IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

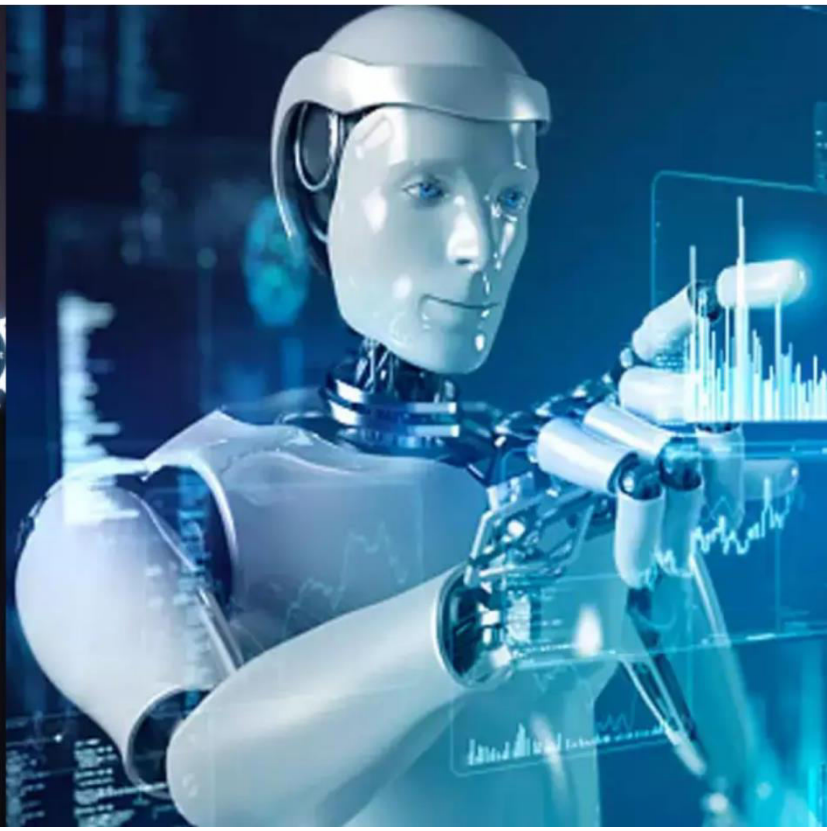
ISSN(O): 2319-8753
ISSN(P): 2347-6710



International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)





Impact Factor: 9.935

Volume 15, Issue 11, November 2026

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 11, November 2026

|DOI: 10.15680/IJIRSET.2026.1511047|

Securing IoT against DDoS Attack using Machine Learning

Suresh K, B H Trivedi, Deepali, J Suma, Kanthi Simha

Associate Professor, Department of CSE, RYMEC, Ballari, Karnataka, India

Research Scholar, Department of CSE, RYMEC, Ballari, Karnataka, India

ABSTRACT: The increasing adoption of Internet of Things (IoT) technology has led to the connection of numerous devices across different domains. While this development offers greater convenience and automation, it also introduces security risks, particularly Distributed Denial of Service (DDoS) attacks. Such attacks generate excessive network traffic, which can consume available resources and interrupt the normal functioning of IoT services. Detecting these attacks remains challenging because malicious traffic may exhibit patterns similar to legitimate network activity.

This project presents a machine learning-based system for identifying and responding to DDoS attacks in IoT networks. The system employs the Random Forest algorithm to analyse 40 network traffic features and categorize incoming traffic as Normal, Suspicious, or DDoS. Model development and evaluation are performed using a synthetic dataset consisting of 10,000 network traffic records. The application is implemented using Python and Flask, with MQTT supporting IoT communication and SQLite maintaining information related to devices, traffic records, alerts, and audit activities. Additional capabilities include traffic monitoring, risk assessment, security notifications, and simulated IP blocking, along with operator-controlled firewall actions.

