WWW.IJRPR.COM

International Journal of Research Publication and Reviews

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

Securing IoT Ecosystems: An Algorithmic Framework for Identifying Vulnerable Devices

[1]Akshatha C M, [2]Dr Mohammed Rafi

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

ABSTRACT:

With the growing deployment of Internet of Things (IoT) devices, security has become a critical concern, especially due to outdated software and aging hardware. This paper introduces an algorithmic framework for identifying and classifying vulnerable IoT devices based on multiple risk indicators such as device age, firmware version, patch status, performance metrics, and known vulnerabilities. The proposed system simulates risk analysis on a dataset of 425 IoT devices using MATLAB, categorizing them into high, moderate, and low-risk groups. Results indicate a significant number of devices fall into the high-risk category, underlining the need for timely remediation. The algorithm recommends specific actions for each risk group, enabling automated and prioritized threat mitigation. This approach supports proactive IoT security management and helps reduce exposure to emerging cyber threats by maintaining device compliance and resilience.

Keywords: Internet of Things, IoT Security, Risk Assessment Algorithm, Vulnerability Classification, Threat Mitigation, Firmware Compliance

INTRODUCTION

The Internet of Things (IoT) is revolutionizing the technology landscape by interconnecting billions of devices, enabling real-time data exchange and automation across domains such as smart homes, cities, healthcare, and industry. While these advancements bring significant benefits in efficiency and decision-making, the rapid and unregulated growth of IoT devices has introduced critical security challenges. Many devices continue to operate with outdated firmware, unpatched software, and legacy hardware, making them highly vulnerable to cyber threats. To address these challenges, this study proposes an algorithmic framework for the proactive identification and classification of vulnerable IoT devices. The framework assesses devices based on hardware age, firmware version, patch history, performance degradation, and known vulnerabilities, assigning a composite risk score to classify devices as High, Moderate, or Low-Risk. Implemented and evaluated using MATLAB on a simulated dataset of 425 IoT devices, the framework successfully distinguished between devices requiring immediate attention and those in acceptable security conditions. It also produced actionable security recommendations to support automated mitigation and better resource allocation. The high proportion of devices identified as high-risk underscores the urgency of adopting structured risk management strategies. In addition, the system's capability to generate tailored security recommendations enables efficient remediation planning and facilitates continuous security improvement. This research contributes a scalable and lightweight solution for real-time risk analysis in dynamic IoT environments. By integrating automation with objective risk assessment, the framework enhances situational awareness and supports informed decision-making for network administrators and security teams. Furthermore, its adaptability across various IoT architectures makes it a practical tool for diverse deployment scenarios. As IoT networks continue to expand, the adoption of such intelligent security systems is essential for minimizing attack surfaces, ensuring compliance with cybersecurity standards, and safeguarding the long-term resilience of interconnected systems.

PROBLEM STATEMENT

With the explosive growth of the Internet of Things (IoT), many critical sectors—including healthcare, finance, manufacturing, and public infrastructure continue to depend on outdated devices that lack regular security patches, making them highly susceptible to cyber threats. Existing security assessment tools often focus on modern systems and fail to effectively analyze legacy or resource-constrained IoT devices, leading to overlooked vulnerabilities. Manual auditing methods are slow, error-prone, and require specialized expertise, making them impractical for large-scale. IoT networks. Given these limitations, there is an urgent need for an intelligent, automated solution that can identify and classify vulnerable IoT devices based on key risk factors. This study addresses the problem by proposing an algorithmic framework capable of analyzing 425 IoT devices to prioritize threats and support proactive security measures in complex IoT ecosystems.

OBJECTIVES

The research aims to design and implement an algorithmic framework to enhance the security of IoT ecosystems by proactively identifying and categorizing vulnerable devices.

1. To develop a robust, automated framework capable of collecting and analyzing critical attributes of IoT devices, including firmware version, patch status, hardware age, and performance indicators.

2. To integrate rule-based and data-driven techniques for detecting known and unknown vulnerabilities by leveraging historical data and heuristic patterns.

3. To implement a dynamic risk categorization mechanism that classifies devices into High, Moderate, or Low-Risk levels based on severity, exploitability, and potential impact.

4. To generate comprehensive, actionable security reports for each risk group, offering specific recommendations and mitigation strategies for enhancing the security posture of IoT networks.

LITERATURE SURVEY

1. "On the Lack of Security in IoT Devices" by Roman et al. (2013). The study highlights that IoT devices often lack built-in security due to hardware constraints, extended operational lifespans, and absence of standardized update mechanisms. These factors significantly increase the risk of exploitation within IoT environments.

