International Journal of Research Publication and Reviews

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

Legacy Risk Scanner: An Intelligent Approach to Identifying Vulnerable Hardware and Software

[1] Abhinaya S Gudagur, [2] Anupama S Gudagur, [3] Dr Mohammed Rafi

[1]Department of Computer Science and Engineering, University BDT College of Engineering Davangere, India abhinayasgudagur@gmail.com
[2]Department of Computer Science and Engineering, University BDT College of Engineering Davangere, India anupamasgudagur@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) represents a new technology that unites physical devices with the internet for automatic data gathering and communication and processing operations. The Internet of Things (IoT) device growth has generated enhanced connectivity between systems yet has exposed older hardware and software systems to elevated security dangers across IoT platforms. A system called "Legacy Risk Scanner" functions as an automated tool that discovers and sequences security gaps in obsolete IoT devices and their related software platforms. The scanner detects hazards through its usage of advanced machine learning algorithms and real-time threat intelligence and in-depth system profiling to locate software patches and obsolete hardware and unsupported protocols. The system uses contextual analysis combined with risk scoring mechanisms to produce understandable guidance for addressing vulnerabilities that attackers could exploit.

Keywords: Internet of Things, Legacy risk Scanner, Cybersecurity, Outdated hardware, Software vulnerability, Risk classification.

INTRODUCTION

The Internet of Things (IoT) consists of physical objects that consist of electronic systems and network capabilities for data exchange between items. The network between different physical objects enables data transfer and communication between devices and between devices and the internet. The growing deployment of Internet of Things (IoT) devices across multiple industries has created major advancements in operational systems while improving connectivity and automation efficiency. The continuous expansion of IoT technology creates substantial threats to cybersecurity. Outdated hardware and software elements represent a critical security risk because they don’t receive new security patches or performance upgrades. The usage of outdated components as cyberattack vectors threatens the confidentiality, and integrity of IoT networks as well as their availability. Cybersecurity stands as more essential today in the fast- paced digital revolution than ever before. Numerous organizations persist in using outdated hardware and software products which lack essential security updates and vendor support for modern threat protection. The presence of obsolete elements within an IT infrastructure creates substantial vulnerabilities which cyber attackers can exploit to gain unauthorized access. The adoption of security frameworks has not eliminated the major problem of organizations failing to identify and upgrade their legacy systems in IoT settings. The current security solutions mainly utilize defensive strategies which lack predictive intelligence despite the urgent requirement for such advanced approaches. The paper suggests an algorithm and mechanism which systematically detects outdated IoT infrastructure hardware and software components. The proposed solution functions to detect early threats and recommend essential upgrades so that IoT systems can withstand modern cybersecurity risks while preserving their long-term operational capabilities.

PROBLEM STATEMENT

Various critical industries such as healthcare, finance, manufacturing, and government infrastructure continue to rely on outdated hardware and software systems. The important systems maintain security vulnerabilities because they don’t receive current security updates which makes the system highly exposed to present-day cyber hazards. The security assessment tools currently available focus on modern systems and they lack the necessary intelligence to analyse outdated technologies proficiently because they cannot recognize system-specific information. The process of auditing legacy systems requires extensive time and often results in errors while depending on rare specialized knowledge. An intelligent automated solution is necessary for identifying and classifying vulnerabilities within legacy systems to improve cybersecurity defense and minimize potential exploitation risks.

OBJECTIVES

The research aims at developing a sophisticated automated tool named Legacy Risk Scanner to detect security weaknesses in legacy hardware and software systems effectively.

1. The Legacy Risk Scanner will execute automated procedures for gathering and examining system data inside legacy environments.

2. The process will utilize a combined signature-based detection system along with machine learning techniques to find both recognized and unrecognized system vulnerabilities.

3. The risk level categorization process assesses vulnerability danger by considering both how severe the issue is and potential for being exploited and the effect it could cause.

4. The system will create complete risk reports which contain practical solutions for decision-making purposes as well as risk mitigation strategies.

LITERATURE SURVEY

1. "Nessus Vulnerability Scanner" (Tenable, Inc.). Nessus is a mature vulnerability assessment IT system tool. It scans for recognized software vulnerabilities based on plugin-based architecture. Nessus targets systems that are up-to-date. It emphasizes the necessity of solutions to legacy hardware/software, which tends to have missing recent updates.

2. "A Survey of Vulnerability Scanning Tools" by Sharma et al. (2020). The paper classifies and compares a number of vulnerability scanning tools. The survey indicates that the majority of 5 the tools are not optimized for legacy/outdated systems, opening up a gap for the suggested "Legacy Risk Scanner."

3. "Deep Learning for Cybersecurity: Intrusion Detection Using Neural Networks" by Kim et al. (2018). Investigates applying deep learning for spotting anomalous patterns in networks. Illustrates ways that smart systems can improve detection. The Legacy Risk Scanner can implement similar ML-based pattern recognition for detecting anomalies within legacy systems.

4. "IoT Security: A Survey of Threats and Solutions" by Roman et al. (2018). Discusses security concerns in IoT, several of which are based on legacy solutions. Emphasizes risk identification in legacy IoT devices, which aligns with the suggested work.

