508.v1

Gelgi, Metehan, Yueting Guan, Sanjay Arunachala, Maddi Samba Siva Rao, and Nicola Dragoni. 2024. "Systematic Literature Review of IoT Botnet DDOS Attacks and Evaluation of Detection Techniques." *Sensors* 24 (11): 3571. https://doi.org/10.3390/s24113571.

Hariprasad, S. 2022. "Detection of DDoS Attack in IoT Networks Using Sample Selected RNN-ELM."

Hussain, Faisal, Syed Ghazanfar Abbas, Muhammad Husnain, Ubaid U. Fayyaz, Farrukh Shahzad, and Ghalib A. Shah. 2020. "IoT DoS and DDoS Attack Detection Using ResNet." In *2020 IEEE 23rd International Multitopic Conference (INMIC)*, 1–6. IEEE.

Hussein, AbdelRahman H. 2019. "Internet of Things (IOT): Research Challenges and Future Applications." *International Journal of Advanced Computer Science and Applications* 10 (6).

"Intrusion Detection Systems: NSL-KDD | Saylor Academy." n.d. Saylor Academy. Accessed January 26, 2025. https://learn.saylor.org/mod/book/view.php?id=29755&chapterid=5443.

Ismail, Muhammad Ismail Mohmand, Hameed Hussain, Ayaz Ali Khan, Ubaid Ullah, Muhammad Zakarya, Aftab Ahmed, Mushtaq Raza, Izaz Ur Rahman, and Muhammad Haleem. 2022. "A Machine Learning-Based Classification and Prediction Technique for DDoS Attacks." *IEEE Access* 10:21443–54. https://doi.org/10.1109/ACCESS.2022.3152577.

Jullian, Olivia, Beatriz Otero, Eva Rodriguez, Norma Gutierrez, Héctor Antona, and Ramon Canal. 2023. "Deep-Learning Based Detection for Cyber-Attacks in IoT Networks: A Distributed Attack Detection Framework." *Journal of Network and Systems Management* 31 (2): 33. https://doi.org/10.1007/s10922-023-09722-7.

Mahadik, Shalaka, Pranav M. Pawar, and Raja Muthalagu. 2023. "Efficient Intelligent Intrusion Detection System for Heterogeneous Internet of Things (HetIoT)." *Journal of Network and Systems Management* 31 (1): 2. https://doi.org/10.1007/s10922-022-09697-x.

Motylinski, Michal, Áine MacDermott, Farkhund Iqbal, and Babar Shah. 2022. "A GPU-Based Machine Learning Approach for Detection of Botnet Attacks." *Computers & Security* 123 (December):102918. https://doi.org/10.1016/j.cose.2022.102918.

Mu, Xiaoshao, and Maxwell Fordjour Antwi-Afari. 2024. "The Applications of Internet of Things (IoT) in Industrial Management: A Science Mapping Review." *International Journal of Production Research* 62 (5): 1928–52. https://doi.org/10.1080/00207543.2023.2290229.

Nižetić, Sandro, Petar Šolić, Diego López-de-Ipiña González-de-Artaza, and Luigi Patrono. 2020. "Internet of Things (IoT): Opportunities, Issues and Challenges towards a Smart and Sustainable Future." *Journal of Cleaner Production* 274 (November):122877. https://doi.org/10.1016/j.jclepro.2020.122877.

Radouan Ait Mouha, Radouan Ait. 2021. "Internet of Things (IoT)." *Journal of Data Analysis and Information Processing* 09 (02): 77–101. https://doi.org/10.4236/jdaip.2021.92006.

Revathi, M., V. V. Ramalingam, and B. Amutha. 2021. "A Machine Learning Based Detection and Mitigation of the DDOS Attack by Using SDN Controller Framework." *Wireless Personal Communications*, 1–25.

Sadek, Ibrahim, Josué Codjo, Shafiq Ul Rehman, and Bessam Abdulrazak. 2022. "Security and Privacy in the Internet of Things Healthcare Systems: Toward a Robust Solution in Real-Life Deployment." *Computer Methods and Programs in Biomedicine Update* 2:100071. https://doi.org/10.1016/j.cmpbup.2022.100071.

Sanmorino, Ahmad, Luis Marnisah, and Hendra Di Kesuma. 2024. "Detection of DDoS Attacks Using Fine-Tuned Multi-Layer Perceptron Models." *Engineering, Technology & Applied Science Research* 14 (5): 16444–49. https://doi.org/10.48084/etasr.8362.

Silivery, Arun Kumar, Ram Mohan Rao Kovvur, Ramana Solleti, Lk Suresh Kumar, and Bhukya Madhu. 2023. "A Model for Multi-Attack Classification to Improve Intrusion Detection Performance Using Deep Learning Approaches." *Measurement: Sensors* 30 (December):100924. https://doi.org/10.1016/j.measen.2023.100924.

Taherdoost, Hamed. 2023. "Security and Internet of Things: Benefits, Challenges, and Future Perspectives." *Electronics* 12 (8): 1901. https://doi.org/10.3390/electronics12081901.