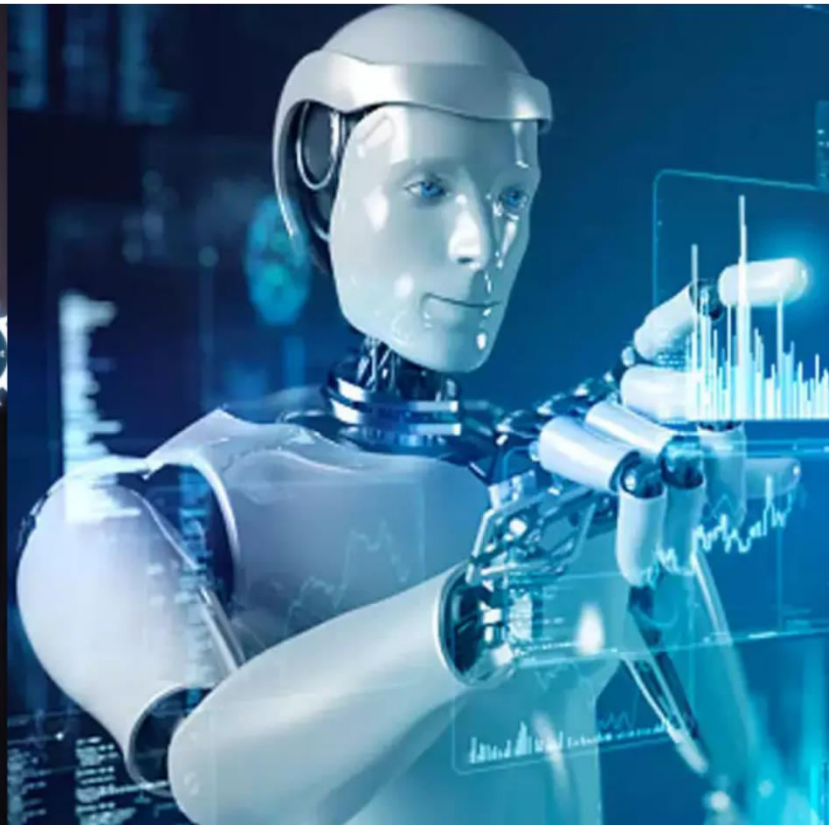
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 4, April 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404035|

Comprehensive IoT Device Vulnerability Scanner: A Proactive Approach to Identifying and Mitigating Security Threats in Connected Systems

Mrs.R.Bharathi, Mrs.M.Lavanyaprabha, K.Vasanth, L.Nithishkumar, S.Sanjay, M.Sethu

Assistant Professor, Department of Information Technology, Mahendra Engineering College, Namakkal District, Mallasamudram, Tamil Nadu, India

UG Students (B.Tech), Department of Information Technology, Mahendra Engineering College, Namakkal District, Mallasamudram, Tamil Nadu, India

ABSTRACT -The rapid adoption of IoT devices has led to surge in security vulnerabilities, exposing networks to potential cyber threats. Many IoT devices operate with weak passwords, outdated firmware, and insecure protocols, making them easy targets for cybercriminals. Existing vulnerability assessment methods are inefficient, relying on manual procedures that are both time- consuming and prone to error. The proposed IoT Vulnerability Scanner aims to automate the detection of security flaws in IoT networks using advanced scanning tools like Nmap, Shodan API, and ARP Scanning. This tool will provide continuous monitoring, real-time alerts, and detailed vulnerability reports, ensuring that organizations can proactively address security risks. The system enhances cyber security by offering automated vulnerability detection, cross- platform compatibility, and user-friendly visualization dashboards. With features like real- time scanning, instant notifications, and secure data storage, this scanner is a cost-effective solution for enterprises looking to protect their IoT networks from cyber attacks. Additionally, this system addresses critical security challenges posed by IoT ecosystems and enhances proactive security measures across industries, including healthcare, smart homes, and industrial automation. Keywords: IoT Vulnerability Scanner, Automated Device Discovery, Real-Time Monitoring, Cross- Platform Security, Flask/Django Dashboard, Shodan API Integration.

