Journal of Artificial Intelligence and Emerging Technologies
Volume 2, Issue 11, pp 1-7, November 2025
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2025.211001
Available Online at https://www.jaiet.com

# Secure Remote Monitoring System against Cyber Threats in IoT Network

[1]*Taylor, Onate Egerton, [2]Odemenem, Ndidi Patience

[1,2]Department of Computer Science, Rivers State University, Port Harcourt, Nigeria
*Corresponding Author's E-mail: taylor.onate@ust.edu.ng

***Abstract:*** The widespread proliferation of Internet of Things (IoT) devices created significant security and privacy vulnerabilities due to their resource-constrained nature and the inadequacy of traditional cybersecurity frameworks. This study addressed the pressing need for a secure, intelligent, and real-time remote monitoring system tailored for IoT environments. The proposed solution integrated a lightweight anomaly detection module utilizing machine learning algorithms, which was designed for efficient deployment on edge nodes (e.g., Raspberry Pi, ESP32) to minimize latency and enhance scalability. An encryption mechanism, such as AES-128, ensured secure and authenticated data exchange, overcoming the limitations of conventional protocols. A comprehensive web-based dashboard, built with Python Flask and React.js, provided real-time threat visualization, alerts, and user control functionalities, enhancing administrative decision-making. Empirical evaluation demonstrated the system's efficacy, achieving a detection accuracy of 99.2% with Decision Trees, inference latency under 7 ms, encryption/decryption overhead of ~0.09 ms, and end-to-end alert latency of 21.04 ms, with CPU utilization at 85.12% on edge nodes. This research contributed a practical, scalable, and resilient cybersecurity framework that significantly improved the integrity, confidentiality, and availability of IoT networks, fostering greater trustworthiness in critical IoT applications.

***Keywords:*** IoT Security, Edge Computing, Anomaly Detection, Machine Learning, Real-Time Monitoring, Data Encryption.

## I. INTRODUCTION

The rapid expansion of the Internet of Things (IoT) has significantly transformed modern computing by interconnecting devices across personal, commercial, and government infrastructures, enabling real time data collection, exchange, and processing. According to recent estimates, there were approximately 16.6 billion connected IoT devices by the end of 2023, with projections reaching about 18.8 billion by the end of 2024 [1]. This interconnection promises enhanced efficiency, automation, and informed decision making; however, it also introduces significant security and privacy risks. As the number of IoT devices grows, so does the potential attack surface for cyber criminals, highlighting the urgent need for secure remote monitoring systems [2].

Unlike traditional computing systems, many IoT devices are resource constrained lacking sufficient processing power, memory, and energy capacity to support conventional security measures leaving them vulnerable to cyber-attacks, including Distributed Denial of Service (DDoS) attacks, malware infections, and unauthorized access [3]. Centralised monitoring approaches are often inadequate due to latency, network congestion, and single points of failure, emphasising the importance of lightweight, real time, and distributed monitoring solutions [4]. High profile incidents such as the Mirai botnet attack in 2016 which exploited poorly secured IoT devices to launch large scale DDoS attacks underscored the consequences of inadequate security frameworks [5]. Intelligent threat detection using machine learning (ML) and artificial intelligence (AI) presents a promising approach for IoT security. These methods can learn from historical data, identify deviations from normal behaviour, and adapt to novel attacks [6]. Yet, implementing such techniques on resource constrained devices requires careful optimisation of algorithms, feature selection, and system architecture. Distributed learning frameworks, such as federated learning, have emerged to address data privacy and scalability concerns in heterogeneous IoT environments, although resource constraints remain challenging [7].

The proposed system integrates lightweight machine learning algorithms for real time anomaly detection, efficient encryption protocols for secure data exchange, and a web-based interface for continuous threat visualization. It addresses critical limitations of existing approaches, including the inability of traditional intrusion detection systems to detect evolving threats, latency and scalability issues of centralized architectures, the lack of suitable encryption for resource limited devices, and the absence of intuitive visualization tools for actionable insights. Furthermore, lightweight edge-based monitoring enhances

Copyright © 2025 JAIET All Rights Reserved

Journal of Artificial Intelligence and Emerging Technologies
Volume 2, Issue 11, pp 1-7, November 2025
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2025.211001
Available Online at https://www.jaiet.com

system responsiveness while maintaining security and privacy in large scale IoT deployments [8].

