ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25jul021

Enhancing IoT Security: Addressing Wi-Fi Vulnerabilities and Mitigation Strategies

Md Mazedul Alam[1]

[1]Department of Computer Science and Engineer, University of South Asia, Bangladesh

Publication Date: 2025/07/10

Abstract: IoT security is essential to prevent data breaches, as most IoT devices lack built-in security mechanisms. These devices often go undetected by traditional cybersecurity systems, transferring unencrypted data over the internet, which leaves them vulnerable to attacks. IoT security refers to the measures designed to protect connected devices and systems from unauthorized access, cyberattacks, and other security threats. This encompasses securing the devices themselves, safeguarding data transmission, and fortifying the underlying network infrastructure. IoT security faces several challenges, including the vast number of devices with varying security levels, the complexity of interconnected networks, and the growing sophistication of cyber threats. This research study emphasizes the importance of enhancing IoT security. It examines the most common communication technologies—Bluetooth, Wi-Fi, and LTE—and evaluates the safeguards available for them, focusing specifically on Wi-Fi technology in this article. The EBIOS risk assessment method is employed to identify potential vulnerabilities and threats within the Wi-Fi ecosystem. The ultimate objective of this work is to highlight and mitigate security risks associated with using Wi-Fi in IoT environments. The broader goal of IoT security is to ensure the confidentiality, integrity, and availability of data and systems while maintaining the functionality and usability of connected devices.

Keywords*: IoT, Cyber-attack, Bluetooth, Wi-Fi, LTE, IoT Security, Data Breach, Network Infrastructure, EBIOS Technique, Vulnerability Assessment.*

How to Cite: Md Mazedul Alam (2025) Enhancing IoT Security: Addressing Wi-Fi Vulnerabilities and Mitigation Strategies. *International Journal of Innovative Science and Research Technology*, 10(7), 150-156. https://doi.org/10.38124/ijisrt/25jul021

I. INTRODUCTION

The Internet of Things (IoT) represents a vast network of interconnected devices, machinery, and electronic appliances that can communicate and share information across networks without requiring human-to-computer interaction. From smart homes to advanced corporate offices, IoT has transformed the way we interact with technology, creating smarter environments for personal and professional use. However, this convenience comes with a significant concern: security vulnerabilities. As IoT applications, such as smart homes and automotive systems, become more prevalent, the lack of robust security measures poses serious risks. IoT devices are increasingly targeted by hackers and cybercriminals, who exploit their vulnerabilities due to inadequate security designs. This article aims to provide a foundation of well-researched IoT encryption standards and best practices. By doing so, it seeks to inspire the development of future standards through certifications, regulations, product ratings, and policies that ensure IoT security. While many of the proposed measures apply broadly to all internet-connected devices, this study focuses on security protocols uniquely relevant to IoT. The research follows an end-to-end approach to IoT systems, emphasizing security mechanisms from network endpoints to hardware components of client and server applications. It highlights the importance of implementing security features—such as upgrading, patching, and encryption—during the production design process. IoT devices rely on two main types of connectivity: cable-based and wireless. While wireless connections offer the advantage of mobility over traditional cable connections, they also introduce additional security risks. These risks make it imperative to design security measures that address vulnerabilities inherent to wireless IoT devices. In a world governed by stringent international data protection and privacy laws, securing IoT devices is not just beneficial—it is essential. Governments, businesses, and consumers alike must work toward strengthening IoT security to ensure the safety of sensitive data and maintain trust in these transformative technologies.

II. LITERATURE REVIEW

To ensure IoT systems are secure and dependable, it is crucial to monitor security threats from the initial stages, authenticate devices, detect unauthorized access, and implement robust security provisioning mechanisms. Several methodologies have been proposed to develop secure IoT

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25jul021

systems, including software cryptology, lightweight encryption, security protocol selection, Data Encryption Standard (DES), and Counter-Motion Cipher Block Chaining Message Authentication Code Protocol (CCMP) [1][2].

