International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 06 June 2025, pp: 519-525 www.ijaem.net ISSN: 2395-5252

Hacking the Internent of Things (Iot): Security Risks in Connected Devices

Nakibuuka Jamirah, Mohamad Fadli bin Zolkipli
School of Computing, College of Arts and Sciences, Universiti Utara Malaysia
06010 Sintok Kedah, MALAYSIA.

Date of Submission: 20-06-2025 Date of Acceptance: 30-06-2025

ABSTRACT: Therapid expansion of the Internet of Things (IoT) has transformed modern living enabling seamless connectivity, intelligence and automation across homes, enterprises, healthcare systems, transportation and critical infrastructures. As billions of IoT devices become increasingly integrated into daily life and national infrastructure, they introduce a wide and complex attack surface. Most of these IoT devices are designed with limited security features often relying on default passwords or weak authentication mechanisms which makes them easy targets for hackers seeking to gain unauthorized access and once compromised can be manipulated to serve malicious purposes including data theft, privacy invasion and participation in large cyberattacks. Key findings highlight the prominent frequency use of attack vectors such as hijacking, data breaches, firmware manipulation and botnet participation emphasizing the need for security-by-design principles and AI-driven threat detection mechanisms in enhancing the real-time threat monitoring and response. Ultimately, this research aims to contributing to the development of proactive cybersecurity measures, ensuring the integrity and resilience of IoT ecosystems in the face or emerging threats. The insights are intended to support device manufacturers, developers, policymakers, and security practitioners in building more resilient IoT ecosystems that can withstand evolving cyber threats in an increasingly connected world.

KEYWORDS: Security-by-design, Ethical Hacking, Edge Computing, Penetration Hacking.

I. INTRODUCTION

The Internet of Things (IoT) refers to interconnected devices embedded with sensors, software, and other technologies enabling them to collect, exchange and processdata autonomously. (Chen, 2024). These devices include smart home gadgets like thermostats and lights, wearable fitness trackers, industrial sensors, connected vehicles and healthcare monitors. TheseIoT devices are used to accelerate across industries in sectors like transportation, healthcare, manufacturing, smart home automation (Laghari, 2024) and also helped businesses increase efficiency, real-time monitoring and data-driven decision making. (Nag, 2024). Many devices are released to market with inadequate testing, insecure default configurations or proprietary protocols that hinder security audits (Li, 2023). There are diverse devices and manufacturers that lead to inconsistence in security policies and standards (Wei, 2024). A key concern is that IoT devices function in unattended environments making them easy physical targets and yet once compromised, can be used to spy on users, steal data, launch denial-of-service(DoS) attacks, or act as stepping stones into large networks (Nandhini, 2024) (Nag, 2024).

Additionally, regulatory and compliance efforts have not kept pace with technological development. As stated by (Vescovi, 2023), there is lack of global cooperation standards for IoT cybersecurity which has led to inconsistent protection across regions and yet many users remain unaware of the risks posed by these devices especially when it comes to data collection, storage and third-party access. As the technology advances, regulations and industry standards are evolving to address IoT security concerns advocating for secure-by-design principles that enforce stronger encryption access control mechanisms and compliance requirements.

Recent studies highlight cases of IoT security failures, with vulnerabilities in smart home systems that allow attackers to hijack connected appliances (Laghari, 2024).The rapid expansion of the Internet of Things (IoT) has transformed modern living enabling seamless connectivity, intelligence and automation across homes, enterprises, healthcare systems, transportation and critical infrastructures. Most of these IoT devices are designed with limited security features often relying on default passwords or weak authentication mechanisms which makes them easy

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 06 June 2025, pp: 519-525 www.ijaem.net ISSN: 2395-5252

targets for hackers seeking to gain unauthorized access and once compromised can be manipulated to serve malicious purposes including data theft, privacy invasion and participation in large cyberattacks.

Key findings highlight the prominent frequency use of attack vectors such as hijacking, data breaches, firmware manipulation and botnet participation emphasizing the need for security-by-design principles and AI-driven threat detection mechanisms in enhancing the real-time threat monitoring and response.

Ultimately, this research aims to contributing to the development of proactive cybersecurity measures, ensuring the integrity and resilience of IoT ecosystems in the face or emerging threats. The insights are intended to support device manufacturers, developers, policymakers, and security practitioners in building more resilient IoT ecosystems that can withstand evolving cyber threats in an increasingly connected world.

IoT devices have become deeply embedded in daily lives and their compromise not only leads to data breaches but also to physical harm and disruption of critical services or businesses (Xu, 2024). Therefore, this study addresses some of the cybersecurity challenges in the modern digital ecosystem. Additionally, it explores AI-driven intrusion detection mechanisms that enhance the ability to identify and mitigate cyber threats in real time. (Radanliev, 2024).

