2026 Volume: 02 Issue: 05 www.ijrpa.com ISSN 2456-9995 Research Article

International Journal Research Publication Analysis

Page: 01-15

MACHINE LEARNING-BASED DDOS DETECTION AND PREVENTION SYSTEM WITH REAL-TIME MONITORING DASHBOARD

***[1]S. Saila, [2]Saniya, [2]Sankhya Hegde, [2]Shrilakshmi T. Hegde, [2]Yallutla Mounika**

[1]Assistant Professor, Department of Computer Science and Engineering, Jyothy Institute of Technology, Bengaluru, India.

[2]Department of Computer Science and Engineering, Jyothy Institute of Technology, Bengaluru, India.

Article Received: 27 March 2026
Article Revised: 17 April 2026
Published on: 07 May 2026

***Corresponding Author: S. Saila**
Assistant Professor, Department of Computer Science and Engineering, Jyothy Institute of Technology, Bengaluru, India.

DOI: https://doi-doi.org/101555/ijrpa.8992

ABSTRACT

The rapid growth of internet-based services, cloud computing, and digital communication has significantly increased the risk of cyber threats, particularly Distributed Denial of Service (DDoS) attacks. These attacks aim to disrupt services by overwhelming systems with excessive traffic, leading to service unavailability, financial losses, and reduced reliability of online platforms. Despite the availability of various security mechanisms, most existing systems either focus only on detection or rely on traditional rule-based techniques that are ineffective against dynamic and evolving attack patterns.

This project proposes a unified system that integrates machine learning-based DDoS detection, simulated prevention mechanisms, and real-time monitoring to address these limitations. The system analyzes network traffic data and extracts important features such as packet rate, protocol type, connection duration, and traffic flow behavior. Machine learning models are trained to classify traffic as normal or malicious, enabling accurate detection of anomalies compared to traditional approaches.

Upon detecting abnormal traffic, the system initiates a prevention module that simulates actions such as IP blocking and rate limiting. Although actual network-level blocking is not implemented, the system demonstrates how real-world security mechanisms respond to threats. In addition, a real-time monitoring dashboard visualizes network activity, traffic trends, and alerts, providing users with better situational awareness and understanding of

system behavior.

I. INTRODUCTION

The increasing dependence on digital technologies and internet-based services has transformed modern society, enabling communication, commerce, and data exchange on a global scale. Organizations across various domains, including banking, healthcare, education, and e-commerce, rely heavily on uninterrupted network connectivity to provide services to users. However, this growing reliance has also increased the vulnerability of systems to cyber threats. Among the various types of cyberattacks, Distributed Denial of Service (DDoS) attacks are particularly dangerous due to their ability to disrupt services by overwhelming systems with excessive traffic.

By integrating detection, response, and visualization into a single framework, the proposed system offers a comprehensive and scalable solution for network security. It highlights the importance of combining machine learning techniques with real-time analytics to develop intelligent and adaptive cybersecurity systems.

KEYWORDS: DDoS Detection; Machine Learning; Network Security; Intrusion Detection; Anomaly Detection; Real-Time Monitoring.

A DDoS attack involves multiple compromised devices, often referred to as a botnet, which generate a massive volume of requests directed toward a target server. This flood of traffic consumes system resources such as bandwidth, CPU, and memory, preventing legitimate users from accessing the service. The consequences of such attacks include service downtime, financial loss, reduced customer trust, and damage to organizational reputation. As attack techniques continue to evolve, defending against DDoS attacks has become a major challenge in network security.

Traditional approaches for detecting DDoS attacks rely on predefined rules, thresholds, or known attack signatures. While these methods are effective for identifying known attack patterns, they are unable to detect new or sophisticated attacks that do not match existing signatures. Additionally, threshold-based systems may misclassify legitimate traffic spikes as attacks, resulting in false positives. These limitations highlight the need for more intelligent and adaptive detection mechanisms.