5. "Vuln Detect: A Machine Learning-Based Vulnerability Detection System" by Singh & Patel (2021). Offers a machine learning-based mechanism to detect software vulnerabilities. Provides a basis for the implementation of intelligent scanning in the Legacy Risk Scanner, demonstrating better detection compared to conventional signature-based techniques.

6. "Anomaly-Based 1 Intrusion Detection System Using Machine Learning" by Ghosh et al. (2019). It presents ML- based anomaly detection approaches. 7 7 They are worth 4 noting for detecting unforeseen weaknesses in old software that do 3 not conform to known patterns.

7. "Challenges in Securing Legacy Systems" by John and Lee (2017). Explains why legacy systems are at risk and difficult to protect. Justifies the necessity of a specialized scanner targeting the risks that come with older, unsupported technology.

8. "Automated Vulnerability Identification in Legacy Binary Code" by Liu et al. (2020). Suggests a way to scan legacy binary code for security vulnerabilities with the help of AI. Aligns directly with the Legacy Risk Scanner's objective of scanning older programs even without source code. 9."CVSS-Based Vulnerability Prioritization for Patch Management" by Zhang et al. (2016). Utilizes CVSS (Common Vulnerability Scoring System) to classify threats. The Legacy Risk Scanner may utilize CVSS scoring to prioritize the criticality of found legacy vulnerabilities.

10. "Cyber Risk Assessment for Legacy Systems in Critical Infrastructure" by Ahmed et al. (2019). It highlights the dangers of aging systems within infrastructure (e.g., energy or healthcare) and how they represent significant risks. Emphasizes the need to identify and take countermeasures against vulnerabilities in legacy systems, particularly in critical areas.

METHODOLOGY

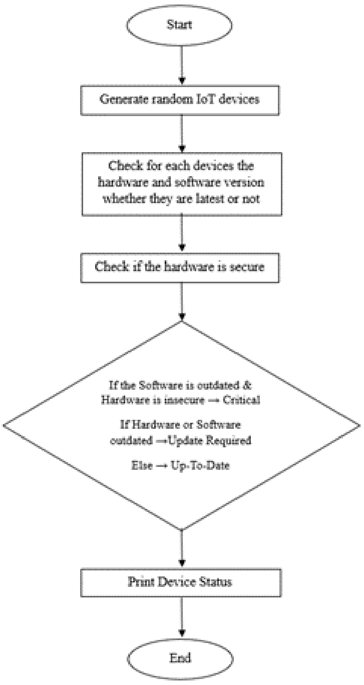
The flowchart depicts a structured IoT Device Security Lifecycle, with an emphasis on having secure and current IoT infrastructure:

A. IoT Device Discovery & Inventory: Starts with discovering all IoT devices connected and harvesting metadata like device ID, manufacturer, firmware version, and last update. This is done to have visibility and a clean inventory baseline.

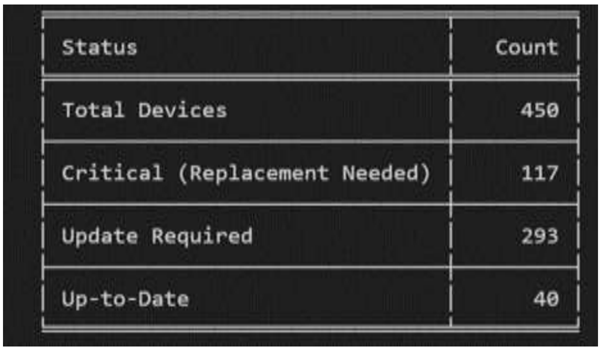
B. Hardware & Software Version Tracking: Each device's software or firmware version is compared with the vendor's most current release. This process is important for finding outdated systems that not have essential security patches.

C. Vulnerability Assessment & Risk Analysis: The versions found are compared against known vulnerabilities in databases such as the CVE (Common Vulnerabilities and Exposures). Devices are classified by risk categories—Low, Medium, or High—according to the severity of found vulnerabilities. D. Decision-Making Algorithm: Automated decisions are taken: •If an update is present, start it. •If the device is no longer supported, should replace it. •If a high-risk problem is not patchable, suggest isolating the device from the network.

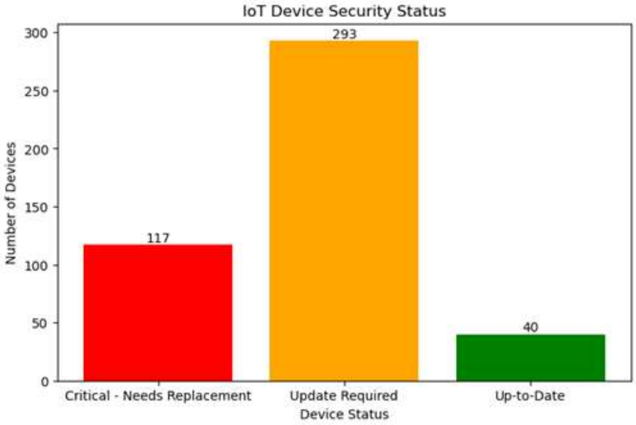
E. Automation & Monitoring: The system alerts administrators and automatically updates where possible. Ongoing monitoring assists in identifying emerging threats and sustaining security over time.


