WWW.IJRPR.COM

International Journal of Research Publication and Reviews

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

Assessing Firmware and Hardware Obsolescence in IoT Networks Using Automated Baseline Comparison

Shashank R Chowla[1]*, Shashwath N*[2]*, Dr. Mohammed Rafi R*[3]

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

ABSTRACT

This paper presents a Python-based compliance evaluation system aimed at identifying outdated hardware and software across a simulated network of 200 heterogeneous IoT devices. The system ingests device specifications from a structured CSV dataset, including attributes such as device ID, CPU speed, RAM size, storage capacity, operating system version, and firmware version. Baseline thresholds for minimum performance and security compliance are predefined. Each device is programmatically compared against these baselines to determine deficiencies. The system then classifies devices into two categories: Up-to-Date or Outdated. Devices failing to meet one or more requirements are flagged, and specific areas of non- compliance are documented. Visual analytics, including bar charts, provide a summary of device compliance distribution. The methodology offers a scalable and automated approach for real-time IT asset auditing and risk reduction, supporting proactive decision-making in enterprise IoT environments. While based on a simulated dataset, the system architecture is adaptable for real-world deployment across large-scale networks.

Key words: Internet Of Things, Device Compliance, Cybersecurity, Hardware Baseline, Firmware Risk Detection, Python Automation, System Assessment, IT Infrastructure Monitoring.

I. INTRODUCTION

In today’s rapidly evolving technological landscape, maintaining up-to-date hardware and software is essential to ensure optimal system performance, security, and compatibility. Devices running outdated components pose significant risks, including security vulnerabilities, decreased operational efficiency, and lack of support for modern applications.

This project focuses on assessing the compliance of IoT devices against predefined baseline standards. By identifying non-compliant hardware and software, organizations can make informed decisions regarding upgrades, replacements, and overall IT infrastructure management.

The Internet of Things (IoT) is a transformative technology that interconnects physical devices with the internet, enabling them to collect, exchange, and process data autonomously. These devices—typically embedded with sensors, software, and communication modules—interact with each other and centralized systems to automate tasks and improve operational efficiency. IoT has significantly impacted industries such as healthcare, agriculture, manufacturing, transportation, and smart homes. It enables real-time monitoring, predictive maintenance, and data-driven decision-making, thereby enhancing productivity and user convenience.

The core components of IoT include:

- Sensors and Actuators – Collect and respond to data.
- Connectivity – Facilitates data transmission (Wi Fi, Bluetooth, 5G, etc.).
- Cloud Computing – Stores and processes vast amounts of data.
- Data Analytics – Extracts insights for better decision making.
- User Interface – Allows interaction with IoT systems.

Despite its advantages, IoT also introduces challenges such as security vulnerabilities, data privacy concerns, and interoperability issues. Without proper maintenance, many IoT devices remain active for years without receiving necessary updates, making them attractive targets for cyberattacks. This project explores the role of automated compliance checking in enhancing threat detection and securing IoT networks

II. LITERATURE REVIEW

The exponential growth of the Internet of Things (IoT) has led to a proliferation of interconnected devices across various sectors, including healthcare, manufacturing, agriculture, and smart cities. While this connectivity enhances operational efficiency, it also introduces substantial cybersecurity and maintenance challenges. A critical issue lies in the continued use of outdated hardware and unpatched firmware, which can create severe vulnerabilities in IoT ecosystems [1].

Recent studies have emphasized the need for automated systems that can assess device compliance with baseline security and performance standards. According to Fernandes et al. (2017), IoT devices often lack the capability to self-report their firmware status or receive over- the-air updates, necessitating external auditing systems to detect potential risks. Tools like IoTScope [5] and IoTSan [7] provide frameworks for security policy enforcement, but they focus primarily on runtime behavior and network communication, rather than static compliance with hardware/software baselines.

Firmware vulnerability databases, such as the National Vulnerability Database (NVD), have been integrated into risk scoring algorithms to proactively identify known threats associated with outdated firmware versions [3]. However, much of the research remains theoretical or lab- scale due to the lack of publicly available datasets representing real-world device states. Simulation-based approaches have become increasingly common to model IoT environments with synthetic data, allowing researchers to test auditing algorithms in a controlled manner [4].

Moreover, studies have highlighted the importance of visualization and reporting tools in enhancing administrators' ability to make informed decisions. Real-time dashboards and classification summaries improve the interpretability of audit results and help prioritize remediation efforts [2].

This project builds upon these foundations by implementing a Python-based compliance auditing system that classifies 200 IoT devices as up-to-date or outdated based on predefined hardware and software baselines. Unlike prior works that often focus narrowly on either hardware or software, this system combines both dimensions and includes reporting and visualization functionalities. It serves as a modular framework that can be adapted to real-world IT asset monitoring scenarios and extended to include advanced features such as CVE integration and machine learning–based threat prediction.

III. PROBLEM STATEMENT

In a simulated IoT environment containing 200 interconnected devices, ensuring system integrity and cybersecurity is a growing concern. Devices running outdated hardware or unpatched software pose significant threats, including reduced performance, increased vulnerability to cyber-attacks, and incompatibility with modern applications. Manually identifying non-compliant devices in large-scale networks is both inefficient and error-prone. There is a need for an automated, scalable solution capable of auditing device specifications against predefined performance and security standards, thereby enabling timely updates and informed infrastructure management decisions.

