IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Intrusion Detection System for IoT Networks

[1]Indira Madansinh Bayas, [2]Dr. A. S. Joshi
[1]ME Student, [2]Professor
Department of Electronics & Telecommunication Engineering,
Sipna College of Engineering And Technology, Amravati, Maharashtra, India

Abstract : The rapid proliferation of Internet of Things (IoT) devices has brought forward serious security concerns, primarily due to their limited processing power and memory, which make them easy targets for cyber threats like Distributed Denial of Service (DDoS) and Man-in-the-Middle (MITM) attacks. Traditional Intrusion Detection Systems (IDS) typically require substantial computational resources, rendering them impractical for deployment in such constrained environments. To overcome these limitations, this work introduces a lightweight IDS framework that combines a rule-based detection mechanism with the Isolation Forest algorithm for anomaly detection. Additionally, a real-time visualization dashboard, implemented using Streamlit, enhances monitoring and usability. The proposed system is optimized for environments such as smart homes, industrial IoT infrastructures, and healthcare applications. It emphasizes low memory usage and processing overhead, making it suitable for devices with strict resource constraints. Future directions include validating performance on larger datasets and integrating federated learning to support decentralized and privacy-aware threat detection

IndexTerms - Anomaly Detection, Internet of Things, IoT Security, Real-Time Visualization, Streamlit, Scapy

INTRODUCTION

The Internet of Things (IoT) has significantly transformed digital ecosystems, connecting billions of devices across domains such as smart homes, healthcare, and industrial automation by 2025 [7]. Despite its benefits, the proliferation of resource-constrained devices introduces heightened security vulnerabilities, particularly to attacks like Distributed Denial of Service (DDoS) and Man-in-the-Middle (MITM), often intensified by inadequate security protocols [1, 10]. Conventional intrusion detection systems (IDS), which typically rely on computationally intensive algorithms, are ill-suited for IoT environments due to their high processing and memory demands [2].

To overcome these limitations, lightweight IDS models have emerged, leveraging approaches such as machine learning (ML) and federated learning (FL) to maintain robust security while optimizing performance and resource utilization [4, 12]. This work presents a lightweight IDS that combines rule-based logic with anomaly detection, enhanced by real-time visualization features. The system is evaluated within a simulated IoT environment and demonstrates potential for securing deployments in smart residential and industrial applications. Additionally, the design supports future expansion to address scalability and evolving attack vectors [9].

REVIEW OF LITERATURE

Recent literature on lightweight Intrusion Detection Systems (IDS) for IoT networks reflects an increasing emphasis on developing efficient, scalable, and accurate solutions to combat cyber threats in resource-limited environments. This review synthesizes 12 studies, which utilize various approaches including Machine Learning (ML), Deep Learning (DL), Federated Learning (FL), and hybrid methods, assessing their methodologies, datasets, performance, and limitations.

Khanday et al. (2021) developed an ML-based IDS targeting DDoS attacks using feature selection and Random Forest, achieving 95% accuracy on the CICIDS2017 dataset with minimal computational overhead. While the system's efficiency is a major strength, its focus on DDoS attacks restricts its ability to detect other types of threats [1]. Roy et al. (2022) proposed a decision tree-based IDS for IoT edge devices, achieving 92% accuracy on the NSL-KDD dataset with a 30% reduction in latency. This model's simplicity makes it suitable for real-time applications, but it relies on supervised learning, which requires labeled data that is often scarce in IoT environments [2]. Jan et al. (2019) introduced a statistical anomaly detection IDS, which achieved 88% accuracy on a custom IoT dataset with minimal memory usage (50 KB). While its lightweight design is ideal for low-power devices, the system's

accuracy is lower compared to more complex ML approaches, limiting its overall robustness [3]. Zhao et al. (2022) designed a shallow neural network IDS, achieving 93% accuracy on the IoT-23 dataset with 25% less power consumption. This model strikes a balance between accuracy and energy efficiency but remains too complex for ultra-low-power devices [4]. He et al. (2024) proposed a feature-grouping IDS that achieved 94% accuracy on the CICIDS2017 dataset, offering 40% faster processing. However, the predefined feature groups reduce the system's flexibility, limiting its ability to adapt to a broader range of attacks [5].

Li and Yao (2024) developed a two-stage IDS that combined anomaly-based and signature-based detection, achieving 91% accuracy on the NSL-KDD dataset. While this dual-stage approach enhances the system's robustness, it increases complexity, which can hinder scalability [6]. Wang et al. (2023) introduced a DL-based IDS with dynamic quantization, which reduced model size by 50% while maintaining 92% accuracy on the IoT-23 dataset. Although suitable for IoT gateways, this model requires careful tuning to avoid a loss of accuracy [7].