The experimental results show an accuracy of 100% on the synthetic test dataset, with an average prediction time of approximately 161 milliseconds per observation. Testing with simulated traffic demonstrated successful identification of normal and DDoS activities. However, the system showed difficulty in consistently separating suspicious traffic from DDoS traffic. Therefore, evaluation using real-world IoT network datasets is necessary to establish its performance in practical environments. Overall, the project demonstrates the applicability of machine learning-based traffic classification as a means of supporting DDoS detection and security monitoring in IoT networks.

KEYWORDS: Internet of Things (IoT), Distributed Denial of Service (DDoS), Machine Learning, Random Forest Classifier, Network Traffic Analysis, Intrusion Detection, Flask, Network Security.

I. INTRODUCTION

The Internet of Things (IoT) has become an important technology in areas such as smart homes, healthcare, agriculture, transportation, and industrial automation. It enables connected devices to exchange information and perform tasks with minimal human involvement. However, the increasing number of connected devices has also created security challenges. One of the major threats is the Distributed Denial of Service (DDoS) attack, in which multiple compromised devices generate excessive traffic towards a target system, affecting network performance and service availability.

Traditional security mechanisms mainly depend on predefined rules and known attack patterns, which may not always identify changing or unfamiliar traffic behaviour. Detecting malicious activities in IoT networks is particularly challenging because legitimate and suspicious traffic can share similar characteristics. Therefore, an effective approach is required to analyse network traffic and identify potential attacks while supporting continuous security monitoring.

To address this challenge, this project proposes a machine learning-based DDoS detection system using the Random Forest classification algorithm. The model uses 40 network traffic features to classify incoming records into three categories: Normal, Suspicious, and DDoS. A synthetic dataset containing 10,000 traffic records is used for model training and evaluation. The system is implemented using Python and Flask, with MQTT support for IoT

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 11, November 2026

|DOI: 10.15680/IJIRSET.2026.1511047|

communication and SQLite for storing traffic records, device information, alerts, and audit logs. It also provides traffic monitoring, risk assessment, alert generation, and simulated or operator-controlled firewall blocking.

The experimental evaluation achieved 100% classification accuracy on the synthetic test dataset, with an approximate prediction time of 161 milliseconds per observation. Although the system successfully identified normal and DDoS traffic generated by the simulator, distinguishing suspicious traffic from DDoS activity remains a limitation. The main contribution of this work is the integration of machine learning-based traffic classification with a web-based monitoring and mitigation prototype for IoT network security. Further evaluation using real-world IoT datasets is required to assess its effectiveness in practical environments.

The remainder of this paper is organized as follows: Section II presents the literature survey, Section III explains the proposed methodology, Section IV discusses the experimental results and performance evaluation, and Section V concludes the paper with future enhancements.

II. LITERATURE SURVEY

Jameel Ahmad et al. [1] proposed a framework for detecting and preventing Distributed Denial of Service (DDoS) attacks using real-time network traffic data. Their approach combines machine learning algorithms, including Random Forest and Support Vector Machine (SVM), with Apache Kafka and Apache Spark for processing large volumes of streaming data. The framework focuses on identifying malicious network activities through continuous traffic analysis and reported a detection accuracy of up to 95%. Although the approach supports real-time traffic processing, its implementation requires additional infrastructure and computational resources, which may increase deployment complexity.

Muhammad Rashid Minhas et al. [2] introduced F-OSFA, a fog-level architecture designed to detect both known and zero-day DDoS attacks. The methodology combines Convolutional Neural Networks (CNN), Decision Trees, few-shot learning, and contrastive autoencoders to identify different attack patterns. The approach was evaluated using the CICDDoS2019 and CICIDS2017 datasets, with the aim of improving detection across different attack scenarios. Its use of fog-level processing and multiple learning techniques provides an approach for handling complex attacks. However, the combination of several models increases architectural complexity and requires additional computational resources for deployment and maintenance.