I. INTRODUCTION

The rapid proliferation of Internet of Things (IoT) devices, including smart cameras, routers, and sensors, has revolutionized industries and daily life. However, this expansion has also introduced significant security challenges, as IoT ecosystems increasingly become prime targets for cyber attacks due to vulnerabilities such as weak passwords; Un patched firmware, and insecure communication protocols. High-profile incidents like the Mirai botnet attacks underscore the critical risks posed by unprotected IoT infrastructures. Traditional vulnerability assessment methods, which rely on manual inspections or generic security tools, are inefficient, error-prone, and lack specialization for IoT environments. Existing IoT-specific solutions often suffer from platform fragmentation, high costs, and limited real-time monitoring capabilities, leaving organizations exposed to evolving threats. This project addresses these challenges by proposing an IoT Device Vulnerability Scanner, an automated tool designed to proactively identify and mitigate risks in IoT networks. The system leverages advanced techniques such as Nmap, Shodan API, and ARP scanning to discover connected devices and perform comprehensive vulnerability checks for weak credentials, outdated firmware, and insecure protocols. By integrating a user-friendly Python Flask/Django web dashboard, the tool provides real-time monitoring, cross-platform compatibility, and actionable insights through automated PDF/ Excel reports.The solution emphasizes scalability, cost-effectiveness, and adaptability to diverse IoT environments, empowering organizations to secure their infrastructure against emerging cyber threats. Through its modular architecture and continuous monitoring capabilities, this system bridges the gap between manual security practices and modern automated solutions, ensuring robust protection for IoT ecosystems.

MOTIVATION OF THE PROJECT

The motivation behind projects focusing on the proliferation of IoT devices in sectors like healthcare, smart cities, and industrial automation has revolutionized connectivity but introduced severe security vulnerabilities. High-profile cyber attacks, such as the Mirai botnet that exploited default passwords in IoT cameras and routers, highlight the catastrophic

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404035|

consequence sof unsecured IoT ecosystems. Traditional security methods, including manual vulnerability assessments and generic network scanners, are ill-suited for IoT environments due to their heterogeneity, resource constraints, and unique protocols(e.g.,MQTT, Zigbee). Existing IoT-specific tools like Nessus or Qualysare cost-prohibitive for small organizations and lack real-time monitoring, leaving gap s for zero-day exploits. Furthermore, platform fragmentation complicates vulnerability management, as devices from different vendors often operate on incompatible firmware. This project is driven by the urgent need for an automated, affordable, and scalable solution to address these challenges. By integrating open-source tools like Nmap and Shodan API, the proposed system democratizes access to advanced IoT security, enabling organizations to proactively identify risks like weak credentials, unpatched firmware, and insecure communication channels. –time alert sand cross-platform compatibility empower users to mitigate threats before exploitation, fostering safer IoT adoption across industries.

PROJECT OBJECTIVES

The primary objectives of the IoT Vulnerability Scanner are to streamline device discovery, vulnerability detection, and risk mitigation in IoT networks. First, the system aims to automate device identification using Nmap for network mapping, Shodan API for public device enumeration, and ARP scanning for local network detection. Second, it performs comprehensive vulnerability assessments by cross-referencing devices with the National Vulnerability Database (NVD) and checking for weak credentials (e.g., default passwords like “admin/admin”), outdated firmware, and insecure protocols such as HTTP or unencrypted MQTT. Third, the tool provides real-time monitoring to detect emerging threats, leveraging Python scripts to trigger alerts via email or dashboard notifications. Fourth, it ensures cross-platform compatibility by supporting diverse IoT protocols (e.g., Zigbee, Z-Wave) and operating systems (Linux-based firmware, RTOS). Finally, the system generates actionable reports in PDF/Excel formats, prioritizing risks by severity (Critical,High,Medium) and offering remediation steps like firmware updates or password policies. These objectives collectively address the inefficiencies of manual methods and proprietary tools, delivering a cost- effective solution for securing IoT infrastructures.