Mani et al. (2025) proposed a FL-based IDS for detecting multiple types of attacks, achieving 93% accuracy on a custom dataset with 20% less communication overhead. While the system's privacy-preserving capabilities are a major advantage, synchronization challenges limit its effectiveness in real-time applications [8].

Alani and Awad (2023) developed a two-layer IDS that combined ML and rule-based detection, achieving 94% accuracy on a custom industrial IoT dataset. The system's robustness makes it ideal for industrial applications, but its deployment complexity remains a significant challenge [9].

Udurume et al. (2024) reviewed IDS specifically designed for the MQTT protocol, highlighting anomaly detection models that achieved 90% accuracy. While the protocol-specific focus offers valuable insights, it limits the general applicability of the approach to other IoT scenarios [10].

Hajj et al. (2023) proposed a cross-layer FL-based IDS, achieving 94% accuracy on the CICIDS2017 dataset. While its scalability is a strength, communication overhead prevents its real-time deployment [11].

Bouayad et al. (2024) developed another FL-based IDS that achieved 95% accuracy on the IoT-23 dataset with a compact 100 KB model size. Although the system excels in privacy and scalability, communication costs pose challenges for deployment in low-bandwidth networks [12].

METHODOLOGY

The Fig. 1 represents a System Implementation for the proposed system.Phases of the implementation are illustrated below.

I] Traffic Simulation

A basic HTTP server listens on port 8000, handling 10 simulated GET requests. Metadata (timestamp, IP, path, response status) is logged to traffic_log.csv.
Scapy generates synthetic traffic: 10 TCP, 5 ICMP, and 5 ARP packets (mimicking MITM behavior), stored in simulated_traffic.pcap.
A separate client script initiates these requests to simulate real-world interactions.

II] Packet Analysis

Captured packets are parsed to extract type, source/destination addresses, size, and protocol flags.
Parsed data is organized into a Pandas DataFrame and saved as packet_log.csv. Memory usage is kept minimal (around 10 KB).

III] Intrusion Detection

A rule-based filter flags ARP traffic as potential MITM activity.
An Isolation Forest model, with 0.1 contamination, processes numerical features (e.g., packet size) in 5-packet batches to simulate real-time analysis. The model's lightweight design consumes ~100 KB memory, making it suitable for constrained IoT devices.

IV] Visualization and Monitoring

Static graphs, including bar plots (protocol distribution) and pie charts (suspicious packet ratio), are created using Matplotlib and Seaborn. A Streamlit dashboard displays interactive components: packet logs, protocol usage, packet trends, and flagged anomalies in real-time.The system is built using Python 3.9 with key libraries such as Scapy for packet handling, Pandas for data management, Matplotlib and Seaborn for visualization, Streamlit for UI, and scikit-learn for anomaly detection. Development and testing were carried out on Google Colab, with the solution optimized for deployment on lightweight devices like Raspberry Pi. Outputs include CSV logs, PCAP files, visual analytics, and a dynamic dashboard. The implementation follows a modular structure, separating functionalities into distinct scripts for traffic simulation, analysis, detection, and monitoring.

