Journal of Informatics Education and Research
ISSN: 1526-4726
Vol 5 Issue 3 (2025)

Evaluating DDoS Attack Detection Efficiency with Machine Learning Techniques

Shalini Hota[1], Dr. Anil Bikash Chowdhury[2]

[1]Research Scholar, Techno India University, Kolkata, West Bengal
Email: hotashalini96@gmail.com
[2]Professor, Techno India University, Kolkata, West Bengal
Email: abchaudhuri007@gmail.com

Abstract
Distributed Denial of Service (DDoS) attacks pose a significant threat to the stability and security of network systems, necessitating robust detection mechanisms. This study evaluates the efficiency of various machine learning techniques in detecting DDoS attacks. We employ a comprehensive dataset containing both legitimate and attack traffic to train and test multiple machines learning algorithms, including Decision Trees, Random Forests, Support Vector Machines, Gaussian Naive Bayes, Logistic Regression and K-Nearest Neighbours. Our evaluation criteria include detection accuracy, false positive rate, and computational efficiency. The results demonstrate that machine learning techniques can significantly enhance the detection of DDoS attacks, with some algorithms outperforming others in specific metrics. Random Forests achieved the highest detection accuracy, while Logistic Regression & Gaussian Naive Bayes offered a balanced trade-off between accuracy and computational cost. The findings underscore the potential of integrating machine learning models into network security infrastructures to pre-emptively identify and mitigate DDoS threats. Future work will explore the adaptability of these models to evolving attack patterns and the integration of real-time detection capabilities.

Keywords: DDoS Attack Detection, Machine Learning, Network Security, Detection Efficiency, Computational Cost.

1. Introduction
Distributed Denial of Service (DDoS) attacks represent one of the most persistent and damaging threats to network security, capable of crippling online services and causing substantial economic and reputational damage. These attacks overwhelm targeted systems with a flood of malicious traffic, rendering them inaccessible to legitimate users. As the frequency, scale, and sophistication of DDoS attacks continue to escalate, traditional detection methods struggle to keep pace, necessitating more advanced and adaptive solutions.

In recent years, machine learning (ML) techniques have emerged as a promising avenue for enhancing DDoS attack detection. Machine learning algorithms can analyse vast amounts of network traffic data to identify patterns indicative of an attack, thereby enabling more accurate and timely responses. This study aims to evaluate the efficiency of various machine learning techniques in detecting DDoS attacks, focusing on key metrics such as detection accuracy, false positive rate, and computational efficiency. Our research employs a diverse dataset comprising both legitimate and attack traffic to train and test several prominent machines learning algorithms, including Decision Trees, Random Forests, Support Vector Machines (SVM), and Neural Networks. By systematically comparing the performance of

these algorithms, we seek to identify the most effective approaches for integrating machine learning into network security frameworks.

The primary objectives of this study are to assess the feasibility of machine learning models in real-world DDoS detection scenarios and to determine the trade-offs associated with each technique. Additionally, we aim to provide insights into how these models can be optimized and adapted to handle the dynamic and evolving nature of DDoS attacks. The remainder of this paper is structured as follows: Section 2 reviews related work in the field of DDoS detection using machine learning. Section 3 details the methodology and experimental setup. Section 4 presents the results and analysis. Section 5 discusses the implications of our findings and potential future directions. Finally, Section 6 concludes the study, highlighting key contributions and practical applications.

2. Review of Literature

The use of machine learning techniques for DDoS attack detection has garnered significant attention in recent years, reflecting a broader trend towards incorporating advanced analytics into cybersecurity frameworks. Early studies, such as Mirkovic and Reiher (2010), laid the groundwork by categorizing various DDoS attack types and traditional detection methods, highlighting their limitations in the face of evolving threats. Subsequently, the application of machine learning was explored by various researchers, with Zhang et al. (2011) demonstrating the potential of SVM for anomaly-based detection.