IV. METHODOLOGY

The methodology of this study follows a structured approach to evaluate the compliance status of 200 IoT devices based on predefined hardware and software standards. The process begins with the definition of baseline requirements, which serve as the reference for assessing whether each device is up to date. These baselines include the minimum acceptable specifications for CPU speed, RAM capacity, and storage space, as well as the required versions of the operating system and firmware. The goal of this step is to establish objective thresholds that ensure adequate performance and security across the network.

Following the baseline definition, device data is collected from a structured CSV file containing detailed records for each IoT device. The dataset includes key attributes such as device ID, CPU speed, RAM size, storage capacity, operating system version, and firmware version. This data is loaded and preprocessed to ensure it is clean, consistent, and ready for analysis.

Once the dataset is prepared, each device's specifications are systematically compared against the baseline standards using a comparison engine. This module performs a field-by-field evaluation to identify any attributes that fall below the defined thresholds. Devices with one or more non-compliant attributes are flagged for further classification.

The system then classifies all devices into two categories: up-to-date and outdated. A device is labeled as up-to-date if all its hardware and software attributes meet or exceed the baseline requirements. Conversely, a device is considered outdated if it fails to satisfy at least one of the defined criteria. This binary classification provides a clear and interpretable output regarding the compliance status of each device.

Finally, the results of the assessment are compiled into a comprehensive report that includes a list of all outdated devices along with specific details about their deficiencies. To enhance interpretability, the system also generates visual analytics in the form of a bar chart, illustrating the distribution of up-to-date and outdated devices. This visual representation facilitates quick assessment of the network's health and helps decision-makers prioritize maintenance and upgrades. Overall, the methodology ensures a systematic and scalable approach for auditing large-scale IoT deployments with minimal manual intervention.

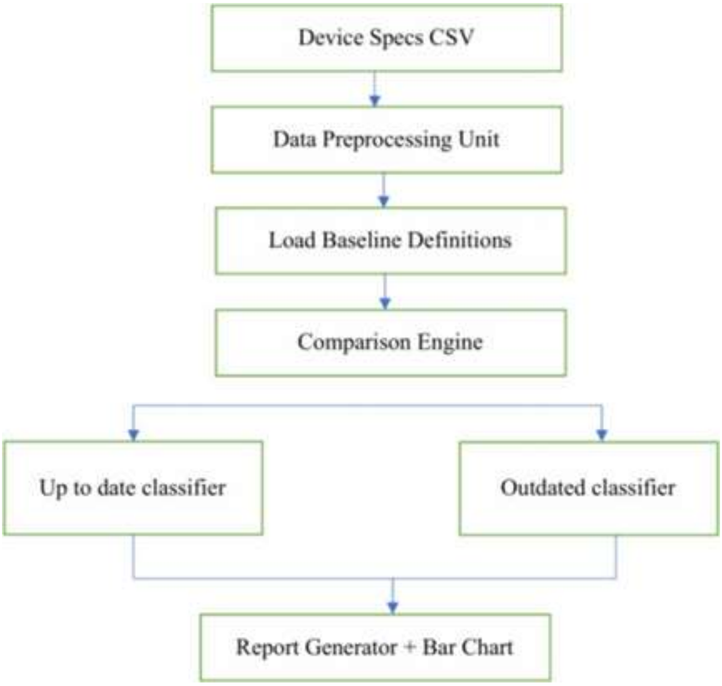

Fig 1. System Architecture Diagram

V. IMPLEMENTATION

The proposed system is implemented in Python due to its simplicity, readability, and extensive support for data analysis and visualization. Device specifications are loaded from a structured CSV file containing records for 200 IoT devices, with each entry comprising fields such as CPU speed, RAM size, storage capacity, operating system version, and firmware version. The dataset is parsed into an appropriate data structure for efficient processing and validation.

The compliance evaluation module performs hardware and software checks by comparing each device’s specifications against the predefined baseline standards. Devices that do not meet the minimum required specifications in any of the evaluated attributes are flagged as non- compliant. This evaluation includes verification of processing power, memory capacity, storage adequacy, operating system version, and firmware recency.

Based on the results of the compliance checks, the system classifies devices into two categories: up-to-date and outdated. Devices that meet or exceed all baseline criteria are considered compliant, while those failing one or more checks are categorized as outdated.

To support interpretability and decision-making, the system generates a textual report listing all outdated devices along with the specific deficiencies identified in each. Additionally, a bar

chart is produced using Python's data visualization libraries to visually summarize the distribution of up-to-date versus outdated devices. This visual aid enhances the administrator’s ability to quickly assess the overall compliance status of the network.