For IoT security, critical characteristics include biometric authentication, device-specific IMEI numbers, cryptography, and TCP/IP socket communication [3]. However, specific technologies like Bluetooth have significant security flaws, highlighting the need for better understanding and addressing vulnerabilities as technology advances [4]. Wi-Fi Fine Timing Measurement (FTM) communications, for instance, are demonstrated to lack encryption when analyzed with an on-air sniffer, raising concerns about the protocol's security implications [5]. Key challenges in IoT security include object naming, identity management, and authentication, which are fundamental for secure communication and data retrieval [6][14]. To address these issues, researchers emphasize the need to design new security protocols incorporating strong encryption and authentication schemes [7]. Legacy authentication methods have proven unsuitable for IoT due to the limited resources and large scale of devices [8]. Additionally, the Perceptual Layer of IoT systems remain highly vulnerable due to the physical proximity of devices, restricted resource availability, and technological heterogeneity [9]. Secure gateways are proposed as a means to connect IoT and digital communication, offering enhanced security at various layers of IoT ecosystems [10]. The OCTAVE Allegro methodology emphasizes information asset protection, considering multiple carriers such as databases, physical documents, and individuals [11]. The Constrained Application Protocol (CoAP), a key application layer protocol in IoT, is noted for its inadequacies in certain scenarios, which may pose risks to system procedures [12]. Understanding an IoT system's dependencies, advantages, and vulnerabilities provides insights into the various types of attacks it may face [13]. Many IoT devices lack robust security due to the absence of standardized protocols, secure hardware, and sufficient resources [15]. Current research focuses on lightweight encryption methods, the use of neural networks to enhance security assurances, block chain for addressing IoT safety issues, and the implications of IoT adoption in 5G networks [16]. Ensuring the security of IoT environments at every layer is critical to improving the overall security of connected devices and the data they generate [17]. Researchers continue to explore fundamental security technologies, such as encryption, as part of their efforts to strengthen IoT ecosystems [18].

III. CONCEPTUAL FRAMEWORK

Despite the immense significance and diverse applications of the Internet of Things (IoT), it presents significant challenges in scenarios where security and privacy are of paramount importance. As IoT devices continue to proliferate across various domains, their inherent vulnerabilities expose users and systems to increasing risks of cyber threats and data breaches.

IoT security remains a complex and evolving field that demands further research and innovation to address these pressing concerns. The interplay between device security, data confidentiality, network integrity, and user privacy form the foundation of this conceptual framework. It underscores the necessity of a comprehensive approach that includes:

- Risk Assessment: Identifying and prioritizing vulnerabilities in IoT devices and networks.
- Encryption and Authentication: Implementing robust encryption standards and authentication mechanisms to secure data transmission and access control.
- Device and Network Resilience: Developing security protocols to enhance the resilience of IoT devices and networks against cyberattacks.
- Regulatory Compliance: Aligning IoT security practices with international data protection and privacy laws.
- User Awareness: Educating users about best practices to mitigate security risks.
- This framework provides a roadmap for exploring security strategies that ensure the confidentiality, integrity, and availability of IoT systems while addressing the evolving challenges of security and privacy in the IoT landscape.

IV. METHODOLOGY

An investigation investigates possibilities might legitimize the adoption of Internet of Things (IoT) technology as safety concerns. The purpose of this inquiry seeks to put forward a form for secured yet fruitful IoT investing. The document inspects the conducive circumstances for IoT security breakthroughs to prosper. The methodology explores the potential of legitimizing Internet of Things (IoT) adoption through a focus on safety and security concerns, aiming to establish a secure yet effective investment framework for IoT technology. The study employs both qualitative and quantitative approaches to gather personalized insights and objective data, offering a well-rounded view of current.

Security practices and user experiences. It involves analyzing IoT devices to uncover potential vulnerabilities in their operation and communication channels, particularly through IoT Instrument Profiling, which helps in identifying weaknesses in both device hardware and wireless connections like Wi-Fi. Functional assessments are conducted to examine cross-account and cross-system incidents using realistic, accessible environments for accurate testing and detailed scenario mapping. Based on the analysis, different testing techniques—such as application, mobile, and cloud security testing—are applied, depending on the device’s structure and network. Furthermore, continuous monitoring and adaptive testing strategies are recommended to keep pace with the rapidly evolving IoT landscape. Additionally, network-based investigations assess the exposure of TCP and UDP ports across the IoT infrastructure, identifying possible risks and weak configurations that could be exploited by attackers. This comprehensive methodology supports the creation of resilient IoT ecosystems and informed decision-making for secure technological investments.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25jul021

V. SECURITY ANALYSIS IN IOT (INTERNET OF THINGS)

The Internet of Things (IoT) connects billions of devices, enabling smart automation but also introducing significant security risks. A proper security analysis of IoT involves identifying vulnerabilities, assessing risks, and implementing protective measures.

