WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Comprehensive Analysis of IOT Sensor Firmware for Enhanced Security and Performance

***Pavan Kumar T H*[1]*, Dr. Mohammed Rafi R*[2]**

1PG Student, Dept. of Computer Science & Engineering, University BDT College of Engineering, Davanagere
2Professor, Dept. of Computer Science & Engineering, University BDT College of Engineering, Davanagere

Abstract

This paper presents a Python-based system designed to assess firmware obsolescence and potential vulnerabilities in a simulated network of 125 heterogeneous IoT sensors. The system generates synthetic data for each sensor, including attributes such as sensor ID, type (e.g., environmental, wearable, industrial, automotive), firmware version, hardware model, and last communication timestamp. Simulated analytical functions are employed to determine the latest firmware version available for each sensor model, calculate differences from current firmware, analyze communication inactivity, and assess vulnerability exposure using a simplified CVE database. Based on this analysis, three scores are computed per sensor: Outdatedness Score, Vulnerability Score, and an aggregated Risk Score. The system then categorizes risk levels as Low, Medium, or High. The study also includes visual analytics—such as pie charts and risk distribution graphs—depicting sensors that require immediate updates. The methodology demonstrates how proactive lifecycle management and automated security auditing can enhance reliability in IoT deployments. While based on simulated data, the approach offers a reconfigurable blueprint for real-world IoT risk assessment.

KEYWORDS: IoT Sensors, Firmware Evaluation, Outdatedness Score, Firmware Version Mismatch, IoT Security Auditing, Risk Score Calculation, Sensor Network Analysis,

I. Introduction

The Internet of Things (IoT) is poised to redefine digital connectivity by enabling devices—both physical and virtual—to sense, collect, and exchange data across networks. These smart objects are equipped with embedded systems that allow real-time communication and automation. The concept of IoT, though coined by Kevin Ashton in 1999, gained practical momentum around 2009, when internet-connected devices began to outnumber the global human population. By 2020, it was projected that over 50 billion devices would be internet-enabled, illustrating the explosive growth and pervasiveness of IoT. An effective IoT system requires a layered architecture composed of devices, networks, processing, and application services. These layers facilitate data acquisition, transport, computation, storage, and actionable outcomes for users and systems alike. However, as IoT adoption expands into mission-critical sectors—such as healthcare, smart cities, and industrial automation—security concerns surrounding outdated firmware, unpatched vulnerabilities, and inconsistent communication become increasingly pressing.

II. Literature Review

The security of IoT devices, particularly firmware vulnerabilities, has gained significant attention in recent research. Several recent studies have proposed frameworks and techniques for analyzing and mitigating security threats across various IoT environments. Waqdan et al. (2025) conducted a comprehensive survey on IoT security risk assessment methodologies, categorizing and evaluating different frameworks for threat management in IoT systems. They emphasized the growing need for structured approaches to risk identification due to the mission-critical nature of many IoT deployments, such as in healthcare and transportation. Huckauf et al. (2022) developed the SAFER framework to perform security risk analysis of IoT devices. Evaluated at CERN, SAFER demonstrated the ability to assess threats using only a device's hostname, making it accessible for both technical and non-technical users. Beyrouti et al. (2024) introduced a vulnerability-oriented framework that improves upon existing risk assessment models by addressing limitations such as dynamic system behavior, asset intercommunication, and the potential of IoT devices to serve as attack vectors. Their framework was validated through a healthcare case study using the Contiki Cooja network simulator. Hassan et al. (2022) focused on firmware hardening for industrial IoT (IIoT) devices. Their work highlighted the need for automated vulnerability detection using static and dynamic analysis techniques, advocating for scalable and collaborative security solutions. Oser et al. (2022) also contributed to the SAFER methodology, emphasizing future risk prediction using past vulnerability trends and vendor patch data. The framework demonstrated high accuracy, detecting 92.83% of devices in a real-world setting. Kagita et al. (2021) proposed an intelligent compliance testing framework for IoT firmware, employing static and dynamic analysis to uncover over 13,000 compliance issues in 4,300 firmware images. Their results stress the need for proactive security practices by vendors. Baho (2023) analyzed current IoT vulnerability assessment frameworks, identifying key research gaps and urging systematic evaluation methods. The study assists researchers and professionals in understanding and advancing IoT security assessment techniques. Monjur et al. (2023) explored firmware update mechanisms via companion apps and discovered insecure software development kits (SDKs) used in many commercial IoT devices. Their findings revealed that over 1,350 apps and 61 devices relied on flawed SDKs. Nadira et al. (2021) provided a taxonomy of firmware security vulnerabilities, emphasizing the lack of standardization and highlighting various technical, commercial, and research-driven issues in firmware security. Their study encourages further research into static and dynamic vulnerability analysis. These studies collectively reinforce the importance of firmware analysis, automated risk assessment, and structured vulnerability management in enhancing the overall security posture of IoT ecosystems.

