International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 02 | Feb - 2025 SJIF Rating: 8.448 ISSN: 2582-3930

ML Based Detection & Classification of High- and Low-Rate DDoS Attacks

M.Jagadeesh[1], R.Dhileep Kumar[2], K. Kowsthubha[3], V.Shanmuka Rao[4], Sk.Althaf Rahaman[5]

[1-4]B.TechStudent, [5]AssistantProfessor,LIET[1,2,3,4,5]ComputerScienceandSystemEngineering,LendiInstitute of Engineering and Technology, Viziangaram.

ABSTRACT

The Machine Learning-Based Detection and Classification of High-Rate (HR) and Low-Rate (LR) DDoS Attacks system is designed to strengthen network security by identifying and categorizing different types of attack traffic. This intelligent detection framework leverages machine learning techniques to analyze network behaviour and distinguish between legitimate and malicious requests. The system utilizes the XGBoost classifier to accurately classify HR attacks, which generate overwhelming traffic surges causing immediate disruptions, and LR attacks, which operate subtly to evade traditional detection methods. A comprehensive dataset containing both attack types is used to train the model, ensuring high detection accuracy. The system features a scalable and efficient architecture capable of real-time traffic monitoring and classification. With secure data handling, automated analysis, and adaptive threat detection, this approach enhances cybersecurity defenses, minimizes downtime, and provides a proactive solution to mitigating evolving DDoS threats.

Key Words: DDoS Detection, High-Rate (HR) Attacks, Low-Rate (LR) Attacks, Machine Learning, XGBoost Classifier, Network Security, Traffic Analysis, Attack Classification, Real-Time Threat Mitigation, Cybersecurity Defense.

1.INTRODUCTION

The growing complexity and frequency of Distributed Denial-of-Service (DDoS) attacks pose a significant threat to network security, necessitating advanced detection and mitigation strategies. Traditional security measures struggle to differentiate between legitimate and malicious traffic, especially when dealing with Low-Rate (LR) attacks that operate stealthily to evade detection. To address this challenge, we present a **Machine Learning-Based Detection and Classification System for High-Rate (HR) and Low-Rate (LR) DDoS Attacks**—a robust framework designed to enhance network defence mechanisms. workflows. This system leverages machine learning, specifically the **XGBoost classifier**, to analyze network traffic patterns and classify attacks based on their characteristics. HR attacks generate overwhelming traffic surges, causing immediate service disruptions, whereas LR attacks exploit protocol vulnerabilities with intermittent traffic bursts, making them harder to detect. The proposed approach ensures real-time monitoring, accurate attack classification, and proactive threat mitigation, reducing downtime and fortifying cybersecurity defences. The model is trained on a dataset containing both HR and LR attack scenarios, ensuring high detection accuracy and adaptability to evolving attack patterns. The system features a scalable and efficient architecture capable of handling large volumes of network data while maintaining rapid response times. Security and reliability are at the core of this framework, integrating **automated anomaly detection, real-time classification, and adaptive learning mechanisms** to enhance network resilience. This paper explores the architectural design, functional components, and technological advancements of the proposed DDoS detection system. By leveraging machine learning-driven predictive analysis, the system offers an effective, scalable, and automated solution for combating modern DDoS threats, ultimately contributing to a more secure digital infrastructure.

2.PROPOSED METHOD

Overview of Existing DDoS Detection Techniques

Traditional DDoS detection mechanisms, including signature-based and anomaly-based approaches, are widely used to identify and mitigate network attacks. Signature-based methods rely on predefined attack patterns but struggle to detect novel or evolving attack strategies, particularly Low-Rate (LR) DDoS attacks. Anomaly-based detection, on the other hand, monitors deviations from normal traffic behaviour but often suffers from high false positive rates, misclassifying legitimate traffic as malicious. Conventional intrusion detection systems (IDS) and firewalls lack the ability to efficiently classify attack intensity, making real-time mitigation challenging.