II. LITERATURE REVIEW

The literature review integrates research from various scholars and technical sources to examine the underlying structure of IoT systems, their common security vulnerabilities, the real-world cyberattacks, challenges faced by users with device security and the emerging technological and regulatory developments aimed at mitigating these risks.

Overview of IoT architecture components

The internet of things (IoT) represents a network of interconnected devices equipped with sensors, embedded systems and communication modules, allowing for seamless interaction between physical and digital environments (Chen, 2024). This consists of three layers inclusive: perception layer which collects raw data through sensors and electricals that enable real-time monitoring and automation, the network layer that facilitates data transmission across networks using protocols like Bluetooth, Wi-Fi often vulnerable to security vulnerabilities because of the weak encryptions or the authentication mechanisms, and the application layer that delivers actionable services like smart home applications and industrial IoT systems to users. (Chen, 2024) (Laghari, 2024).Each layer represents unique security challenges, necessary for robust security frameworks to mitigate risks effectively like network protocols in the communication layer can be intercepted while in the perception layer, unprotected sensors can be physically tampered with (Wei, 2024).

The reliance on low-cost and constrained devices limits the implementation of traditional security mechanisms like encryption, intrusion detection system(IDS) and regular software updates. Modern IoT ecosystems encompass a wide variety of hardware, firmware and communication protocols creating significant challenges in maintaining consistent and scalable security controls (Singh, 2024).

Common IoT vulnerabilities

IoT devices commonly lack standardized security measures making them targets for cyberattacks some of the common vulnerabilities include: weak authentication and default credentials where many IoT devices are shipped with default passwords that users neglect to change or are unable to change leaving them open to exploitation. (Li, 2023).

According to McWeeney (2024) vulnerabilities also extend to communication stack where protocols like LoRa used in Low Power wide Area Networks(LPWAN) lacks strong payload confidentiality, making them susceptoble to eavesdropping and manupulation like issues magnified when deployed in large-scale smart city or industrial IoT projects.

Li (2023) show a study of how common household IoT products, including smart toasters and locks can be compromised due to haedcoded credentials and open slots. Further highlighting on these vulnerabilities, Singh (2024) shows that many devices integrate with cloud services using insecure APIs leaving them exposed to unauthorized access and dat leackage.

Preview of attack case studies

Numerous real-world cyberattack scenarios of weaknesses have been highlighted in IoT security inclusive:

The Mirai Botnet Attack that occurred in 2016 where the Mirai malware exploited weak credentials in IoT devices, including routers and cameras creating massive botnet that launched distributed denial-of-servise (DDoS) attacks

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 06 June 2025, pp: 519-525 www.ijaem.net ISSN: 2395-5252

disrupting major websites and intenet services (Singh, 2024).

Vallabhaneni (2024) highlights the impact of IoT-related data breaches on daily-life devices and exlores how the attackers can infiltrate home automation systems to control smartTVs, cameras, refrigderators violating user privacy and posing physical safety risks. These systems are also targeted by ransomware where criminals gain control over the devices like security cameras and locks demanding ransom payments in exchange for restoring user access (Xu, 2024).

In another study, Radanliev (2024) states the use of artificail inteligence by attackers to develop sophisicated malware capable of mimicking legiyimate device behaviour to avoid detection marking a shift in the landscape from the traditional signature-based attacks to AI-powered context-awareness thtreats. Also a case from the medical IoT exploits where haelthcare IoT devices like insulin pumps and pacemakers posed lief-threatening risks from reports that suggested that attackers could remotely manipulate these devices to lead to severe damage to patients as they do not have enough cybersecurity protection.

Security challenges in consumeer devices

Common IoT devices are mainly designed for ease of use and affordability but not cybersecurity so these devices come with poor encryption, lacking proper access controls and do not receive regular firmware updates (Oduwale, 2024) making them stand a high chance of being co-opted into botnets or used as attack vectors against other devices.

Many IoT devices have limited processing capabilities that restricts the implementation of advanced security measures like encryption and multi-layer authentication (Radanliev, 2024).

Intergrating cyber resilience principles with IoT security strategies is paramount for mitigating emerging cyber threats and fortifying the interconnected digital landscape (Sahu, 2024). These devices, while enhancing operational efficiency and connectivity, also introduce unprecedent vulnerabilities that malicious actors can exploit (Doifode S. P., 2024). Leveraging Threat-Led Penetration Testing methodologies, organizations can simulate real-world cyberattacks to identify weaknesses in their defense mechanisms and proactively address potential breaches (Pourrahmani, 2023). TLPT provides a structured and ethical approach to assessing an organization's security posture by emulating the tactics, techniques, and procedures of advanced persistent threats. This enables organizations to strenghten their stringent regulations such as the Digital Operational Resilience Act, which mandates robust cybersecurity frameworks for financial entities (Doifode S. P., 2024).