Amir Pakmehr et al. [3] presented a survey of DDoS attack detection techniques used in IoT networks. Their study examined existing detection methods, network security challenges, and different defence strategies applicable to IoT environments. By reviewing and comparing available approaches, the authors provided an overview of the methods used to identify and respond to DDoS attacks. The study is useful for understanding the current research landscape and the challenges associated with IoT security. However, since it is primarily a survey, it does not introduce a new detection model or provide an independently implemented system. Further experimental implementation and validation are required to assess the practical effectiveness of the reviewed techniques.

Amal A. Alahmadi et al. [4] reviewed machine learning and deep learning techniques for detecting DDoS attacks in IoT-based networks. Their research compared different classification approaches and discussed how these models can be applied to identify malicious network traffic. The study also examined existing research challenges and suggested directions for improving IoT attack detection. Its major contribution is the comparison of different learning techniques and the identification of research opportunities in IoT network security. However, the study highlights the need for evaluating detection models using larger and more realistic datasets to understand their performance in practical network environments.

Jianhua Liu et al. [5] proposed FLEAM, a Federated Learning Empowered Architecture for mitigating DDoS attacks in Industrial IoT environments. The methodology uses federated learning together with fog computing and distributed processing to support collaborative attack detection across participating devices. Instead of depending entirely on a centralized learning process, the architecture enables distributed participation in the detection process. The proposed approach reported approximately 98% detection accuracy while supporting distributed learning. Despite these advantages, effective implementation requires coordination among participating nodes and careful management of communication and computational resources.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 11, November 2026

|DOI: 10.15680/IJIRSET.2026.1511047|

Nahida Islam et al. [6] investigated machine learning-based intrusion detection techniques for IoT networks. Their study considered both traditional machine learning and deep learning approaches, including Random Forest, Support Vector Machine, Decision Tree, and neural networks. The research evaluated different detection techniques using benchmark datasets and discussed their suitability for identifying malicious network activities. The study demonstrates the relevance of machine learning approaches in IoT intrusion detection. However, the effectiveness of these techniques depends on dataset quality, the characteristics of network traffic, and the computational resources available in IoT environments.

III. RESEARCH GAP

The reviewed studies demonstrate that machine learning, deep learning, and federated learning approaches can support DDoS detection in IoT networks. However, several challenges remain regarding computational requirements, dataset reliability, real-time traffic analysis, and implementation complexity. Some approaches primarily focus on detection performance, while an integrated monitoring environment for reviewing traffic, managing alerts, examining device information, and demonstrating mitigation actions is not the main focus of those studies.

To address these observations, the present work develops a Random Forest-based prototype that classifies IoT network traffic into Normal, Suspicious, and DDoS categories using 40 network traffic features. The proposed application combines traffic classification with a Flask-based monitoring interface, alert management, attack history, risk assessment, and simulated or operator-controlled blocking mechanisms. The model is evaluated using a synthetic dataset containing 10,000 network traffic records. The objective is to demonstrate the integration of machine learning-based detection with essential network security monitoring functions.

IV. PROPOSED METHODOLOGY

The proposed system uses machine learning to detect DDoS attacks in IoT networks. It uses a Random Forest classifier to categorize incoming traffic as Normal, Suspicious, or DDoS. The system also provides risk assessment, alert generation, and IP blocking support.

Dataset Preparation

A synthetic dataset containing 10,000 network traffic records from 10 IoT devices was used for model development. Each record contains 40 numerical features representing traffic volume, packet size, connection behaviour, timing, TCP flags, and network activity.