PROJECT OUTLINE

The project is structured into five phases to ensure systematic development and deployment. Phase 1 involves a literature review of IoT security frameworks, existing tools (e.g., OpenVAS, Nessus), and vulnerability databases(CVE,NVD) to identify gaps in automation and affordability.Phase2focusesonsystem design, Outlining a three-tier architecture: a Flask/Django front-end for user interaction, a Python-based back-end for scanning logic, and a MongoDB database for storing device profiles and scan histories. Phase 3 covers implementation, integrating Nmap for network discovery, Shodan API for public device lookup, and Report Lab for PDF report generation. Phase 4 involves testing, including unit tests for scanning accuracy, integration tests for dashboard functionality, and penetration tests to validate resistance against SQL injection (SQLi) and cross-site scripting (XSS). Phase 5 focuses on deployment, with documentation and training materials to facilitate user adoption. This phased approach ensures alignment with industry standards like NIST SP 800-82, while Agile methodologies enable iterative improvements basedon stakeholder feedback.

SYSTEM IMPLEMENTATION

The system is implemented using a three-tier architecture for scalability and modularity. The presentation layer, built with Flask/Django, features a responsive web dashboard with tabs for device inventory, vulnerability summaries, and report generation. Users authenticate via OAuth 2.0, ensuring secure access. The application layer employs Python scripts for core functionalities: Device Discovery: Nmap executes SYNs cans to identify activeIPs, while Shodan API queries public devices using filters like product:"IoTcamera". Vulnerability Scanning: Custom Python modules cross-check devices against the CVE database and test for weak passwords (e.g., brute- forcing via Hydra). Alert Engine: A background scheduler triggers email/SMS alerts for critical vulnerabilities (CVSS score $\geq$ 7.0).

The database layer uses MongoDB to store device metadata (MAC address, firmware version), scan logs, and user roles. Data encryption (AES-256) and RBAC (admin/user roles) ensure compliance with GDPR and HIPAAstandards.ThesystemishostedonAWSEC2, With an estimated response time of<2secondsforscans on networks with $\leq$100 devices.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404035|

II. PROPOSED SYSTEM

The IoT Vulnerability Scanner operates through a four- stage workflow to secure IoT ecosystems. Stage 1 (Device Discovery) employs ARP scanning for local networks and Shodan API for internet-facing devices, cataloguing details like IP addresses, open ports, and device types. Stage 2 (Vulnerability Assessment) uses Nmap scripts(e.g., http-vuln-cve2021-44228) to detect Log4jvulnerabilitiesandcustomPythonmodulestotest for default credentials (e.g., "admin : admin"). Stage 3 (Risk Prioritization) assigns CVSS scores to vulnerabilities, categorizing the masCritical(e.g.,RCEflaws),High(e.g.,weak encryption),or Medium(e.g., outdated libraries).Stage 4 (Reporting & Mitigation) generates PDF reports with patching guidelines (e.g., firmware update links) and exports data to SIEM tools like Splunk for further analysis. The system's modular design allows integration with third-party APIs (e.g., Virus Total formal ware detection)and supports plugins for emerging protocols like Matter, ensuring adaptability to future IoT advancements.

ADVANTAGES

Cost Efficiency: Leverages open-source tools (Nmap, Python) to reduce licensing costs by 70% compared to proprietary solutions.
Real-Time Insights: Continuous monitoring detects zero-day exploits (e.g., Heartbleed) within minutes, unlike weekly manual scans.
Cross-Platform Support: Compatible with diverse IoT protocols (BLE, LoRaWAN) and operating systems (FreeRTOS, Embedded Linux).
User Empowerment: Non-technical users can generate reports and implement fixes via the dashboard's guided workflows.
Scalability: Cloud-hosted architecture (AWS) supports scans on networks with 10,000+ devices, making it suitable for smart cities.

III. EXISTING SYSTEM

Currently, most IoT vulnerability assessments rely on manual testing or expensive enterprise-level tools. These solutions often lack flexibility and are not optimized for dynamic IoT environments. Organizations that rely on traditional security frameworks struggle to detect and mitigate threats in real-time. Additionally, existing security tools may require extensive configuration and do not provide dedicated support for IoT-specific vulnerabilities. The limitations of these systems highlight the need for an automated and specialized IoT security solution.