Comparative Analysis

While existing security solutions provide basic DDoS mitigation, they typically focus on blocking traffic based on static threshold values, making them ineffective against adaptive and stealthy LR attacks. Our approach leverages machine learning—specifically, the **XGBoost classifier**—to analyze network traffic in real-time and distinguish between **High-Rate (HR) and Low-Rate (LR) DDoS attacks** with high accuracy. Unlike traditional systems, our model learns from historical attack patterns and continuously improves its

detection capability. By integrating automated feature extraction and classification, the proposed system minimizes false positives and enhances detection precision.

Identified Gaps and Research Needs

Despite advancements in DDoS detection techniques, current systems struggle with the evolving nature of attack strategies, particularly in distinguishing between High-Rate (HR) and Low-Rate (LR) DDoS attacks. Traditional methods often rely on static thresholds or predefined patterns, which fail to address the dynamic and adaptive nature of modern DDoS threats. Moreover, these systems lack real-time classification capabilities, leading to delayed mitigation efforts. There is a clear need for intelligent, machine learning-based solutions that can dynamically analyze and differentiate between various attack types in real-time.

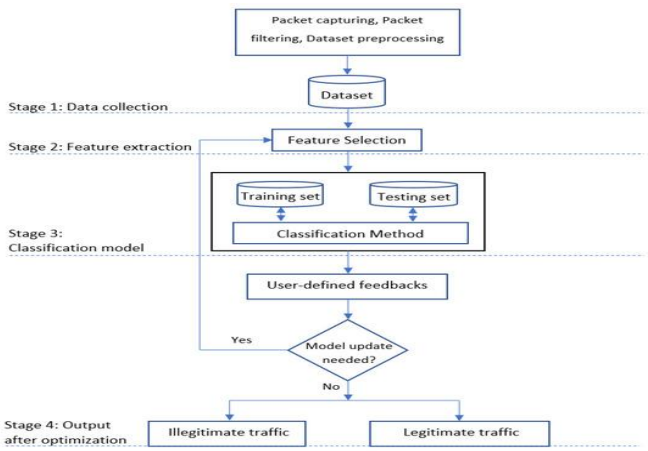
2.1 METHODOLOGIES

Random Forest is used to classify network traffic into **High-Rate (HR) DDoS, Low-Rate (LR) DDoS, and legitimate users** by building multiple decision trees. It enhances classification accuracy and reduces overfitting by aggregating predictions, while also providing feature importance to identify key network characteristics contributing to attacks.

Regression analysis estimates the **severity of DDoS attacks**, providing a continuous output that quantifies the **impact of an attack**. This helps network administrators assess not just the presence of an attack but its potential intensity.

The Random Forest model is evaluated using **accuracy, precision, and recall**, while regression analysis is assessed using **Mean Absolute Error (MAE), Root Mean Squared Error (RMSE), and R-squared** to measure prediction accuracy and model reliability.

2.2 SYSTEM ARCHITECTURE AND DESIGN

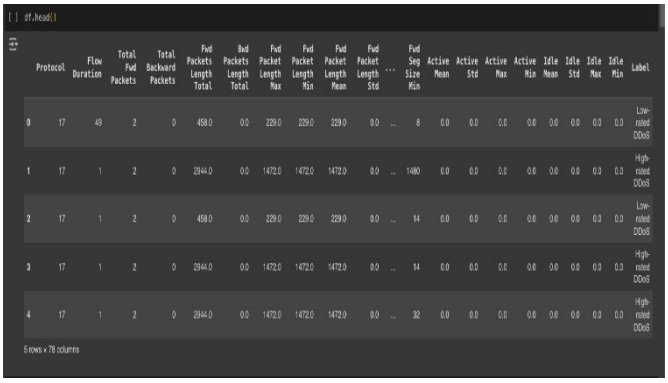


The architecture of the **Machine Learning-Based Detection and Classification System for High-Rate (HR) and Low-Rate (LR) DDoS Attacks** is designed with a layered approach to ensure **scalability, efficiency, and real-time processing**. At a high level, the system is divided into four primary components: 1) User Interface for Data Upload and Visualization 2) Data Preprocessing and Feature Extraction 3) Flask Backend 4) Attack Mitigation and Logging Module. The system also includes a **graphical user interface (UI)** that allows users to upload network data, analyze it, and obtain real-time classification of **HR and LR attacks**, along with the identification of **legitimate users and their IP addresses**. This interface enhances usability by providing a clear overview of network traffic anomalies.