VI. RESULTS

The compliance assessment system was applied to a simulated network of 200 IoT devices, generating a detailed summary of their status relative to predefined hardware and software baselines. The evaluation revealed that a significant portion of devices were operating below the required standards. Specifically, 165 devices were classified as outdated due to one or more deficiencies, such as insufficient RAM, outdated operating systems, or inadequate storage capacity. In contrast, only 35 devices met all baseline criteria and were considered up to date. The system also identified common patterns among the outdated devices. The most frequent issues included devices with legacy operating system versions that no longer receive security patches, firmware versions lagging behind the latest releases, and hardware configurations that failed to meet performance thresholds. These findings highlight potential vulnerabilities and performance bottlenecks that could compromise the overall reliability and security of the network.

To support intuitive understanding and facilitate quick decision-making, the system generated a visual summary of the device status distribution. As illustrated in Fig 2, a bar chart clearly depicts the total number of devices analyzed, along with the breakdown into outdated and up- to-date categories. This graphical representation enables administrators and stakeholders to quickly assess the current state of the infrastructure and prioritize necessary updates or replacements.

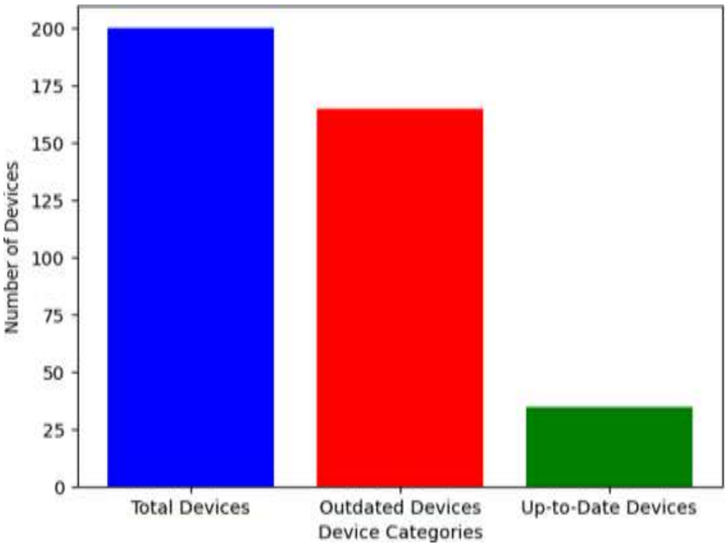

Fig 2. Bar chart illustrating the number of total, outdated, and up-to-date IoT devices

VI. CONCLUSION

This study demonstrates the effectiveness of an automated Python-based system for assessing the hardware and software compliance of IoT devices against predefined baseline standards.

By systematically evaluating 200 devices, the system successfully identified those with outdated configurations, enabling targeted remediation efforts. The findings underscore the importance of regular audits to maintain the reliability, performance, and security of IoT infrastructures.

The results highlight that a significant proportion of devices operate below acceptable thresholds, posing potential risks to system integrity and cybersecurity. Organizations can leverage the generated reports and visual analytics to prioritize critical updates, allocate resources efficiently, and make data-driven decisions regarding device lifecycle management. Continuous compliance monitoring ensures that devices remain capable of supporting modern workloads and reduces the likelihood of failures or security breaches. Integrating such automated assessment tools into IT operations not only improves operational efficiency but also strengthens the overall resilience of interconnected environments. Moving forward, the system offers a scalable and adaptable foundation for real-world deployments, with future enhancements potentially incorporating real-time vulnerability databases, predictive analytics, and automated update mechanisms.

References

1. Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). *Security, privacy and trust in Internet of Things: The road ahead*. Computer Networks, 76, 146–164. https://doi.org/10.1016/j.comnet.2014.11.008

2. Alrawais, A., Alhothaily, A., Hu, C., & Cheng, X. (2017). *Fog Computing for the Internet of Things: Security and Privacy Issues*. IEEE Internet Computing, 21(2), 34–42. https://doi.org/10.1109/MIC.2017.36

3. Ali, S., Rodrigues, J. J. P. C., et al. (2020). *A Review of Firmware Vulnerabilities in IoT Devices.* IEEE Access, 8, 219655–219675. https://doi.org/10.1109/ACCESS.2020.3041839

4. Chhetri, S. R., Faezi, S., & Hayat, M. (2019). *Secure Lifecycle Management of IoT Devices: Challenges and Opportunities*. IEEE Transactions on Industrial Informatics, 15(6), 3046–3054. https://doi.org/10.1109/TII.2018.2873587

5. Zhang, C., Yu, F. R., Nekovee, M., Liu, Y., & Xie, S. (2018). *IoTScope: Establishing Effective Context-Aware Security Policies for Smart IoT Devices*. IEEE Internet of Things Journal, 5(3), 2126–2138. https://doi.org/10.1109/JIOT.2017.2781252

6. Fernandes, E., Jung, J., & Prakash, A. (2016). *Security Analysis of Emerging Smart Home Applications*. In 2016 IEEE Symposium on Security and Privacy (SP), 636–654. https://doi.org/10.1109/SP.2016.44

7. Jia, Y., Wang, Q., Tian, Y., et al. (2017). *ContexIoT: Towards Providing Contextual Integrity to Appified IoT Platforms*. Proceedings of the Network and Distributed System Security Symposium (NDSS). https://doi.org/10.14722/ndss.2017.23091