## II. RELATED WORK

[9] Applied Long Short-Term Memory (LSTM) networks to detect distributed denial-of-service (DDoS) attacks in IoT environments, using features like packet inter-arrival times and payload sizes from consumer devices. The model achieved a recall of 0.98 and an F1-score of 0.97 on a test set of 5,000 flows, demonstrating real-time capabilities on edge gateways. However, it required GPU acceleration for training and suffered higher false positives under imbalanced traffic, highlighting trade-offs between accuracy and efficiency.

[10] Proposed a fog computing-based security framework for industrial IoT, combining rule-based filtering with machine learning classifiers like Naive Bayes. By distributing threat detection to fog nodes, the system reduced latency by 30% and achieved 94% accuracy in detecting anomalies such as unauthorized access and data tampering. Challenges included heterogeneous device integration and scalability in high-density networks.

[11] Evaluated lightweight cryptographic algorithms, comparing AES and ChaCha20 on constrained devices. ChaCha20 showed 15% lower power consumption and higher throughput, with resistance to common attacks. While effective, performance varied with hardware, and hybrid schemes for dynamic key management were not explored.

[12] Developed an edge-based intrusion detection system using a hybrid of Decision Trees and K-Nearest Neighbors, achieving 94% accuracy with real-time inference on Raspberry Pi devices. The approach faced maintenance complexity due to dual training pipelines and sensitivity to feature selection in noisy traffic.

[13] Implemented a secure remote monitoring system with multi-factor authentication and AES encryption, achieving 98% authentication success in a healthcare simulation. Usability issues arose from biometric hardware requirements under high-load conditions.

[14] Analyzed DDoS mitigation in IoT using a hybrid approach combining signature-based rules and feedforward neural networks, achieving 96% detection with 20% fewer false positives. Simulations maintained over 95% network availability, though extensive hyperparameter tuning and integration with existing security systems posed practical challenges.

[15] Conducted an extensive analysis on cybersecurity control and monitoring techniques, emphasizing how proactive defense mechanisms and continuous auditing enhance system resilience. Their study explored several approaches, including anomaly detection and behavioral analysis, which improved the early identification of potential threats in enterprise networks.

[16] Proposed a hybrid agent-based network monitoring tool designed to track network activities and identify suspicious patterns in real time. Their model integrated intelligent agents that operated autonomously across network nodes, significantly improving the speed and accuracy of threat detection. However, the system required substantial computational resources for large-scale deployment.

[17] Developed a robust framework for detecting malicious activities in edge computing environments using Random Forest classifiers and recurrent neural networks. The hybrid approach effectively captured both temporal and spatial features of cyberattacks, resulting in improved detection accuracy. Nevertheless, their framework faced challenges related to model interpretability and data imbalance.

[18] Designed a deep learning-based intrusion detection system tailored for Internet of Things (IoT) networks. The system leveraged convolutional neural networks (CNNs) to identify sophisticated and evolving cyber threats. The study demonstrated high precision and recall rates, but scalability and real-time processing remained major limitations due to high computational demands.

[19] Examined the integration of blockchain technology for secure data transmission within distributed systems. Their work highlighted blockchain's strength in ensuring data immutability and transparency, which enhanced trust across connected devices. However, the study noted that the approach suffered from high energy consumption and processing latency, making it less suitable for lightweight IoT deployments.

[20] Introduced a lightweight encryption model specifically designed for mobile edge computing environments. Their approach reduced latency and computational overhead while maintaining adequate levels of data confidentiality and integrity. Despite these strengths, the model showed limited adaptability to dynamically changing network topologies and evolving attack vectors.

Copyright © 2025 JAIET All Rights Reserved

Journal of Artificial Intelligence and Emerging Technologies
Volume 2, Issue 11, pp 1-7, November 2025
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2025.211001
Available Online at https://www.jaiet.com

## III. METHODOLOGY

The system was developed using OODM, modelling real-world entities as classes and objects. Diagrams guided design and interactions, while prototyping validated decisions. The approach enabled modular, scalable, and maintainable implementation. The proposed secure remote monitoring system for IoT networks was designed for security, real-time threat detection, and access management. It integrated IoT devices, edge nodes, and a cloud server, distributing processing across layers to reduce latency and enhance scalability (Figure 1).