Emerging research and technology trends

The landscape of IoT cybersecurity is undergoing a seismic shift propelled by escalating sophisicationof cyber threats targeting interconnected devices. The proliferation of IoT devices projected to reach 84 billion by 2024 has expanded the attcak surface making these devices attractive targets for maliciuos actors (Qaddos, 2024).

Securing these devices is not just about protecting invidual gadgets, but also safeguarding entire ecossytems and critical infrastructure dependent on them (Doifode S. P., 2024).

The influnce of Artificial Intelligence and Machine Learning paradims has ushered in a transformative era for bolstering security infrastructure particularly within the intricate ecosystems of the internet of things where conventional security mechanisms often prove inadequence against sophisticated cyber threats (Oduwale, 2024). AI-powered intrusion detection systems exhibit a heightened capacity to descern and interpret complex behavioral anomalies inherent in IoT networks, thereby facilitating the proactive identification and mitigation of potential cyber intrusions before they can manifest into full-scale breaches (Wei, 2024). The deployment of AI not only augmants the precision of the threat detection but also significantly reduces the incidence of false positives, a common impediment in traditional security systems that can overwhelm security personnel and obfuscate genuine threats (Chen, 2024).

The convergence of blockchain technology and the internet of things presents a paradigm shift in securing decentralized communication and ensuring data integrity across interconnected devices. Blockchain's immutable and transparent nature is particularly advantageous in mitigating security vulnerabilities inherent in IoT ecosystems, where a multitude of devices generate and exchange data (Oduwale, 2024). By leveraging distributed technologies, blockchain offers a robust framework for decentralized authentication, access control, and secure data storage effectively addressing the limitations of traditional centralized security models (Chen, 2024) (Khatun, 2023). The integration of blockchain-based identity and access management systems in IoT environments is crucial for

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 06 June 2025, pp: 519-525 www.ijaem.net ISSN: 2395-5252

establishing secure and reliable authentication layers, mitigating the risk associated with identity theft and unauthorized access to sensitive data (Wei, 2024).

The relentless march or quantum computing poses an existential threat to the security paradigms underpinning the internet of things, necessitating a paradigm shift towards quantum-resistant and cryptographic solutions. Convetional cryptographic algorithms such as RSA and Elliptic Curve cryptography which have long been the conerstone of IoT security are projected to become vulnerable to cryptanalytic attacks executed on quantum computers particularly Shor's algorithm (Oduwale, 2024). This vulnerability stems from the ability of quantum computers to efficiently solve mathematical problems like integer factorization and discrete logarithms that are computationally intractable for classical computers (Chen, 2024).

III. METHODOLOGY

The qualitative component of this study encopasses an extensive review of peer-review scholarly literature, technical white papers and detailed post-incident reports of significant security breaches affecting IoT deployments facilitating the identification of frequently exploited attack patterns, weaknesses and consequences of successful compromises across interconnected operational tiers. Sourecs like Chen (2024), Khatun (2023) and Wei (2024) provided a strong foundation for understanding how threats have developed and where future risks may lie.

Data collection methods

Academic journals as scholarly publications provide rigorous and peer-reviewed platform for disseminating findings, methodologies and comprehesive analyses of emerging threats targeting IoT ecosystems. The information used in the research was drawn from mainly four sources namely:

Table 1. Comparison Table of the four main sources used in the research study.

Data Source	Purpose	Key References
Academic Journals	To explore known vulnerabilities and current research trends	Chen (2024), Khatun (2023), Wei (2024)
Case Study Analysis	To examine actual IoT breaches and draw lessons form them	Vallabhaneni (2024), Pourrahmani (2023)
Security Frameworks	To understand technical defenses and encryption strategies	Radanliev (2024), Singh (2024)
Industry Reports and Guidelines	To incorporate real-world policies and best practices	Oduwale (2024), Vescovi (2023), Nag (2024)