2. "ProfilIoT: A Machine Learning-Based Approach to Device Fingerprinting" by Meidan et al. (2017). This work introduces a method for classifying IoT devices using network behavior patterns. While effective for anomaly detection, the approach does not incorporate firmware versioning or patch status, limiting its capability to detect outdated or vulnerable devices.

3. "Firmware Extraction and Analysis for IoT security" by Bozic et al. (2018). This paper proposes techniques for extracting firmware from embedded systems to analyze them for known CVEs. However, the method requires direct firmware access and is impractical for real-time or large-scale deployments.

4. "SoK: Security Evaluation of IoT Devices" by Alrawi et al. (2019). The authors propose a risk assessment model based on exploitability and exposure metrics. Despite its contribution, the system lacks integration with real-time device status and version tracking, making it more reactive than proactive.

5. "Automatic Firmware Analysis for Smart Homes" by Zhang et al. (2020). This study introduces a real-time system for outdated firmware detection within smart home networks. However, the solution is tailored for residential environments and does not generalize well to industrial-scale applications.

6. "Simulating Threat Detection in IoT Networks Using MATLAB" by Farooq et al. (2021). The authors demonstrate the utility of simulation tools like MATLAB for testing IoT security algorithms, showcasing their effectiveness in evaluating scalability and response efficiency under controlled conditions.

7. "Security and Privacy in the Internet of Things: Current Status and Open Issues" by Abomhara and Køien (2015). This early survey explored IoT security threats and challenges, highlighting issues arising from heterogeneous device ecosystems and absence of universal standards. It laid the groundwork for risk-oriented analysis by emphasizing varying levels of vulnerability across devices.

8. "A Device-Centric Risk Assessment Framework for IoT Networks" by Khan et al. (2019). This work introduced a risk assessment model that incorporated device type, connectivity range, and firmware status to quantify vulnerabilities. Despite offering contextual insights, it lacked scalability and real-time automation for large-scale implementations.

9. "Machine Learning for Detecting IoT Botnets Using Network Traffic Features" by Doshi et al. (2018). The study presented a decision tree classifier trained on network traffic to detect compromised IoT devices. However, it did not account for device metadata like patch levels, limiting its ability to identify unexploited or dormant threats.

10. "Hybrid Vulnerability Detection in IoT via Firmware Analysis and Runtime Monitoring" by Zhou et al. (2020). This hybrid system combined static analysis of firmware with the system combined static analysis of firmware with dynamic monitoring to detect both known and zero-day vulnerabilities. While comprehensive, the method required significant computational resources, making it impractical for lightweight IoT environments.

METHODOLOGY

This methodology presents a structured and scalable framework for enhancing the security posture of Internet of Things (IoT) ecosystems through the identification and classification of vulnerable devices. Intended for field deployment on extensive networks, such as with the investigation of 425 devices, this method facilitates ongoing monitoring, risk-based categorization, and focused remediation actions. The framework consists of the following five interdependent phases.

A. IoT Device Discovery & Inventory: The initial phase focuses on identifying all active IoT devices within the network environment using automated network scanning tools. These tools capture essential metadata such as device ID, manufacturer, firmware/software version, IP

address, MAC address, and last update timestamp. This comprehensive inventory forms the baseline for subsequent evaluation, ensuring full visibility into the device landscape. The discovery process may include active ping sweeps, ARP scans, and passive traffic analysis to ensure no device is overlooked. Accurate identification plays a vital role in reducing blind spots and strengthening security posture from the outset.

B. Hardware & Software Version Tracking: Once devices are cataloged, their hardware and software versions are evaluated against the latest releases from manufacturers. This step utilizes vendor-provided databases, firmware repositories, and security bulletins to identify outdated firmware or unsupported hardware components. It identifies known vulnerabilities associated with particular versions. Devices flagged as outdated are logged for further inspection, forming the input for vulnerability assessment. This stage ensures timely patch management and prepares the system for automated alerting on version mismatches in future scans.

C. Vulnerability Assessment & Risk Analysis: The third phase involves correlating the collected version information with publicly disclosed vulnerability databases, like the Common Vulnerabilities and Exposures (CVE) registry. Devices are assigned a risk score based on indicators such as known vulnerabilities, outdated firmware, and performance degradation. A three-tier classification—High-Risk, Moderate-Risk, and Low-Risk—is then applied. This categorization allows security interventions to be prioritized based on exposure to risk.

