WWW.IJRPR.COM

International Journal of Research Publication and Reviews

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

Upgrade Sentinel:Automating the Detection of Outdated Systems to Strengthen Cyber Defence

[1] Nandini LB, [2] Sanjana K, [3] Dr Mohammed Rafi

[1] Department of Computer Science and Engineering, University BDT College of Engineering Davangere, India
nandinilb123@gmail.com@gmail.com
[2] Department of Computer Science and Engineering University BDT College of Engineering Davangere, India
sanjanaachar19@gmail.com
[3] Department of Computer Science and Engineering,University BDT College of Engineering Davangere, India
mdrafi2km@ubdtce.org

ABSTRACT:

The Internet of Things(IoT) is a emerging technology that connects physical devices to networks,enabling them to collect, share and process data autonomously. These devices, loaded w sensors, software and communication tools, enhance automation and efficiency across different indusies. However, as IoT adoption grows, so do concerns around security ,data privacy, and system interoperability. This project examines thee of IoT in threat detection, focusing on its architecture,implementation, and benefits. A key goal is to develop an algorithm that identifies devices with outdated hardware or software, helping to reduce risks such as cyberattacks, unauthorized access, and data leaks. By encouraging timely updates and strongsecurity practices, this approach aims to build safer and more reliable IoT systems.

Keywords: Internet of Things (IoT), Threat Detection, Cybersecurity, Device Vulnerabilities, Outdated Firmware, Security Updates, Data Privacy, IoT Architecture, Automation, Interoperability.

Introduction:

The IoT(Internet of Things) has experienced rapid expansion, transforming how we interact with technology by bridging the physical and digital realms. From intelligent home systems and health-tracking wearables to industrial control systems and smart transportation networks, IoT has dramatically improved efficiency, productivity, and daily convenience across numerous fields. Yet, this widespread interconnectivity also exposes users and organizations to new and complex security risks that threaten individuals, enterprises, and even national infrastructures.

One of the most critical issues in the IoT space is the continued use of devices containing outdated hardware or obsolete software components. Many IoT products are introduced into the market with limited built-in security protections. Once deployed, these devices often lack mechanisms for receiving timely updates or patches. Consequently, they are frequently exposed to cyber threats including malware infections, unauthorized access, data theft, and large-scale DDoS attacks. Notable examples like the Mirai botnet incident have demonstrated the serious consequences of neglecting IoT security.

Security professionals warn that device aging—especially in terms of outdated firmware, unpatched flaws, declining performance, and outdated hardware—is a major entry point for cybercriminals. Conventional IoT protection strategies, which depend largely on manual checks and after-the-fact responses, are inadequate for managing the scale and complexity of today's interconnected environments. Therefore, the demand is increasing for automated threat detection systems capable of continuously monitoring device status and responding swiftly to emerging threats.

To tackle this issue, this paper introduces "Upgrade Sentinel" , an innovative algorithmic system designed to detect and categorize outdated IoT devices using a detailed risk evaluation model. The framework assesses various factors including device age, software versions, patch history, performance indicators, and exposure to known vulnerabilities by comparing real-time device information with databases like the Common Vulnerabilities and Exposures (CVE) repository. Based on this analysis, each device receives a calculated risk score and is grouped into high-risk, medium-risk, or low-risk categories, allowing stakeholders to take appropriate action efficiently.

The methodology integrates automation at every step—from device identification and cataloging to update validation and vulnerability correlation—reducing reliance on manual efforts and streamlining operational processes. A MATLAB-based simulation environment was used to evaluate the algorithm's effectiveness using a dataset of 250 virtual IoT devices. The findings show that the system can accurately classify devices and provide clear visualizations through charts and graphs, aiding in prompt decision-making and strategic planning for upgrades.

In addition, this research reviews current studies to identify shortcomings in existing IoT security measures and highlights the importance of proactive maintenance and real-time monitoring in safeguarding against evolving cyber threats. The proposed framework supports modern cybersecurity standards and offers a scalable solution suitable for deployment in smart cities, healthcare technologies, and industrial IoT ecosystems.

