Journal of Information Systems Engineering and Management
2025, 10(55s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Security Threats and Risk Mitigation in Home Automation: A Qualitative Review of Challenges and Public Safety Considerations

Yash Patel[1]
ypatel1@capellauniversity.edu
[1]*Capella University, Minneapolis, MN, USA.*

ARTICLE INFO

Received: 30 Dec 2024

Revised: 19 Feb 2025

Accepted: 27 Feb 2025

ABSTRACT

The adoption of home automation technologies has improved residential convenience and energy efficiency, but it has also introduced various cybersecurity risks. This qualitative literature review examines the primary security threats and risk mitigation strategies related to smart home environments. Key issues identified include unauthorized access, data breaches, device tampering, and privacy violations, often due to weak default configurations, user negligence, and the lack of unified security standards. The review synthesizes recent research findings and emphasizes the importance of integrating technical defences (e.g., encryption, multi-factor authentication), promoting cybersecurity literacy among users, and advancing regulatory frameworks. It stresses the need for collaboration among manufacturers, policymakers, researchers, and consumers to ensure smart home systems are secure, resilient, and privacy-preserving. These insights provide a foundation for future research and development aimed at improving security within the domain of smart home automation.

Keywords: Smart Home Security, Internet of Things (IoT), Cybersecurity Risks, Risk Mitigation, Home Automation Privacy.

INTRODUCTION

The emergence of the Internet of Things (IoT) has transformed domestic living by integrating smart technologies into residences, leading to the concept known as “home automation” or “smart homes.” These setups encompass interconnected devices such as sensors, cameras, thermostats, lighting systems, and appliances that communicate and operate autonomously or semi-autonomously to enhance convenience, energy efficiency, and overall quality of life (Touqeer et al., 2021; Hamdan, 2021). As these systems become more widespread and intricate, there are increasing concerns regarding their security, reliability, and implications for public safety.

Smart homes present various security challenges, including cyber intrusions, data breaches, unauthorized surveillance, and compromised device control. These issues are often exposed by insecure networks and insufficient user awareness (Farooq & Hassan, 2021; Nehme & George, 2022). Additionally, the distributed and diverse nature of smart home ecosystems, which involve multiple manufacturers, communication protocols, and deployment standards, leads to significant technical and regulatory difficulties (Hammi et al., 2022; Cvitić et al., 2023). As these systems increasingly manage sensitive personal data and critical safety functions such as door locks, smoke detectors, and medical monitoring devices the risks associated with cybersecurity and privacy breaches impact not only individual households but also broader public safety concerns (Popoola et al., 2024; Bansal & Bhardwaj, 2024). Furthermore, emergency response capabilities and societal resilience may be compromised if such infrastructures lack robust security measures.

This paper presents a qualitative literature review of recent studies addressing the security threats, challenges, and risk mitigation strategies associated with smart home environments, with a particular focus on public safety

Journal of Information Systems Engineering and Management
2025, 10(55s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

considerations. The aim is to synthesize existing knowledge across technological, human, and policy dimensions and provide a consolidated understanding that can guide future work in this space.

LITERATURE REVIEW

The advent of smart home systems has heralded a new era in digital living, characterized by interconnected devices designed to improve convenience, energy efficiency, and safety. Nevertheless, the increasing complexity and widespread adoption of these technologies have also led to notable security, privacy, and public safety concerns. Recent scholarly literature presents a comprehensive yet fragmented body of research focused on security vulnerabilities from multiple perspectives, including technical threats, architectural weaknesses, regulatory deficiencies, and human factors. A common theme across many studies is the recognition of the multi-layered architecture inherent in smart home systems, typically categorized into perception, network, and application layers, each offering distinct security challenges. Touqeer et al. (2021) highlight that these layers are susceptible to various types of threats, such as physical tampering, data interception, or unauthorized access. This layered perspective is supported by Hammi et al. (2022), who advocate for more holistic and coordinated defensive strategies that address inter-layer vulnerabilities rather than isolated risks.