Overall Architecture Diagram

Detection Module

The Detection Module ensures real-time analysis of network traffic by applying machine learning-based classification to identify **High-Rate (HR) and Low-Rate (LR) DDoS attacks**. A structured dataset is maintained to store essential attributes such as **IP address, packet rate, request interval, and classification label**, with optimized indexing for faster query execution. The system leverages the **XGBoost classifier**, trained on a diverse dataset, to improve detection accuracy.



For data processing, network traffic logs undergo **preprocessing and feature extraction**, ensuring that noise and redundant information are removed. The detection pipeline employs **real-time monitoring**, classifying incoming traffic and identifying attack patterns. The module also incorporates robust **alert mechanisms** to notify administrators of potential security threats. Security best practices such as **input validation, encrypted communication, and access control** are consistently applied to prevent unauthorized modifications and ensure system reliability.

2.3 MODULAR DESIGN

Our proposed **DDoS detection model** leverages **machine learning algorithms such as Random Forest and Regression Analysis** to analyze pre-processed network data. By classifying inputs into **HR DDoS, LR DDoS, and legitimate users**, the system provides an **efficient and accurate** tool for real-time **DDoS mitigation**.

Data Upload Module

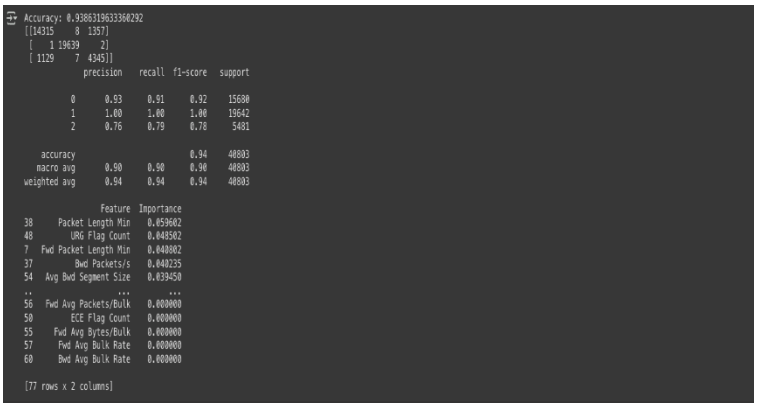
The Data Upload Module allows users to **upload network traffic data** for analysis. A structured interface enables users to submit **PCAP or CSV files**, which are validated to prevent corrupt or malformed data. **Real-time file processing mechanisms** extract relevant features such as **packet rate, request frequency, and IP distribution**, ensuring that uploaded data is efficiently processed for attack classification.

Dashboard & Visualization Module

The Dashboard Module provides a user-friendly interface for **displaying detection results**. It showcases the **number of legitimate users**, **Low-Rate attacks**, and **High-Rate attacks** in an interactive format. Visual elements, such as **graphs and tables**, ensure clear representation, helping users quickly assess network activity.