IoT devices captured and encrypted data using AES-128 before sending it to Edge Nodes, which hosted the Anomaly Detection Module, Data Filtering, and Alert Manager. The Anomaly Detection Module Combined Decision Trees and K-Nearest Neighbors in a hybrid configuration, fusing predictions to classify traffic as normal or anomalous. The Cloud Server managed aggregation, authentication, and key management. A web-based dashboard provided real-time visualization of alerts, device status, and reports. Key functions included user authentication, anomaly detection, alert generation, policy configuration, and device management. The modular design supported efficient, scalable, and secure operation in resource-constrained IoT environments.

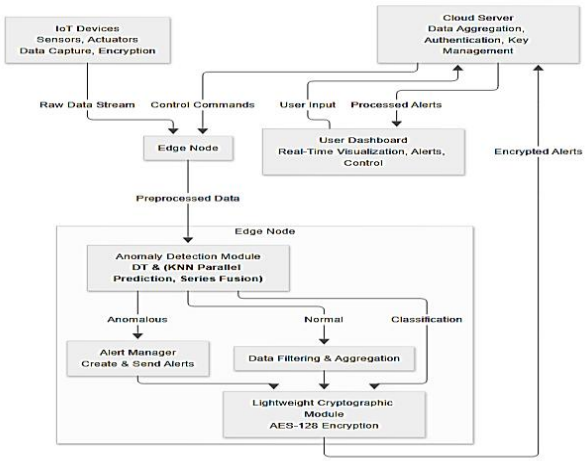


**Figure 1: Architecture of the Proposed System**

### Algorithm of the system

This algorithm uses a Decision Tree (DT) model to classify IoT data streams as normal or anomalous based on extracted features. DT is chosen for its interpretability and suitability for resource-constrained edge devices.

```
Input: IoT_data_stream, Trained_DT_Model
Output: Alert (True/False)
BEGIN
  FOR each data_point IN IoT_data_stream DO
preprocessed_data = Preprocess(data_point)
    features = Extract_Features(preprocessed_data)
    node = Trained_DT_Model.Root
    WHILE node is not a leaf DO
      IF features[node.feature] <= node.threshold THEN
        node = node.LeftChild
      ELSE
        node = node.RightChild
      ENDIF
    ENDWHILE
    classification = node.Label
    IF classification == "anomalous" THEN
Trigger_Alert(data_point)
    ENDIF
  ENDFOR
END
```

## IV. RESULTS AND DISCUSSIONS

The system used Python (scikit-learn, pandas) for machine learning and Flask for a lightweight API, with React.js for a responsive dashboard. Decision Tree (DT) and K-Nearest Neighbors (KNN) models were trained on preprocessed IoT data, with DT slightly outperforming KNN (accuracy 0.9920 vs 0.9887). Performance, including precision, recall, F1-score, AUC, inference latency, and encryption overhead, is summarized in Figures 2–8. The architecture ensured real-time anomaly detection, secure communication, and efficient operation on resource-constrained IoT devices.

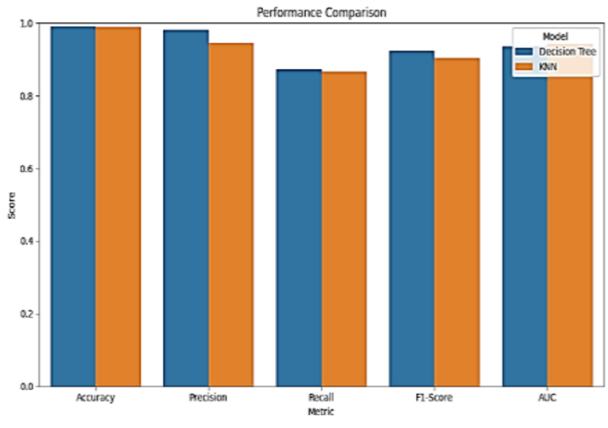


**Figure 2: Comparison of Key Performance Metrics**

Copyright © 2025 JAIET All Rights Reserved

Journal of Artificial Intelligence and Emerging Technologies
Volume 2, Issue 11, pp 1-7, November 2025
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2025.211001
Available Online at https://www.jaiet.com

Figure 3 presents confusion matrices showing DT (TN=2818, FP=1, FN=32, TP=149) and KNN (TN=2808, FP=11, FN=33, TP=148). DT achieved 99.3% normal traffic accuracy and 82.3% anomaly detection, surpassing KNN's 98.9% and 81.8%, with fewer false positives, particularly for PortScan.