Machine learning has emerged as a powerful tool for improving intrusion detection systems. By analyzing historical network traffic data, machine learning models can learn patterns associated with normal and malicious behavior. These models can identify anomalies in real

time and adapt to new attack patterns, making them more effective than traditional methods. Algorithms such as Support Vector Machine (SVM), Random Forest, and anomaly detection techniques are widely used in cybersecurity applications due to their ability to handle large datasets and complex patterns.

Despite advancements in detection techniques, many systems focus only on identifying attacks and do not provide a complete solution that includes prevention and monitoring. Detection alone is insufficient, as timely response is essential to minimize the impact of attacks. In real-world systems, prevention is implemented using firewalls and intrusion prevention systems that block malicious traffic. However, such implementations require administrative privileges and infrastructure, making them difficult to replicate in academic projects.

The proposed project addresses this limitation by developing a Machine Learning-Based DDoS Detection and Prevention System with a Real-Time Monitoring Dashboard. The system integrates detection, simulated prevention, and visualization into a single framework. Machine learning models are used to classify network traffic, while a prevention module simulates actions such as blocking malicious IP addresses and limiting traffic flow.

An important component of the system is the real-time monitoring dashboard, which provides a visual representation of network activity. It displays traffic patterns, alerts, and system status, enabling users to monitor and understand system behavior effectively. Visualization plays a key role in improving usability and bridging the gap between detection results and decision-making.

Furthermore, the integration of detection, prevention, and monitoring contributes to the development of intelligent cybersecurity systems that can respond to threats dynamically. The system demonstrates how machine learning and real-time analytics can be combined to enhance network security.

In conclusion, the proposed system aims to provide a comprehensive solution for DDoS detection and prevention by integrating multiple components into a unified platform. It reflects the shift toward data-driven and automated security systems capable of adapting to evolving cyber threats.

II. Literature Survey

To understand the current developments in DDoS attack detection and cybersecurity intrusion prevention systems, several research papers related to machine learning, deep learning, intrusion detection systems (IDS), wireless sensor networks, and real-time attack mitigation

were studied. These papers focused on various techniques such as rule-based detection, supervised and unsupervised learning models, ensemble neural networks, and hybrid frameworks for identifying malicious network traffic. The studies helped in identifying commonly used algorithms like Decision Tree, Random Forest, XGBoost, KNN, LSTM, CNN, and Autoencoders, along with tools and datasets such as CIC-DDoS2019. They also highlighted the importance of real-time monitoring systems, intelligent threat prioritization, and adaptive models for handling evolving cyber threats. However, most of the existing systems face limitations such as high computational cost, dependency on large datasets, difficulty in detecting zero-day attacks, and challenges in real-time deployment in dynamic environments.

Al-Quayed et al. [1] in their research paper titled "A Situation Based Predictive Approach for Cybersecurity Intrusion Detection and Prevention Using Machine Learning and Deep Learning Algorithms in Wireless Sensor Networks of Industry 4.0" proposed a predictive framework for detecting and preventing cyber-attacks in Industry 4.0 environments. Their approach integrates machine learning and deep learning models such as Decision Tree, Multilayer Perceptron (MLP), and Autoencoder to identify and classify different types of attacks including blackhole, grayhole, flooding, and scheduling attacks. The system also introduces an intelligent prioritization mechanism that ranks threats based on their impact and severity, enabling proactive prevention. Experimental results showed high detection accuracy (above 99% for Decision Tree and MLP), demonstrating the effectiveness of the approach. However, the model mainly focuses on known attack types and may require further improvements to handle unknown or evolving cyber threats in real-time systems.

Hussain et al. [2] in their research paper titled "Rule-Based With Machine Learning IDS for DDoS Attack Detection in Cyber-Physical Production Systems (CPPS)" proposed a hybrid intrusion detection system that combines machine learning techniques with rule-based detection to improve the accuracy of DDoS attack detection. The system follows multiple stages including data acquisition, preprocessing, feature selection, model training, and attack detection. Various supervised and unsupervised machine learning algorithms such as Random Forest, KNN, and XGBoost were used to detect malicious network traffic, while rule-based detection was applied to enhance decision-making and identify attack patterns based on traffic frequency. The experimental results showed very high detection performance with accuracy above 99% for supervised models and effective real-time detection capability.

