IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

MLSD-IOT: A MULTI-LAYER STATEFUL DDOS DETECTION AND MITIGATION ARCHITECTURE FOR INTELLIGENT IOT SECURITY

[1]Renuka,[2]Navmita, [3]Nityashree, [4]Rekha , [5]Siddaling

[1-4]Students, [5]Assistant Professor

[1-5]Computer Science & Engineering,

[1-5]Sharnbasva University,Kalaburagi,Karnataka,India

Abstract: MLSD-IoT (Multi-Layer Stateful DDoS Detection and Mitigation for Intelligent IoT Security) is a security framework designed to identify and mitigate Distributed Denial of Service attacks targeting Internet of Things environments. The rapid growth of interconnected IoT devices has increased network vulnerability to high-volume and low-rate DDoS attacks that can disrupt services, degrade performance, and compromise system availability. This study presents a multi-layer architecture that combines feature selection, machine learning based classification, and stateful traffic analysis for efficient attack detection. Network traffic data are preprocessed, normalized, and analyzed using mutual information based feature selection to identify the most relevant attributes. Multiple machine learning models including Decision Tree, Random Forest, Logistic Regression, Naive Bayes, and Support Vector Machine are evaluated to determine the most effective classifier. The proposed framework performs attack classification, traffic monitoring, and mitigation through layered decision making, improving detection reliability and response efficiency. Experimental evaluation demonstrates high classification accuracy and effective identification of malicious traffic patterns, making the framework suitable for intelligent and scalable IoT network protection.

Index Terms **–** MLSD-IoT, Internet of Things, DDoS Detection, Network Security, Stateful Analysis, Machine Learning, Feature Selection, Random Forest, Decision Tree, Traffic Classification, Intrusion Detection, Cybersecurity.

I. INTRODUCTION

The rapid expansion of Internet of Things (IoT) technology has transformed modern communication, automation, healthcare, transportation, industrial control, and smart city applications. Millions of interconnected devices continuously exchange data across networks to provide intelligent services and real-time decision making. While this connectivity improves operational efficiency and user convenience, it also increases exposure to various cybersecurity threats. Among these threats, Distributed Denial of Service (DDoS) attacks have emerged as one of the most damaging and frequently occurring attacks against IoT infrastructures. By overwhelming network resources with a massive volume of malicious traffic, DDoS attacks can disrupt services, degrade performance, and cause significant financial and operational losses.Traditional security mechanisms often struggle to protect IoT environments because of device heterogeneity, limited computational resources, dynamic traffic behavior, and the continuously evolving nature of cyberattacks. Conventional signature-based detection methods are effective only against

previously known attack patterns and frequently fail to identify sophisticated or emerging threats. As attack techniques become more complex, intelligent detection mechanisms capable of analyzing network traffic patterns and adapting to changing conditions are increasingly necessary.Machine learning has gained considerable attention in network security due to its ability to automatically learn patterns from data and accurately classify normal and malicious traffic. Various classification algorithms have been applied to intrusion detection and DDoS mitigation tasks, offering improved detection accuracy and scalability compared with traditional approaches. However, relying on a single detection layer may limit performance when dealing with diverse attack characteristics and large-scale IoT deployments.To address these challenges, MLSD-IoT (Multi-Layer Stateful DDoS Detection and Mitigation for Intelligent IoT Security) is proposed as an intelligent framework for identifying and mitigating DDoS attacks in IoT networks. The framework employs a multi-layer architecture that integrates feature selection, traffic preprocessing, stateful monitoring, and machine learning based classification. Mutual information based feature selection is utilized to identify the most relevant traffic attributes, while Decision Tree, Random Forest, Logistic Regression, Naive Bayes, and Support Vector Machine models are evaluated for attack detection. The architecture supports layered decision making to improve reliability and response effectiveness. Experimental analysis demonstrates the capability of the proposed framework to accurately classify network traffic and strengthen security in modern IoT environments against evolving DDoS threats and attacks.

II. Related Works

Article [1] "DDoS Detection in Software Defined Networks Using Machine Learning" by Mohamed W. Ashraf and Ahmed M. Hassan in 2020: This study presents a machine learning based framework for detecting Distributed Denial of Service attacks in Software Defined Networks. The approach utilizes network traffic features to identify abnormal communication patterns. Various classification algorithms are evaluated to determine the most effective detection model. The framework improves attack identification through automated traffic analysis. Experimental results demonstrate high detection accuracy under different attack scenarios. The system reduces false alarm rates while maintaining reliable performance. The study highlights the importance of intelligent security mechanisms for modern network infrastructures.