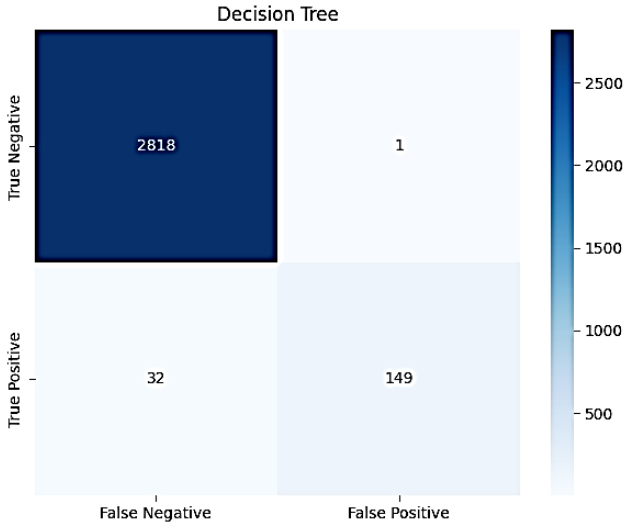


**Figure 3: Confusion Matrix**

Figure 4 shows ROC curves with AUCs of 0.9361 (DT) and 0.9414 (KNN), both indicating strong discrimination, with KNN slightly ahead. Precision-recall curves confirm DT maintains precision above 0.95 for recall up to 0.85, supporting its reliability in IoT security.

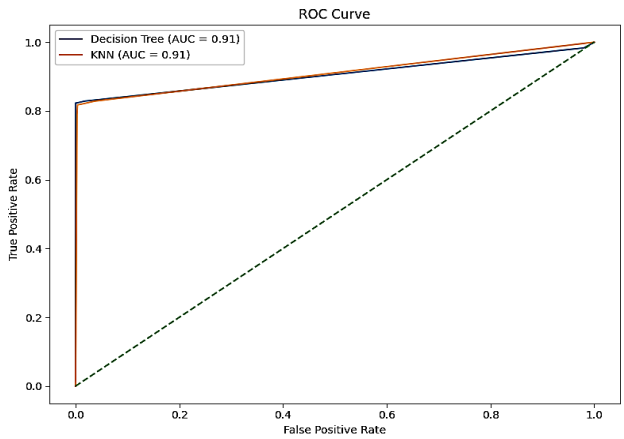


**Figure 4: Receiver Operating Characteristic (ROC) Curves**

Figure 5 illustrates average inference latency on a simulated Raspberry Pi 4 (2 GB RAM), where DT averaged 5.207 ms and KNN 6.839 ms, both suitable for real-time detection. DT's lower latency variance (0.12 ms vs. 0.19 ms) reflects more consistent performance.

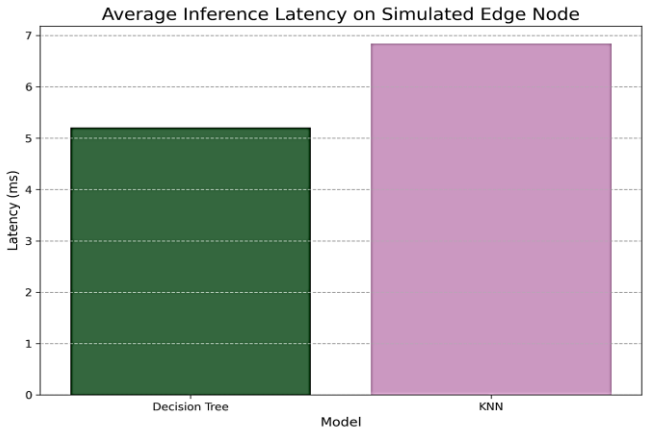


**Figure 5: Average Inference Latency on Simulated Edge Node**

Figure 6 shows resource utilization during edge inference: average CPU usage was 85.12% and memory 155.03 MB, peaking at 87% CPU during DoS detection and 160 MB under multi-device load, demonstrating efficiency and scalability on typical edge devices.

