iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** II **Month of publication:** February 2026

DOI: https://doi.org/10.22214/ijraset.2026.77312

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue II Feb 2026- Available at www.ijraset.com

AI Powered IoT Security Monitoring System

Sarthak Pagar[1], Shashwat Deshmukh[2], Vivek Dake[3], Tushar Dalave[4], Prof. Suvarna Potdukhe[5]
Information Technology, RMD Sinhgad School of Engineering, Warje, Pune

Abstract: ***The rapid growth of Internet of Things (IoT) technology has led to its widespread adoption in critical applications such as smart cold storage systems, healthcare, and industrial automation. However, IoT devices are highly vulnerable to cyberattacks due to limited computational power, insecure communication channels, and lack of intelligent security mechanisms. Traditional rule-based security systems fail to detect advanced attacks such as replay attacks and data injection attacks. This paper proposes an AI-powered IoT security monitoring system designed to detect anomalies and replay attacks in a smart cold storage environment. Sensor data collected using NodeMCU (ESP8266) is transmitted to a Flask-based server where a machine learning model analyzes the data for abnormal behavior. If an anomaly is detected, the system automatically blocks the attacker's IP address and generates alerts; otherwise, the data is forwarded to the cloud for monitoring using ThingSpeak. Experimental results demonstrate that the proposed system improves real-time security, enhances detection accuracy, and ensures reliable cold storage monitoring.***

Keywords: Internet of Things (IoT), Artificial Intelligence, Anomaly Detection, Replay Attack, Cybersecurity, Smart Cold Storage Problem Statement---In IoT-based systems, especially in critical environments like cold storage, the absence of robust security mechanisms makes them vulnerable to cyberattacks such as Denial of Service (DoS), Replay, and Data Poisoning, leading to manipulated sensor data, operational failures, and loss of reliability.

I. INTRODUCTION

The Internet of Things (IoT) has transformed traditional systems by enabling real-time data collection, automation, and remote monitoring. IoT-based cold storage systems play a vital role in preserving food, medicines, and vaccines by continuously monitoring temperature, humidity, and storage conditions. Despite these advantages, IoT environments are highly susceptible to cyber threats due to weak authentication mechanisms, unsecured communication protocols, and resource constraints. Cyberattacks such as replay attacks, false data injection, and Distributed Denial of Service (DDoS) attacks can compromise sensor data, leading to incorrect decision-making and system failure. Conventional security solutions rely on predefined rules and thresholds, which are ineffective against sophisticated and evolving attack patterns. Artificial Intelligence (AI) and Machine Learning (ML) provide intelligent security mechanisms capable of learning normal behaviour and identifying anomalies automatically. This research focuses on designing an AI-based IoT security monitoring system that not only monitors environmental parameters but also detects malicious activities in real time.

II. RELATED WORK

Several studies have explored IoT security using traditional cryptographic techniques, firewall-based protection, and rule-based intrusion detection systems. While encryption ensures data confidentiality, it does not address malicious data injection or replay attacks effectively. Rule-based systems require constant updates and fail to adapt to new attack patterns.

Recent research highlights the use of machine learning algorithms such as Support Vector Machines (SVM), Random Forest, and Neural Networks for intrusion detection in IoT networks. These methods show improved detection accuracy; however, many systems focus only on network traffic analysis and ignore sensor-level data manipulation. Moreover, few solutions implement automatic response mechanisms such as IP blocking. The proposed system overcomes these limitations by combining sensor-level anomaly detection, AI-based replay attack detection, and automatic mitigation mechanisms.

III. LITERATURE SURVEY

[1] Gajjar et al. present a comprehensive survey on security challenges in the Internet of Things (IoT) ecosystem and explore the role of Machine Learning (ML) and Blockchain in mitigating these threats. The study analyzes security vulnerabilities across the perception, network, and application layers, including attacks such as DoS, replay attacks, node capture, and malware injection. The authors highlight blockchain's capability to ensure data integrity and decentralized trust, while ML techniques improve anomaly detection and intrusion prevention. Although the paper provides a broad taxonomy of IoT threats and solutions, it lacks in-depth technical implementation details.

©IJRASET: All Rights are Reserved

[2] Menon et al. examine the integration of Artificial Intelligence with IoT, commonly referred to as AIoT, focusing on improvements in security, efficiency, and automation. The survey discusses how ML and Deep Learning (DL) enhance IoT systems by enabling intelligent decision-making and adaptive security mechanisms across domains such as healthcare, smart cities, and industrial automation. The study emphasizes AI-driven analytics for real-time monitoring and threat detection, highlighting the transformative impact of AI on large-scale IoT deployments.