However, the system still faces challenges in real-world deployment, such as dependency on large datasets and limited evaluation in diverse industrial environments.

Bhardwaj et al. [3] in their research paper titled “Hybrid Deep Learning Approach for DDoS Detection Using Ensemble of Neural Networks” proposed an advanced detection model that combines multiple deep learning techniques to improve the accuracy of DDoS attack detection. The system integrates Long Short-Term Memory (LSTM), Convolutional Neural Networks (CNN), and Artificial Neural Networks (ANN) to capture both spatial and temporal features of network traffic. This ensemble approach enhances the model’s ability to detect complex and evolving attack patterns more effectively than single-model approaches. The experimental results demonstrated high accuracy and improved detection performance compared to traditional machine learning methods. However, the model requires high computational resources and large datasets, which may limit its applicability in real-time or resource-constrained environments.

Onaolapo and Ojo [4] in their research paper titled “Development of a Machine Learning-Based Framework for Real-Time Detection and Mitigation of Distributed Denial of Service Attacks” proposed a real-time DDoS detection and prevention system using supervised machine learning techniques. The framework utilizes algorithms such as Random Forest, XGBoost, and Multi-Layer Perceptron (MLP) trained on the CIC-DDoS2019 dataset to accurately classify network traffic. The system integrates tools like Scapy for traffic capture, Apache Kafka for message processing, and Flask with Plotly for real-time monitoring dashboards. Experimental results demonstrated high detection performance with improved precision, recall, and F1-score, while adaptive models like SGD and Passive-Aggressive enhanced the system’s ability to handle evolving attack patterns. However, the system depends heavily on dataset quality and may face computational overhead during high network traffic conditions, which can affect real-time performance.

Cañola Garcia and Blandon [5] in their research paper titled “A Deep Learning-Based Intrusion Detection and Prevention System for Detecting and Preventing Denial-of-Service Attacks” proposed an advanced intrusion detection and prevention system using deep learning techniques. The system utilizes models such as Deep Feedforward Neural Network (DFNN), Recurrent Neural Network (RNN), and Long Short-Term Memory (LSTM) to classify network traffic as malicious or benign. The CICDDoS2019 dataset was used for training and evaluation, with feature extraction performed using CICFlowMeter. The results

showed extremely high performance, with the best model achieving accuracy of 99.94%, precision of 99.95%, recall of 99.9%, and F1-score of 99.93%, demonstrating the effectiveness of deep learning in DoS attack detection. The system was also implemented as a web-based application (Dique) for real-time monitoring and prevention. However, the model requires proper preprocessing and high computational resources, and performance may vary with different datasets or real-time environments.

Chukwuani et al. [6] in their research paper titled "Machine Learning Techniques for Real-Time Malware Classification and Threat Detection in Distributed Systems" proposed a scalable and intelligent framework for real-time malware detection in distributed environments such as cloud, IoT, and edge systems. The system integrates machine learning models like Random Forest, Support Vector Machine (SVM), and Gradient Boosting along with deep learning techniques such as Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) to analyze system logs, network traffic, and executable files. It also incorporates federated learning to ensure data privacy across distributed nodes. The model was evaluated using benchmark datasets like CICIDS, EMBER, and industrial control system logs, achieving over 96% detection accuracy with low false-positive rates. The framework supports real-time detection, anomaly identification, and adaptive retraining to handle evolving cyber threats. However, it requires high computational resources, continuous dataset updates, and careful handling of model drift and scalability challenges in real-world deployments.