➢ *Security Challenges in IoT*

IoT ecosystems face a range of security vulnerabilities across multiple layers, starting with device-level weaknesses such as poor authentication and authorization—often relying on default or hardcoded passwords—and outdated firmware that leaves devices exposed to known exploits. Their limited computational power further restricts the implementation of robust security measures. At the network level, threats like Man-in-the-Middle (MITM) attacks, Denial-of-Service (DoS/DDoS) attacks, and unauthorized data interception through eavesdropping or sniffing are common. In the cloud, weak access controls can lead to unauthorized data access, while insecure APIs and data breaches pose significant privacy concerns. Additionally, physical security threats such as device tampering and side-channel attacks, which exploit physical characteristics like power consumption or electromagnetic emissions, add another layer of risk. Addressing these vulnerabilities requires a holistic approach combining hardware security, encrypted communication, secure software updates, and robust cloud policies.

➢ *Security Measures & Best Practices*

To mitigate the diverse risks in IoT ecosystems, a multi-layered security approach is essential. At the device level, strong authentication such as multi-factor authentication (MFA), secure boot mechanisms, encrypted firmware updates, and robust data encryption help prevent unauthorized access and tampering. Network security is enhanced through the use of secure communication protocols like TLS/SSL, MQTT with TLS, or DTLS, alongside firewalls, intrusion detection systems (IDS), and network segmentation to isolate IoT devices from critical systems. In the cloud, security is reinforced by implementing role-based access control (RBAC), data anonymization to protect user privacy, and securing APIs with technologies like OAuth, API gateways, and rate limiting. Physical security is also critical, requiring tamper-resistant hardware, secure boot mechanisms, and strict physical access controls.

➢ *Security Analysis Tools for IoT:*

Security analysis tools play a vital role in identifying, assessing, and mitigating risks within IoT environments. Shodan, often called the "search engine for IoT," scans the internet to locate publicly exposed and potentially vulnerable IoT devices, providing insight into open ports, software versions, and misconfigured systems. Wireshark is a powerful network protocol analyzer that captures and inspects packet-level data, making it invaluable for monitoring IoT communication channels, detecting anomalies, and uncovering signs of attacks such as Man-in-the-Middle or data leakage. Nmap (Network Mapper) is widely used for network discovery and security auditing, capable of identifying open ports, running services, and device operating systems across IoT networks—helping security analysts assess the attack surface and prioritize remediation. For deeper analysis, firmware analysis tools like Binwalk and QEMU are essential for reverse engineering IoT device firmware. Binwalk extracts firmware components to detect hidden scripts or backdoors, while QEMU emulates embedded environments, allowing researchers to safely examine the behavior of firmware without using actual hardware. Together, these tools form a comprehensive toolkit for IoT vulnerability assessment, enabling proactive security measures across device, network, and software layers.

VI. FUTURE TRENDS IN IOT SECURITY

➢ *AI-Driven Threat Detection*

Artificial intelligence (AI)-driven threat detection refers to the use of machine learning (ML) and deep learning (DL) algorithms to identify and respond to cybersecurity threats. Solutions like Sentinel One's AI-powered security utilize advanced AI technologies to enhance endpoint protection by autonomously detecting and mitigating risks. These AI algorithms are trained on massive datasets containing information about known security threats. This extensive training enables the system to recognize malicious patterns in real time—patterns that may otherwise go unnoticed by traditional or manual detection methods. Initially, AI in cybersecurity was primarily used to identify known threats—those already detectable by conventional systems. However, as AI algorithms have advanced, they now enable organizations to continuously monitor network traffic, user behavior, and system activity. Any deviations from normal patterns are flagged as potential unknown threats. Unlike traditional threat detection approaches, AI-based systems can identify threats earlier in the attack lifecycle, significantly reducing potential damage and preventing data breaches. One of the standout features of AI threat detection is its ability to automate the entire process—from identifying a threat and alerting security teams to preventing subsequent attacks.