In summary, "Upgrade Sentinel" seeks to significantly improve the cybersecurity resilience of IoT systems by automating the identification and classification of outdated devices. It provides a practical and scalable approach to strengthening defenses, reducing vulnerabilities, and ensuring the reliability of IoT-driven services in our increasingly connected world.

Problem Statement

The extensive adoption of IoT devices has led to growing security vulnerabilities, particularly due to outdated components that rarely receive updates. Aging hardware and obsolete software increase susceptibility to cyber threats, unauthorized intrusions, and declining performance, creating serious risks for connected networks. Traditional manual inspection techniques struggle to keep up with large-scale IoT deployments, and many current tools lack the capability for continuous, automated risk evaluation. To address this challenge, there is a clear demand for an adaptive system that can automatically identify outdated devices, evaluate their risk levels, and suggest targeted security measures to enhance overall network resilience in IoT environments.

Objectives:

This study aims to design and implement an intelligent, automated system called Legacy Risk Scanner, which identifies and evaluates security risks associated with outdated (legacy) hardware and software components.

Key Objectives:

1. Automate the identification and analysis of legacy systems to detect potential weaknesses and vulnerabilities efficiently.
2. Integrate signature-based detection techniques with machine learning models to recognize both known threats and newly emerging (unknown) risks.
3. Classify identified risks based on severity, exploitability, and potential impact , enabling prioritization of remediation efforts.
4. Generate comprehensive, user-friendly risk reports that assist stakeholders in making informed decisions and implementing effective mitigation actions.

LITERATURE SURVEY

The widespread adoption of IoT technologies has led to increased research efforts focused on improving device security, functional performance, and cross-platform compatibility. Numerous studies have examined different aspects of IoT applications and the associated risks, underscoring the need for more systematic and forward-looking security strategies.

1. "A Survey on Automated Vulnerability Detection and Mitigation," IEEE, 2020. This work provides an overview of current methodologies used for automatically identifying software vulnerabilities. It highlights the importance of static and dynamic analysis, symbolic execution, and fuzzing as key techniques in detecting outdated or insecure components within systems.
2. "Software Component Vulnerability Detection: A Machine Learning Approach," ACM, 2019. This paper explores the use of machine learning models to categorize software elements based on their version history and known security flaws. It advocates for the use of training data from databases like CVE and NVD to automate the detection of obsolete software components.
3. "Outdated Libraries: An Empirical Study on the Impact and Detection," Empirical Software Engineering Journal, 2018. The authors analyze how outdated libraries contribute to heightened security risks and propose automated mechanisms for real-time identification and upgrading of such dependencies.
4. "Static Analysis Tools for Detecting Security Flaws in Legacy Software," Springer, 2021. This survey evaluates a range of static analysis tools and assesses their effectiveness in uncovering outdated or insecure code segments within legacy systems.
5. "A Comprehensive Study on Patch Management in Cybersecurity," Journal of Cybersecurity, 2020. The study outlines strategies for automating patch detection and installation, aligning with the goal of this project to enable proactive responses to outdated systems.
6. "Dependency Management and Vulnerability Detection in DevOps Pipelines," ACM DevOps, 2020. This paper discusses the integration of vulnerability scanning tools such as Snyk and Dependabot into CI/CD pipelines, promoting early detection of outdated packages before deployment.
7. "Security Technical Debt Due to Outdated Software Components," IEEE Security & Privacy, 2021. The article examines how the use of outdated software contributes to technical debt and emphasizes the importance of timely detection and updates in reducing long-term cybersecurity risks.
8. "Real-Time Threat Intelligence for Software Vulnerability Detection," Elsevier Computers & Security, 2022. This paper introduces approaches that combine live threat intelligence with local system scans to identify outdated and vulnerable components in real time.
9. "Automated System Auditing Tools: Current Capabilities and Limitations," NIST Technical Report, 2019. The report reviews widely-used auditing tools such as Nessus, OpenVAS, and Qualys, which can detect outdated software components and suggest appropriate upgrades as part of automated audit processes.