In terms of specific threat types, researchers have proposed various classifications based on attack methods, affected components, and attacker motives. Farooq and Hassan (2021) highlight the increasing range of threats, from malware injections and man-in-the-middle attacks to device hijacking and botnet inclusion. Vardakis et al. (2024) and Hamdan (2021) further note that weak default passwords, unsecured wireless communications, and outdated firmware often serve as common entry points for attackers. Beyond purely technical exploits, emerging threats also include social engineering tactics that exploit user behaviour and psychological vulnerabilities. In contrast, there is a growing emphasis on the broader implications of smart home adoption, particularly regarding privacy, ethics, and public safety. Nehme and George (2022) argue that many users are unaware of the extent of data being collected by smart home systems or the potential for unauthorized surveillance. Popoola et al. (2024) expands this concern in the context of smart home healthcare, where sensitive medical data is transmitted across distributed systems often relying on blockchain or third-party providers. The tension between user convenience and security is clearly outlined by Westbrook (2021), who points out that user behaviours often Favor automation over safety, leading to underutilization or misconfiguration of critical security settings.

Efforts to mitigate these risks have led to a diverse array of proposed solutions, ranging from technical frameworks and encryption protocols to AI-powered monitoring systems. Researchers such as Albela (2021) and Alsabilah (2024) have developed architectural models that integrate security principles directly into system design, rather than treating them as secondary considerations. Saad et al. (2023) propose adaptive cybersecurity frameworks that respond in real time to emerging threats, while Ahmed and Zeebaree (2021) underscore the significance of user-centred approaches, highlighting the role of education, awareness, and interface design in promoting safer user practices. Despite these advancements, a major challenge persists due to the lack of standardized regulatory and technical guidelines. Cvitić et al. (2023) and Aldahmani et al. (2023) both contend that inconsistent security implementations among device manufacturers create vulnerabilities that cannot be addressed through isolated interventions. The literature calls for coordinated policy frameworks and regulatory oversight to ensure baseline security standards across all devices and platforms.

METHODOLOGY

This study employs a qualitative literature review approach to explore security threats, challenges, and risk mitigation strategies in smart home environments. Academic sources were identified using Google Scholar, focusing on peer-reviewed journal articles, conference papers, and dissertations published between 2020 and 2024. Keyword combinations such as “smart home security,” “IoT vulnerabilities,” “risk mitigation,” and “public safety in automation” guided the search. Studies were included if they addressed technical, behavioural, or policy aspects of smart home security, while general IoT articles, non-academic sources, and outdated publications were excluded. From an initial pool of over 60 works, 18 were selected based on relevance and thematic alignment. These sources were analyzed and coded across recurring themes such as architectural vulnerabilities, attack vectors, privacy issues, and regulatory frameworks, forming the foundation for the structured review presented in this paper.

Journal of Information Systems Engineering and Management
2025, 10(55s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

SECURITY THREATS IN HOME AUTOMATION

Smart home environments are increasingly targeted by cyber threats due to their reliance on interconnected IoT devices, often characterized by weak default configurations, limited computational capacity, and inconsistent security standards. As these systems become more embedded in daily life managing everything from lighting and climate control to surveillance and healthcare the potential attack surface expands dramatically, inviting a wide range of security threats. One of the most prevalent threats in smart home systems is unauthorized access, often resulting from default or weak passwords, lack of encryption, or poorly configured access controls. As Farooq and Hassan (2021) highlight, many smart devices are deployed with minimal security hardening, allowing attackers to enter the home network with basic techniques such as brute-force or dictionary attacks. Once inside, intruders can monitor user activity, control devices, or steal sensitive data.

Another significant threat is man-in-the-middle (MitM) attacks, were adversaries intercept communication between devices and users. These attacks can occur when data is transmitted over unencrypted Wi-Fi or Bluetooth channels, enabling attackers to manipulate commands or steal credentials (Touqeer et al., 2021). Similarly, eavesdropping on unsecured communication protocols remains a critical concern, particularly in voice-activated devices or smart assistants that are always listening.

Malware and Ransomware attacks are also increasingly observed in smart homes. Devices with outdated firmware or lacking antivirus protection can be infected and used as entry points into the broader home network. Vardakis et al. (2024) warn that these compromised devices can become part of larger botnets, such as those used in the infamous Mirai attack, turning home automation systems into tools for widespread denial-of-service (DoS) attacks. Physical attacks on smart home components, especially in the perception layer (e.g., cameras, motion sensors), can lead to device manipulation or destruction. Touqeer et al. (2021) explains that without tamper-proof designs, smart devices are vulnerable to direct interference by intruders, particularly in unattended outdoor installations.