[3] Gilbert and Gilbert investigate AI-driven threat detection mechanisms in IoT environments, emphasizing the limitations of traditional security approaches. The paper identifies major vulnerabilities such as insecure boot processes, unauthorized access, and data leakage, supported by statistical analysis of reported IoT security incidents. The authors propose the use of ML, DL, and Reinforcement Learning (RL) models to enable adaptive and real-time threat detection, demonstrating the potential of AI-based frameworks in enhancing IoT security resilience.

[4] Prabhakar et al. provide an extensive survey of IoT security challenges, threats, and emerging countermeasures across different architectural layers. The study highlights physical attacks and node tampering at the perception layer, communication-based attacks at the network layer, and data privacy issues at the application layer. The authors emphasize the need for scalable and adaptive security solutions, reviewing cryptographic, authentication, and intrusion detection mechanisms suited for resource-constrained IoT environments.

[5] Raj and Kamble review the role of Artificial Intelligence in strengthening IoT security, focusing on Machine Learning and Deep Learning-based approaches. The paper discusses the shortcomings of traditional security mechanisms and demonstrates how AI-based models can detect anomalies, identify zero-day attacks, and automate security responses. The study concludes that AI-driven security solutions are essential for handling the dynamic and heterogeneous nature of modern IoT networks.

IV. ALGORITHM

The proposed AI-powered IoT security monitoring system follows a structured algorithm to ensure secure data acquisition, anomaly detection, and automated mitigation in a smart cold storage environment.

1) Step 1: Initialize all sensors, NodeMCU (ESP8266), Flask server, and the pre-trained AI anomaly detection model.
2) Step 2: Periodically collect environmental data from sensors deployed in the cold storage unit.
3) Step 3: Convert sensor readings into JSON format and transmit the data to the Flask server using the HTTP protocol.
4) Step 4: Preprocess the received data by normalizing values and extracting relevant features.
5) Step 5: Apply the trained AI model to classify incoming data as normal or anomalous.
6) Step 6: If the data is classified as normal, forward it to the ThingSpeak cloud platform for storage and visualization. If the data is classified as anomalous (replay attack or fake data injection), block the source IP address, generate an alert, and log the incident.
7) Step 7: Control actuators such as cooling fan and door mechanism based on predefined thresholds and system logic.
8) Step 8: Repeat the process continuously for real-time monitoring and security enforcement.

V. CONCLUSION

This research presents an AI-powered IoT security monitoring system capable of detecting anomalies and replay attacks in smart cold storage environments. By integrating machine learning with IoT infrastructure, the system enhances security, reliability, and automation. The proposed solution effectively identifies malicious activities and responds automatically through IP blocking and alert generation.

