

Design and Development of an AI Enabled to Detect the DDOS Cyber Attack

Meena D G M¹, Dr. Basavaraj S Pol²

¹M.Tech Student, Department of Computer Science and Engineering,
R. L. Jalappa Institute of Technology, Doddaballapur, Karnataka, India

²Associate Professor & HOD, Department of Computer Science and Engineering (Cyber Security),
R. L. Jalappa Institute of Technology, Doddaballapur, Karnataka, India

Abstract : Distributed Denial of Service (DDoS) attacks are one of the most common cyber threats that affect the availability and reliability of online services. These attacks overload network resources with excessive traffic, making websites and applications inaccessible to legitimate users. This paper presents an AI-enabled DDoS detection system using the Random Forest machine learning algorithm to identify malicious network traffic accurately. Network traffic is collected using Wireshark and Netscan, preprocessed, and classified into normal and attack traffic. A Streamlit-based web application enables users to upload datasets, analyze network traffic, and visualize detection results. Zapier is integrated to generate real-time email alerts whenever a DDoS attack is detected. Experimental results show that the proposed system achieves high detection accuracy with a low false positive rate, making it an effective and user-friendly solution for network security.

Keywords

DDoS Attack, Random Forest, Machine Learning, Streamlit, Wireshark, Network Security, Zapier, Cybersecurity.

1. INTRODUCTION

The rapid advancement of digital technologies has significantly transformed the way organizations operate and deliver services. Modern systems rely heavily on continuous network availability to ensure the smooth functioning of applications such as online banking, cloud computing, e-commerce, healthcare systems, and communication platforms. As businesses increasingly adopt digital infrastructure, maintaining secure, reliable, and uninterrupted network services has become a critical requirement. However, this growing dependence on interconnected networks has also increased the exposure of systems to a wide range of cybersecurity threats, making network protection more challenging than ever before.

Among these threats, Distributed Denial of Service (DDoS) attacks are particularly harmful because they aim to disrupt services by overwhelming target systems with massive amounts of malicious traffic. These attacks are carried out using multiple compromised devices, commonly known as botnets, which collectively flood the target server, exhausting its resources and preventing legitimate users from accessing the service. DDoS attacks can result in financial losses, operational downtime, and damage to an organization's reputation, making their early detection and mitigation essential.

Traditional security mechanisms often struggle to identify sophisticated and rapidly evolving attack patterns. To address this challenge, intelligent systems based on Artificial Intelligence (AI) and Machine Learning (ML) are being developed. These systems can analyze large volumes of network traffic, identify abnormal behavior, learn from historical data, and respond quickly to potential threats with greater accuracy than conventional methods. By enabling real-time detection and automated decision-making, AI-based solutions provide a more effective approach to protecting modern network infrastructures. This project focuses on building an AI-enabled DDoS attack detection system that analyzes network traffic patterns to accurately distinguish between normal and malicious activities. The proposed solution aims to improve detection efficiency, reduce false alarms, and enhance the overall security and reliability of network services.

2. LITERATURE SURVEY

The rapid advancement of cloud computing, Internet of Things (IoT), Software Defined Networking (SDN), and large-scale internet services has significantly improved digital communication and data exchange. However, this technological growth has also increased the number and complexity of cyber threats. Among these threats, Distributed Denial of Service (DDoS) attacks have emerged as one of the most dangerous network attacks because they can disrupt online services by flooding target systems with massive volumes of malicious traffic. Such attacks affect organizations, government services, banking systems, healthcare applications, educational institutions, and cloud platforms by making services unavailable to legitimate users.

Initially, DDoS attacks were detected using traditional rule-based and signature-based Intrusion Detection Systems (IDS). Although these techniques successfully identified previously known attacks, they struggled to recognize unknown or evolving attack patterns. The increasing size of network traffic and the rapid evolution of attack strategies have reduced the effectiveness of conventional security mechanisms.

Machine Learning (ML) has become an effective solution for addressing these challenges. ML algorithms can automatically learn network traffic behavior, identify abnormal patterns, and classify malicious traffic with high accuracy. Various supervised learning algorithms, including Random Forest, Decision Tree, Support Vector Machine (SVM), K-Nearest

K-Nearest Neighbor (KNN), Naïve Bayes, and XGBoost, have been widely adopted for DDoS detection due to their capability to improve detection accuracy while reducing false alarms.

Apart from attack detection, recent research has emphasized the importance of real-time monitoring and visualization. Security administrators require dashboards that display live traffic statistics, attack alerts, packet analysis, and graphical reports to facilitate rapid decision-making. Consequently, integrating machine learning with interactive dashboards has become an important research direction in modern network.