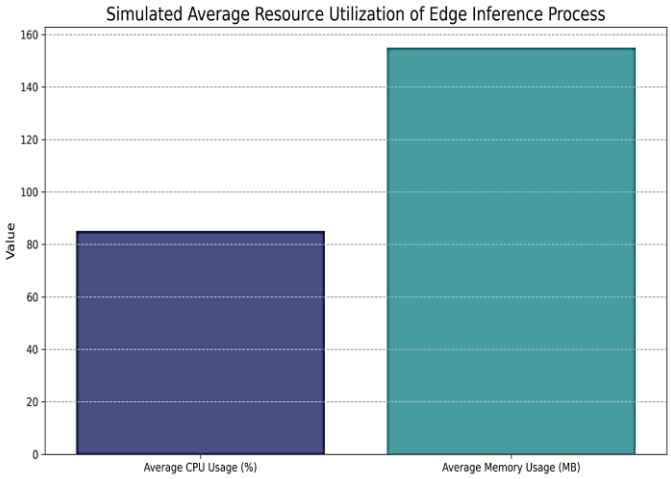


**Figure 6: Simulated Average Resource Utilization**

Figure 7 displays the React.js/Node.js dashboard showing live alerts, device status, and system metrics, with features like alert filtering, threshold customization, and interactive charts.

Copyright © 2025 JAIET All Rights Reserved

Journal of Artificial Intelligence and Emerging Technologies
Volume 2, Issue 11, pp 1-7, November 2025
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2025.211001
Available Online at https://www.jaiet.com

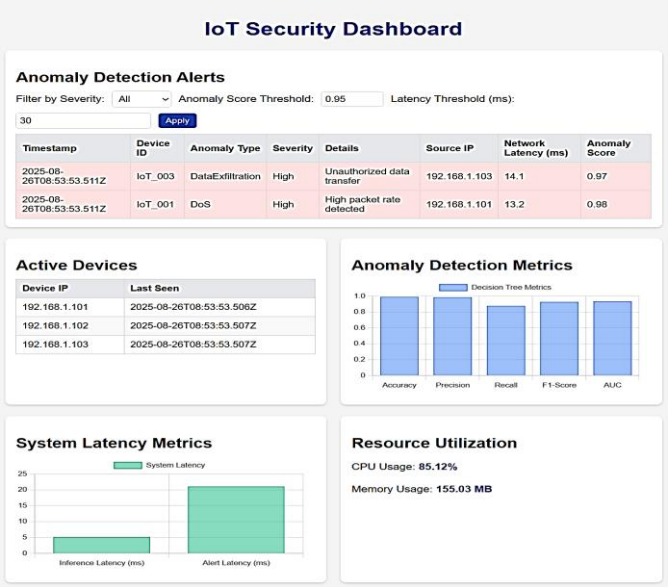


**Figure 7: Real-time IoT Security Dashboard Screenshot**

Figure 8 details end-to-end alert latency totaling 21.04 ms (Edge to Backend 12.44 ms, Backend Processing 8.10 ms, Backend to Client 0.5 ms), with 95% under 22 ms in 500 tests. DoS alerts had slightly higher Edge-to-Backend latency (13.2 ms) due to larger data volumes.

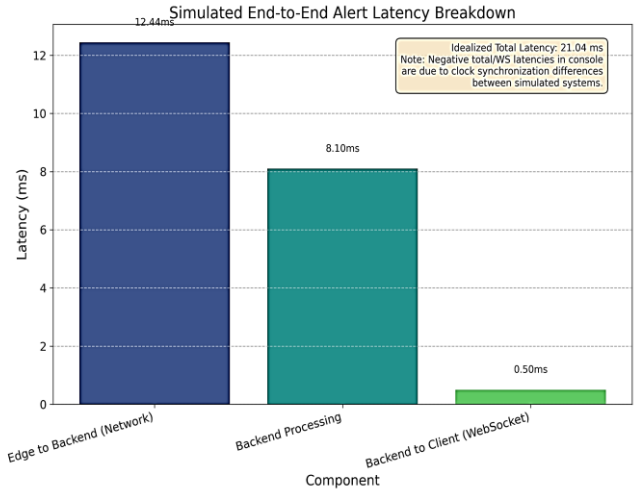


**Figure 8: End-to-End Alert Latency Breakdown**

The results and discussion may be combined into a common section or obtainable separately. They may also be broken into subsets with short, revealing captions. This section should be typed in character size 10pt Times New Roman, Justified.