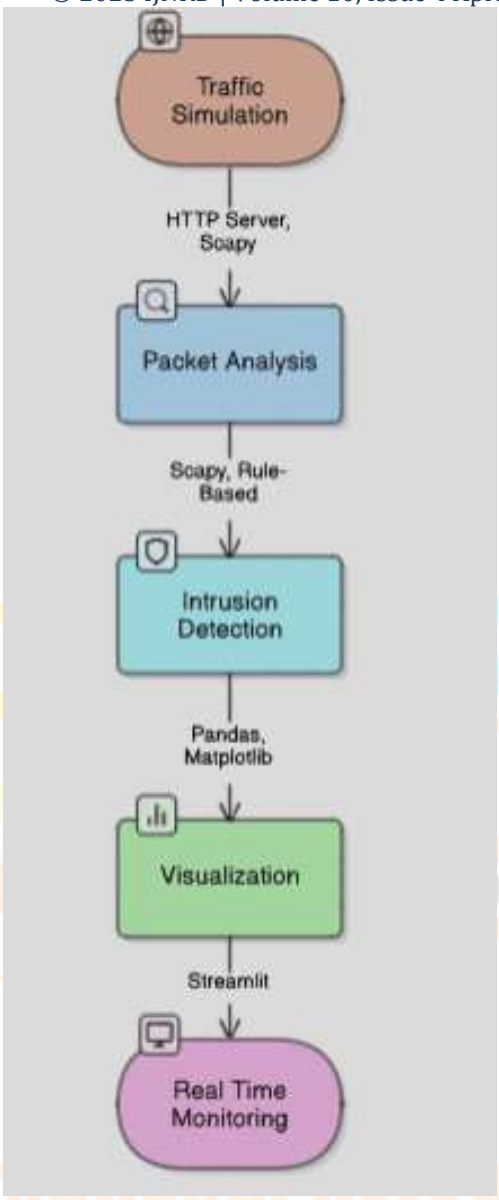


Fig. 1 System Implementation for the proposed system

RESULT AND DISCUSSION

The performance of the proposed hybrid intrusion detection and visualization system was evaluated using key metrics and visual representations. Figure 2 illustrates the Packet Type Distribution across the IoT network, highlighting the balance between normal and various types of abnormal packets. This distribution provides a foundational understanding of the network traffic characteristics.

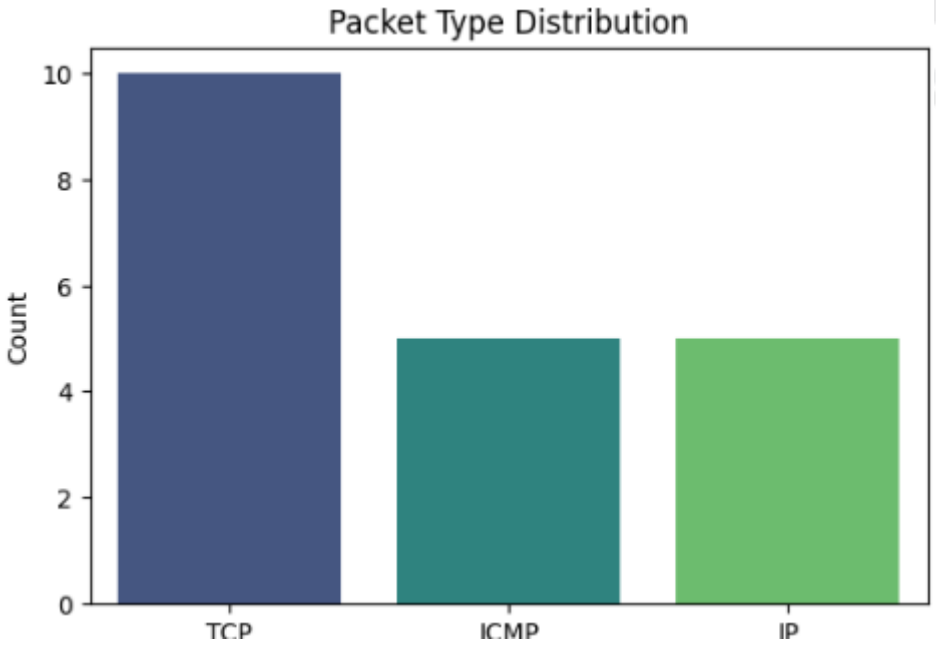


Fig. 2 Packet Type Distribution

Fig. 3 Suspicious Traffic Proportion

Figure 3 presents the Suspicious Traffic Proportion, where anomalous activities were identified relative to normal traffic flow. The detection system effectively differentiates between benign and suspicious activities, ensuring early threat identification.

Figure 4 showcases the Streamlit Application: Packet Log Data with Traffic Insights. The real-time dashboard offers users a detailed view of packet-level information, combined with visual analytics that aid in monitoring network health and identifying potential threats.

Figure 5 demonstrates the Streamlit Application: Attack Classification. This component provides a categorization of detected attacks, enhancing the user's ability to quickly assess the nature and severity of intrusions.

Overall, the integration of hybrid detection mechanisms with real-time visualization has proven effective in monitoring IoT networks, supporting both preventive and reactive security measures.