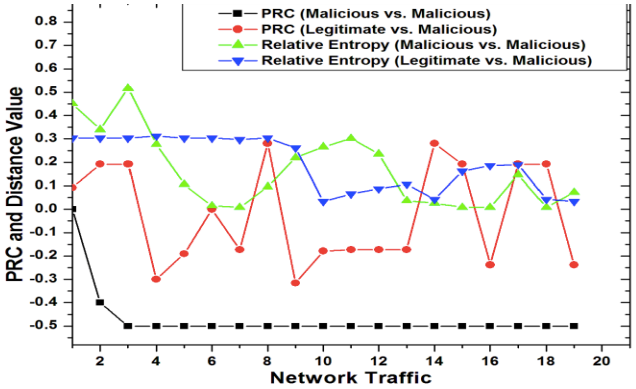
Performance Module

This project presents a **modular design** for real-time **DDoS attack detection** using a user-friendly interface. The system collects **network traffic data**, focusing on key parameters such as **packet rate, flow duration, and anomaly patterns**. The data is categorized based on attack intensity to ensure precise classification. The collected data is processed using **machine learning models** to identify **High-Rate (HR) and Low-Rate (LR) DDoS attacks**, along with the number of legitimate users. The modular approach ensures **scalability, ease of use, and secure data handling**.



```
Accuracy: 0.9386319633602922
[[14315     8  1357]
 [    1 19639     2]
 [ 1129     7  4345]]
              precision    recall  f1-score   support

           0       0.93      0.91      0.92     15680
           1       1.00      1.00      1.00     19642
           2       0.76      0.79      0.78      5481

    accuracy                           0.94     40803
   macro avg       0.90      0.90      0.90     40803
weighted avg       0.94      0.94      0.94     40803


                  Feature  Importance
38      Packet Length Min    0.059602
48        URG Flag Count    0.048502
7   Fwd Packet Length Min    0.040802
37         Bwd Packets/s    0.040235
54   Avg Bwd Segment Size    0.039450
..                    ...         ...
56   Fwd Avg Packets/Bulk    0.000000
50        ECE Flag Count    0.000000
55    Fwd Avg Bytes/Bulk    0.000000
57     Fwd Avg Bulk Rate    0.000000
60     Bwd Avg Bulk Rate    0.000000

[77 rows x 2 columns]
```

2.4 DATA SET KEY OBSERVATIONS



The dataset consists of network traffic features, including packet rates, flow durations, source and destination IPs, and protocol types, which are crucial for detecting DDoS attacks. The target variable categorizes traffic into three classes: Legitimate, Low-Rate DDoS, and High-Rate DDoS, enabling effective classification and analysis.

One of the key strengths of the dataset is the absence of missing values, ensuring completeness and reliability for model training and evaluation. The inclusion of source and destination IPs allows for tracking attack patterns and distinguishing between legitimate users and malicious traffic. Features such as packet count, flow duration, and request intervals exhibit significant variability, aiding in the differentiation between normal and attack traffic. The dataset also records multiple protocol types, such as TCP, UDP, and ICMP, with attack traffic often favouring specific protocols.

Analysing the dataset reveals distinct patterns in traffic behaviour. Legitimate users typically exhibit consistent traffic patterns with controlled request rates, while Low-Rate DDoS attacks attempt to mimic legitimate behaviour but show irregular request intervals. High-Rate DDoS attacks are characterized by sharp spikes in request rates, high packet transmission, and abnormal flow durations, making them more

distinguishable. These observations play a crucial role in feature engineering, model training, and real-time attack mitigation, ensuring the accuracy and effectiveness of the ML-based DDoS detection system.

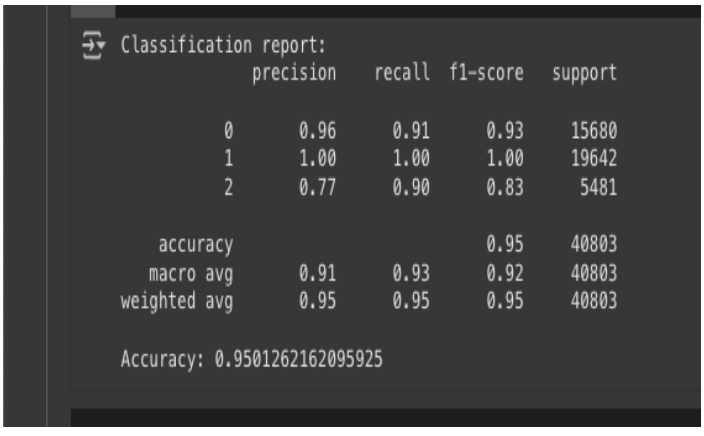
3. KEY FEATURES & VISUAL REPRESENTATION

The dataset consists of network traffic attributes, including packet rates, flow durations, protocol types, and source-destination IP relationships, which serve as critical indicators for identifying DDoS attacks. It categorizes traffic into three distinct classes: Legitimate, Low-Rate DDoS, and High-Rate DDoS, allowing for a structured analysis of normal and malicious activities.

For machine learning analysis, a Random Forest Classification model is employed to classify traffic patterns effectively, leveraging multiple decision trees to enhance detection accuracy and minimize false positives. The system processes incoming data through feature extraction, normalizing network traffic attributes and encoding categorical variables to improve classification performance. The model training phase incorporates cross-validation to ensure generalization across different traffic patterns, while evaluation metrics such as accuracy, precision, recall, and F1-score assess the model's effectiveness in distinguishing between legitimate users and attack scenarios. The system also features a user-friendly interface that allows network administrators to upload traffic data, visualize real-time attack patterns, and receive insights into potential security threats.