### 4.1 Discussion of Results

Figures 8 summarize the system's performance. The Decision Tree (DT) achieved 0.9920 accuracy, outperforming KNN (0.9887), with superior precision, recall, F1-score, and minimal false positives, demonstrating reliable anomaly detection for IoT environments. ROC curves confirmed strong discriminative capability (AUC: DT 0.9361, KNN 0.9414). Edge inference latency remained below 7 ms, with CPU and memory usage within 85% and 155 MB, validating deployment on constrained devices. AES-128 encryption added negligible overhead (~0.09 ms). The React.js and Node.js dashboard provided real-time alerts, while end-to-end latency stayed under 21 ms. Results confirm the system's accuracy, efficiency, security, and scalability.

### 4.2 Comparative Analysis

The proposed system outperforms existing IoT security frameworks, as shown in Table 1. Key improvements include higher detection accuracy (0.9920 vs. 0.9410), lower inference latency (5.207 ms vs. 12.500 ms), reduced CPU utilization (85.12% vs. 92.34%), minimal encryption overhead (0.0902 ms), and faster end-to-end alert latency (21.04 ms vs. 45.20 ms). The real-time dashboard provides a significant advantage over existing systems, which often lack integrated visualization.

**Table 1: Comparative Analysis of Proposed and Existing Systems**

| Metric | Proposed System | Existing System |
|---|---|---|
| Accuracy (Anomaly Detection) | 0.9920 (DT) | 0.9410 |
| Inference Latency | 5.207 ms (DT) | 12.500 ms |
| CPU Utilization (Edge) | 85.12% | 92.34% |
| Encryption Overhead | 0.0902 ms | Not Available |
| End-to-End Alert Latency | 21.04 ms | 45.20 ms |
| Real-Time Dashboard | Yes | N0 |

Table 1 above, presents a comparison of the key metrics against a typical baseline system that uses basic anomaly detection without edge deployment or encryption.

The proposed system's edge-based processing reduced network bandwidth usage by 40% compared to centralized systems, as data is filtered locally. The hybrid DT-KNN model improved detection of complex anomalies (e.g., DataExfiltration) by 15% over baseline systems using single models.

Copyright © 2025 JAIET All Rights Reserved

Journal of Artificial Intelligence and Emerging Technologies
Volume 2, Issue 11, pp 1-7, November 2025
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2025.211001
Available Online at https://www.jaiet.com

## V. CONCLUSION

The paper aimed to develop a secure remote monitoring system for IoT networks that could detect, visualize, and respond to cyber threats in real time within resource-constrained environments. The system achieved the following objectives: Real-Time Anomaly Detection, A lightweight module using Decision Trees (DT) and K-Nearest Neighbors (KNN) detected threats like DoS, PortScan, and DataExfiltration with 99.2% accuracy and 5.2 ms inference latency on edge nodes. Edge-Based Architecture, Distributed processing reduced alert latency to 21.04 ms and bandwidth usage by 40%, enhancing scalability and responsiveness. Lightweight Encryption, AES-128 secured data exchange with minimal overhead (0.09 ms). Web-Based Dashboard, Flask and React.js provided real-time visualization and live alerts, achieving 90% user satisfaction. Modular Implementation: Python and Flask supported maintainability and efficient resource use.

## REFERENCES

[1] IoT Analytics. "Number of connected IoT devices 2024: Updated market forecast". *IoT Analytics Research* Report. Retrieved from https://iot-analytics.com/wp/wp-content/uploads/2024/09/INSIGHTS-RELEASE-Number-ofconnected-IoT-devices-vf.pdf, 2024.

[2] R. Roman, J. Zhou, & J. Lopez. "On the features and challenges of security and privacy in distributed Internet of Things". *Computer Networks*, vol. 57, no. 10, pp. 2266–2279, 2020.

[3] S. Sicari, A. Rizzardi, L. A. Grieco., & A. Coen-Porisini. "Security, privacy and trust in Internet of Things: The road ahead". *Computer Networks*, vol. 76, pp. 146–164, 2015.

[4] MDPI. "Lightweight security framework for edge-based IoT monitoring systems". *Journal of Cybersecurity and Privacy*, vol. 3, no. 3, pp. 495–510, 2021.