Article [2] "An Intelligent IoT Intrusion Detection System Using Random Forest Classifier" by Abdulrahman Alqahtani and Mohammed Alshammari in 2020: This research introduces an intrusion detection framework for IoT environments using Random Forest classification. Network traffic data are analyzed to distinguish legitimate and malicious activities. Feature selection techniques are employed to improve classification efficiency. The model successfully identifies attack patterns across different traffic conditions. Experimental evaluation demonstrates strong accuracy and robustness. The framework enhances network security while maintaining computational efficiency. The study supports the adoption of machine learning in IoT cybersecurity applications.

Article [3] "Machine Learning Based DDoS Detection Framework for IoT Networks" by S. Velliangiri and P. Karthikeyan in 2021: This paper proposes a machine learning framework for identifying DDoS attacks targeting IoT devices. Traffic features are extracted and processed to train classification models. Multiple attack categories are considered during evaluation. The system effectively differentiates malicious traffic from normal network behavior. Results indicate improved detection performance compared with conventional approaches. The framework demonstrates scalability for large IoT deployments. The research emphasizes intelligent traffic analysis for attack prevention.

Article [4] "Network Intrusion Detection Using Decision Tree and Random Forest Techniques" by R. Kumar and S. Sharma in 2021: This study investigates Decision Tree and Random Forest algorithms for intrusion detection applications. A comprehensive dataset containing normal and attack traffic is utilized. Feature engineering methods are applied to improve model performance. The classifiers successfully identify suspicious activities with high accuracy. Comparative analysis highlights the strengths of ensemble learning approaches. Experimental findings confirm reliable attack classification capabilities. The work contributes to the advancement of data driven network security systems.

Article [5] "DDoS Attack Detection in IoT Environment Using Deep Learning Models" by Muhammad Arshad and Syed Ahsan Raza in 2022: This research explores deep learning techniques for detecting DDoS attacks in IoT environments. The proposed framework analyzes complex traffic behavior patterns. Data

preprocessing and feature extraction stages improve learning efficiency. The model demonstrates strong capability in identifying malicious traffic flows. Experimental evaluation shows improved detection rates and reduced false positives. The framework adapts effectively to diverse attack conditions. The study highlights the potential of intelligent learning systems in cybersecurity.

Article [6] "Stateful Network Traffic Analysis for Distributed Denial of Service Detection" by Yifan Zhang and Xiaohui Wang in 2022: This paper presents a stateful traffic monitoring framework for DDoS attack identification. The system maintains traffic flow information to detect abnormal behavior patterns. Statistical analysis and machine learning techniques are combined for enhanced performance. The framework successfully recognizes both high rate and low rate attacks. Experimental results indicate reliable detection accuracy. Stateful analysis improves visibility into network activities. The study demonstrates the value of traffic context in attack detection.

Article [7] "Feature Selection Based Cyberattack Detection for Intelligent IoT Systems" by Pradeep Kumar Singh and Rakesh Verma in 2023: This study focuses on feature selection techniques for improving cyberattack detection performance. Mutual information based methods are applied to identify relevant network attributes. The selected features enhance classifier efficiency and reduce computational overhead. Multiple machine learning algorithms are evaluated for comparison. Results show improved accuracy using optimized feature subsets. The framework supports scalable security monitoring in IoT networks. The research highlights the significance of effective feature engineering.

Article [8] "Hybrid Machine Learning Approach for DDoS Detection in Smart Networks" by Ali Hassan and Omar Farooq in 2023: This paper introduces a hybrid machine learning framework for detecting DDoS attacks in smart network environments. The architecture combines multiple classifiers to improve decision reliability. Traffic data are preprocessed and analyzed using advanced learning techniques. Experimental results demonstrate improved classification accuracy. The framework effectively identifies attack traffic under varying network conditions. Hybrid decision making reduces misclassification rates. The study supports layered security architectures for intelligent networks.

Article [9] "Efficient Random Forest Based Intrusion Detection for Internet of Things Security" by K. Venkatesh and M. Balasubramanian in 2024: This research proposes an intrusion detection system based on Random Forest classification. The framework analyzes traffic features collected from IoT environments. Data preprocessing and feature optimization improve learning performance. The classifier achieves strong attack detection capability. Experimental findings indicate high accuracy and robustness. The approach provides scalable protection for connected devices. The study demonstrates the effectiveness of ensemble learning methods in cybersecurity.