Furthermore, the use of analysis techniques to make sense of collected data with strategies like coparative analysis which contrasts defferent vulnerabilities like network infiltration and physical tampering from the work of McWeeney (2024) and Nag (2024) to evaluate which are most exploited or damaged. Also used the trend identification techniques where the threat patterns were reviewed for anticipation of future risks. Xu (2024), Sahu (2024) and Wei (2024) offered IoT incidents and forecasts that elaborated how threats are evolving and where future vulneraborities might emerge especially regarding new devices types and new aoutomation. Lastly, AI and Machine based evaluation that was explored to flag and prevent intrusions with particular focus on Khatun (2023) and Radanliev (2024) who examined how intelligent systems are used to detect and respond to unusual device behavior.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 06 June 2025, pp: 519-525 www.ijaem.net ISSN: 2395-5252

IV. PROPOSED SOLUTIONS AND MITIGATIONS

Mitigation security risks in the IoT requires a layered approach that combines technological solutions, policy implementations and user behavioral adaptations. This section explores multiple angles to reinforce the security of IoT systems. Looking at an IoT ecosystem, a diagram belolw looks at a how IoT security requires defenses across multiple layers from the physical device level to the cloud and user layer where each layer is protected through specific mechanisms like firmware authentication, network segmentation, encryption, AI threat detection and user training.

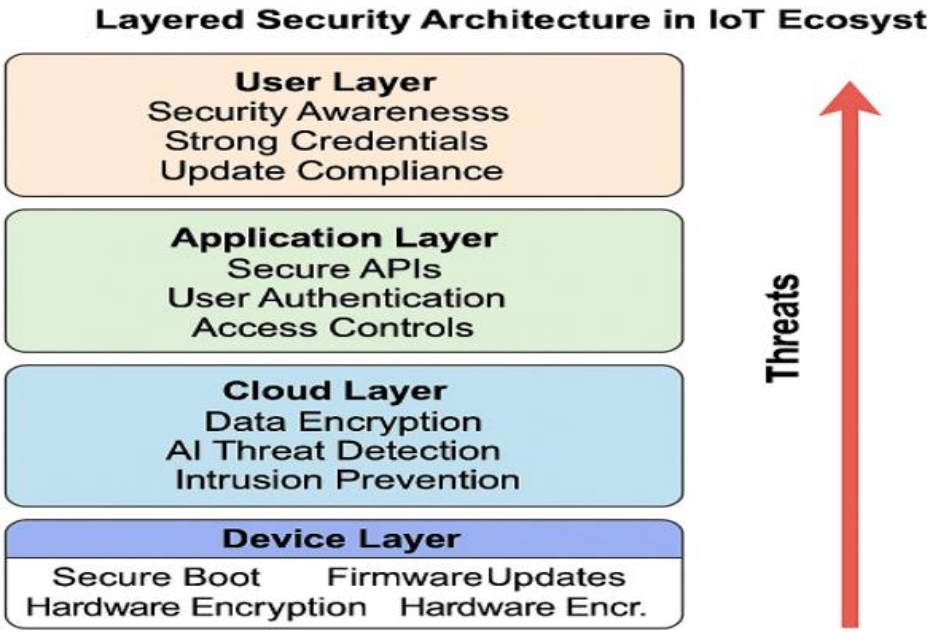

Figure 1.layered security Architecture in IoT ecosystem

Frameworks outline best practices for securing data flow, authenticating users and maintaining secure device lifecycles. For example, the **Zero Trust Architecture (ZTA)** that removes implicit trust from devices requiring continuous verification and segmentation. Singh (2024) and Radanliev (2024) discuss the integration of ZTA within IoT ecosystems reducing lateral movement during attacks and strengths the entire network.

Mitigating threats requires active engagement from both end users who must change default passwords, regulary update firmwareand disable unnecessary device permissions and the developers who must build security in mind avoiding hardcoded credentials, disabling open ports and enforcing software validation processes. Figure 1 has practices under Device Layer and User Layer that contain secure critical roles for each and educating users about risks and sceurity equally being important as even the most secure system can be undermined by negligent behaviors.

Machine learning can detect anomalies in device behavior, flagging potential intrusions in real time. These AI-driven systems can also learn from past incidents to improve their accuracy overtime as they can also process vast data streams makes it a powerful tool in threat detection. Radanliev (2024) and Khatun (2023) support the use of machine learning algorithms to analyse behavioral patterns in device communications which systems automatically isolate compromised devices, alert administrators and recommend mitigation actions in real-time.

The use of a secure-by-design approach is more effective than patching vulnerabilities as it integarates protective measures into both hardware and software during development. (Li, 2023)identifies the pressure manufactureres face in releasing cost-effective devices as a major risk factor. This design can mandate devices passing security testing before release however speedy the development is.