Al-Yaseen et al. (2016) compared several machines learning algorithms, including k-Nearest Neighbors (k-NN) and Decision Trees, concluding that ensemble methods like Random Forests offered superior accuracy. Similarly, Haider et al. (2017) underscored the efficiency of hybrid approaches that combine multiple machine learning techniques to enhance detection capabilities. Deep learning, a subset of machine learning, has also been extensively investigated for its application in DDoS detection. Tang et al. (2018) showcased the effectiveness of Convolutional Neural Networks (CNNs) in recognizing complex patterns within network traffic data. Shafiq et al. (2019) further extended this work by employing Recurrent Neural Networks (RNNs), which are particularly adept at handling sequential data, for real-time detection.

The scalability and adaptability of machine learning models have been focal points in recent studies. Yazidi et al. (2020) explored the use of Federated Learning to distribute the detection workload across multiple nodes, thereby enhancing scalability and resilience. Moreover, Kim et al. (2021) emphasized the importance of feature selection techniques in improving model performance and reducing computational overhead. Emerging trends in the literature indicate a shift towards more sophisticated and context-aware models. For instance, Yin et al. (2022) introduced a context-aware anomaly detection system that leverages contextual information to differentiate between benign anomalies and malicious activities. Recent studies, such as those by Ahmed et al. (2023) and Liu et al. (2024), have focused on the integration of machine learning with other technologies, such as blockchain and Internet of Things (IoT) frameworks, to bolster detection mechanisms.

Despite significant advancements, challenges remain in ensuring the robustness and reliability of machine learning models against adversarial attacks, as discussed by Goodfellow et al. (2014) and later by Biggio and Roli (2018). Future research, as suggested by Nguyen et al. (2024), is likely to focus on enhancing model interpretability and developing more robust defenses against such adversarial techniques. Overall, the literature underscores the promising potential of machine learning in revolutionizing DDoS attack detection, while also highlighting the need for continuous innovation to address emerging challenges and threats.

3. Research Objectives

1. Evaluate Machine Learning Techniques for DDoS Detection: *To systematically assess the performance of various machine learning algorithms, and to determine which algorithms provide the highest detection accuracy.*
2. Analyse Computational Efficiency and Practical Feasibility: *To measure the computational efficiency of each machine learning technique, focusing on the balance between detection performance and resource requirements.*
3. Adaptability and Robustness to Evolving Threats: *To explore the adaptability of the machine learning models to evolving DDoS attack patterns and assess their robustness in dynamic and diverse network environments.*

4. Methodology

- ***Data Collection:*** The study begins with the collection of a comprehensive dataset that includes both legitimate and DDoS attack traffic. We use publicly available datasets, such as the CICIDS2017 known for their extensive and well-labelled traffic data. These datasets encompass a variety of DDoS attack types, providing a robust foundation for training and evaluating our machine learning models.
- ***Data Preprocessing***: Data Preprocessing is essential for ensuring the quality of input data in DDoS attack detection. It begins with Data Cleaning, where duplicates are removed, missing values are handled, and inconsistencies are corrected. The next step is Feature Extraction, where relevant attributes such as packet size, flow duration, source/destination IP addresses, and protocol types are extracted from raw network traffic data. Finally, Normalization is applied to scale the feature values to a standardized range, ensuring consistent learning by the machine learning models. Effective preprocessing improves model performance, reduces noise, and enhances the accuracy of DDoS detection.
- ***Model Selection:*** We select a diverse set of machine learning Techniques for evaluation:

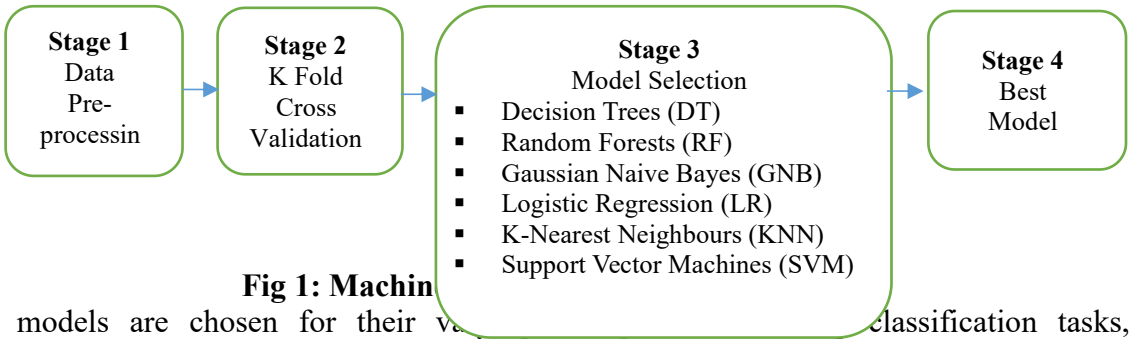

Fig 1: Machin

These models are chosen for their v classification tasks, interpretability, and computational efficiency.