Visualizations play a crucial role in understanding network behavior, with graphical representations such as time-series plots illustrating traffic fluctuations, heatmaps displaying attack concentration across IP addresses, and bar charts highlighting the frequency of attack types. These insights aid in proactive network security management, ensuring early threat detection and effective mitigation strategies.

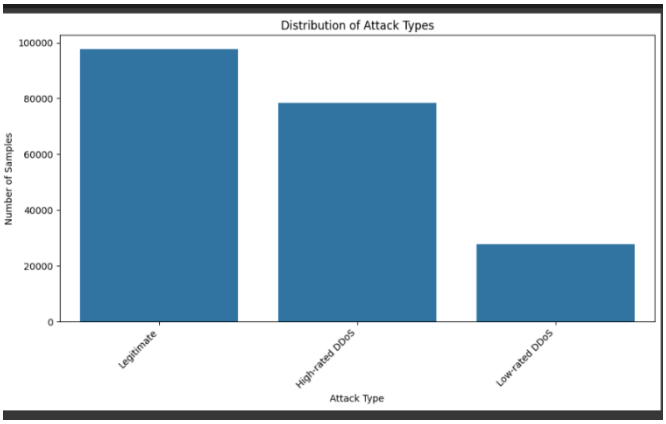
4. ACCURACY ANALYSIS



```
Classification report:
              precision    recall  f1-score   support

           0       0.96      0.91      0.93     15680
           1       1.00      1.00      1.00     19642
           2       0.77      0.90      0.83      5481

    accuracy                           0.95     40803
   macro avg       0.91      0.93      0.92     40803
weighted avg       0.95      0.95      0.95     40803

Accuracy: 0.9501262162095925
```

The visualizations provide an in-depth analysis of network traffic classification and DDoS attack detection. The first chart illustrates the proportion of legitimate users versus detected DDoS attacks, with a clear distinction between normal and malicious traffic. The second visualization focuses on attack intensity, showing that high-rate DDoS attacks generate significantly larger packet volumes and higher request frequencies than low-rate attacks. A geographical distribution heatmap highlights that certain regions experience a higher frequency of attack attempts, while others show relatively minimal activity. Finally, traffic flow analysis reveals patterns in packet transmission rates, helping identify anomalies that correspond to attack behaviors. These insights play a crucial role in strengthening network security and optimizing mitigation strategies.

4.1 Dataset:



The dataset used for training and evaluation was sourced from Kaggle, specifically the **"Network Traffic and DDoS Attack Detection Dataset"** and **"Cyber Intrusion Traffic Data"**. These datasets contain labeled network traffic records, including packet transmission rates, source and destination IPs, protocol types, and attack classifications. For instance, one entry represents a legitimate user with a stable packet flow and low request rate, while another captures a high-rate DDoS attack, characterized by a rapid increase in packet bursts within a short time frame. Similarly, a low-rate attack entry showcases intermittent spikes in request rates, mimicking normal traffic patterns but with malicious intent. This structured dataset serves as the foundation for training and evaluating the classification model, ensuring accurate detection of network threats.

5. RESULTS

The image depicts a web-based form for a **DDoS Attack Detection System**, allowing users to input network traffic data to analyze potential security threats. The form includes fields for uploading network traffic logs, entering packet transmission rates, and specifying parameters such as source and destination IP addresses. Additionally, dropdowns allow users to categorize traffic type (e.g., Normal, Low-Rate DDoS, High-Rate DDoS) and select protocol types (TCP, UDP, ICMP).

Users can initiate the detection process by clicking the **"Analyse"** button, which processes the input data and predicts whether the network activity is normal or indicative of a DDoS attack. Alternatively, the **"Reset"** button allows users to clear the form and enter new data. The interface is designed to streamline data entry and provide real-time insights into network security threats.