Governemt regulations can elevate baselines of IoT security by holding manufacturers accountable and protecting users. Vescovi (2023) states that fragmented regulation often leave

loopholes across jurisdictions and here applying comprehesive ploicies can complement the technological layers forming complete security. International alignment on cybersecurity standards could also reduce the gaps exploited by attackers and also enable users to make informed decisions when purchasing smart devices as these devices carry clear labeling with security features.

V. CONCLUSION

Conclusively,the interconnected nature of IoT devices creates a wide attack surface where a single compromised device can serve as a gateway to a broader network potentially impacting sensitive data and critical systems. Malicious exploitation of these vulnerabilities can precipate severe consequences leading to large-scale data exfiltration, economic effect via ransomware and tangible physical harm through the manipulation of devices controlling infrastructure or personal safety.

This study through literature reviews, case studies and security models highlights the importance or proactive measures like secure-by-design, Zero Trust Architecture, AI and machine threat detection and alo educating users to reduce vulnerabilities. It aslo emphasizes strong policies and regulatory standard in holding manufacturers accountable to protect users.

Securing the internet of things exceeds mere technological implementation necessitating a comprehensive strategy that integarates awareness, collaboration and unwavering commitement from all particpants within the ecosystem as it requires a shared responsibility to build a safer and more resilient future for connected technologies.

VI. ACKNOWLEDGEMENT

The authors would like to thank all members of school of computing who are involved in this study. This study was carried out as part of the Hacking and Penetration Testing Project. This was supported by Universiti Utara Malaysia.

REFERENCES

[1]. Chen, Z. G. (2024). Internet of Things and Cyber-Physical Systems.
[2]. Doifode, S. P. (2024). Cybersecurity in the Internet of Things (IoT): Challenges and Solutions. International Journal of Scientific Research in Modern Science and Technology, 3(7), 17-21.
[3]. Doifode, S. P. (2024). Cybersecurity in the Internet of Things (IoT): Challenges and Solutions. International Journal of Scientific Research in Modern Science and Technology, 3(7), 17-21.
[4]. Khatun, M. A. (2023). Machine learning for healthcare-iot security: A review and risk mitigation. IEEE Access, 11, 145869-145896.
[5]. Laghari, A. A. (2024). Internet of Things (IoT) applications security trends and challenges. Discover Internet of Things, 4(1), 36.
[6]. Li, Y. M. (2023). Who let the smart toaster hack the house? An investigation into the security vulnerabilities of consumer IoT devices. arXiv preprint arXiv, 2306.09017.
[7]. McWeeney, B. M. (2024). Analysis of Payload Confidentiality for the IoT/LPWAN Technology'Lora. CISSP, 90-102.
[8]. Nag, A. H. (2024). Exploring the applications and security threats of Internet of Thing in the cloud computing paradigm: A comprehensive study on the cloud of things. Transactions on Emerging Telecommunications Technologies, 35(4), e4897.
[9]. Nandhini, S. R. (2024). yber attack detection in IOT-WSN devices with threat intelligence using hidden and connected layer based architectures. Journal of Cloud Computing, 13(1), 159.
[10]. Oduwale, A. &. (2024). INTERNET OF THINGS (IoT) SECURITY RISK MANAGEMENT SYSTEM. sciforum.
[11]. Pourrahmani, H. Y. (2023). A review of the security vulnerabilities and countermeasures in the Internet of Things solutions: A bright future for the Blockchain. Internet of Things, 23, 100888.
[12]. Qaddos, A. Y.-S. (2024). A novel intrusion detection framework for optimizing IoT security. Scientific Reports, 14(1).
[13]. Radanliev, P. D. (2024). AI security and cyber risk in IoT systems. Frontiers in Big Data, 7, 1402745.
[14]. Sahu, S. K. (2024). Exploring security threats and solutions Techniques for Internet of Things (IoT): from vulnerabilities to vigilance. Frontiers in Artificial Intelligence, 7, 1397480.
[15]. Singh, N. B. (2024). Securing cloud-based internet of things: challenges and mitigations. Sensors, 25(1), 79.
[16]. Vallabhaneni, R. (2024). Effects of Data Breaches on Internet of Things (IoT) Devices within the Proliferation of Daily-Life Integrated Devices. Engineering And Technology Journal, 9(7), 4439-4442.

[17]. Vescovi, C. (2023). Complexity of IoT technologies: European regulations in progress and patterns of customer communication. MEDIA LAWS, 299-321.
[18]. Wei, Z. W. (2024). A Survey on IoT Security: Vulnerability Detection and Protection. In Proceedings of the 2024 International Conference on Artificial Intelligence of Things and Computing, 1-8.
[19]. Xu, H. L. (2024). Security risks concerns of generative AI in the IOT. IEEE Internet of Things Magazine, 7(3), 62-67.