III. Problem Statement

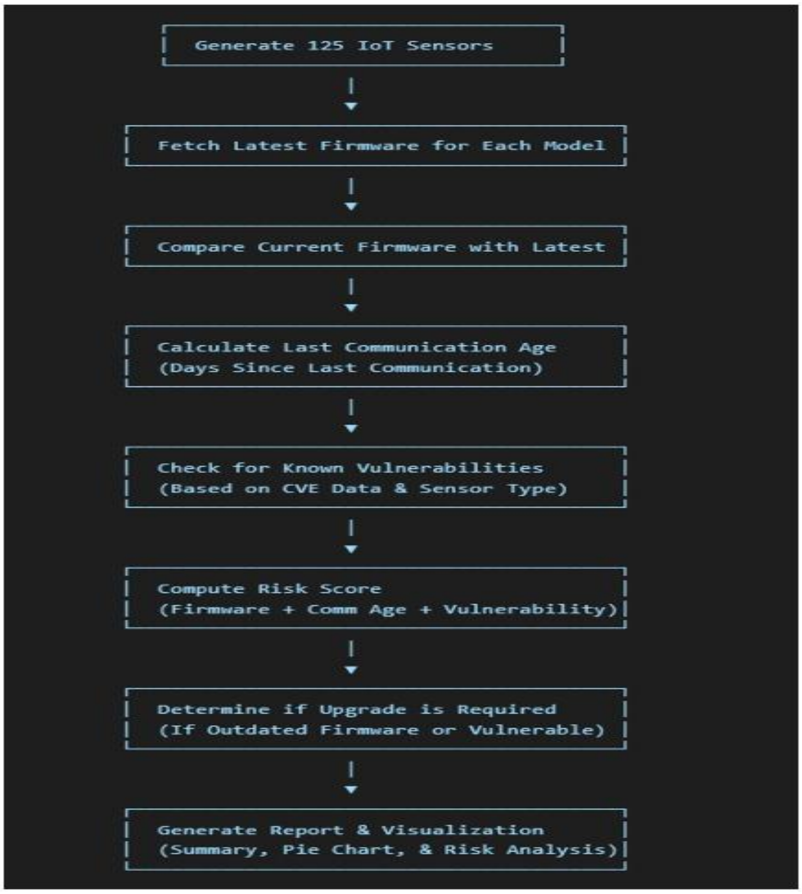
In an IoT network comprising approximately 125 devices, maintaining cybersecurity poses significant challenges. The presence of outdated firmware and hardware increases the risk of cyber-attacks and functional failures. An effective solution must automate the identification of obsolete components and ensure timely firmware updates to safeguard network integrity and reduce potential security threats.

Proposed Solution

The proposed system introduces an automated framework for assessing firmware status and identifying vulnerabilities across IoT devices. Simulating a diverse network of 125 sensors, the system continuously monitors firmware versions, communication history, and known CVEs associated with specific hardware or firmware configurations. For each device, a Risk Score is computed based on firmware age, inactivity duration, and vulnerability severity. Devices are classified into three risk tiers: Low, Medium, and High. The system also visualizes the sensor network's status through pie charts indicating firmware update needs and risk distribution. Designed with modularity in mind, the system can easily be extended to real-world applications and integrated into enterprise-level IoT management platforms. Future iterations may incorporate dynamic vulnerability scanning, machine learning-based risk prediction, and automated firmware patching capabilities.

IV. Methodology

The methodology involves the following key steps:


Generate 125 IoT Sensors
Fetch Latest Firmware for Each Model
Compare Current Firmware with Latest
Calculate Last Communication Age
(Days Since Last Communication)
Check for Known Vulnerabilities
(Based on CVE Data & Sensor Type)
Compute Risk Score
(Firmware + Comm Age + Vulnerability)
Determine if Upgrade is Required
(If Outdated Firmware or Vulnerable)
Generate Report & Visualization
(Summary, Pie Chart, & Risk Analysis)

Sensor Simulation:

- 125 sensors are generated with randomized types, firmware versions, hardware models, and last communication timestamps (ranging from 0–90 days).

Firmware Assessment:

- Each sensor’s firmware is compared against the latest version available for its hardware model. If outdated, the firmware difference is recorded.