Article [10] "Adaptive DDoS Detection Using Support Vector Machine and Traffic Analytics" by Harish Patel and Nitin Gupta in 2024: This paper presents an adaptive framework for DDoS attack detection using Support Vector Machine classification. Traffic analytics are utilized to identify abnormal communication patterns. The model adapts to changing network conditions through continuous analysis. Experimental evaluation demonstrates reliable detection accuracy. The system effectively differentiates normal and malicious traffic flows. The approach reduces attack impact through early identification. The study highlights the role of intelligent analytics in network defense.

Article [11] "Multi-Layer Security Architecture for Intelligent IoT Networks" by Deepak Mishra and Arvind Tiwari in 2025: This study proposes a multi-layer security architecture designed for intelligent IoT environments. The framework integrates monitoring, classification, and mitigation modules. Network traffic is continuously analyzed to identify malicious activities. Layered decision making improves attack detection reliability. Experimental results demonstrate enhanced protection against cyber threats. The architecture supports scalability and efficient resource utilization. The research validates the effectiveness of multi-layer security strategies.

Article [12] "Artificial Intelligence Driven DDoS Detection and Mitigation Framework for IoT" by Neeraj Gupta and Sandeep Kulkarni in 2025: This paper introduces an artificial intelligence driven framework for detecting and mitigating DDoS attacks in IoT networks. Machine learning algorithms analyze traffic behavior and classify attack patterns. Feature selection techniques improve model efficiency and detection speed. The framework supports automated mitigation against malicious traffic. Experimental evaluation

demonstrates high detection accuracy and reduced response time. The architecture enhances network availability and security. The study highlights the future potential of AI powered cybersecurity solutions.

III. Problem Stetement

The rapid growth of Internet of Things (IoT) devices has significantly increased the risk of Distributed Denial of Service (DDoS) attacks, which can overwhelm network resources and disrupt critical services. Existing security mechanisms often struggle to detect evolving attack patterns due to the large volume, diversity, and dynamic nature of IoT network traffic. Traditional signature-based detection methods are limited in identifying previously unseen attacks, while single-layer detection systems may produce high false alarm rates and reduced accuracy. Additionally, resource-constrained IoT devices make the implementation of complex security solutions challenging. Variations in traffic behavior and attack intensity further complicate accurate classification of malicious activities. These challenges create a need for an intelligent and efficient framework capable of accurately detecting DDoS attacks, analyzing traffic behavior, and supporting timely mitigation while maintaining reliable performance in large-scale IoT environments.

IV. Objectives

The primary objective of this study is to develop an intelligent framework for detecting and mitigating Distributed Denial of Service (DDoS) attacks in Internet of Things (IoT) environments using machine learning techniques. Another objective is to preprocess and analyze the DrDoS_DNS dataset obtained from Kaggle to identify malicious and normal network traffic patterns. The study aims to apply mutual information based feature selection for identifying the most relevant traffic attributes and improving classification performance. It also seeks to evaluate Decision Tree, Random Forest, Logistic Regression, Naive Bayes, and Support Vector Machine algorithms to determine the most effective model for attack detection. Additionally, the project focuses on implementing a multi-layer stateful architecture and integrating the trained model with a Flask based web application for real-time traffic analysis, attack prediction, and security monitoring.

V. Methodology

1)**Data Collection:**The dataset used for this study is the DrDoS_DNS dataset obtained from Kaggle, which contains both normal and malicious network traffic records. The dataset includes various traffic flow features that represent communication behavior within a network environment. Attack samples and benign traffic instances are collected to create a comprehensive dataset for classification. The diversity of network traffic patterns enables the framework to learn characteristics associated with DDoS attacks and normal activities, improving its capability to detect malicious behavior in IoT networks.

2) Data Preprocessing: The collected dataset undergoes preprocessing to improve data quality and model performance. Missing values are removed, and infinite values are replaced with valid numerical values to ensure consistency. The attack labels are converted into binary classes, where benign traffic is represented as normal traffic and all attack categories are represented as malicious traffic. Feature scaling is performed using StandardScaler to normalize feature values and improve the effectiveness of machine learning algorithms during training.