3. PROPOSED METHODOLOGY

The proposed AI-enabled DDoS detection system is designed to identify malicious network traffic using the Random Forest machine learning algorithm. The overall workflow consists of network traffic collection, data preprocessing, model training, attack detection, result visualization, and email alert generation.

Initially, network traffic is captured using Wireshark and Netscan, while the CICIDS2017 dataset is used for training and testing the machine learning model. The collected data is preprocessed by removing missing values, selecting important features, and converting the data into a suitable format for classification. This preprocessing step improves the quality of the dataset and enhances the performance of the detection model.

The processed dataset is then provided to the Random Forest classifier, which learns the patterns of normal and malicious traffic. Once the model is trained, users can upload a network traffic dataset through the Streamlit web application. The system analyzes the uploaded data and classifies each record as either Normal Traffic or a DDoS Attack. The detection results are displayed on the Streamlit dashboard using tables and graphical visualizations, making it easy for users to understand the network status. Whenever a DDoS attack is detected, the system automatically triggers Zapier, which sends a real-time email notification to the administrator. This enables quick response to potential attacks and helps improve overall network security.

The proposed methodology combines machine learning, interactive visualization, and automated alert generation to provide an accurate, efficient, and user-friendly DDoS detection system suitable for educational institutions and other organizations.



Fig . 1 : Proposed methodology

4. SYSTEM DESIGN ARCHITECTURE

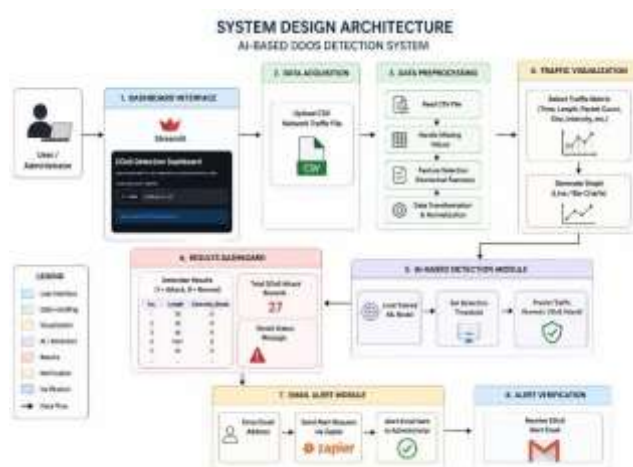


Fig .2 System design architecture

1. Network Traffic Upload Module

The user uploads a network traffic CSV dataset through the Streamlit dashboard. The uploaded dataset acts as the input for the detection process.

2. Data Preview and Preprocessing Module

After successful upload, the system displays the uploaded dataset in tabular format. The preprocessing stage removes unnecessary values, validates the dataset, selects useful traffic features, and prepares the data for machine learning analysis.

3. Traffic Visualization Module

The user selects a traffic metric such as:

- Time
- Packet Length
- Packet Count
- Traffic Intensity

The system generates graphical plots showing traffic behavior, helping users identify abnormal spikes that may indicate attacks.

4. AI-Based DDoS Detection Module

The processed traffic data is passed to the trained AI model.

The model compares the selected traffic values against the configured threshold and predicts whether each record represents:

- Normal Traffic (0)
- DDoS Attack (1)

The prediction results are displayed in tabular format.

5. Attack Detection Module

After classification, the system counts the total number of detected attack records and displays the result on the dashboard. If attacks are detected, the dashboard highlights the detection status using warning messages.

6. Email Alert Module

When an attack is detected, the administrator enters an email address.

The system uses Zapier automation to trigger an email notification containing the attack alert.

7. Notification Confirmation Module

Once the email is successfully delivered, the administrator receives a confirmation email stating that a DDoS attack has been detected.

This allows immediate action to prevent further network damage.

4. RESULTS AND DISCUSSION

The dataset analysis is an important stage in evaluating the effectiveness of the proposed AI- Enabled DDoS Detection System. It provides an understanding of the characteristics of the uploaded network traffic data and forms the foundation for accurate attack detection. The proposed system accepts network traffic datasets in CSV (Comma-Separated Values) format, which contain records of network communication captured over a specific period. These records include various traffic attributes that are analyzed to identify patterns associated with normal network behavior and Distributed Denial-of-Service (DDoS) attacks.