Data privacy breaches also constitute a serious threat, as many smart devices constantly collect and transmit data to cloud servers. Inadequate encryption or weak privacy policies can result in sensitive data being exposed or sold without consent. Nehme and George (2022) emphasize that users often remain unaware of what data is being collected and how it is used, making them easy targets for privacy violations. In addition, social engineering attacks are emerging as a non-technical yet highly effective threat. Attackers may deceive users into granting access, sharing passwords, or installing malicious apps. Ahmed and Zeebaree (2021) note that many users lack cybersecurity literacy, increasing the success rate of such human-centric exploits.

CHALLENGES IN SECURING SMART HOMES

The implementation of effective and sustainable security measures in smart home environments is a complex issue, despite growing awareness of cybersecurity risks. These issues include technical limitations, inconsistent standards, user behaviour, and broader policy and regulatory gaps. A significant challenge is the diversity of devices and lack of interoperability standards among manufacturers. Smart home ecosystems typically incorporate devices from various vendors, each utilizing different protocols, software stacks, and security architectures. As noted by Aldahmani et al. (2023), this lack of uniformity leads to fragmented security implementations, where vulnerabilities in one device can affect the entire system. The absence of standardized security baselines means manufacturers may prioritize speed to market over robust protection, resulting in widespread vulnerabilities. Additionally, resource constraints in many IoT devices complicate the deployment of advanced security mechanisms. Embedded systems in smart homes often have limited processing power, memory, and energy capacity, making it challenging to support encryption, intrusion detection, or frequent software updates (Touqeer et al., 2021). These constraints necessitate trade-offs between functionality and protection, particularly in low-cost consumer-grade devices.

User-related challenges are equally significant. Many homeowners are not well-versed in cybersecurity practices, and often fail to change default credentials, apply updates, or configure devices securely. As Westbrook (2021) notes, the convenience of automation often outweighs security considerations in the user's mind. Moreover, users may not fully understand the risks associated with third-party integrations or cloud data storage, inadvertently exposing themselves to privacy violations and cyberattacks. The dynamic and evolving nature of cyber threats also presents a moving target for smart home security. Attackers continuously develop new methods to exploit emerging

Journal of Information Systems Engineering and Management
2025, 10(55s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

technologies, including AI-powered automation, biometric access systems, and interconnected cloud platforms. Traditional security models, which rely on static defences, are often insufficient in this adaptive threat landscape (Saad et al., 2023).

Another significant barrier is the lack of comprehensive regulatory frameworks governing IoT and home automation. In many jurisdictions, security guidelines are voluntary or poorly enforced. This regulatory vacuum allows companies to cut corners in security implementation without facing accountability. Cvitić et al. (2023) argue that until stronger policy interventions are introduced such as mandatory security certifications, compliance audits, or penalties for negligence the industry will continue to underperform on security. Data governance and privacy management also remain unresolved. Nehme and George (2022) highlight that many smart home platforms collect user data without clear disclosures or consent mechanisms, and users have limited control over how their data is stored or shared. The complexity of data flows often spanning multiple third-party services and international servers makes transparency and oversight difficult to achieve.

RISK MITIGATION STRATEGIES AND GUIDELINES

Given the diverse and evolving threats in smart home systems, effective risk mitigation requires a multi-faceted approach that addresses technical vulnerabilities, user behaviors, privacy concerns, and regulatory gaps. Several strategies have been identified in the literature to enhance security, focusing on securing the architecture of IoT devices, promoting user education, strengthening privacy protections, and advocating for robust policy frameworks.

The foundation of smart home security lies in the implementation of robust technical measures designed to protect devices, communication channels, and data. A critical recommendation is employing end-to-end encryptions for all communications between devices and cloud services. Touqeer et al. (2021) advocate for secure communication protocols such as TLS or SSL to prevent eavesdropping and man-in-the-middle (MitM) attacks. Furthermore, multi-factor authentication (MFA) is essential to ensure unauthorized access is prevented, not only for user interfaces but also for device-to-device interactions within the network, as suggested by Farooq and Hassan (2021). This additional layer of authentication significantly mitigates the risk of device hijacking or unauthorized control. Regular updating of software and firmware is another vital strategy for safeguarding against malware and ransomware. Saad et al. (2023) emphasize the importance of automated update mechanisms, particularly for low-interaction devices, to ensure timely application of security patches. Additionally, embedded intrusion detection systems (IDS) are instrumental in monitoring unusual activity and blocking malicious traffic, further enhancing security.