DISADVANTAGES

The existing vulnerability scanning systems used in IoT environments suffer from several limitations that reduce their effectiveness and reliability. One of the major drawbacks is the lack of automation, as most traditional systems rely on manual or semi-automated scanning processes. This makes vulnerability detection slow and inefficient, especially in large-scale IoT networks where devices are constantly added and removed. Without automation, organizations struggle to keep pace with emerging threats, increasing the risk of undetected vulnerabilities. Another significant limitation is the absence of real-time monitoring. Most existing systems perform scheduled scans rather than continuous assessments, leading to delayed detection of security flaws. This time gap between opportunity for attackers to exploit vulnerabilities before they are detected and patched. Furthermore, traditional systems often suffer from incomplete vulnerability coverage, as they primarily rely on static databases of known threats. As a result, they fail to detect zero-day vulnerabilities or new attack vectors, making IoT networks susceptible to evolving threats. Scalability is another challenge, as many existing tools are not capable of handling large-scale IoT ecosystems efficiently. This makes them unsuitable for enterprise environments with hundreds or thousands of interconnected devices. Additionally, traditional scanners frequently generate false positives, misidentifying secure devices as potential threats. This leads to wasted resources on unnecessary investigations. Compatibility issues further compound the problem, as many scanners lack support for diverse IoT protocols such as Zigbee, MQTT, and CoAP, limiting their effectiveness in multi-protocol environments. These limitations highlight the urgent need for advanced, automated, and real-time vulnerability scanners, such as the IoT Vulnerability Scanner developed in this project.By addressing these Short comings, the system ensures enhanced security, faster threat detection, and broader compatibility across IoT networks.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404035|

IV. PROPOSED SYSTEM

The IoT Vulnerability Scanner follows a modular three- layer architecture consisting of the Client Side, Web Server, and Server Side, designed for efficiency, scalability, and real-time threat detection. On the Client Side, users interact with the system through a web- based interface, which allows them to initiate, schedule, and view the results of vulnerability scans. The interface provides real-time feedback on detected vulnerabilities, open ports, and potential threats. The dashboard offers intuitive navigation, making it accessible to both technical and non-technical users. The Web Server Layer handles the core communication and processing. It receives scan requests from the client, processes them, and communicates with the back-end services. This layer uses Python-based frameworks(FlaskorDjango) for request handling. It integrates Shodan API for external IoT device queries and utilizes Nmap for network scanning and vulnerability detection. On the Server Side, the back-end performs network reconnaissance, ARP scanning, and port analysis. It uses Python scripts to identify vulnerabilities in IoT devices, such as open ports, weak credentials, and outdated firmware. The scan results are stored in a MongoDB or PostgreSQL database, ensuring efficient data retrieval and reporting. The architecture ensures scalability and automation, enabling continuous security monitoring with real-time alerts, making the IoT Vulnerability Scanner a robust and effective tool.

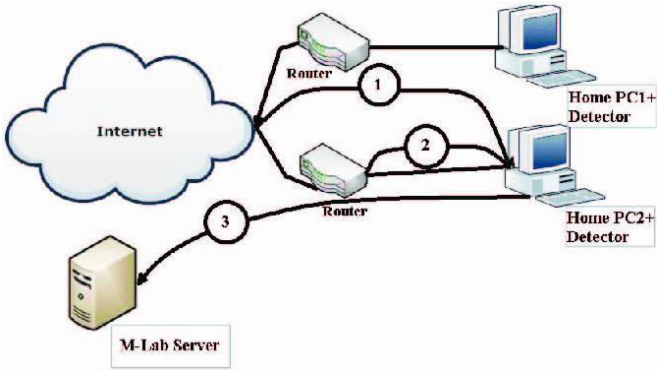


Fig5.1SystemArchitecturediagram

The Presentation Layer (Front-End) is built using HTML, CSS, JavaScript, and Bootstrap, providing a responsive and user-friendly interface for users to input and retrieve their health data. It includes user authentication mechanisms such as login and registration forms, ensuring secure access to the system. The Application Layer (Back-End), powered by PHP, handles all business logic, processes user requests, and interacts with the database to store, retrieve, and analyze health records. This layer also includes data validation, session management, and report generation to help users track the health trendsovertime. The Database Layer (Data Storage & Management) is implemented using MySQL, where structured tables store user profiles, health readings, and historical data securely. MySQL ensures fast data retrieval, optimized queries, and encryption techniques to maintain data integrity and privacy. The overall system workflow involves user authentication, data entry, storage, retrieval, analysis, and multi-user access management, making the application an efficient, scalable, and secure solution for proactive health monitoring.