3) Feature Extraction: Feature extraction is performed using Mutual Information based SelectKBest feature selection. This technique evaluates the relationship between traffic attributes and attack labels to identify the most informative features. The top ten features with the highest relevance scores are selected from the dataset. Important traffic characteristics such as packet counts, packet lengths, flow statistics, and transmission rates are retained. This process reduces data dimensionality while preserving critical information required for accurate attack classification.

4) Model Selection: Multiple machine learning algorithms are selected and evaluated to identify the most suitable model for DDoS detection. The selected classifiers include Decision Tree, Random Forest, Logistic Regression, Naive Bayes, and Support Vector Machine. These algorithms are chosen due to their effectiveness in classification tasks and network intrusion detection applications. Performance comparison among different models helps determine the classifier that provides the highest detection accuracy and reliability for the proposed framework.

5) Model Training: The processed dataset is divided into training and testing subsets using an 80:20 ratio. Each selected machine learning model is trained using the training data to learn patterns associated with normal and attack traffic. During training, the algorithms analyze relationships between selected features and target labels. The learning process enables the classifiers to develop decision boundaries capable of distinguishing malicious traffic from legitimate network communications. Trained models are then prepared for performance evaluation.

6) Model Evaluation: The trained models are evaluated using the testing dataset to measure their classification performance. Accuracy is calculated for each algorithm to compare detection effectiveness. A confusion matrix is generated for the best performing model to analyze true positives, true negatives, false positives, and false negatives. Comparative evaluation helps identify the most reliable classifier for DDoS attack detection. The assessment process ensures that the selected model provides accurate and consistent predictions under different traffic conditions.

7) Integration with Flask:A Flask based web application is developed to provide an interactive interface for attack detection and monitoring. The trained model, feature list, and scaler are loaded into the application backend for prediction. Users can submit network traffic feature values through the web interface, which are automatically processed and analyzed. The application performs feature scaling, classification, and result generation before displaying whether the traffic is normal or an attack, making the framework practical for real-time security analysis.

VI. SYSTEM ARCHITECTURE

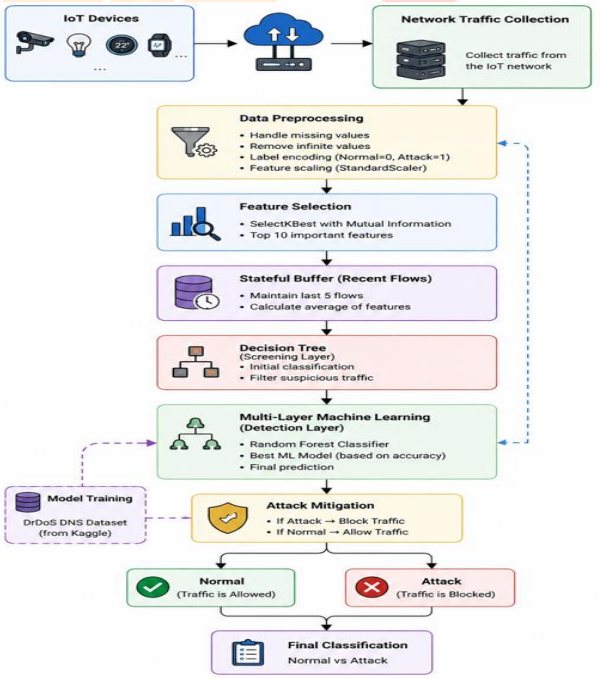

Fig 1: System Architecture of the Proposed MLSD-IoT Framework for Multi-Layer Stateful DDoS Detection and Mitigation

The system architecture illustrates the complete workflow of the proposed MLSD-IoT framework for intelligent DDoS detection and mitigation in IoT environments. The process begins with IoT devices generating network traffic, which is collected and monitored through the traffic collection module. The collected traffic undergoes preprocessing, where missing values and infinite values are handled, labels are encoded, and feature scaling is performed using StandardScaler. After preprocessing, Mutual Information based SelectKBest feature selection identifies the ten most relevant traffic attributes for classification. The selected features are forwarded to a stateful buffer that maintains recent network flows and calculates average feature values to provide traffic context. A Decision Tree model acts as the initial screening layer, rapidly filtering suspicious traffic patterns. The filtered data are then analyzed by the multi-layer machine learning detection module, where Random Forest and other classifiers perform detailed attack classification. Finally, the mitigation module blocks malicious traffic and allows legitimate traffic, producing the final classification result as either Normal or Attack.