While technical solutions are paramount, user behavior plays an equally significant role in securing smart homes. Westbrook (2021) notes that many homeowners prioritize convenience over security, often overlooking basic measures such as changing default credentials and updating device settings. To address this, user education is crucial. Public awareness campaigns and user-friendly setup guides can educate users on the importance of strong, unique passwords, secure configurations, and ongoing device maintenance. Simplifying the process of securing devices through intuitive interfaces and step-by-step instructions will promote proactive user engagement. Ahmed and Zeebaree (2021) advocate for cybersecurity literacy programs aimed at homeowners to enhance their understanding of potential risks, such as insecure third-party integrations or the dangers of using unsecured networks. By empowering users with knowledge, the probability of common security mistakes, such as reusing passwords or neglecting updates, can be substantially reduced.

Privacy concerns are a central aspect of securing smart homes, particularly as many devices collect sensitive data about users' daily routines and behaviors. Nehme and George (2022) stress the importance of data minimization, where only essential information is collected, and all data is securely encrypted both during transmission and at rest. Users should be provided with clear, transparent privacy policies that outline how their data will be used, stored, and shared. Additionally, devices should offer users control over the data they share, with easy-to-use opt-in/opt-out mechanisms for data collection. For enhanced privacy, decentralized storage solutions such as blockchain can be explored. Popoola et al. (2024) suggest that blockchain offers a transparent and secure way of managing data, allowing users to maintain control over their information while enabling smart devices to function autonomously. This approach can reduce the risks associated with centralized cloud storage, which is often vulnerable to breaches.

Journal of Information Systems Engineering and Management
2025, 10(55s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

The lack of regulatory oversight significantly hampers effective security in smart homes. Currently, security standards for IoT devices are fragmented, with inconsistent enforcement of security practices across manufacturers. Cvitić et al. (2023) advocate for the development of global security standards for IoT devices, ensuring that manufacturers adhere to baseline security and privacy measures. These standards should include mandatory security certifications and periodic audits to verify compliance. Furthermore, penalties for non-compliance would incentivize manufacturers to prioritize security in their product development. Equally important is addressing the interoperability issue within smart home ecosystems. Devices from different manufacturers often lack compatibility in terms of security measures; therefore, establishing universal security protocols is essential. Aldahmani et al. (2023) argue that stronger international regulations would help create a more secure and cohesive smart home ecosystem, ensuring that devices from various vendors can operate together without compromising overall security.

Securing smart homes will require a collaborative approach that involves manufacturers, cybersecurity experts, policymakers, and consumers. A cooperative effort can lead to the development of more secure devices, standardized security protocols, and a stronger regulatory framework to protect users. Saad et al. (2023) suggest that future developments in adaptive cybersecurity systems and machine learning algorithms will be crucial for improving threat detection and response. These technologies can enable smart home systems to autonomously identify and mitigate risks in real-time, making the environment more resilient to evolving threats.

DISCUSSION & FUTURE CONSIDERATIONS

Securing smart homes presents a complex challenge due to the diverse range of IoT devices, differing security standards, and the limited resources available in many of these devices. The literature highlights vulnerabilities such as unauthorized access, data breaches, and device tampering as significant risks that require immediate attention. These threats are exacerbated by user behaviors, as many homeowners neglect fundamental security practices, including proper password management and regular software updates, often prioritizing convenience over security. Nonetheless, several mitigation strategies have been identified, such as end-to-end encryption, multi-factor authentication, and consistent software updates. These measures can substantially enhance security by preventing unauthorized access and ensuring timely defences against emerging threats.

Privacy is a significant concern in smart homes. With many devices collecting sensitive data, decentralized storage solutions like blockchain are suggested to offer users greater control over their information and reduce reliance on centralized cloud systems. User education is crucial for better security practices since many vulnerabilities stem from a lack of awareness. Regulatory frameworks are important; the absence of consistent global security standards for IoT devices leaves gaps in protection. Developing international standards and certifications, along with improved interoperability between devices from different manufacturers, could improve the overall security and reliability of smart home ecosystems. Research into adaptive security systems using machine learning and privacy-preserving technologies such as federated learning will be important for developing smarter, real-time security measures. Collaborative efforts between manufacturers, policymakers, and users will be essential to creating secure and privacy-respecting smart homes, ensuring that future smart homes are efficient, safe, and trustworthy.