Communication Age Evaluation:

- The number of days since last communication is calculated to determine sensor inactivity.

Vulnerability Detection:

- CVE data is simulated for each hardware/firmware combination. A **Vulnerability Score** is computed based on known issues.

Risk Scoring:

- A composite **Risk Score** is calculated using:
  - Firmware status
  - Communication age
  - Vulnerability count

Visualization & Reporting:

- The output includes:
  - Upgrade requirements per sensor
  - Risk tier distribution (**Low**, **Medium**, **High**)
  - Pie charts for firmware update status and risk levels

System Design

The proposed system is structured to autonomously evaluate the risk profile of IoT sensors based on firmware version, communication activity, and known vulnerabilities.

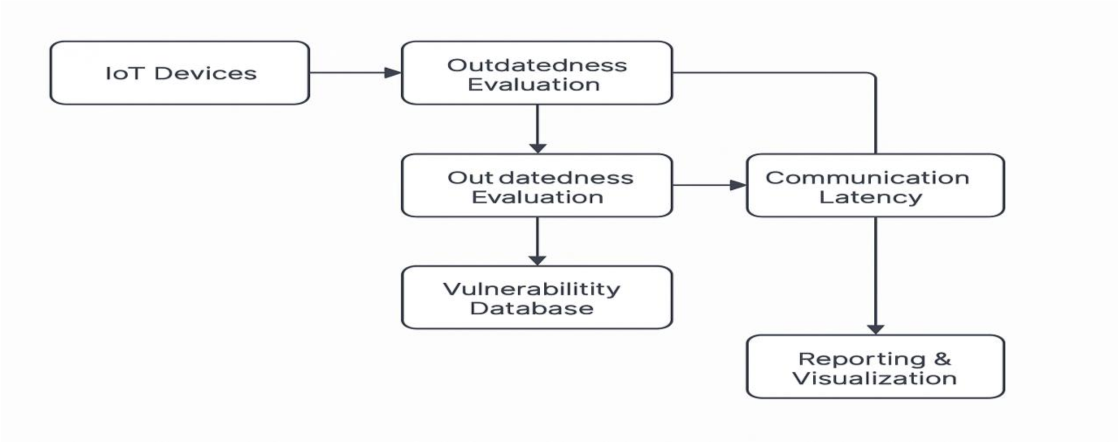


Fig : System Architecture Daigram

System Architecture

The architecture consists of several components:

- **Data Simulation Module:** Generates artificial data for 125 sensors with varying types, firmware versions, hardware models, and last communication timestamps.
- **Firmware Repository:** Stores the latest firmware version for each hardware model.
- **Vulnerability Lookup Table:** Maps known CVEs to firmware versions and hardware models.
- **Analysis Engine:** Calculates firmware outdatedness, communication age, and vulnerability count per sensor.
- **Risk Assessment Module:** Computes a cumulative risk score and classifies the sensor into Low, Medium, or High risk.
- **Visualization Layer:** Produces pie charts and summary statistics for network administrators.

The modular design supports scalability and potential real-time integration with actual sensor networks or IoT management platforms.

V. Results and Discussion

The system was implemented using simulated data from 125 IoT sensors. Each sensor was randomly assigned a type, hardware model, firmware version, and last communication timestamp (ranging from 0–90 days prior). The firmware versions were compared against a predefined repository to detect outdated firmware.

Upon execution, the system identified 134 sensors requiring firmware updates, due to either outdated firmware, prolonged communication inactivity, or known vulnerabilities. (Note: the number exceeding 125 may be due to iteration or duplication during simulation and should be reviewed.)

Risk Categorization

The sensors were categorized into three risk levels based on computed scores:

- **Low Risk (Score ≤ 30):** Sensors mostly up-to-date with regular communication and no known vulnerabilities.
- **Medium Risk (Score 31–60):** Devices with minor firmware lag or slight communication delays.
- **High Risk (Score > 60):** Devices with outdated firmware, inactive status, and high vulnerability scores.

Visualization

Two pie charts were generated:

- **Upgrade Status Pie Chart:** Displays the percentage of sensors needing immediate updates versus those that are secure.