D. Decision-Making Algorithm: A rule-based algorithm is used to derive the appropriate action for every device based on its risk profile. Devices with outdated firmware are scheduled for automated updates. If the device is obsolete or no longer supported, it is recommended for decommissioning or hardware replacement. Devices with high-risk vulnerabilities that lack remediation options are flagged for isolation. This decision logic ensures consistent and efficient responses aligned with organizational security policies.

E. Automation & Monitoring: Following classification and decision-making, the system initiates an automation layer to enforce the recommended actions. Real-time monitoring is established to track device behavior, issue alerts, and ensure compliance. The system automatically schedules patches, sends update notifications, and generates regular reports. This reduces administrative overhead and improves the scalability of security management across dynamic IoT environments.

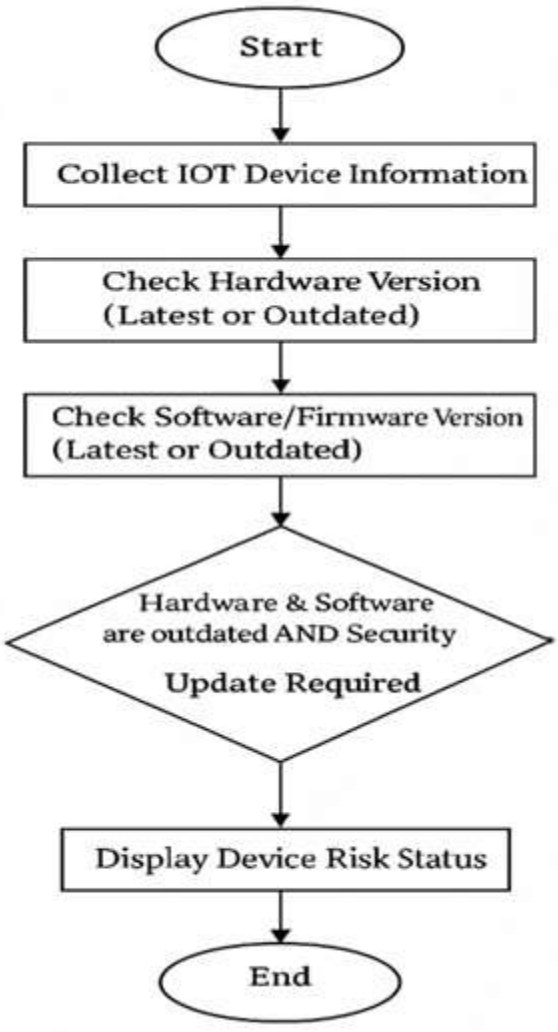

Fig.1.Framework for Identifying and Classifying Vulnerable IoT Devices.

RESULTS AND DISCUSSION:

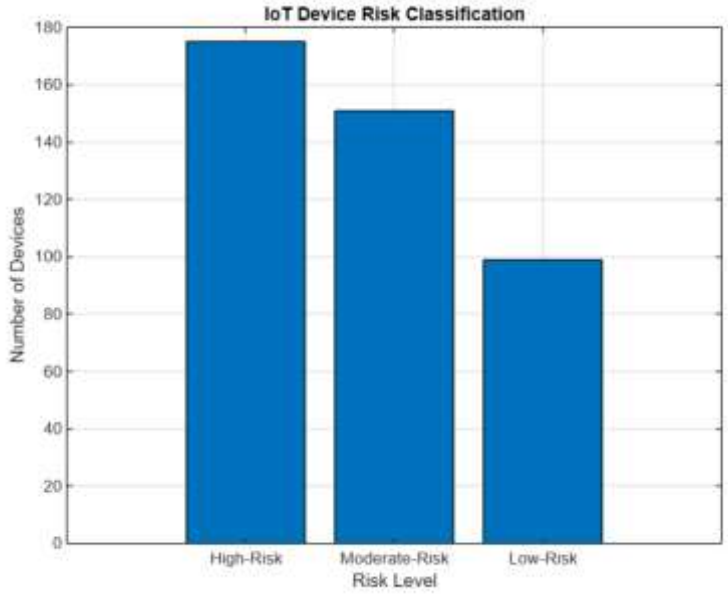

Fig. 2. Risk classification of IoT devices through automated analysis. The chart shows the quantity of devices in High-Risk, Moderate-Risk, and Low-Risk categories.