Jabed et al. [7] in their research paper titled "Integrating Business Intelligence with AI-Driven Machine Learning for Next-Generation Intrusion Detection Systems" published in the International Journal of Research and Applied Innovations (IJRAI) proposed a hybrid intrusion detection framework that combines Business Intelligence (BI) with AI-based Machine Learning (ML) techniques to enhance cybersecurity decision-making. The system integrates BI pipelines for data collection, preprocessing, and visualization with ML models such as supervised learning, unsupervised learning, and deep learning techniques to detect anomalies and cyberattacks. It utilizes benchmark datasets like NSL-KDD and CICIDS2017 and incorporates contextual features such as user behavior and asset criticality to improve detection accuracy. The results show that the proposed BI-ML IDS achieved higher performance compared to traditional IDS, with around 95% detection rate and significantly reduced false positives. Additionally, BI dashboards provide real-time insights, risk

prioritization, and decision support for security teams. However, the system requires high computational resources, faces challenges in data integration and privacy, and depends heavily on data quality for optimal performance

Reddy [8] in their research paper titled "A Survey of Distributed Denial of Service (DDoS) Attack Mitigation Techniques" published in the International Journal of Computer Trends and Technology (IJCTT) proposed a comprehensive survey of various DDoS attack mitigation strategies. The paper categorizes mitigation techniques into three main phases: prevention, detection, and response. It discusses traditional methods such as rate limiting, IP blacklisting, and firewalls, as well as advanced approaches like anomaly-based detection and machine learning-based techniques. The study compares signature-based, anomaly-based, and ML-based detection methods, showing that ML-based approaches achieve the highest accuracy (around 95%) with low false positives and high scalability. It also highlights emerging trends such as AI-driven systems, blockchain-based defense, and collaborative security frameworks for real-time mitigation of large-scale attacks. However, the paper notes challenges such as high computational requirements, false positives in some methods, scalability issues, and the need for large datasets. The study concludes that hybrid and adaptive systems combining multiple techniques are the most effective solution for modern DDoS attacks.

Hasan et al. [9] in their research paper titled "DDoS: Distributed Denial of Service Attack in Communication Standard Vulnerabilities in Smart Grid Applications and Cyber Security with Recent Developments" published in the Energy Reports (Elsevier) proposed a comprehensive study on DDoS attacks in smart grid systems. The paper analyzes smart grid communication standards such as IEC 61850 and IEEE C37.118 and
highlights their security vulnerabilities that can be exploited by DDoS attacks. It provides a detailed overview of different DDoS attack techniques, their impact on smart grid infrastructure, and various detection strategies including anomaly detection, spoofing detection, and fingerprint-based methods. The study also explores a hybrid machine learning-based detection approach combining algorithms like SVM, ANN, KNN, Naïve Bayes, and Random Forest, achieving improved detection accuracy (around 81%). The paper concludes that hybrid and intelligent security mechanisms are essential for ensuring reliable and secure smart grid operations, although challenges such as computational complexity, real-time implementation, and evolving attack patterns remain.

Priambodo et al. [10] in their research paper titled "Collaborative Intrusion Detection

System with Snort Machine Learning Plugin" published in the International Journal on Informatics Visualization (JOIV) proposed a collaborative intrusion detection system that integrates Network-Based IDS (NIDS) and Host-Based IDS (HIDS) to improve detection accuracy. The system enhances traditional Snort IDS by incorporating a machine learning plugin using algorithms such as Support Vector Machine (SVM), K-Means, and Neural Networks, trained on the NSL-KDD dataset. The proposed approach combines real-time traffic monitoring with machine learning-based classification to detect DoS and Probe attacks more effectively. Experimental results show that the SVM model achieved the best performance, with detection accuracy up to 99% for DoS attacks and improved real-time detection with minimal false positives and false negatives. The system also uses tools like Wazuh and the ELK stack for centralized logging and visualization. However, the approach involves complex integration, requires computational resources, and depends on proper preprocessing and dataset quality for optimal performance.

III. Proposed System

The proposed system is designed to provide a comprehensive and integrated solution for detecting and preventing Distributed Denial of Service (DDoS) attacks using machine learning techniques along with real-time monitoring capabilities. Unlike traditional systems that focus only on detection, this system combines traffic analysis, intelligent classification, response simulation, and visualization into a single unified framework. The primary objective is to build a system that not only identifies malicious traffic but also demonstrates how preventive actions can be applied in real-world scenarios.

The system follows a modular architecture where each component performs a specific function, and the output of one module serves as the input to the next. This design ensures scalability, flexibility, and ease of implementation. The overall workflow begins with network traffic data collection and ends with visualization of results through an interactive dashboard.