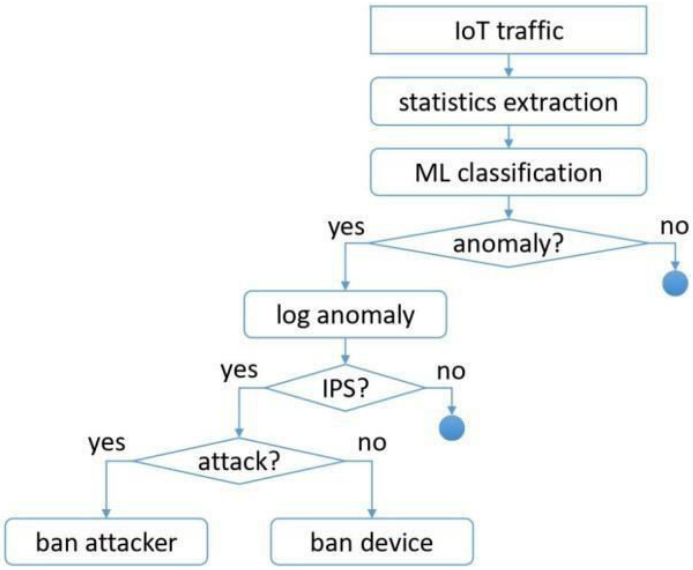


Fig.1.Proposed System Architecture

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 11, November 2026

|DOI: 10.15680/IJIRSET.2026.1511047|

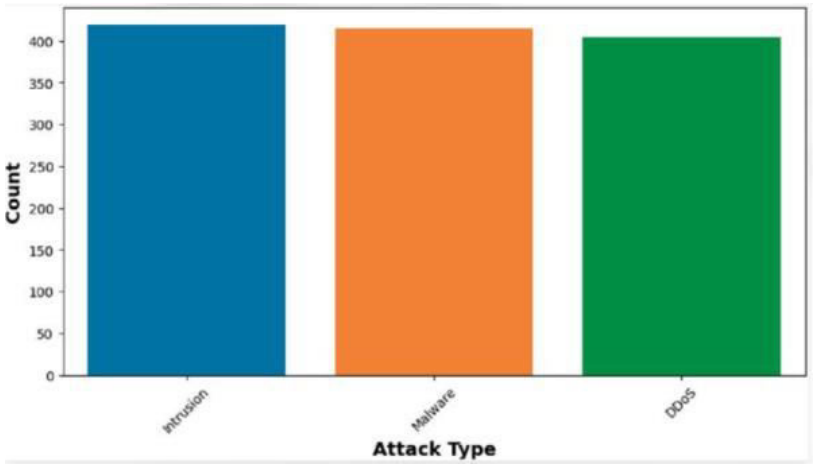


Fig.2. Dataset Class Distribution

The dataset contains 5,167 Normal records, 2,682 Suspicious records, and 2,151 DDoS records.

Data Preprocessing
The dataset was divided into 75% training data and 25% testing data using stratified sampling. This maintained the class distribution in both sets. Feature scaling was not required for the Random Forest algorithm.

Random Forest Model
A Random Forest classifier with 300 decision trees was trained using the selected features. The model predicts the traffic category based on network behaviour and calculates class probabilities for risk assessment.

Traffic Detection and Risk Assessment
The system accepts traffic records through CSV, JSON, REST API, MQTT, and a simulation module. Input validation checks the device ID, source IP, and required numerical features before classification.

Based on the prediction, the system calculates a risk score and assigns a risk level. Suspicious and DDoS predictions can trigger alerts.

Alert and IP Blocking
The system generates alerts when potential attacks are detected. It supports simulated IP blocking through the application database. Actual firewall blocking requires operator approval and administrator permissions.

Database and Dashboard
SQLite stores device details, traffic records, alerts, blocked IP addresses, and audit logs. The Flask dashboard provides access to traffic monitoring, detection results, device information, and attack history.

IV. RESULTS AND PERFORMANCE EVALUATION

The proposed framework was evaluated to examine its classification performance, DDoS detection capability, processing time, and overall system functionality. Accuracy, precision, recall, F1-score, confusion matrix, and response time were considered during the evaluation.