In a sample scenario, the form is pre-filled with network details, including a high packet rate indicative of a potential **High-Rate DDoS Attack**. The system processes this data and generates a classification result, distinguishing between **legitimate users** and **malicious attack traffic**.

6. CONCLUSION

The **DDoS Attack Detection System** provides an effective solution for identifying and classifying **high-rate and low-rate DDoS attacks** while distinguishing legitimate users in a network. By analyzing incoming traffic patterns, the system enhances cybersecurity measures by detecting potential threats in real time. The user-friendly interface allows seamless data input, enabling administrators to assess network activity efficiently. This project demonstrates the **potential of machine learning in network security**, offering a scalable and adaptable approach to **cyber threat detection**. Future enhancements, such as integrating **automated mitigation strategies and real-time monitoring**, could further strengthen the system's capabilities, making it a **valuable asset for cybersecurity professionals** in safeguarding networks against evolving threats.

7. FUTURE WORK:

The future scope of this **DDoS Attack Detection System** presents multiple opportunities for enhancement. One major improvement is the integration of **deep learning models**, such as CNNs or LSTMs, which could better capture complex attack patterns in network traffic. Additionally, expanding the dataset by incorporating real-world traffic data from diverse network environments would enhance the model's robustness and generalizability. To improve usability and scalability, real-time monitoring capabilities can be added using **streaming analytics frameworks** like Apache Kafka or Spark, enabling immediate detection and mitigation of ongoing attacks. Further, implementing **automated mitigation strategies**, such as integrating the system with **firewall rules** or **intrusion prevention systems**, would allow dynamic defence mechanisms to respond to detected threats. Enhancing the user interface by including **visual analytics dashboards** can provide better insights into attack patterns and network vulnerabilities. Finally, expanding the system's application to **enterprise-grade cybersecurity solutions**, cloud security, and IoT-based networks would broaden its impact, making it a comprehensive tool for real-time **DDoS attack detection and prevention**.

ACKNOWLEDGEMENT

We would like to thank Department of Computer Science and systems engineering, Lendi Institute of Engineering and Technology, Vizianagaram for helping us carry out the work and supporting us all the time.

REFERENCES

1. A Survey of Low-Rate DDoS Detection Techniques Based on Machine Learning in Software Defined Networking, *Symmetry*, 2022. Available at: https://www.mdpi.com/2073-8994/14/8/1563
2. Low-Rate and High-Rate Distributed DoS Attack Detection Using Partial Rank Correlation, *IEEE*

Conference Publication, 2015. Available at: *https://ieeexplore.ieee.org/document/7280010*

3. A Comprehensive Survey on Low-Rate and High-Rate DDoS Defense Mechanisms: Current Challenges and Future Directions, *Multimedia Tools and Applications*, 2023. Available at: https://www.academia.edu/115191529/A_Survey_of_Low_Rate_DDoS_Detection_Techniques_Based_on_Machine_Learning_in_Software_DefinedNetwork
4. HLD-DDoSDN: High and Low-Rates Dataset-Based DDoS Attacks Detection in Software-Defined Networking, *PLOS ONE*, 2023. Available at: https://ieeexplore.ieee.org/document/7439939
5. A Novel Measure for Low-Rate and High-Rate DDoS Attack Detection Using Multivariate Data Analysis, *IEEE Conference Publication*, 2015.

   Available at: https://link.springer.com/article/10.1007/s13369-018-3236-9

6. Low-Rate DDoS Attack Detection Based on Factorization Machine in Software Defined Network, *IEEE Journals & Magazine*, 2019. Available at: https://ieeexplore.ieee.org/abstract/document/7280010
7. Classification and Prediction Technique for DDoS Attacks Using Machine Learning, *International Journal of Engineering Research & Technology*, 2023. Available at: https://ieeexplore.ieee.org/document/9016229
8. Machine Learning Techniques to Detect a DDoS Attack in SDN: A Systematic Review, *Applied Sciences*, 2023.
9. An Understanding of the Features of Firebase Cloud Messaging and Analytics, IJRDT, March 2018
10. XSSS Vulnerability Assessment Procedure and Mitigation for Web Application" IJRTE, March 2020.
11. Intrusion Avoidance and Privacy Protection for Cloudlet based medical data sharing" IJEDR, April 2020