Despite the valuable insights provided by these works, there remains a notable gap in the existing literature—specifically, the lack of lightweight, threshold-based algorithms capable of performing real-time risk assessment and classification of IoT devices. This research seeks to address this gap by proposing a proactive threat detection system that evaluates multiple parameters and delivers actionable security recommendations.

Methodology:

The proposed methodology presents a structured framework for overseeing and safeguarding Internet of Things (IoT) devices operating within interconnected environments. This approach is engineered to facilitate early detection of security weaknesses, enhance device adherence to best practices, and support intelligent automation across extensive IoT deployments. The overall architecture is composed of five primary stages:

A. *IoT Device Discovery and Inventory:*The initial phase of the Upgrade Sentinel framework focuses on discovering and recording all IoT devices present within the network. This process utilizes network scanning tools to detect active endpoints and gather critical device metadata such as unique identifiers, manufacturer details, firmware or software versions, and the date of the last update. The primary objective is to build a detailed and current inventory of connected devices, which forms the essential basis for subsequent steps including analysis, continuous monitoring, and risk evaluation.

B. *Hardware and Software Version Tracking:*After devices are detected and recorded in the inventory, the next stage involves version monitoring . This step entails comparing each device's current firmware and software versions against the latest releases provided by their respective manufacturers. The system accesses official vendor update databases and public repositories to retrieve up-to-date version information. Any device found to be operating on an older or unsupported version is marked for further evaluation, as it may be missing critical security patches or bug fixes, thereby increasing its susceptibility to cyber threats or operational failures.

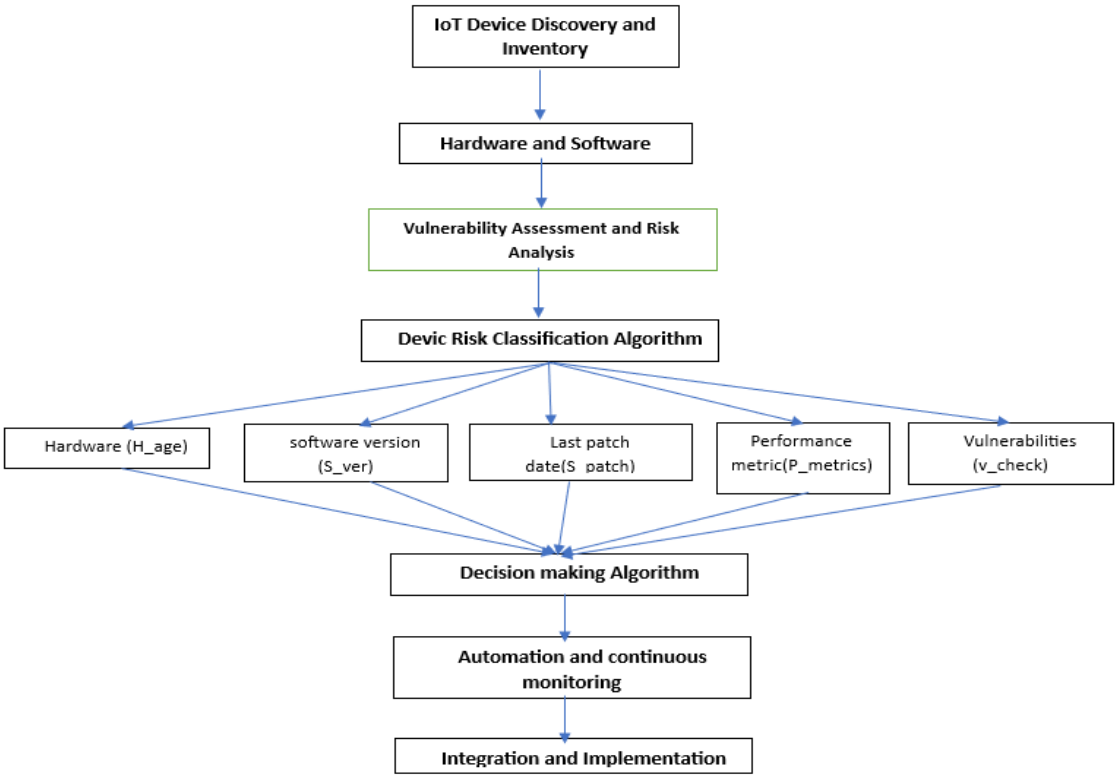
C. *Vulnerability Assessment and Risk Analysis:* In this step, the system analyzes the security status of each connected device by referencing its current software and firmware versions against known threats listed in public vulnerability databases such as the CVE catalog. Based on this comparison, a risk assessment is conducted, taking into account the factors like the presence of obsolete components, signs of performance decline, and potential exposure to documented threats. Each device is then assigned a calculated risk level—categorized as Low, Medium, or High—according to the severity of the identified issues. This classification enables administrators to focus their efforts on those devices that pose the greatest risk and require immediate corrective measures..