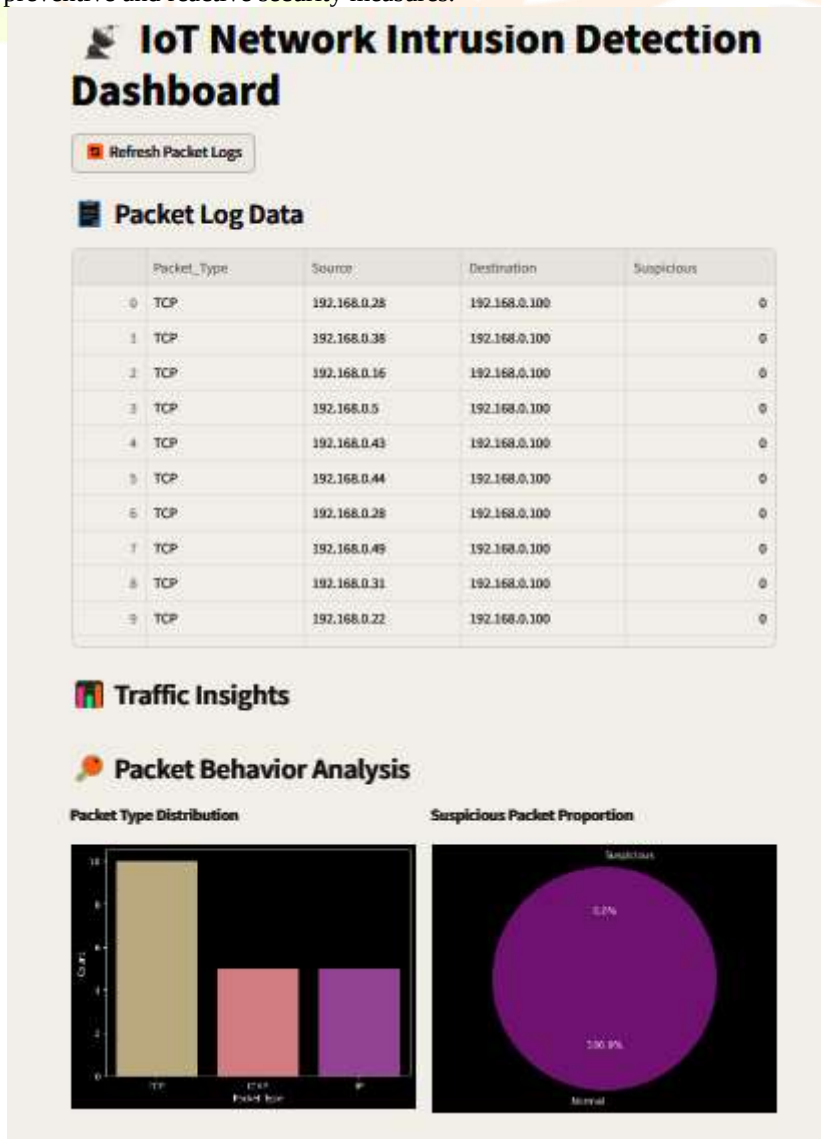
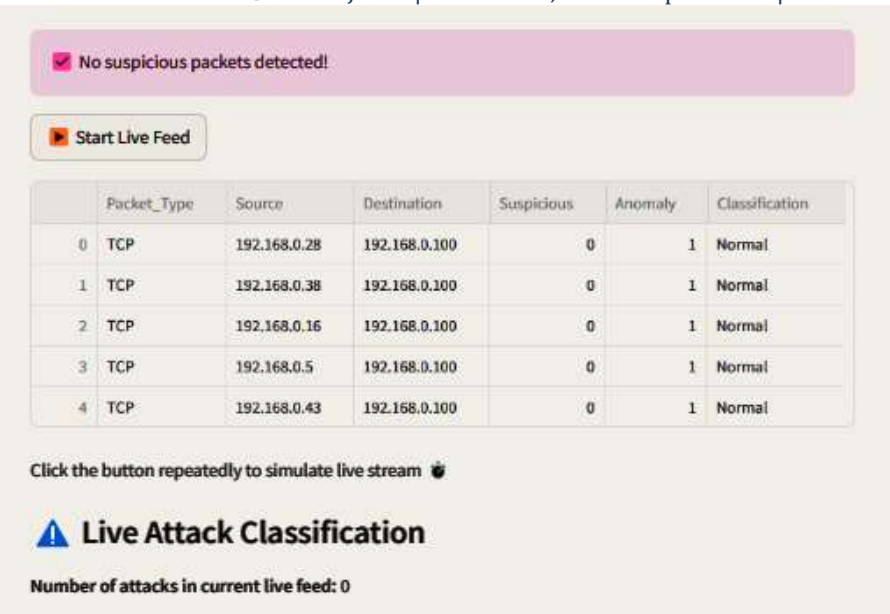