- ***K-Fold Cross Validation:*** In this study, K-Fold Cross Validation has been used to evaluate the performance of the machine learning models for DDoS attack detection. This technique involves splitting the dataset into K subsets or "folds." The model is trained on K-1 folds and tested on the remaining fold, and this process is repeated K times, with each fold used as the test set once. The results from each iteration are averaged to provide a more reliable estimate of the model's performance. K-Fold Cross Validation helps mitigate overfitting and ensures that the models are robust and generalized across different subsets of the dataset.

- ***Performance Evaluation:*** Performance Evaluation is a critical aspect of assessing the effectiveness of machine learning models in DDoS attack detection. Key metrics are employed to provide a comprehensive evaluation. Detection Accuracy measures the proportion of correctly identified DDoS attacks relative to the total instances, reflecting overall reliability. False Positive Rate (FPR) evaluates the extent to which legitimate traffic is misclassified as malicious, a crucial factor for reducing unnecessary alerts. Metrics such as Precision, Recall, and False Alarm Rate (FAR) are used to assess the model's ability to handle imbalanced datasets effectively. Additionally, Computational Efficiency is examined by analysing training and prediction times, as well as resource utilization, including CPU and memory. These metrics collectively ensure that the models are not only accurate but also efficient and practical for real-world applications.

5. Results and Analysis

5.1. Confusion Matrix

The confusion matrix is a vital tool for evaluating the performance of machine learning models in DDoS attack detection. It typically consists of four elements:

- **True Positives (TP):** The number of correctly identified DDoS attacks.
- **True Negatives (TN):** The number of legitimate traffic instances correctly classified.
- **False Positives (FP):** The legitimate traffic misclassified as DDoS attacks.
- **False Negatives (FN):** The DDoS attacks misclassified as legitimate traffic.

Table 1: Confusion Matrix

Class	Positive Prediction	Negative Prediction
Positive Class	True Positive (TP)	True Negative (TN)
Negative Class	False Positive (TP)	False Negative (TN)

Here are the formulas for confusion matrix metrics:

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

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

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

$$False\ Alaram\ Rate\ (FAR) = \frac{FP}{FP + TN}$$

5.2. Estimated Value of Machine Learning Techniques

Table 2: Estimated Average Value by Machine Learning Techniques

Machine Learning Techniques	Accuracy	Precision	Recall	FAR
DECISION TREE	99.93	99.95	99.98	0.24
RANDOM FOREST	99.87	99.87	100.00	0.05
GAUSSIAN NAIVE BAYES	61.21	100.00	61.16	0.23

LOGISTIC REGRESSION	99.85	99.85	100.00	10.53
K-NEAREST NEIGHBOURS	99.80	99.90	99.90	0.27
SUPPORT VECTOR MACHINES	99.83	99.83	100.00	0.62