D. *Decision-Making Algorithm:* The system utilizes an automated decision-making model based on predefined rules to determine the most suitable course of action for each device, depending on its risk rating and update status. When a safe and compatible software or firmware update is available, the framework triggers the update automatically. In cases where a device is no longer receiving manufacturer support, the system suggests replacement as the best long-term solution. For high-risk devices that cannot be updated or substituted, the framework recommends isolating them from the network to prevent potential exploitation by malicious actors. This structured approach ensures consistent and efficient handling of security risks across all identified threat levels.

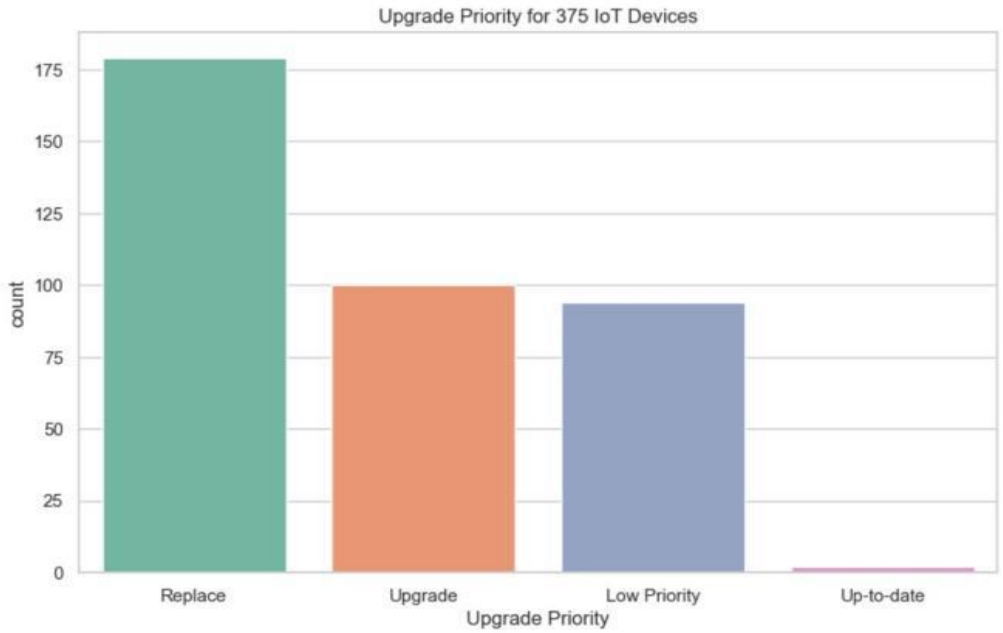
E. *Automation and Continuous Monitoring:* Automation is a core element in executing the decisions made by the system's analytical model. The framework is capable of delivering instant notifications to network administrators, scheduling and applying software or firmware updates as needed, and continuously tracking device behavior for anomalies. By handling routine tasks like scanning, alerting, and report generation automatically, the system significantly reduces the need for human oversight and supports efficient security management at scale—particularly in large-scale IoT deployments. Additionally, it produces regular status reports that provide insights into the current level of security and the success of implemented corrective actions.