CONCLUSION

This research examines security challenges, risk mitigation strategies, and guidelines for smart homes. With the rise of IoT devices in home automation, ensuring their security and privacy is crucial. Key threats include unauthorized access, data breaches, and privacy invasions, arising from technical vulnerabilities and user behaviors. The diversity and limited resources of smart home devices complicate security implementations. Mitigation strategies like end-to-end encryption, multi-factor authentication, and regular updates can reduce vulnerabilities. User education is essential for promoting better security practices. Privacy concerns can be addressed with decentralized solutions like blockchain, allowing users to control their data. Regulatory frameworks and global security standards are vital for compliance. Future research should explore adaptive security systems using machine learning and privacy-preserving technologies. Collaboration among manufacturers, security experts, policymakers, and consumers are crucial for secure smart homes. A coordinated approach can create safe, resilient environments that offer both convenience and protection.

Journal of Information Systems Engineering and Management
2025, 10(55s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

REFRENCES

[1] Touqeer, H., Zaman, S., Amin, R., Hussain, M., Al-Turjman, F., & Bilal, M. (2021). Smart home security: challenges, issues and solutions at different IoT layers. The Journal of Supercomputing, 77(12), 14053-14089.
[2] Hamdan, Y. B. (2021). Smart home environment future challenges and issues-a survey. Journal of Electronics, 3(01), 239-246.
[3] Popoola, O., Rodrigues, M., Marchang, J., Shenfield, A., Ikpehai, A., & Popoola, J. (2024). A critical literature review of security and privacy in smart home healthcare schemes adopting IoT & blockchain: problems, challenges and solutions. Blockchain: Research and Applications, 5(2), 100178.
[4] Farooq, M., & Hassan, M. (2021). IoT smart homes security challenges and solution. International Journal of Security and Networks, 16(4), 235-243.
[5] Nehme, A., & George, J. F. (2022). Approaching IT security & avoiding threats in the smart home context. Journal of Management Information Systems, 39(4), 1184-1214.
[6] Vardakis, G., Hatzivasilis, G., Koutsaki, E., & Papadakis, N. (2024). Review of Smart-Home Security Using the Internet of Things. Electronics, 13(16), 3343.
[7] Aldahmani, A., Ouni, B., Lestable, T., & Debbah, M. (2023). Cyber-security of embedded IoTs in smart homes: challenges, requirements, countermeasures, and trends. IEEE Open Journal of Vehicular Technology, 4, 281-292.
[8] Saad, R. M., Soufy, K. A. A., & Shaheen, S. I. (2023). Security in smart home environment: issues, challenges, and countermeasures-a survey. International Journal of Security and Networks, 18(1), 1-9.
[9] Hammi, B., Zeadally, S., Khatoun, R., & Nebhen, J. (2022). Survey on smart homes: Vulnerabilities, risks, and countermeasures. Computers & Security, 117, 102677.
[10] Cvitić, I., Peraković, D., Periša, M., Jevremović, A., & Shalaginov, A. (2023). An overview of smart home iot trends and related cybersecurity challenges. Mobile Networks and Applications, 28(4), 1334-1348.
[11] Ahmed, S. H., & Zeebaree, S. (2021). A survey on security and privacy challenges in smarthome based IoT. International Journal of Contemporary Architecture, 8(2), 489-510.
[12] Bansal, N., & Bhardwaj, E. (2024, January). Internet of Things for Public Safety. In 2024 2nd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT) (pp. 150-156). IEEE.
[13] Albela, M. S. (2021). New Secure IoT Architectures, Communication Protocols and User Interaction Technologies for Home Automation, Industrial and Smart Environments (Doctoral dissertation, Universidade da Coruña).
[14] Wolniak, R., & Grebski, W. (2023). THE USAGE OF SMART CAMERAS IN SMART HOME. Scientific Papers of Silesian University of Technology. Organization & Management/Zeszyty Naukowe Politechniki Slaskiej. Seria Organizacji i Zarzadzanie, (188).
[15] Alsabilah, N. (2024). Adaptive Cyber Security for Smart Home Systems (Doctoral dissertation, Howard University).
[16] Westbrook, T. (2021). Home security and emergency response: The Convenience vs Security Trade-off. Salus Journal, 9(1), 66-74.
[17] Hassan, Y. G., Collins, A., Babatunde, G. O., Alabi, A. A., & Mustapha, S. D. (2024). Secure smart home IoT ecosystem for public safety and privacy protection. International Journal of Multidisciplinary Research and Growth Evaluation, 5(1), 1151-1157.