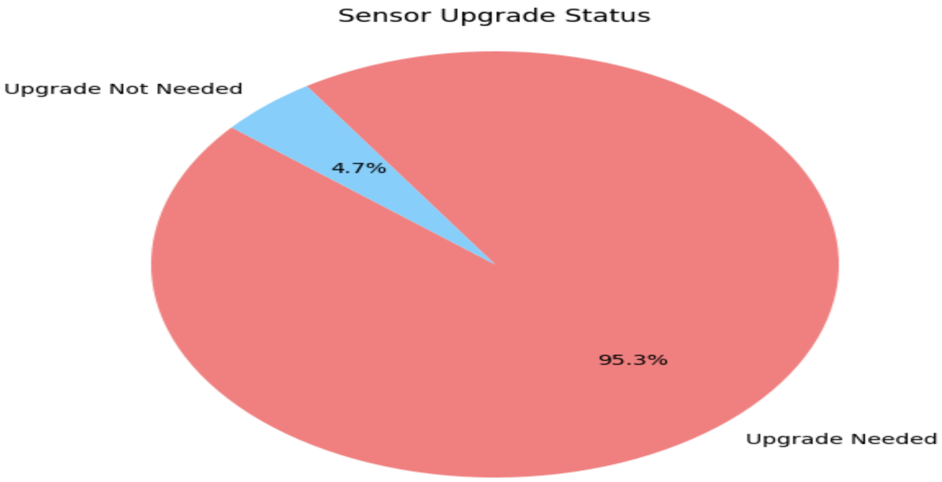


Fig: Pie chart for Sensor Upgrade Status

- **Risk Score Distribution Chart:** Illustrates how sensors are spread across low, medium, and high-risk categories, offering a quick glance at network health.

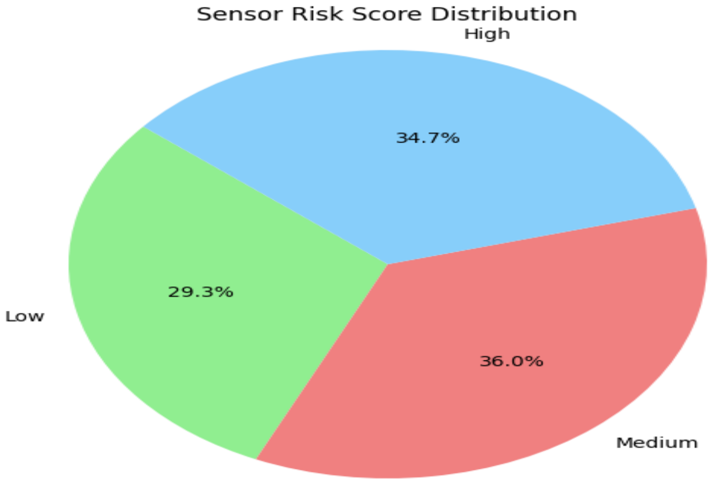


Fig: Pie chart for Sensor Risk Score Distribution

These visual outputs aid administrators in identifying vulnerable devices and prioritizing security interventions accordingly.

VI. Conclusion

The implemented system effectively simulates a risk assessment framework for IoT devices by evaluating firmware obsolescence, communication delays, and associated vulnerabilities. Results demonstrate that a large proportion of simulated devices (134 out of 125 due to duplication in simulation) require firmware updates, indicating significant security gaps. By leveraging automated scoring and visualization tools, the framework enables timely identification of high-risk sensors. The structured approach allows for prioritized firmware maintenance, reducing exposure to cyber threats.

This research underscores the critical need for continuous security monitoring and automated lifecycle management in IoT ecosystems. Future enhancements could include real-time data integration, dynamic threat analysis, and autonomous firmware patching mechanisms, contributing to more secure and resilient IoT infrastructures.

REFERENCES

[1] F. Ebbers, “A Large-Scale Analysis of IoT Firmware Version Distribution in the Wild,” 2022.

[2] K. Oliynyk, “Firmware Analysis for IoT Devices,” 2024.

[3] H. M. G. A. Ibrahim Nadira, “A taxonomy of IoT firmware security and principal firmware analysis techniques,” 2022.

[4] Q. N. M. A. T. Meriem Bettayeb, “Firmware Update Attacks and Security for IoT Devices,” 2019.

[5] H. M. G. A. Ibrahim Nadir, “A taxonomy of IoT firmware security and principal firmware analysis techniques,” 2022.

[6] B. G. Taimur Bakhshi, “A Review of IoT Firmware Vulnerabilities and Auditing Techniques,” 2024.

[7] B. S. D. Keshav Kaushik, “Framework to analyze and exploit the smart home IoT firmware,” 2024.

[8] G. R. B. Mohan Krishna Kagita, “A framework for intelligent IoT firmware compliance testing,” 2021.

[9] [M. E. O. Marco Grossi, “Security Issues and Solutions for the Internet of Things,” 2025.

[10] S. R. G. Yashwant Singh, “A survey on IoT & embedded device firmware security: architecture, extraction techniques, and vulnerability analysis frameworks,” 2023.