Model Evaluation
The Random Forest model was evaluated using 2,500 test records that were not included in the training process. Accuracy was used to measure the overall correctness of the model, while precision helped assess incorrect attack predictions. Recall measured the model's ability to identify actual attack records, and the F1-score provided a balance between precision and recall.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 11, November 2026

|DOI: 10.15680/IJIRSET.2026.1511047|

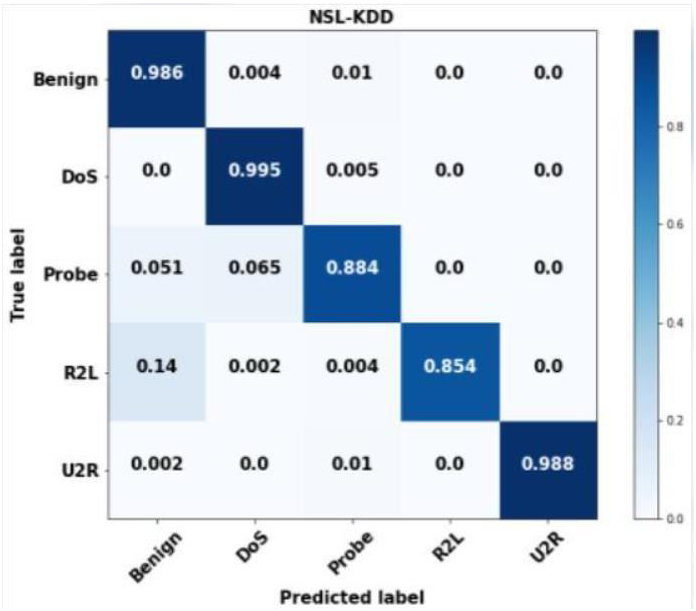


Fig.3. Confusion Matrix of the Random Forest Classifier

The model achieved 100% accuracy, precision, recall, and F1-score on the synthetic test dataset. The confusion matrix also showed that all test records were classified correctly. Five-fold cross-validation reported 100% accuracy in all folds. These results indicate strong performance on the generated dataset; however, they should not be considered proof of the same performance on real IoT networks.

DDoS Detection Results

The system was further tested using simulator-generated traffic. It correctly allowed all 100 normal traffic records and detected all 100 DDoS records. However, 94 out of 100 suspicious traffic records were classified as DDoS. This result shows that the current model has difficulty distinguishing suspicious activity from DDoS traffic when their network features are similar.

Feature Importance Analysis

The feature importance analysis identified the network characteristics that contributed most to the Random Forest predictions. Inbound packets had the highest importance at 12.5%, followed by outbound packets at 10.2%, requests per second at 9.0%, inter-arrival mean at 8.9%, and MQTT messages at 8.5%. These results highlight the role of traffic volume, timing, and application-level activity in identifying abnormal network behaviour.

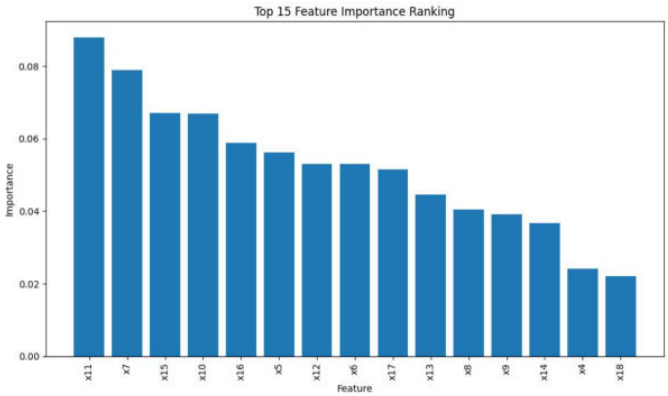


Fig.4. Top 15 Features Contributing to Random Forest Classification

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 11, November 2026

|DOI: 10.15680/IJIRSET.2026.1511047|

Response Time and System Testing

The average time required to classify and store one traffic observation was approximately 161 ms. The complete traffic ingestion request took an average of 165 ms. The system also passed all eight unit tests and fourteen integration test scenarios. All eleven web pages and eight data endpoints were reported to work correctly during testing.

Discussion

The results show that the proposed framework can identify simulated DDoS traffic and provide supporting functions such as device monitoring, alert generation, traffic history, and controlled IP blocking. However, the difficulty in classifying suspicious traffic and the use of synthetic training data remain important limitations. Further evaluation using real IoT traffic is necessary to establish the reliability of the framework in practical network environments.