F. *Device Risk Classification Algorithm:* The algorithm assigns a risk score to each IoT device by evaluating several critical parameters. These factors include the age of the hardware (H_age), the status of its software version (S_ver), the duration since the last security patch was applied (S_patch), signs of performance decline (P_metric), and whether known vulnerabilities are present (V_check). A device is marked for further review if it meets any of the defined criteria—such as being more than five years old or having gone without a patch for over six months. Each of these conditions contributes one point to the overall risk assessment. Based on the cumulative score, devices are grouped into three categories: Low Risk (score < 2), Moderate Risk (score $= 2$), and High Risk (score ≥ 3). This method ensures a uniform and impartial evaluation of security risks across all connected devices.

G. *Integration and Implementation:* The Upgrade Sentinel framework is engineered for smooth integration with current IoT management systems, offering compatibility across a range of operational settings. It supports both periodic and on-demand scanning, allowing it to be deployed effectively in varied environments such as urban smart infrastructure, medical facilities, and industrial control networks. Its resource-efficient architecture ensures functionality even in constrained or low-capacity network setups. Additionally, the system can initiate automated patching procedures and issue real-time notifications based on the risk level assigned to each device. This capability helps organizations streamline their security operations, reduce reliance on manual intervention, and adopt a more proactive approach to threat mitigation.



Results and Discussions:



IoT device risk classification based on the number of devices in each risk category (High-Risk, Moderate-Risk, and Low-Risk). The bar chart illustrates that the majority of devices fall under the High-Risk category, followed by Moderate-Risk and Low-Risk.

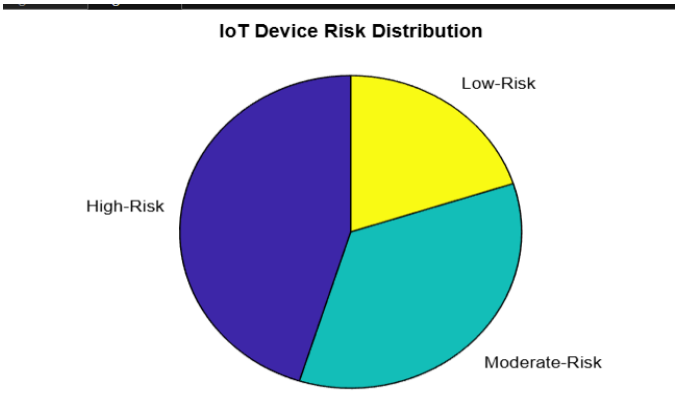


Fig. 1. IoT device risk distribution represented in a pie chart. This visualization highlights the proportion of devices across the three risk levels, emphasizing the dominance of High-Risk and Moderate-Risk categories over Low-Risk devices.

The bar chart titled "Upgrade Priority for 375 IoT Devices" presents a visual breakdown of how devices are distributed across different upgrade categories. The x-axis lists four classifications: Replace , Upgrade , Low Priority , and Up-to-date , while the y-axis reflects the number of devices in each group.

According to the data, the majority—approximately 180 devices—are classified under the Replace category, indicating that almost half of the total require complete replacement due to obsolescence or failure. The second-largest group, comprising about 100 devices, falls into the Upgrade category, signaling a need for software or firmware enhancements to address performance or security concerns. The Low Priority group includes roughly 95 devices, which are currently functioning adequately and may not require immediate action. Lastly, only a small number—fewer than five—devices are marked as Up-to-date , highlighting the limited portion of the system that is already operating with the latest configurations.

This distribution underscores the urgent need for structured maintenance strategies in managing IoT environments, particularly given the large volume of devices that are either outdated or in need of critical updates.

Conclusion and Future Scope:

The Upgrade Sentinel system offers an effective solution to the increasing security risks in IoT networks that arise from outdated hardware and software components. Through automated vulnerability detection, risk classification, and actionable recommendations such as updates, replacements, or network isolation, the system enables organizations to adopt a proactive approach to IoT security management. The structured risk evaluation model, supported by visual reporting tools, enhances clarity and supports informed decision-making. By reducing manual intervention and ensuring prompt threat response, this framework significantly improves the safety, reliability, and resilience of IoT ecosystems.