➢ *Blockchain for IoT Security*

The Internet of Things (IoT) is transforming the way we interact with the world, weaving a network of interconnected devices capable of seamless communication and real-time data exchange. But as this connectivity grows, so do the security challenges. Ensuring the integrity, confidentiality, and trustworthiness of data shared among IoT devices has become a pressing concern. Blockchain technology offers a compelling solution, introducing innovative ways to enhance IoT security. My journey into the convergence of blockchain and IoT security began out of necessity. While working on projects that demanded secure and reliable device communication, I quickly discovered that traditional security measures often fell short—especially when faced with the complexity and scale of modern IoT networks. This realization led me to explore how blockchain could fill the security gaps. Its decentralized nature, immutability, and transparency held promising potential to redefine how we secure connected environments.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25jul021

➢ *Zero Trust Architecture (ZTA)*

Zero Trust Architecture (ZTA) refers to the implementation, practical application, and design of systems that enforce Zero Trust principles within an organization's IT infrastructure. It establishes the technical framework and structural foundation required to ensure secure and controlled access across all digital environments.

- ZTA incorporates a range of security technologies and practices, including:
- Identity and Access Management (IAM)
- Multi-Factor Authentication (MFA)
- Micro-segmentation
- Encryption
- Real-Time Monitoring

These components work together to apply Zero Trust principles across an organization's systems, networks, and workflows. The core idea is that no entity—whether a user, device, or application—is trusted by default. Instead, access is granted only after continuous, context-based verification.

ZTA ensures that every access request is thoroughly validated, minimizing the risk of unauthorized access and lateral movement within the network. This approach represents a significant shift from traditional perimeter-based security models, offering enhanced protection in today's highly dynamic and distributed IT environments.