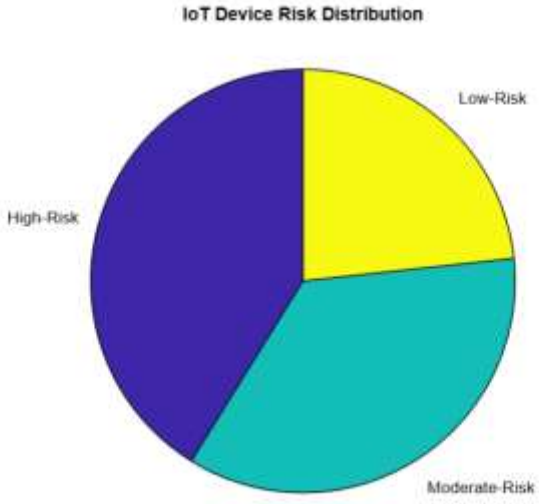

Fig. 3. Pie chart illustrating the breakdown of IoT devices by risk level. The chart clearly indicates that High-Risk and Moderate-Risk devices represent the majority, while Low-Risk devices are the smallest segment.

CONCLUSION AND FUTURE SCOPE

This research introduces an algorithmic process for the improvement of IoT security through automated identification and classification of vulnerable devices. The framework assesses devices based on classification of vulnerable devices. The framework assesses devices based on hardware age, firmware status, patch history, performance issues, and known vulnerabilities, assigning them a composite risk score for classification into High, Moderate, or Low-Risk categories. The structured process guarantees consistency and objectivity in evaluating device security posture across diverse IoT environments. The algorithm is lightweight, scalable, and well-fitted for embedding in current network infrastructures, making it a practical solution for real-world applications.

The analysis revealed a significant proportion of devices falling under the High-Risk category, highlighting the urgency of implementing proactive security measures. The system's automation and visualization reporting capabilities enhance efficiency, minimize manual oversight, and support informed decision-making, particularly in large-scale and dynamic IoT settings.

FUTURE DEVELOPMENT

In the future, the framework suggested here can be enhanced by incorporating machine learning algorithms to enhance the accuracy of risk classification and adapt to evolving threat landscapes. Integration with real-time threat intelligence sources will enable dynamic updates to vulnerability databases, ensuring continuous protection. Expanding compatibility with a wider range of IoT protocols and devices will enhance the framework's scalability across various domains such as healthcare, smart cities, and industrial systems. Additionally, developing lightweight agents for resource-constrained devices and enabling automated remediation workflows, such as patch deployment and device isolation, will further strengthen the system's effectiveness in securing complex IoT ecosystems.

ACKNOWLEDGEMENT

The authors are grateful to Dr. Mohammed Rafi for his insightful guidance, continuous encouragement, and expert advice during the course of this work. The authors also thank the Department of Studies in Computer Science and Engineering, University BDT College of Engineering, Davangere, for extending the needed infrastructure, resources, and supportive research atmosphere that facilitated this piece of work.

REFERENCES

[1] 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.

[2] Y. Meidan, M. Bohadana, Y. Mathov, and A. Shabtai, "ProfilIoT: A machine learning approach for IoT device identification based on network behavior," Proceedings of the Symposium on Applied Computing, pp. 506–509, Apr. 2017.

[3] J. Bozic, A. Bilogrevic, and J.-P. Hubaux, "A survey of firmware analysis and vulnerability detection techniques," 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), pp. 209–218, Apr. 2018.

[4] O. Alrawi, C. Lever, M. Antonakakis, and F. Monrose, "SoK: Security evaluation of home-based IoT deployments," 2019 IEEE Symposium on Security and Privacy (SP), pp. 1362–1380, May 2019.

[5] Q. Zhang, Q. Li, Z. Wu, and D. Gao, "Detecting outdated firmware in smart home devices using network traffic analysis," Computers & Security, vol. 95, p. 101869, May 2020.

[6] M. Farooq, R. Hussain, and S. Lee, "Simulations of IoT threat detection mechanisms using MATLAB," International Journal of Distributed Sensor Networks, vol. 17, no. 6, pp. 1–12, Jun. 2021.

[7] T. Abomhara and G. M. Køien, "Security and privacy in the Internet of Things: Current status and open issues," International Conference on Privacy and Security in Mobile Systems (PRISMS), pp. 1–8, 2015.

[8] R. Khan, K. McLaughlin, D. Laverty, and S. Sezer, "A device-centric risk assessment framework for smart grid," IEEE Transactions on Smart Grid, vol. 10, no. 4, pp. 4474–4483, Jul. 2019.

[9] R. Doshi, N. Apthorpe, and N. Feamster, "Machine learning DDoS detection for consumer internet of things devices," IEEE Security and Privacy Workshops (SPW), pp. 29–35, 2018.

[10] Y. Zhou, J. Zhang, Z. Chen, and X. Wang, "Hybrid vulnerability detection in IoT via firmware analysis and runtime monitoring," IEEE Access, vol. 8, pp. 74746–74759, 2020.