III.I System Architecture

The architecture of the proposed system is divided into four major layers:

1. Data Acquisition Layer
2. Processing and Feature Extraction Layer
3. Machine Learning-Based Detection Layer
4. Prevention and Monitoring Layer This layered structure enables efficient handling of

network traffic data and ensures smooth integration between different components. The system operates in a continuous loop where incoming traffic is analyzed in real time, classified, and processed for further action.

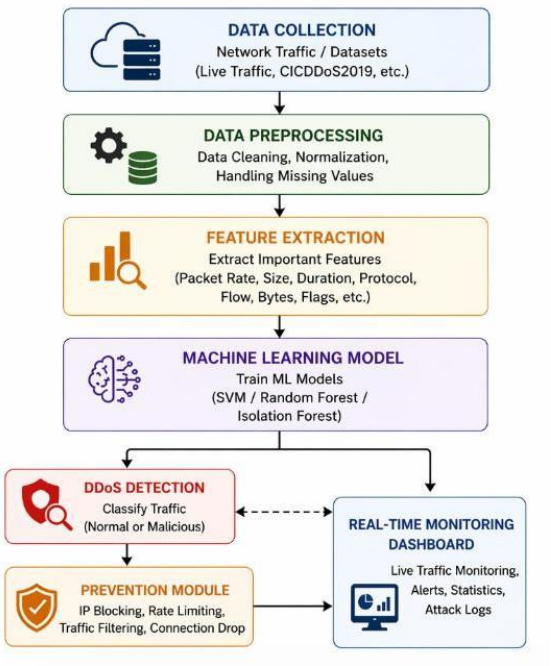

Figure III.I. Architecture Diagram.

III.II System Workflow

The overall workflow of the system can be described as a sequence of interconnected steps:

1. Network traffic data is collected from datasets or simulated environments.
2. The collected data is preprocessed to remove noise and inconsistencies.
3. Important features such as packet rate, protocol type, and connection duration are extracted.
4. The processed data is fed into a trained machine learning model.
5. The model classifies the traffic as normal or malicious.
6. If malicious activity is detected, the prevention module is triggered.
7. Preventive actions such as IP blocking and rate limiting are simulated.
8. All results are displayed on a real-time monitoring dashboard.
9. This workflow ensures that the system performs detection and response in a structured and efficient manner.

III.III Module Descriptions

- **Data Acquisition Layer**

This layer is responsible for collecting network traffic data. The data may be obtained from publicly available datasets or generated through simulation tools. It includes various attributes such as source IP, destination IP, packet size, protocol type, and timestamp. This layer acts as the input stage of the system and provides raw data for further processing.

- **Processing and Feature Extraction Layer**

The raw data collected from the previous layer may contain noise, missing values, or irrelevant information. Therefore, preprocessing is performed to clean and normalize the data. Feature extraction is then carried out to identify the most relevant attributes that contribute to accurate classification. Features such as traffic rate, connection duration, and packet frequency are selected, as they play a significant role in distinguishing between normal and malicious traffic.

- **Machine Learning-Based Detection Layer**

This layer forms the core of the system. Machine learning algorithms such as Support Vector Machine (SVM), Random Forest, or Isolation Forest are used to classify network traffic. The models are trained using labeled datasets, enabling them to learn patterns associated with both normal and attack traffic.

Once trained, the model analyzes incoming traffic in real time and predicts whether it is normal or malicious. The use of machine learning allows the system to detect complex attack patterns and adapt to new threats, making it more effective than traditional rule-based systems.

- **Prevention Layer**

After detecting malicious traffic, the system activates the prevention module. In real-world systems, this would involve blocking IP addresses or limiting traffic through firewall rules. However, in this project, prevention is implemented as a simulation.

The system marks suspicious IP addresses as blocked and logs the action. It may also simulate rate limiting by restricting the number of requests allowed from a particular source. Although these actions are not applied at the network level, they effectively demonstrate how real systems respond to DDoS attacks.