VI. ACKNOWLEDGEMENT

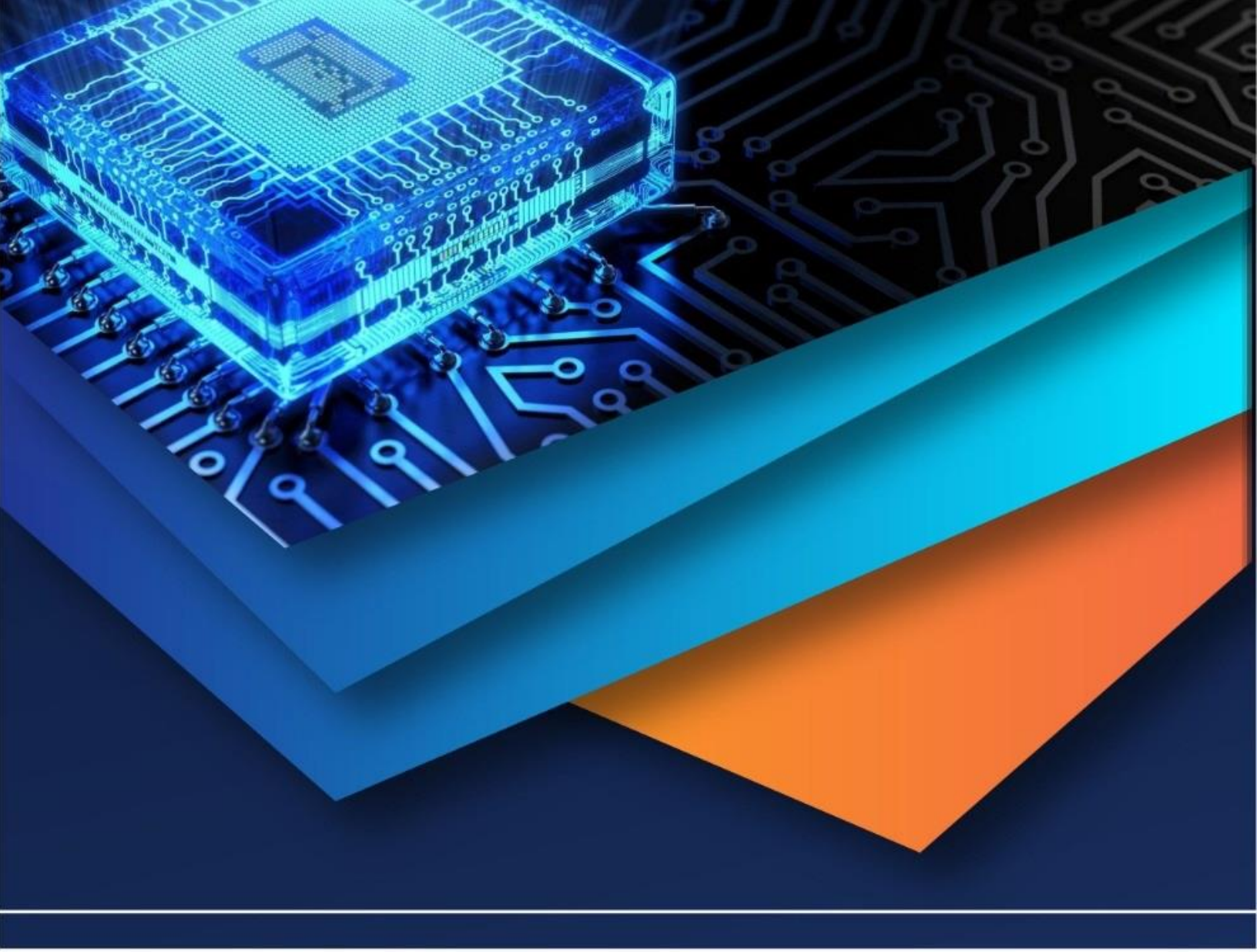
The authors would like to thank their institution and project guide for their support and guidance throughout this research work.

REFERENCES

[1] N. Sharma and P. Dhiman, “A Survey on IoT Security: Challenges and Their Solutions Using Machine Learning and Blockchain Technology,” Cluster Computing, Springer Nature, vol. 28, pp. 1–19, Apr. 2025. doi: 10.1007/s10586-025-05208-0.
[2] V. Menon U., V. B. Kumaravelu, V. Kumar C., R. A., S. Chinnadurai, R. Venkatesan, H. Hai, and P. Selvaprabhu, “AI-Powered IoT: A Survey on Integrating Artificial Intelligence with IoT for Enhanced Security, Efficiency, and Smart Applications,” IEEE Access, vol. 13, pp. 22844–22879, Mar. 2025. doi: 10.1109/ACCESS.2025.3551750.
[3] C. Gilbert and M. A. Gilbert, “AI-Driven Threat Detection in the Internet of Things (IoT): Exploring Opportunities and Vulnerabilities,” International Journal of Research Publication and Reviews, vol. 5, no. 11, pp. 219–236, Nov. 2024. doi: 10.2139/ssrn.5259702.

[4] M. Prabhakar, S. Selvarani, S. Manikandan, M. Preethika, and N. Suganya, "A Comprehensive Survey on IoT Security Challenges, Threats, and Emerging Countermeasures," International Journal of Recent Technology and Engineering (IJRTE), vol. 12, issue 4, Apr. 2024.
[5] Y. Raj and S. D. Kamble, "A Survey on the Role of Artificial Intelligence in Enhancing IoT Security," International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), vol. 12, no. 11, Nov. 2023.
[6] T. Mazhar, D. B. Talpur, T. A. Al Shloul, Y. Y. Ghadi, I. Haq, I. Ullah, K. Ouahada, and H. Hamam,"Analysis of IoT Security Challenges and Its Solutions Using Artificial Intelligence," Brain Sciences, MDPI, vol. 13, no. 4, p. 683, Apr. 2023. doi: 10.3390/brainsci13040683.
[7] A. Imran and W. Shah, "AI-Powered Cyber Security for IoT: Enhancing Network Resilience and Privacy," ResearchGate Preprint, Dec. 2023. doi: 10.13140/RG.2.2.35571.03363.
[8] F. Zaheer, "AI-Powered Cybersecurity for IoT Systems: Threat Detection and Privacy Preservation," International Journal of Advanced Research in Computer Science and Engineering, Dec. 2023.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)