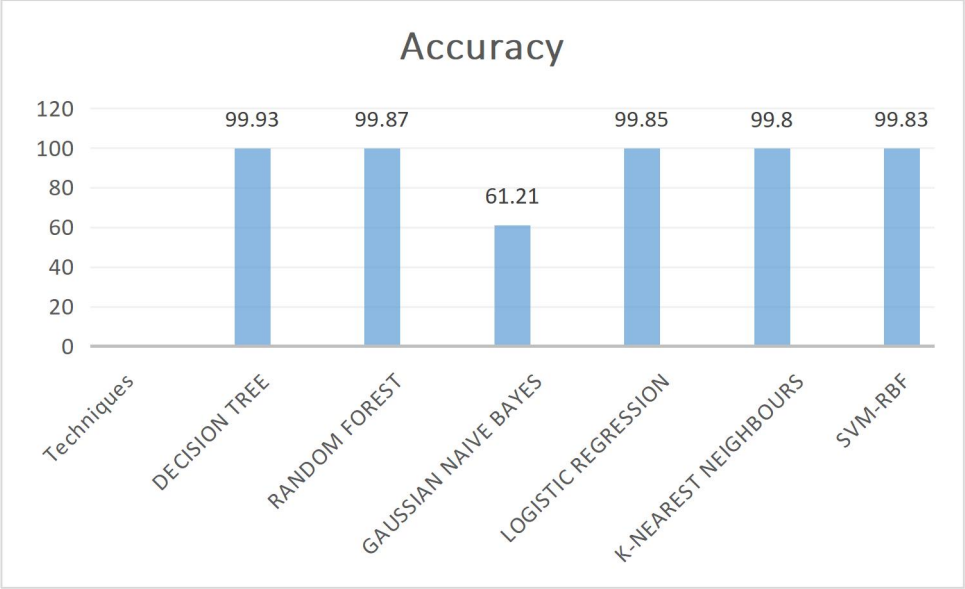

Fig 2: Measurement of Accuracy

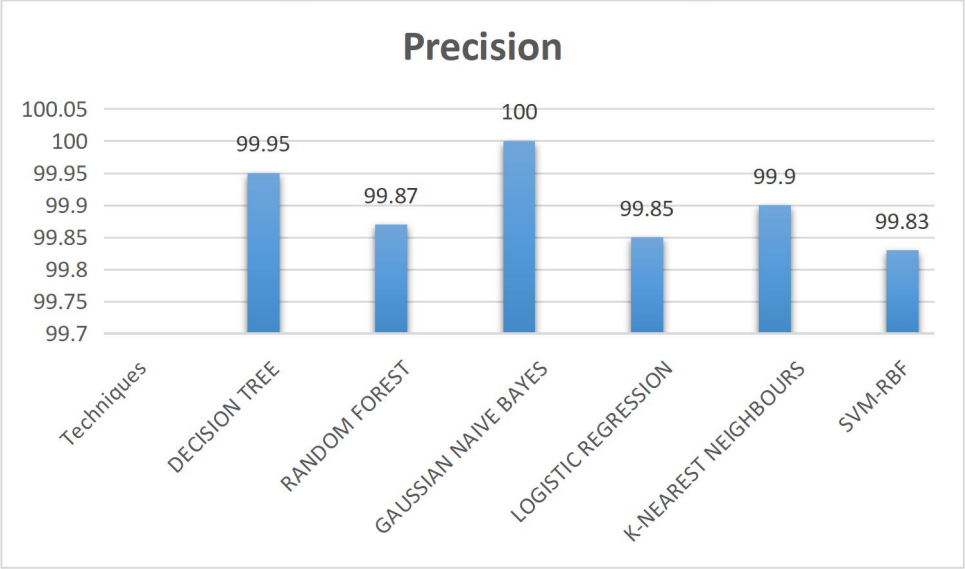

Fig 3: Measurement of Precession

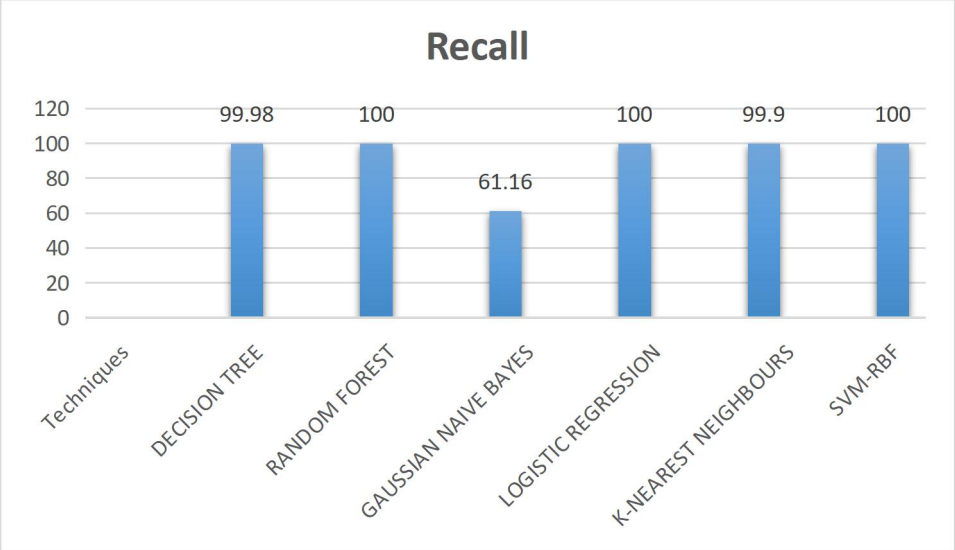

Fig 4: Measurement of Recall

5.3. Analysis

The performance metrics presented in Table 2, Fig-2, Fig-3 and Fig-4 offer valuable insights into the effectiveness of various machine learning techniques for detecting Distributed Denial of Service (DDoS) attacks, focusing on Accuracy, Precision, Recall, and False Alarm Rate (FAR).

- ***Accuracy:*** Decision Tree achieved the highest accuracy (99.93%), closely followed by Random Forest (99.87%) and Logistic Regression (99.85%). All models demonstrated high accuracy, indicating strong general performance in distinguishing between legitimate and malicious traffic. However, the accuracy alone does not reflect the model's effectiveness in identifying DDoS attacks without considering precision and recall.
- ***Precision:*** Precision values were notably high across most models, with Gaussian Naive Bayes achieving perfect precision (100%) but at the cost of poor overall performance, reflected in its low accuracy (61.21%) and recall (61.16%). The Decision Tree and Random Forest showed similar precision scores (99.95% and 99.87%, respectively), demonstrating their ability to avoid false positives effectively. However, the Logistic Regression model, despite good precision (99.85%), has a significantly higher FAR, suggesting a trade-off between accuracy and false alarms.
- ***Recall:*** The Recall metric reflects the model's ability to identify all instances of DDoS attacks. Random Forest and Logistic Regression both achieved perfect recall (100%), indicating that these models never missed an attack. However, high recall values in models like Logistic Regression (with a high FAR of 10.53%) suggest that while the model was excellent at identifying attacks, it was prone to incorrectly classifying legitimate traffic as malicious.