- **Monitoring and Visualization Layer**

The final layer of the system is the monitoring dashboard, which provides a real-time view of network activity. It displays information such as traffic patterns, number of requests, detected attacks, and actions taken. Alerts are generated when malicious activity is identified, allowing users to respond quickly.

The dashboard improves usability by presenting complex data in a visual and easy-to-understand format. It plays a crucial role in bridging the gap between system analysis and user interpretation.

III.IV Comparison with Existing Systems

Table I. Comparison of Existing Systems and Proposed System.

Feature	Traditional Systems	ML-Based Syste ms	Proposed System
Detection Method	Rule-Based	ML-Based	ML-Based
Real-Time Monitoring	Limited	Partial	Yes
Prevention	Limited	Not Included	Simulated
Visualization	No	Partial	Yes
Adaptability	Low	Medium	High

The proposed system differs from existing approaches by integrating detection, prevention, and monitoring into a single platform. This makes it more comprehensive and practical for real-world applications.

III.V Advantages of the Proposed System

The proposed system offers several significant advantages that make it effective for modern network security applications. One of the primary strengths of the system is its ability to provide accurate detection of DDoS attacks using machine learning techniques. Unlike traditional rule-based methods, the system can learn patterns from data and improve its performance over time. This enables it to identify not only known attack patterns but also unknown and evolving threats, making it more robust and adaptable.

Another important advantage is the integration of detection, prevention, and visualization into a single unified system. Instead of handling these components separately, the proposed approach combines them into a cohesive workflow, allowing for better coordination and

efficiency. The system also supports real-time monitoring and analysis of network traffic, which helps in identifying suspicious activities as they occur.

The inclusion of a graphical monitoring dashboard further enhances the usability of the system by presenting complex data in a clear and understandable format. This improves user awareness and simplifies decision-making. Additionally, the system is designed to be scalable and adaptable, making it suitable for different network environments and varying levels of traffic. By automating detection and response processes, the system also reduces dependency on manual monitoring, thereby minimizing human effort and potential errors.

III.VI Future Enhancements

Although the proposed system provides a comprehensive framework for DDoS detection and prevention, there are several areas where further improvements can be made to enhance its functionality and real-world applicability. One of the major enhancements would be the integration of the system with actual firewall mechanisms, enabling real-time blocking of malicious IP addresses instead of simulated prevention. This would make the system more practical for deployment in real network environments.

Another potential improvement is the incorporation of advanced deep learning models, which can further increase detection accuracy, especially for complex and large-scale attack patterns. The system can also be extended to operate in real-time network environments, where it continuously monitors live traffic and responds dynamically to threats.

In addition, implementing automated alert systems and notification mechanisms would improve responsiveness by immediately informing administrators about detected attacks. This can help in faster decision-making and response. The scope of the system can also be expanded to detect other types of cyber threats, such as phishing attacks, malware activities, and intrusion attempts, thereby transforming it into a more comprehensive cybersecurity solution.

IV. CONCLUSION

The system presented in this paper provides an integrated approach for detecting and responding to Distributed Denial of Service (DDoS) attacks using machine learning techniques combined with real-time monitoring capabilities. The primary objective of the project was to address the limitations of traditional security systems that focus only on detection without providing a complete response mechanism. By combining traffic analysis, intelligent classification, simulated prevention, and visualization, the proposed system offers

a more comprehensive and practical solution for modern network security challenges.

One of the key strengths of the system lies in its ability to analyze network traffic dynamically using machine learning models. Unlike conventional rule-based approaches, the system learns patterns from data and adapts to new and evolving attack behaviors. This makes it more effective in identifying both known and unknown threats. The use of algorithms such as Support Vector Machine and Random Forest enables accurate classification of traffic, improving the reliability of the detection process.

Another important aspect of the system is the inclusion of a prevention module. While the project does not implement actual network-level blocking, it simulates preventive actions such as IP blocking and rate limiting. This simulation plays a crucial role in demonstrating how real-world systems respond to detected threats. By incorporating this response mechanism, the system moves beyond simple detection and provides a complete workflow that includes decision-making and action representation. The real-time monitoring dashboard further enhances the usability of the system by providing a clear and interactive visualization of network activity. It allows users to observe traffic patterns, detect anomalies, and understand system behavior effectively. The graphical representation of data improves interpretation and supports faster decision-making compared to raw numerical outputs. This feature is particularly important in practical environments where administrators need to respond quickly to potential threats.