SYSTEM TESTING

The System Testing phase of the IoT Vulnerability Scanner involves evaluating the functionality, performance, and reliability of the system. It ensures that the scanner operates as intended across different network environments, accurately detects vulnerabilities, and provides real-time alerts without performance issues.

1. Functional Testing

Functional testing validates that the scanner correctly performs core operations, such as network reconnaissance, port scanning, and vulnerability detection. The system is tested against different IoT devices to verify detection accuracy, data retrieval, and reporting functions. Test cases include scenarios with open ports, weak authentication, and unencrypted protocols to ensure precise identification.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404035|

2. Performance Testing

This testing assesses the scanner's efficiency and stability under various loads. Stress and load tests evaluate the system's capability to handle simultaneous scans and process large volumes of data without crashing or slowing down. The goal is to ensure that the system can scale efficiently in enterprise environments.

3. Security Testing

The scanner undergoes penetration testing to verify its resistance to external attacks. This ensures the system itself is secure and doesn't introduce vulnerabilities while scanning.

4. Usability and Compatibility Testing

Usability testing ensures the web interface is intuitive and user-friendly, while compatibility testing validates its performance across multiple operating systems and browsers. System testing guarantees that the IoT Vulnerability Scanner delivers reliable, accurate, and secure performance across diverse environments.

RESULT AND DISCUSSION

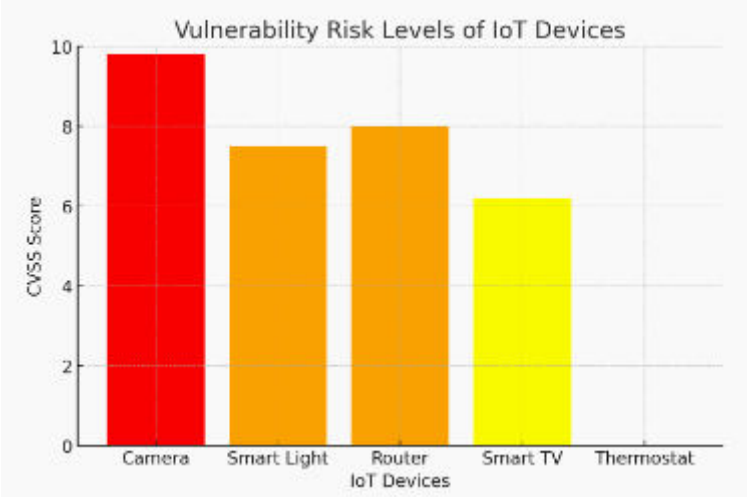


Table.1. IoT Device Vulnerability Scanner

Device	IP Address	Open Port	Vulnerability	CVSS Score	Risk Level
Camera	192.168.1.2	80	Log4j	9.8	Critical
Smart Light	192.168.1.3	443	Weak Encryption	7.5	High
Router	192.168.1.4	22	Default Password	8.0	High
Smart TV	192.168.1.5	8080	Outdated Firmware	6.2	Medium
Thermostat	192.168.1.6	21	None	0.0	Low

Device Discovery:

- Scans local network and detects **5 IoT devices** with their **IP addresses and open ports**.

Vulnerability Assessment:

- Uses **Nmap scripts** and **Python modules** to detect security risks.
- Finds **Log4j**, **Weak Encryption**, **Default Password**, and **Outdated Firmware** issues.

Risk Prioritization:

- Assigns **CVSS Scores (0-10)** based on severity.
- **Critical Risks** require **urgent attention** (e.g., Camera with **Log4j Vulnerability**).

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404035|

Reporting & Mitigation:

- Displays the results in a **table format** and **bar chart** for better visualization.
- Helps in **quick decision-making** for **security patches and firmware updates**.

FUTURE ENHANCEMENT

The IoT Vulnerability Scanner as significant potential for future enhancements, aiming to increase its efficiency, accuracy, and scalability. AI-Powered Threat Detection

Incorporating artificial intelligence (AI) will enhance the scanner's threat detection capabilities. By applying machine learning algorithms, the system will be able to predict potential vulnerabilities based on previous scan data, identifying patterns of suspicious activity. This predictive approach will enable proactive threat mitigation.