➢ *Routing Attack on IoT devices:*

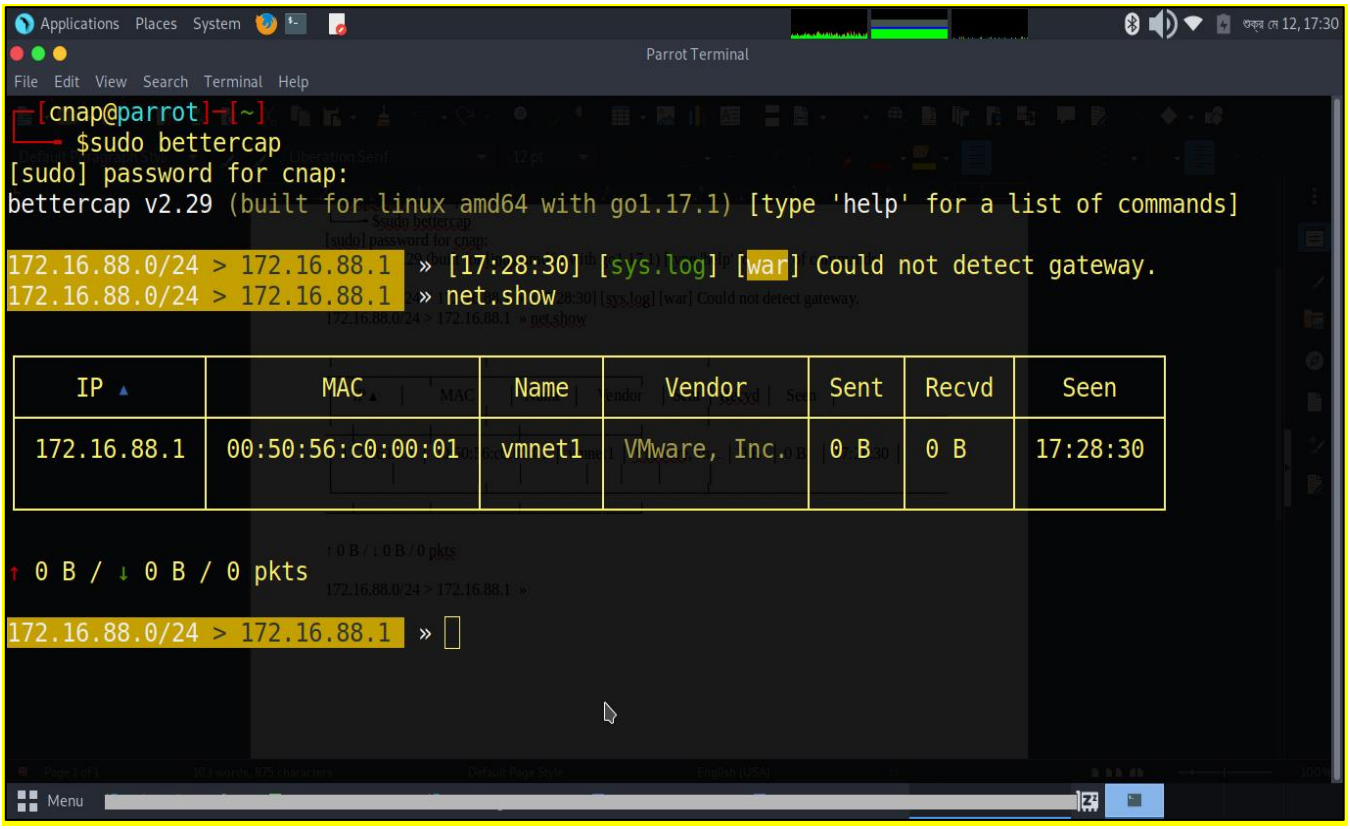

Fig- 1: Routing Attack on Wi-Fi Caused by IoT

In this discussion, we previously focused on a specific vulnerability pathway exploited through IoT devices and the reasons behind its occurrence. As illustrated in Figure 1, an attacker can compromise any user's router through this type of attack. Prior to launching the assault, an eavesdropping mechanism is used to gather critical network information such as the perpetrator's network mask, ESSID, MAC address, and IP address. Once the attack is executed, it results in the victim's network being completely compromised, as evidenced by the "net.show" command displaying 0B data sent and 0B data received—indicating that the network has been hijacked and rendered non-functional. At this stage, the attacker gains full control over all connected IoT devices through command-line interactions, highlighting the severe impact of such a breach and the need for stronger IoT security defenses.

➢ *Hacking IoT Device (A Smart Plug) with Python:*

Python-based hacking serves as a powerful tool in the context of IoT applications, offering flexibility for both backend development and device-level software manipulation within the IoT development lifecycle. Python, along with Micro Python, can be leveraged effectively in embedded systems, particularly on Linux-based IoT devices. Smart plugs, which are commonly used to monitor and control home appliances, are often susceptible to security flaws if not