Fig. 3. DDoS Detection Dashboard

It is the home page of the proposed DDoS Detection Dashboard developed using the Streamlit framework. The dashboard provides a simple and user-friendly interface for monitoring network traffic and detecting Distributed Denial-of-Service (DDoS) attacks



Fig.4 Network traffic dataset

It illustrates the process of uploading the network traffic dataset in CSV format through the Streamlit dashboard. After the dataset is uploaded, the system validates the file and displays a preview of the network traffic records. This allows users to verify the uploaded data before proceeding with traffic analysis. The dataset preview ensures that the correct input has been provided for accurate DDoS attack detection.



Fig. 5. Packet Length Traffic Analysis

It illustrates the graphical analysis of the packet length values in the uploaded network traffic dataset. The dashboard displays a line graph showing variations in packet sizes across different traffic records. This visualization helps identify abnormal spikes in network traffic, which may indicate potential DDoS attacks. It provides useful insights into traffic behavior before the final detection process.



Fig.5 : DDoS Attack Detection Results

It presents the DDoS attack detection results generated by the proposed system. The dashboard classifies each network traffic record as either normal (0) or attack (1) based on the selected threshold value. It also displays the total number of detected DDoS attack records and the corresponding prediction results in a tabular format. This output enables users to easily identify malicious network traffic for further analysis and response.

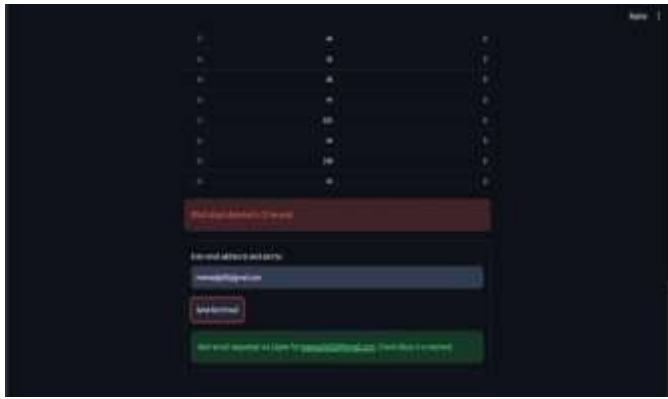


Fig. 6 : Email Alert Notification through Zapier

The dashboard sends an email alert when a DDoS attack is detected. The user enters an email address and clicks the Send Alert Email button to trigger the notification. A confirmation message is displayed after the alert request is successfully sent through Zapier. This feature enables administrators to receive instant notifications about detected attacks for timely response.

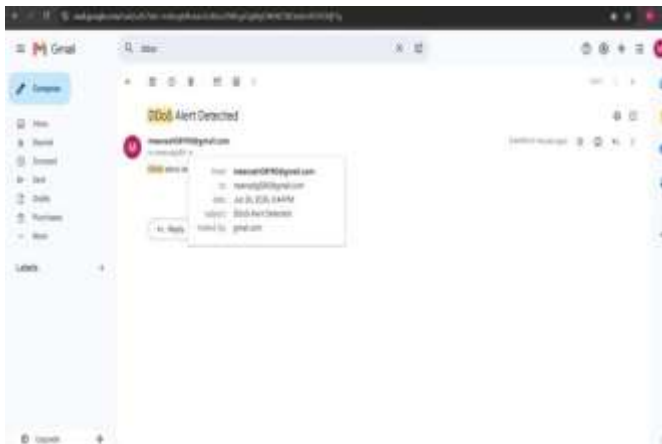


Fig. 7: Email Alert Received in Gmail

The Gmail interface displays the detailed view of the received DDoS alert email. The email includes essential information such as the sender, receiver, date, time, and subject "DDoS Alert Detected." It confirms that the alert message was successfully delivered after detecting abnormal network traffic. This demonstrates that the integrated alert system using Zapier is functioning effectively and ensures that timely notifications are provided for prompt action against potential DDoS attacks.

5. CONCLUSION

In this project, an intelligent system for detecting Distributed Denial of Service (DDoS) attacks has been successfully designed and implemented using machine learning techniques. With the rapid growth of network-based applications, ensuring network security has become a critical requirement. DDoS attacks are one of the most common and dangerous cyber threats, as they overwhelm network resources and disrupt normal services.

The proposed system analyzes network traffic data and identifies abnormal patterns that indicate potential DDoS attacks. A machine learning model is trained using features such as packet size, traffic flow, and request frequency to classify traffic into normal and attack categories. The system demonstrates satisfactory performance in detecting malicious traffic from the dataset used.

To enhance usability, a Streamlit-based dashboard is developed, which allows users to upload network traffic data, visualize patterns through graphs, and observe detection results in an interactive manner. This makes the system accessible even to users with minimal technical knowledge.