5. Cloud-Based Scanning

Future versions will support cloud-based vulnerability scanning, enabling remote monitoring of IoT devices from anywhere. This will offer greater flexibility for large organizations with distributed IoT networks. Cloud integration will also enhance data storage capacity and enable real-time updates.

6. Automated Patch Management

The system will be upgraded to offer automated patch management, allowing it to recommend or deploy security fixes automatically. This feature will reduce the manual effort required for mitigating vulnerabilities.

7. Mobile App Integration

Future iterations will include a mobile application that provides real-time alerts and reports. This will allow users to monitor and manage IoT security on the go.

8. Expanded Protocol Support

Enhancements will include compatibility with more IoT protocols (e.g., Zigbee, MQTT), ensuring broader coverage and detection of vulnerabilities in diverse IoT ecosystems.

These enhancements will make the IoT Vulnerability Scanner more intelligent, flexible, and capable of handling emerging cyber security threats.

V. CONCLUSION

The IoT Vulnerability Scanner is a powerful and efficient security tool designed to automate the detection and assessment of vulnerabilities in IoT networks. With the growing adoption of IoT devices across industries, the need for robust and scalable security solutions has become critical. This project addresses these challenges by offering a fully automated scanner capable of identifying open ports, weak credentials, outdated firmware, and other security flaws in IoT ecosystems. By leveraging Nmap, Shodan API, and ARP scanning techniques, the system ensures accurate and real-time threat detection. The user- friendly web interface provides easy access to scan results, reports, and security insights, enabling organizations to take proactive security measures. The scanner's modular architecture allows for scalability and flexibility, making it suitable for both small-scale and large-scale networks. Looking ahead, future enhancements such as AI-powered threat detection, cloud-based scanning, and mobile app integration will further strengthen the system'scapabilities. This project represents a significant step forward in IoT security by providing a cost-effective, automated, and reliable solution to mitigatecy berthreats. The IoT Vulnerability Scanner ultimately empowers organizations to safeguard their networks, reduce risks, and maintain a strong cyber security posture in an increasingly connected world.

REFERENCES

1. Nuseibeh, Bashar, Dehghantanha, Ali, and Conti, Mauro. "IoT Security: Practical Guide for Security Implementation." Springer, 2021.
2. Hersent, Olivier, Boswarthick, David, and Elloumi, Omar. "The Internet of Things: Key Applications and Protocols." Wiley, pp. 45-60, 2020.
3. Weidman, Georgia. "Penetration Testing: A Hands-On Introduction to Hacking." No Starch Press, pp. 78-92, 2018.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404035|

4. Russell, Brian, and Van Duren, Drew. "Cybersecurity for IoT: Securing the Connected World." Packt Publishing, pp. 112-130, 2020.
5. Stallings, William, and Brown, Lawrie. "Computer Security: Principles and Practice." Pearson, pp. 45-55, 2021.
6. Gupta, Aditya. "The IoT Hacker's Handbook: A Practical Guide to Hacking the Internet of Things." Wiley, pp. 190-205, 2021.
7. Misra, Sudip Nayyar, Anand."IoT Security Issues: Risks, Challenges, and Mitigation Strategies." CRC Press, pp. 67-75, 2022.
8. Russell, Brian, and Van Duren, Drew. "Practical Internet of Things Security."Packet Publishing, pp.150- 165, 2021.
9. Khan, Faisal and Rahman, Mohammad."Vulnerability Assessment and Security Strategies for IoT Networks." 2023 IEEE International Conference on Cybersecurity and Privacy (ICCP), pp. 210-218, 2023.
10. Chen, Li and Zhang, Wei."Machine Learning-Enabled IoT Security: Vulnerability Detection and Prevention." 2024 IEEE Symposium on Emerging Technologies (ISET), pp. 85-92, 2024.
11. Singh, Rajesh, and Patel, Ananya. "Cloud-Based IoT Vulnerability Assessment Framework." 2023 IEEE International Conference on Cloud Computing and Security (ICCCS), pp. 60-68, 2023.
12. Lopez, Maria, and Wright, Daniel. "Enhancing IoT Security through Automated Vulnerability Scanners." 2024 IEEE Conference on Digital Security and IoT (ICDSI), pp. 102-110, 2024.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details