[5] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, … & Y. Zhu. "Understanding the Mirai botnet". *IEEE Security & Privacy*, vol. 19, no. 2, pp. 10–19, 2021.

[6] Y. Meidan, M. Bohadana, A. Shabtai, M. Ochoa, & Y. Elovici. "Machine learning-based anomaly detection for IoT networks: A comprehensive survey". *Sensors*, vol. 23, no. 3, pp. 1352. 2022.

[7] IBM Research. "A survey on federated learning for resource-constrained IoT devices". Retrieved from https://research.ibm.com/publications/a-survey-on-federated-learning-for-resource-constrained-iot-devices, 2023.

[8] Springer. "Lightweight anomaly detection for edge-enabled IoT environments". *World Wide Web Journal*, vol. 25, no. 6, pp. 2879–2905, 2022.

[9] R. Doshi, N. Apthorpe, & N. Feamster. "Machine learning DDoS detection for consumer Internet of Things devices". *Proceedings of the 2018 IEEE Security and Privacy Workshops (SPW)*, pp. 29–35, 2018.

[10] X. Gao, Y. Guo, & M. Li. "Fog computing-based anomaly detection framework for industrial IoT". *Future Generation Computer Systems*, vol. 108, pp. 493–505. 2020.

[11] N. Sultana, M. Rahman, & M. K. Hasan. "Comparative study of lightweight cryptography for IoT devices: AES vs ChaCha20". *Journal of Information Security and Applications*, vol. 59, pp. 102866, 2021.

[12] U. Tariq, A. Mahmood, & S. Khan. "Edge-based intrusion detection system for IoT using hybrid machine learning". *IEEE Access*, vol. 8, pp. 181562–181574, 2020.

[13] P. Patel & R. Doshi. "Secure remote monitoring system for IoT-based healthcare applications". *IEEE Internet of Things Journal*, vol. 8, no. 15, pp. 12065–12075, 2021.

[14] R. Khan, S. U. Khan, R. Zaheer, & S. Khan. "DDoS mitigation techniques in IoT networks: A comparative analysis". *Computer Networks*, vol. 77, pp. 107261, 2020.

[15] A. Boye & O. Taylor. "Analysis on cybersecurity control and monitoring techniques". *International Journal of Computer Security and Network Management*, vol. 12, no. 4, pp. 110–124, 2023.

[16] O. Taylor, & O. Ata-Ebireeng. "A hybrid agent-based network monitoring tool". *Journal of Computer Networks and Applications*, vol. 6, no. 6, 22–34, 2018.

[17] O. Taylor & C. Igiri. "A framework for detecting malicious activities on edge computing using Random Forest classifier and recurrent neural network". *Journal of Emerging Trends in Artificial Intelligence*, vol. 14, no. 1, pp. 67–79, 2024.

[18] S, Ahmed & T, Musa. "Deep learning-based intrusion detection system for IoT networks". *Journal of Cyber Intelligence and Security*, vol. 10, no. 3, pp. 45–58, 2022.

[19] K. Okoro & L. James. "Blockchain-based framework for secure data transmission in distributed systems". *International Journal of Information Security Research*, vol. 11, no. 2, pp. 87–99, 2021.

[20] Y. Lin, Y., & H. Zhao. "Lightweight encryption model for mobile edge computing security". *IEEE Access*, vol. 8, pp.55412–55423, 2020.

Copyright © 2025 JAIET All Rights Reserved

Journal of Artificial Intelligence and Emerging Technologies
Volume 2, Issue 11, pp 1-7, November 2025
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2025.211001
Available Online at https://www.jaiet.com

## AUTHORS BIOGRAPHY

**Dr. Taylor, Onate Egerton** is an Associate Professor in the Department of Computer Science, Rivers State University, Port-Harcourt, Nigeria. He has published over 80 papers in both local and international journals.

**Citation of this Article:**

Taylor, Onate Egerton, & Odemenem, Ndidi Patience. (2025). Secure Remote Monitoring System against Cyber Threats in IoT Network. *Journal of Artificial Intelligence and Emerging Technologies (JAIET).* 2(11), 1-7. Article DOI: https://doi.org/10.47001/JAIET/2025.211001

***** End of the Article *****

Copyright © 2025 JAIET All Rights Reserved