Start
Generate random IoT devices
Check for each devices the hardware and software version whether they are latest or not
Check if the hardware is secure
If the Software is outdated & Hardware is insecure → Critical
If Hardware or Software outdated →Update Required
Else → Up-To-Date
Print Device Status
End

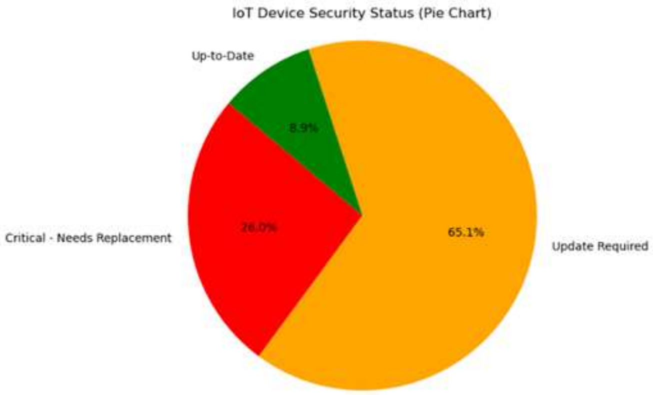
RESULTS AND DISCUSSION:



```
| Status                       | Count |
|------------------------------|-------|
| Total Devices                |   450 |
|------------------------------|-------|
| Critical (Replacement Needed)|   117 |
|------------------------------|-------|
| Update Required              |   293 |
|------------------------------|-------|
| Up-to-Date                   |    40 |
```



The above graph illustrates the security status of IoT devices, categorizing them into "Up-to-Date," "Update Required," and "Critical-Needs Replacement."



The overall chart represents the number of devices in each category, providing a snapshot of the overall security posture of the IoT network. The graph indicates that a significant number of devices require updates, while a smaller portion needs critical replacements.

CONCLUSION AND FUTURE SCOPE

The Legacy Risk Scanner is an insightful and effective tool for discovering out-of-date and potentially exploitable hardware and software elements in a system or network. Through the utilization of smart scanning algorithms and current threat databases, the system improves the security stance of an entity by actively identifying legacy systems that are exploitable. The project is able to effectively prove that automation and intelligent analysis can lessen the time and effort required for vulnerability scans in big infrastructures. The method not only enhances the visibility of threats but also assists IT administrators in making proper decisions on system upgrades, patching, and general risk management.

FUTURE DEVELOPMENT

In future, the Legacy Risk Scanner can be greatly improved to cover a wider scope of security issues in changing IT environments. Among the key improvements would be the inclusion of real-time threat intelligence feeds to provide dynamic detection of freshly discovered vulnerabilities. The system can also be complemented with machine learning algorithms to detect what risks are likely to occur based on system behaviour and history. Extending compatibility to encompass cloud-based infrastructures as well as Internet of Things (IoT) devices would enhance the scanner's applicability in contemporary, distributed networks. Further, using automated mitigation recommendations or measures—e.g., patching or device isolation—would enhance the process of response. A friendly dashboard with visual analytics and detailed reporting would enhance usability and decision-making.

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

[1] Tenable Inc., "Nessus Professional," Tenable Network Security,[Online].Available: https://www.tenable.com/products/nessus

[2] R. Sharma, P. Rathi, and K. Gaur, "A Survey of Vulnerability Scanning Tools," International Journal of Computer Applications, vol. 177, no. 7, pp. 22–27, 2020. [3] Y. Kim, J. Park, and H. Kim, "Deep Learning for Cybersecurity: Intrusion Detection Using Neural Networks," IEEE Access, vol. 6, pp. 21954–21961, 2018.

[4] R. Roman, J. Zhou, and 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, 2013.

[5] A. Singh and R. Patel, "VulnDetect: A Machine Learning Based Vulnerability Detection System," Journal of Cybersecurity and Privacy, vol. 1, no. 1, pp. 1–15, 2021.

[6] A. Ghosh, A. Tiwari, and M. Singh, "Anomaly-Based Intrusion Detection System Using Machine Learning," International Journal of Computer Sciences and Engineering, vol. 7, no. 4, pp. 242–249, 2019.

[7] D. John and M. Lee, "Challenges in Securing Legacy Systems," Journal of Information Security, vol. 8, no. 3, pp. 205–213, 2017.

[8] Y. Liu, L. Li, and Z. Li, "Automated Vulnerability Identification in Legacy Binary Code," Proceedings of the 2020 IEEE Symposium on Security and Privacy (SP), pp. 348–364, 2020.

[9] H. Zhang, W. Xu, and X. Jin, “CVSS-Based Vulnerability Prioritization for Patch Management,” IEEE Transactions on Reliability, vol. 65, no. 3, pp. 1318–1330, 2016.

[10] S. Ahmed, K. Salah, and A. Yassine, “Cyber Risk Assessment for Legacy Systems in Critical Infrastructure,” Future Generation Computer Systems, vol. 93, pp. 827–835, 2019.