From a design perspective, the modular architecture of the system ensures flexibility and scalability. Each component, including data acquisition, preprocessing, detection, prevention, and visualization, operates as part of a connected workflow. This modular approach makes it easier to extend the system by adding new features or improving existing components. For example, more advanced machine learning models or real-time data streaming techniques can be incorporated without affecting the overall structure.

The project also highlights the importance of integrating multiple functionalities into a single platform. Many existing systems focus on isolated aspects such as detection or monitoring, but the proposed system demonstrates the advantages of combining these elements. By providing a unified solution, the system improves efficiency, reduces complexity, and offers better insights into network security.

However, certain limitations remain in the current implementation. The prevention mechanism is simulated rather than applied at the network level, and the system is primarily tested in a controlled environment using datasets or simulated traffic. While this is sufficient for academic purposes, real-world deployment would require integration with firewall

systems, intrusion prevention tools, and large-scale network infrastructure.

Future enhancements can further improve the effectiveness and applicability of the system. Integrating the system with real-time network environments and firewall configurations would enable actual blocking of malicious traffic. The use of deep learning techniques could improve detection accuracy for complex attack patterns. Additionally, incorporating automated alert systems and notification mechanisms would enhance responsiveness. Expanding the system to detect other types of cyberattacks, such as phishing or malware-based attacks, could also increase its scope and usefulness.

In conclusion, the proposed Machine Learning-Based DDoS Detection and Prevention System with Real-Time Monitoring Dashboard demonstrates a comprehensive approach to network security by integrating detection, response, and visualization into a single framework. It reflects the growing importance of intelligent, data-driven systems in cybersecurity and provides a strong foundation for future research and development in this field.

V. REFERENCES

1. A. Al-Quayed, et al., "A Situation Based Predictive Approach for Cybersecurity Intrusion Detection and Prevention Using Machine Learning and Deep Learning Algorithms in Wireless Sensor Networks of Industry 4.0," International Journal of Advanced Computer Science and Applications, 2023.
2. M. Hussain, et al., "Rule-Based With Machine Learning IDS for DDoS Attack Detection in Cyber-Physical Production Systems (CPPS)," IEEE Access, 2022.
3. S. Bhardwaj, et al., "Hybrid Deep Learning Approach for DDoS Detection Using Ensemble of Neural Networks," Procedia Computer Science, 2022.
4. J. Onaolapo and O. Ojo, "Development of a Machine Learning-Based Framework for Real-Time Detection and Mitigation of Distributed Denial of Service Attacks," Journal of Network and Computer Applicatons, 2023.
5. C. Cañola Garcia and E. Blandon, "A Deep Learning-Based Intrusion Detection and Prevention System for Detecting and Preventing Denial-of-Service Attacks," IEEE Access, 2023.
6. C. Chukwuani, et al., "Machine Learning Techniques for Real-Time Malware Classification and Threat Detection in Distributed Systems," Future Generation Computer Systems, 2023.
7. M. Jabed, et al., "Integrating Business Intelligence with AI-Driven Machine Learning for

Next-Generation Intrusion Detection Systems," International Journal of Research and Applied Innovations, 2024.

8. K. Reddy, "A Survey of Distributed Denial of Service (DDoS) Attack Mitigation Techniques," International Journal of Computer Trends and Technology, 2022.
9. M. Hasan, et al., "DDoS: Distributed Denial of Service Attack in Communication Standard Vulnerabilities in Smart Grid Applications and Cyber Security with Recent Developments," Energy Reports (Elsevier), 2023.
10. D. F. Priambodo, A. H. N. Faizi, F. D. Rahmawati, S. U. Sunaringtyas, J. Sidabutar, and T. Yulita, "Collaborative Intrusion Detection System with Snort Machine Learning Plugin," International Journal on Informatics Visualization, vol. 8, no. 3, pp. 1230–1238, 2024.