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25jul021

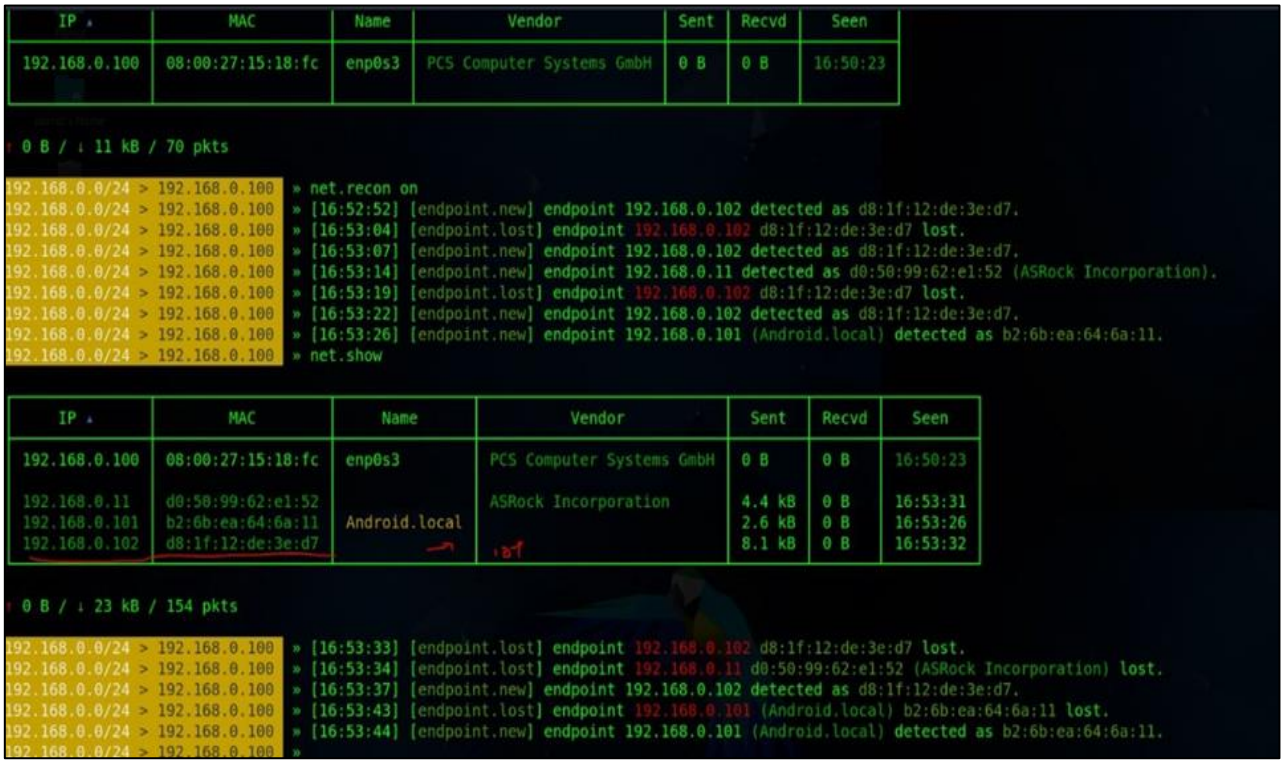

Fig – 2: Controlling Required IoT Device

Properly secured. As shown in Figure 2, I successfully exploited a smart plug IoT device using Python, taking advantage of weak or absent security mechanisms. This demonstration highlights the critical importance of enforcing proper authentication, encrypted communication, and firmware protections in smart home devices to prevent unauthorized access and control.

VII. DISCUSSION & RESULT

IoT devices can be compromised through Wi-Fi networks, allowing attackers or even crypto analysts to gain unauthorized access to sensitive data. Wi-Fi WLANs typically aim to uphold privacy and security through a combination of mechanisms defined in wireless Ethernet standards. Among these, access control stands out as a key security objective, alongside the traditional principles of confidentiality, integrity, and availability. Access control ensures that only authorized users or devices can access network resources. To safeguard IoT devices, it is essential to protect the Wi-Fi infrastructure. User gateways should be configured to limit the number of concurrent connections, and session durations should not extend unnecessarily, especially when the user is not present. Risk analysis in this context relies on assessing threats and determining appropriate mitigation strategies. Critical risks—those with high severity and significant probability—require strong countermeasures to reduce both their likelihood and potential impact. Meanwhile, risks with limited severity but notable probability also demand monitoring and control. One of the core vulnerabilities in IoT lies in its architecture, which often exposes devices to attacks by revealing identifiable information such as IP and MAC addresses. These details are frequently exploited by hackers to infiltrate IoT ecosystems via Wi-Fi networks. Therefore, the architecture of IoT systems must evolve to include components capable of masking or securing IP and MAC addresses, thereby preventing unauthorized access and enhancing overall system resilience.

VIII. CONCLUSION:

The rapid expansion of the Internet of Things (IoT) ecosystem brings both tremendous opportunities and significant security challenges. As billions of devices become interconnected—ranging from consumer electronics to industrial sensors—the need for robust, scalable, and adaptable security mechanisms becomes paramount. This study critically examined the existing vulnerabilities within current IoT security frameworks and highlighted the gaps that still persist in both technological and regulatory dimensions.

One of the major findings is the overwhelming strain on organizational capabilities to monitor, analyze, and secure vast networks of diverse and often incompatible devices. Fragmentation in hardware and software standards contributes to the difficulty of implementing universal security protocols. In this context, integrating encrypted data flows and secure application development emerges as a foundational strategy to safeguard user privacy and protect sensitive organizational data.

Furthermore, this research emphasizes the importance of protecting individual privacy, securing enterprise-level processes, and establishing trusted relationships with third-party providers. These areas remain critical as the attack surface of IoT systems continues to grow.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25jul021

To address these challenges, this study proposes a practical and impactful solution: the introduction of standardized IoT security and privacy warning labels. These labels would not only empower consumers to make informed choices but also pressure manufacturers to prioritize secure design practices from the outset. By creating greater transparency and accountability, this approach could catalyze industry-wide improvements in IoT security.

Additionally, the study explored hypothetical IoT threat scenarios and evaluated them through contemporary threat modeling techniques. These assessments revealed both the scale of potential damages and the urgency for preemptive mitigation strategies. The findings underscore the necessity of a proactive and layered security approach, combining technical innovation, regulatory oversight, and public awareness.

In conclusion, securing the IoT landscape is a multifaceted challenge that requires coordinated efforts across academia, industry, and government. This research contributes to the ongoing discourse by offering practical recommendations, emphasizing the urgency of standardized security measures, and advocating for consumer-focused transparency. Only through such integrated efforts can the full potential of the IoT be realized without compromising privacy, safety, and trust.onclusion

REFERENCES

[1]. SentinelOne. (n.d.). AI threat detection. SentinelOne. Retrieved April 7, 2025, from https://www.sentinelone.com/cybersecurity-101/data-and-ai/ai-threat-detection/

[2]. Forbes Technology Council. (2024, August 27). Blockchain for IoT security: Enhancing trust in connect https://www.forbes.com/councils/forbestechcouncil/2024/08/27/blockchain-for-iot-security-enhancing-trust-in-connected-devices/

[3]. Palo Alto Networks. (n.d.). What is a zero trust architecture? Palo Alto Networks. Retrieved April 7, 2025, from https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture

[4]. Let me know if you need it in a different format (like MLA, Chicago, or IEEE).