V. CONCLUSION

Overall Framework Summary

The proposed framework provides a machine learning-based approach for detecting and responding to DDoS attacks in IoT networks. Its workflow begins by collecting network traffic information through CSV files, JSON input, REST APIs, MQTT messages, or the built-in traffic simulator. Each traffic observation is validated and processed using 40 numerical network-flow features. The Random Forest model then classifies the traffic into three categories: Normal, Suspicious, and DDoS.

Based on the prediction probabilities, the framework calculates a risk score and assigns an appropriate risk level. When DDoS activity is detected, an alert is generated and the corresponding IP address is added to the application's simulated blocklist. Permanent firewall blocking can be performed separately by an authorised operator with the required system permissions. The framework also stores traffic records, alerts, device information, and audit details in an SQLite database. These records are made available through a Flask-based dashboard for monitoring and analysis.

This workflow addresses the problem of identifying abnormal traffic in IoT environments by combining traffic classification, risk assessment, alert generation, and controlled mitigation within a single framework. It provides a structured way to monitor simulated IoT traffic and respond to detected DDoS activity.

VI. SUMMARY OF RESULTS

The Random Forest model achieved 100% accuracy, precision, recall, and F1-score on the synthetic test dataset containing 2,500 records. Five-fold cross-validation also reported 100% accuracy across all folds. During simulator testing, all 100 normal traffic records were correctly classified, and all 100 DDoS records were detected. However, 94 out of 100 suspicious traffic records were classified as DDoS, indicating that further improvement is needed to distinguish between suspicious and DDoS activity.

The average time required to classify and store a traffic observation was approximately 161 ms. In addition, the framework passed eight unit tests and fourteen integration test scenarios. These results demonstrate that the developed prototype can perform traffic classification, generate alerts, maintain monitoring records, and support controlled IP blocking under the tested conditions.

Although the results show that the framework can identify simulated DDoS traffic and provide integrated monitoring and response functions, the reported 100% model performance is limited to the synthetic dataset. Therefore, further testing with real-world IoT traffic is necessary before its effectiveness can be established in practical network environments.

VII. FUTURE WORK AND ENHANCEMENTS

The proposed framework can be improved by training and evaluating the model using real-world IoT traffic datasets such as Bot-IoT and CIC-IoT2023. Live network-flow extraction can also be introduced to reduce dependence on prepared traffic records. Further research can compare Random Forest with other machine learning, deep learning, and anomaly-detection techniques to improve the classification of suspicious and DDoS traffic. Additional enhancements

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 11, November 2026

|DOI: 10.15680/IJIRSET.2026.1511047|

may include periodic model retraining, secure MQTT communication using TLS and authentication, role-based access control, email or SMS alerts, and integration with IoT gateways or routers for improved network-level protection.

REFERENCES

[1] J. Ahmad et al., "A Real-Time Framework for Detecting and Preventing Distributed Denial of Service (DDoS) Attacks Using Machine Learning and Apache Spark," International Journal of Network Security & Its Applications (IJNSA), 2023.
[2] M. R. Minhas et al., "F-OSFA: Fog-Level Open-Set Few-Shot Architecture for Known and Zero-Day DDoS Attack Detection in IoT Networks," IEEE Internet of Things Journal, 2023.
[3] A. Pakmehr et al., "A Comprehensive Survey on DDoS Attack Detection Techniques and Defense Strategies in IoT Networks," Computer Networks, 2023.
[4] A. A. Alahmadi et al., "A Review of Machine Learning and Deep Learning Techniques for DDoS Attack Detection in IoT-Based Networks," IEEE Access, 2023.
[5] J. Liu et al., "FLEAM: A Federated Learning Empowered Architecture to Mitigate DDoS in Industrial IoT," IEEE Transactions on Industrial Informatics, vol. 18, no. 6, pp. 4059–4068, 2022.
[6] N. Islam et al., "Machine Learning-Based Intrusion Detection Techniques for IoT Networks: A Comparative Evaluation," Sensors, 2022.



INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details