Looking ahead, the system can be enhanced to operate efficiently in larger and more complex environments, including smart homes, industrial automation, and healthcare infrastructures. Integrating advanced tools like machine learning and artificial intelligence could further improve its ability to adapt, learn from historical data, and predict potential threats with greater accuracy. Additionally, collaboration with industry stakeholders will help to establish unified security standards for IoT devices. These future improvements will contribute to making the system more scalable, intelligent, and robust—ultimately supporting the development of a secure and seamlessly connected digital ecosystem.

Future Development:

In the coming years, a primary objective will be to improve the scalability and adaptability of the suggested algorithm so that it can efficiently operate covering multiple IoT environments—including smart homes, industrial facilities, urban infrastructure, and healthcare systems. To further improve its intelligence and accuracy, the system can incorporate advanced tools such as machine learning and artificial intelligence. These tools would enable the framework to analyze the historical data, detect patterns, and autonomously make informed decisions with minimal or no human intervention.

Another critical direction for development involves fostering collaboration among technology providers, industry stakeholders, and security experts. Such partnerships could lead to the establishment of standardized protocols and universal guidelines for IoT devices. These shared standards would not only facilitate compatibility among devices from various manufacturers but also help ensure consistent security practices, including regular patching and vulnerability management.

Taken together, these enhancements aim to build a more secure, resilient, and forward-looking IoT ecosystem. In this environment, connected devices will be capable of seamless communication, intelligent decision-making, and robust protection of user data. These advancements will significantly strengthen the system's role in modern IoT security, ensuring its continued relevance and effectiveness in an increasingly complex digital landscape.

Acknowledgement:

Gratitude is extended to Dr. Mohammed Rafi for his valuable guidance, continuous support, and expert insights throughout the course of this research. Appreciation is also expressed to the Department of Studies in Computer Science and Engineering, University BDT College of Engineering, Davangere, for providing the necessary infrastructure and resources that made this work possible.

REFERENCES

Research Papers:

1. "Farooq et al. (2015) examined the challenges in securing IoT devices and highlighted the role of firmware updates in defense mechanisms." → [1] Farooq, M.U., et al..
2. Mittal, M.; Iwendi, C.; Khan, S.; Rehman Javed, A. Analysis of security and energy efficiency for shortest route discovery inlow-energy adaptive clustering hierarchy protocol using Levenberg-Marquardt neural network and gated recurrent unit forintrusion detection system. *Trans. Emerg. Telecommun. Technol.* 2021, *32*, e3997. [CrossRef]
3. Rehman, A.; Rehman, S.U.; Khan, M.; Alazab, M.; Reddy, T. CANintelliIDS: Detecting in-vehicle intrusion attacks on a controller area network using CNN and attention-based GRU. *IEEE Trans. Netw. Sci. Eng.* 2021, *8*, 1456–1466.
4. "Similarly, Roman et al. (2013) stressed the importance of proactive security measures in distributed IoT systems."→ [2] Roman, R., et al.
5. "Anomaly detection models using machine learning have been explored by Meidan et al. (2017), yet many approaches lack hardware-level analysis."→ [3] Meidan, Y., et al.
6. Ahmed, M.; Litchfield, A.T. Taxonomy for identification of security issues in cloud computing environments. *J. Comput. Inf. Syst.* 2018, *58*, 79–88. [CrossRef]
7. "Alrawais et al. (2017) proposed access control techniques for IoT security, but these do not address performance degradation or aging hardware."→ [4] Alrawais, A., et al.
8. Shahzad, F.; Javed, A.R.; Zikria, Y.B.; Rehman, S.u.; Jalil, Z. Future Smart Cities: Requirements, Emerging Technologies, Applications, Challenges, and Future Aspects. *TechRxiv* 2021. [CrossRef]
9. "In contrast, Li et al. (2018) emphasized the integration of cloud-based update mechanisms."→ [5] Li, S., et al.
10. Alzahrani, A.; Alalwan, N.; Sarrab, M. Mobile cloud computing: Advantage, disadvantage and open challenge. In Proceedings of the 7th Euro American Conference on Telematics and Information Systems, Valparaiso, Chile, 2–4 April 2014; pp. 1–4.