- ***False Alarm Rate (FAR):*** Random Forest exhibited the lowest FAR (0.05%), making it the most reliable model for minimizing false positives. In contrast, Logistic Regression's FAR was excessively high (10.53%), indicating that despite its high recall, it generated an unacceptably high number of false alerts.

6. Findings

- ***Performance of Machine Learning Models:*** Random Forest exhibited the best overall performance with high Accuracy (99.87%), Precision (99.87%), and Recall (100.00%), along with the lowest False Alarm Rate (FAR) of 0.05%. It effectively balances detection capability

and reliability, making it the most suitable choice for DDoS detection in various network environments. Decision Trees achieved the highest Accuracy (99.93%) and Recall (99.98%) but had a slightly higher FAR (0.24%) compared to Random Forest, indicating a marginally greater tendency to misclassify legitimate traffic.

- ***Model Trade-offs:*** SVM-RBF and K-Nearest Neighbours (KNN) delivered strong results with Accuracy above 99.80% and Recall at 100.00% and 99.90%, respectively. However, their FAR values (SVM-RBF: 0.62%, KNN: 0.27%) were higher than Random Forest, limiting their precision in critical applications. Logistic Regression showed high Accuracy (99.85%) and perfect Recall (100.00%) but suffered from an excessive FAR of 10.53%, making it unsuitable for deployment in environments where false alarms are costly or disruptive. Gaussian Naive Bayes demonstrated poor overall performance, with low Accuracy (61.21%) and Recall (61.16%), despite achieving perfect Precision (100.00%).
- ***Suitability for Real-time Detection:*** Models like Random Forest and Decision Trees, with their high Accuracy and low FAR, are well-suited for real-time DDoS detection, ensuring efficient and reliable traffic classification. Techniques like Logistic Regression and Gaussian Naive Bayes require significant optimization to meet the reliability standards needed for real-time applications.
- ***Minimizing False Alarms:*** The study highlights the importance of FAR as a critical metric in DDoS detection. Random Forest's low FAR (0.05%) underscores its capability to distinguish between legitimate and malicious traffic effectively, reducing unnecessary alerts.