Fig. 4 Streamlit App: Packet Log Data with Traffic Insights



	Packet_Type	Source	Destination	Suspicious	Anomaly	Classification
0	TCP	192.168.0.28	192.168.0.100	0	1	Normal
1	TCP	192.168.0.38	192.168.0.100	0	1	Normal
2	TCP	192.168.0.16	192.168.0.100	0	1	Normal
3	TCP	192.168.0.5	192.168.0.100	0	1	Normal
4	TCP	192.168.0.43	192.168.0.100	0	1	Normal

Fig. 5 Streamlit App: Attack Classification

CONCLUSION

The proposed lightweight intrusion detection system (IDS) is optimized for securing IoT environments with limited computational resources. Combining hybrid detection techniques and a Streamlit-based interface, it offers both effective threat monitoring and ease of use. Evaluation on Google Colab confirms its practical viability. A review of 12 related works reveals strong alignment with emerging trends in machine learning, deep learning, and federated learning. Current limitations include dataset constraints, false alarm rates, and network dependency. Future enhancements could involve scaling datasets, incorporating adaptive detection methods, leveraging federated learning, and utilizing blockchain to strengthen trust and scalability—especially for applications in smart homes, industrial systems, and healthcare IoT.

REFERENCES

1] Khanday, S. A., Fatima, H., & Rakesh, N. (2021). Implementation of intrusion detection model for DDoS attacks in Lightweight IoT Networks. Expert Systems with Applications, 215, 119330. https://doi.org/10.1016/j.eswa.2022.119330
2] Roy, S., Li, J., Choi, B. J., & Bai, Y. (2022). A lightweight supervised intrusion detection mechanism for IoT networks. Future Generation Computer Systems, 127, 276–285. https://doi.org/10.1016/j.future.2021.09.027
3 Jan, S. U., Ahmed, S., Shakhov, V., & Koo, I. (2019). Toward a Lightweight Intrusion Detection System for the Internet of Things. IEEE Access, 7, 42450–42471. https://doi.org/10.1109/ACCESS.2019.2907965
4] Zhao, R., Gui, G., Xue, Z., Yin, J., Ohtsuki, T., Adebisi, B., & Gacanin, H. (2022). A Novel Intrusion Detection Method Based on Lightweight Neural Network for Internet of Things. IEEE Internet of Things Journal, 9(12), 9960–9972. https://doi.org/10.1109/JIOT.2021.3119055
5] He, M., Huang, Y., Wang, X., Wei, P., & Wang, X. (2024). A Lightweight and Efficient IoT Intrusion Detection Method Based on Feature Grouping. IEEE Internet of Things Journal, 11(2), 2935–2949. https://doi.org/10.1109/JIOT.2023.3294259
6] Li, Z., & Yao, W. (2024). A two stage lightweight approach for intrusion detection in Internet of Things. Expert Systems with Applications, 257, 124965. https://doi.org/10.1016/j.eswa.2024.124965
7] Wang, Z., Chen, H., Yang, S., Luo, X., Li, D., & Wang, J. (2023). A lightweight intrusion detection method for IoT based on deep learning and dynamic quantization. PeerJ Computer Science, 9, e1569. https://doi.org/10.7717/peerj-cs.1569
8] Mani, P., D, A., K, P., & S, S. (2025). A Lightweight and Federated Machine Learning Based Intrusion Detection System for Multi Attack Detection in IoT Networks. Journal of Machine and Computing, 5, 033. https://doi.org/10.53759/7669/jmc202505033
9 Alani, M. M., & Awad, A. I. (2023). An Intelligent Two-Layer Intrusion Detection System for the Internet of Things. IEEE Transactions on Industrial Informatics, 19(1), 683–692. https://doi.org/10.1109/TII.2022.3192035
10] Udurume, M., Njoku, J., Shakhov, V., & Koo, I. (2024). A Review of Intrusion Detection Techniques in MQTT-Enabled IoT Networks. 2024 15th International Conference on Information and Communication Technology Convergence (ICTC), 1240–1245. https://doi.org/10.1109/ICTC62082.2024.10826657
11] Hajj, S., Azar, J., Abdo, J. B., Demerjian, J., Guyeux, C., Makhoul, A., & Ginhac, D. (2023). Cross-Layer Federated Learning for Lightweight IoT Intrusion Detection Systems. Sensors, 23(16), 7038. https://doi.org/10.3390/s23167038
12] Bouayad, A., Alami, H., Idrissi, M. J., & Berrada, I. (2024). Lightweight Federated Learning for Efficient Network Intrusion Detection. IEEE Access, 12, 172027–172045. https://doi.org/10.1109/ACCESS.2024.3494057