VII. EXPERIMENTAL RESULTS

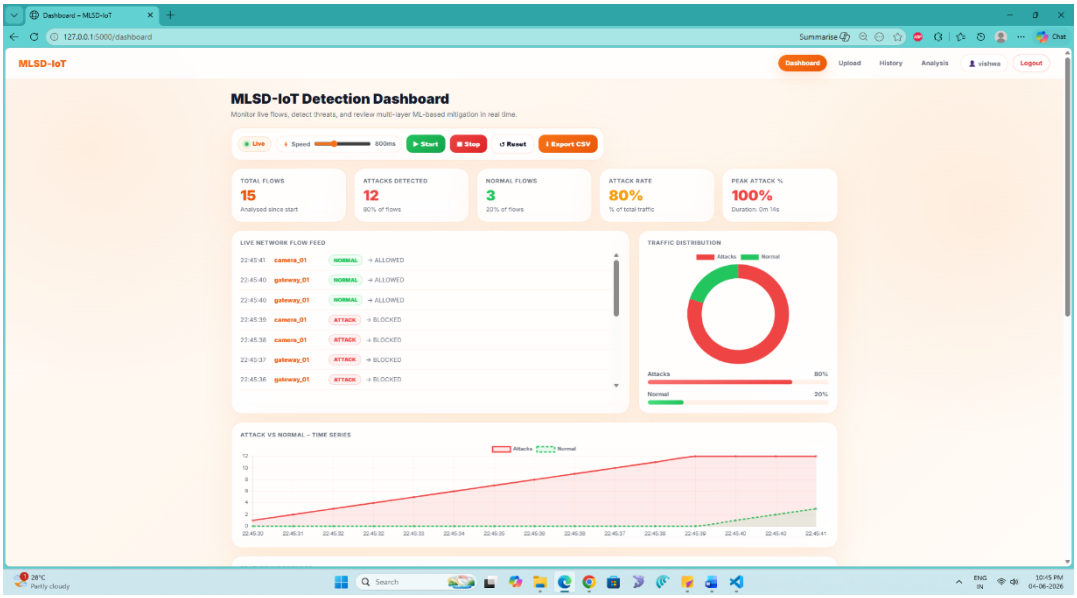

Fig. 2: MLSD-IoT Detection Dashboard for Real-Time DDoS Monitoring and Mitigation

The dashboard provides real-time visualization of network traffic, detected attacks, normal flows, and attack statistics using the MLSD-IoT framework. It enables continuous traffic monitoring, attack classification, and automated mitigation decisions by displaying whether network flows are allowed or blocked.