[5]. Ali, B., & Awad, A. I. (2018). Cyber and physical security vulnerability assessment for IoT-based smart homes. Sensors, 18(3), 817. https://doi.org/10.3390/s18030817

[6]. Ali, I., Sabir, S., & Ullah, Z. (2019). Internet of things security, device authentication and access control: A review. arXiv. https://arxiv.org/abs/1901.07309

[7]. Buenrostro, E., Cyrus, D., Le, T., & Emamian, V. (2018). Security of IoT devices. Journal of Cyber Security Technology, 2(1), 1–13. https://doi.org/10.1080/23742917.2017.1410082

[8]. Deepty, R. R., Alam, A., & Islam, M. E. (2019). IoT and Wi-Fi based door access control system using mobile application. In 2019 IEEE International Conference on Robotics, Automation, Artificial-intelligence and Internet-of-Things (RAAICON) (pp. 21–24). IEEE. https://doi.org/10.1109/RAAICON48939.2019.8970665

[9]. Dineva, K., & Atanasova, T. (2019). Security in IoT systems. International Multidisciplinary Scientific GeoConference SGEM, 19(2.1), 569–577. https://doi.org/10.5593/sgem2019/2.1/S07.072

[10]. Frustaci, M., Pace, P., & Aloi, G. (2017, September). Securing the IoT world: Issues and perspectives. In 2017 IEEE Conference on Standards for Communications and Networking (CSCN) (pp. 246–251). IEEE. https://doi.org/10.1109/CSCN.2017.8088641

[11]. Lonzetta, A. M., Cope, P., Campbell, J., Mohd, B. J., & Hayajneh, T. (2018). Security vulnerabilities in Bluetooth technology as used in IoT. Journal of Sensor and Actuator Networks, 7(3), 28. https://doi.org/10.3390/jsan7030028

[12]. Rahman, R. A., & Shah, B. (2016, March). Security analysis of IoT protocols: A focus in CoAP. In 2016 3rd MEC International Conference on Big Data and Smart City (ICBDSC) (pp. 1–7). IEEE. https://doi.org/10.1109/ICBDSC.2016.7460332

[13]. Sain, M., Kang, Y. J., & Lee, H. J. (2017, February). Survey on security in Internet of Things: State of the art and challenges. In 2017 19th International Conference on Advanced Communication Technology (ICACT) (pp. 699–704). IEEE. https://doi.org/10.23919/ICACT.2017.7890132

[14]. Singh, G., Pandey, A., Prakash, M., Andreoni, M., & Baddeley, M. (2023). Benchmarking and security considerations of Wi-Fi FTM for ranging in IoT devices. arXiv. https://arxiv.org/abs/2303.03766

[15]. Vashi, S., Ram, J., Modi, J., Verma, S., & Prakash, C. (2017, February). Internet of Things (IoT): A vision, architectural elements, and security issues. In 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC) (pp. 492–496). IEEE. https://doi.org/10.1109/I-SMAC.2017.8058207

[16]. Zhang, Z. K., Cho, M. C. Y., & Shieh, S. (2015, April). Emerging security threats and countermeasures in IoT. In Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security (pp. 1–6). https://doi.org/10.1145/2714576.2714635

[17]. Ahmed, M. M., Shah, M. A., & Wahid, A. (2017, April). IoT security: A layered approach for attacks & defenses. In 2017 International Conference on Communication Technologies (ComTech) (pp. 104–110). IEEE. https://doi.org/10.1109/COMTECH.2017.8065759

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25jul021

[18]. Alansari, Z., Anuar, N. B., Kamsin, A., Belgaum, M. R., Alshaer, J., Soomro, S., & Miraz, M. H. (2018, August). Internet of Things: Infrastructure, architecture, security and privacy. In 2018 International Conference on Computing, Electronics & Communications Engineering (iCCECE) (pp. 150–155). IEEE. https://doi.org/10.1109/iCCECE.2018.8658699