These findings emphasize the role of selecting machine learning models based on the specific operational requirements and security priorities of the network environment.

7. Conclusion

In conclusion, this study demonstrates the effectiveness of various machine learning techniques in detecting DDoS attacks, with a focus on evaluating their performance based on accuracy, precision, recall, and false alarm rate (FAR). Random Forest emerged as the most reliable model, achieving high accuracy (99.87%), precision (99.87%), and perfect recall (100%), with the lowest FAR (0.05%), making it an optimal choice for real-time, large-scale DDoS detection systems. Decision Trees also showed strong performance, particularly in computationally constrained environments, while models like SVM-RBF and K-Nearest Neighbours showed potential but need optimization to reduce FAR. Logistic Regression and Gaussian Naive Bayes were less effective, exhibiting high FAR or lower accuracy. The study highlights the importance of selecting the right machine learning model for specific network security needs. Future research should explore hybrid models and focus on improving scalability and adaptability to address evolving DDoS threats more effectively.

References:

1. Ahmed, M., Hameed, R., & Shamsi, J. A. (2023). Integrating blockchain and machine learning for secure DDoS detection.
2. Al-Yaseen, W. L., Othman, Z. A., & Nazri, M. Z. A. (2016). Anomaly-based intrusion detection through K-means clustering and Naive Bayes classification.
3. Al-Yaseen, W. L., Othman, Z. A., & Nazri, M. Z. A. (2016). Multi-level hybrid support vector machine and extreme learning machine based on modified K-means for intrusion detection system.
4. Biggio, B., & Roli, F. (2018). Wild patterns: Ten years after the rise of adversarial machine learning.

5. Diro, A. A., & Chilamkurti, N. (2018). Distributed attack detection scheme using deep learning approach for Internet of Things.
6. Goodfellow, I. J., Shlens, J., & Szegedy, C. (2014). Explaining and harnessing adversarial examples.
7. Haider, W., Hu, J., Slay, J., Turnbull, B., & Xie, Y. (2017). Generating realistic intrusion detection system dataset based on fuzzy qualitative modeling.
8. Huang, L., Joseph, A. D., Nelson, B., Rubinstein, B. I. P., & Tygar, J. D. (2011). Adversarial machine learning.
9. Kim, J., Lee, J., & Kim, H. K. (2021). Feature selection for effective DDoS attack detection using machine learning.
10. Liu, Q., Zhang, Y., & Fan, L. (2024). IoT-based DDoS attack detection using machine learning techniques.
11. Mirkovic, J., & Reiher, P. (2010). A taxonomy of DDoS attack and DDoS defense mechanisms.
12. Nguyen, D., Pham, Q., & Le, T. (2024). Enhancing interpretability of machine learning models for DDoS detection.
13. Shafiq, M., Yu, X., Bashir, A. K., & Saleem, K. (2019). Network traffic classification techniques and comparative analysis using machine learning algorithms.
14. Tang, T. A., McLernon, D., Obaidat, M. S., & Ghogho, M. (2018). Intrusion detection in SCADA systems using convolutional neural networks.
15. Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009). A detailed analysis of the KDD CUP 99 data set.
16. Vinayakumar, R., Soman, K. P., & Poornachandran, P. (2017). Applying deep learning approaches for network traffic classification and intrusion detection.
17. Yazidi, A., Lahmadi, A., & Audra, T. (2020). Federated learning for DDoS detection.
18. Yin, C., Zhu, Y., Fei, J., & He, X. (2022). A context-aware anomaly detection approach for DDoS attacks in IoT environments.
19. Zhang, H., Chen, W., & Huang, D. (2011). SVM-based DDoS detection system.
20. Zheng, Z., Zhu, J., & Zhou, Y. (2020). Machine learning and deep learning methods for cybersecurity.