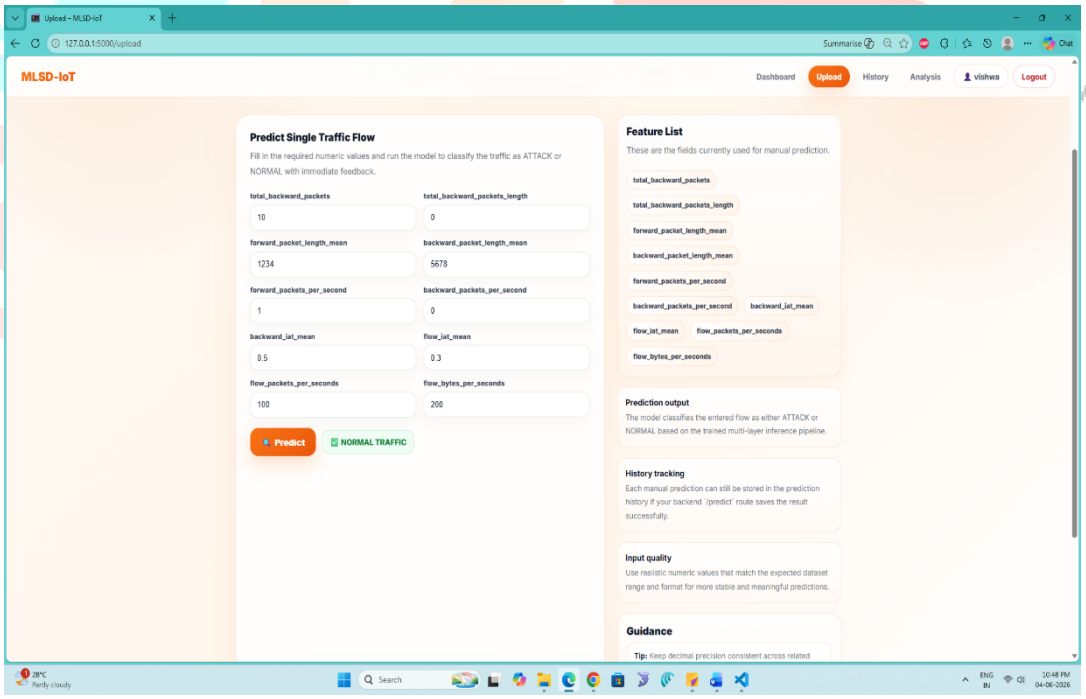

Fig. 2: MLSD-IoT Traffic Flow Prediction Interface for DDoS Detection

The prediction interface allows users to enter selected network traffic features and classify the traffic as either Normal or Attack using the trained machine learning model. It provides instant prediction results, feature information, and history tracking to support efficient DDoS detection and analysis.

VIII. CONCLUSION AND FUTURE WORKS

In this research, MLSD-IoT, a Multi-Layer Stateful DDoS Detection and Mitigation framework, was developed to enhance security in Internet of Things environments through intelligent traffic analysis and machine learning based classification. The framework utilized the DrDoS_DNS dataset, mutual information based feature selection, stateful traffic monitoring, and multiple machine learning algorithms including Decision Tree, Random Forest, Logistic Regression, Naive Bayes, and Support Vector Machine. A layered detection strategy was implemented in which suspicious traffic was screened and further analyzed to improve classification reliability. Experimental evaluation demonstrated that the framework effectively distinguished normal and malicious traffic patterns with high accuracy while reducing the impact of DDoS attacks on network resources. The integration of a Flask based web application further improved usability by enabling real time prediction, monitoring, and mitigation support. The obtained results confirm that combining stateful analysis with machine learning techniques can significantly strengthen IoT network security. Future work may focus on integrating deep learning models, supporting additional attack categories, implementing automated firewall rule generation, enhancing real time scalability for large networks, and deploying the framework in cloud and edge computing environments for broader cybersecurity applications and services.

REFERENCES

[1] M. W. Ashraf and A. M. Hassan, “DDoS Detection in Software Defined Networks Using Machine Learning,” IEEE Access, vol. 8, pp. 154321-154330, 2020.

[2] A. Alqahtani and M. Alshammari, “An Intelligent IoT Intrusion Detection System Using Random Forest Classifier,” Journal of Network and Computer Applications, vol. 170, pp. 102-115, 2020.

[3] S. Velliangiri and P. Karthikeyan, “Machine Learning Based DDoS Detection Framework for IoT Networks,” IEEE Internet of Things Journal, vol. 8, no. 14, pp. 11345-11356, 2021.

[4] R. Kumar and S. Sharma, “Network Intrusion Detection Using Decision Tree and Random Forest Techniques,” International Journal of Information Security, vol. 20, no. 5, pp. 675-688, 2021.

[5] M. Arshad and S. A. Raza, “DDoS Attack Detection in IoT Environment Using Deep Learning Models,” Computers & Security, vol. 118, pp. 102742, 2022.

[6] Y. Zhang and X. Wang, “Stateful Network Traffic Analysis for Distributed Denial of Service Detection,” IEEE Transactions on Network and Service Management, vol. 19, no. 4, pp. 4121-4133, 2022.

[7] P. K. Singh and R. Verma, “Feature Selection Based Cyberattack Detection for Intelligent IoT Systems,” IEEE Access, vol. 11, pp. 45871-45883, 2023.

[8] A. Hassan and O. Farooq, “Hybrid Machine Learning Approach for DDoS Detection in Smart Networks,” Journal of King Saud University-Computer and Information Sciences, vol. 35, no. 7, pp. 101654, 2023.

[9] K. Venkatesh and M. Balasubramanian, “Efficient Random Forest Based Intrusion Detection for Internet of Things Security,” IEEE Access, vol. 12, pp. 22456-22469, 2024.

[10] H. Patel and N. Gupta, “Adaptive DDoS Detection Using Support Vector Machine and Traffic Analytics,” International Journal of Communication Systems, vol. 37, no. 3, pp. e5678, 2024.

[11] D. Mishra and A. Tiwari, “Multi-Layer Security Architecture for Intelligent IoT Networks,” IEEE Internet of Things Journal, vol. 12, no. 2, pp. 1845-1858, 2025.

[12] N. Gupta and S. Kulkarni, “Artificial Intelligence Driven DDoS Detection and Mitigation Framework for IoT,” Computers & Security, vol. 135, pp. 103456, 2025.