A key feature of this project is the integration of an automated alert system using Zapier webhook services. Whenever the system detects a potential DDoS attack, an alert message is automatically sent to a registered email address. This ensures real-time notification and enables network administrators to take immediate action.

The successful implementation of detection, visualization, and alerting demonstrates that the system can serve as a practical solution for basic network intrusion detection. Although the current model is limited to offline data analysis, it provides a strong foundation for future enhancements such as real-time monitoring and automated response systems.

Furthermore, this project highlights the importance of integrating intelligent detection mechanisms with user-friendly interfaces and automated alert systems to strengthen cybersecurity practices. By combining machine learning with visualization and notification tools, the system not only detects attacks but also improves awareness and response efficiency. This approach can significantly reduce the impact of DDoS attacks in real-world scenarios. With further improvements such as real-time data processing, advanced learning models, and seamless integration with network security infrastructure, the system potential to a comprehensive and robust cybersecurity solution.

6. FUTURE SCOPE

The proposed system can be further enhanced in multiple ways to improve its performance and real-world applicability:

- **Real-Time Traffic Monitoring:**
Integrate the system with live network traffic using tools like packet sniffers (Wireshark, Scapy) to detect attacks in real time.
- **Advanced Machine Learning Models:**
Implement deep learning models such as LSTM, CNN, or hybrid models for improved detection accuracy and pattern recognition.
- **Anomaly Detection Techniques:**
Use unsupervised learning methods to detect unknown or zero-day attacks.
- **Integration with Security Systems:**
Connect the system with firewalls, Intrusion Detection Systems (IDS), or Intrusion Prevention Systems (IPS) to automatically block malicious traffic.
- **Multi-Channel Alert System:**
Extend alerts to SMS, mobile apps, or dashboards for faster response.
- **Cloud Deployment:**
Deploy the system on cloud platforms such as AWS, Azure, or Google Cloud for scalability.
- **Big Data Handling:**
Use technologies like Hadoop or Spark to process large-scale network data efficiently.
- **Improved Visualization:**
Add advanced analytics dashboards with real-time graphs, heatmaps, and attack trends.
- **User Authentication System:**
Add login and role-based access control for secure usage.
- **Continuous Learning Model:**
Implement online learning so the model updates itself with new attack patterns over time.

ACKNOWLEDGEMENT

The authors express their sincere gratitude to the Department of Computer Science and Engineering, R. L. Jalappa Institute of Technology, Doddaballapura, Karnataka, for providing the necessary facilities and support to carry out this research work. The authors also thank Dr. Basavaraj S Pol., Associate Professor & HOD, Dept. of CSE (Cyber Security) for his valuable guidance, encouragement, and continuous support throughout the project.

REFERENCES

- [1] M. Abdelmaboud, T. Abdullah, and U. Maiwada, "Enhancing DDoS Attack Detection and Mitigation in SDN Using Ensemble Online Machine Learning Model," *IEEE Access*, 2024.
- [2] Y. Chen et al., "Advanced Detection of DDoS Attacks Using Hybrid Deep Learning and Graph Neural Networks," *IEEE Xplore*, 2024.
- [3] M. S. Alkasassbeh et al., "Efficient Detection of DDoS Attacks in Cloud Environments Using Sparse Neural Networks," *IEEE Conference*, 2024.
- [4] D. Tymoshchuk et al., "Detection and Classification of DDoS Flooding Attacks Using Neural Networks," *arXiv*, 2024.
- [5] A. Alfatemi et al., "Advancing DDoS Detection Using Deep Residual Neural Networks and SMOTE," *arXiv*, 2024.
- [6] X. Fu et al., "Deep Learning Techniques for DDoS Attack Detection: A Review," *Expert Systems with Applications*, 2025.
- [7] A. Apostu et al., "Detecting and Mitigating DDoS Attacks with AI: A Survey," *arXiv*, 2025.
- [8] S. R. Chen et al., "DDoS Detection Using Hybrid CNN-RNN Model," *Electronics*, 2025.
- [9] S. Vijay, "Real-Time DDoS Attack Detection and Prevention Using Hybrid Machine Learning Techniques," *IJSAT*, 2025.
- [10] J. Wang et al., "Modern DDoS Threats and Detection Strategies," *arXiv*, 2025.
- [11] K. Patel et al., "Machine Learning Framework for Zero-Day DDoS Detection in Cloud Systems," *IEEE Xplore*, 2025.
- [12] O. Ebrahim et al., "A Lightweight Machine Learning Approach for Multiclass DDoS Detection," *Scientific Reports*, 2026.
- [13] M. Fathian et al., "Real-Time Machine Learning Model for Detecting DDoS Attacks," *Springer*, 2022.