Computer Networks and Communications
https://ojs.wiserpub.com/index.php/CNC

Review

A Review on Mitigating Privacy Risks in IoT-Enabled Smart Homes

Tushar Dhanraj, Manash Kumar, Suhani Singh, Rounit Kumar, Priyanshu Jaiswal, Hitesh Mohapatra*

School of Computer Engineering, KIIT Deemed to Be University, Bhubaneswar, India
E-mail: hiteshmahapatra@gmail.com

Received: 11 April 2023; **Revised:** 9 May 2024; **Accepted:** 15 May 2024

Abstract: This paper discusses current technologies for lessening these risks and suggests an approach with multiple layers toward tackling these concerns. This plan integrates security measures at the device level, as well as security measures for networks, and even educational measures for users. Real-world instances and illustrations of the efficacy of the suggested method are presented. Various research gaps in IoT security and privacy have been identified, like the necessity for scalable security solutions, business-related problems, security policies focused on users, protection of privacy using data analysis, and the evolving threat landscape! It also emphasizes the need for security measures for energy storage and contemplates the legal and ethical consequences of IoT security and privacy in intelligent homes. The discussion concludes with future research directions and challenges related to IoT security and privacy strategies and recognizes potential areas for innovation and enhancement. The intention is to contribute to the continuing discussion on IoT security and privacy, offering perspectives and recommendations to safeguard the integrity and privacy of the ecosystem in intelligent homes in an increasingly interconnected world.

***Keywords*:** smart home, security, privacy, IoT, multi-layered approach

1. Introduction

The Internet of Things, or IoT, has drawn a lot of interest due to its wide range of potential uses. Many observers predicted at the beginning of the year that 2015 would be a pivotal year for IoT. It has been forecast that this year may mark the decade of the IoT Enterprise category due to the internet's recent surge in popularity. Concerns over IoT security's impact on growth and advancement have also been raised [1, 2, 3, 4]. The public persisted in drawing attention to the shortcomings and holes in every product that connects to the internet. There are legitimate security risks with the Internet of Things, and they must be addressed right away. However, it has also been demonstrated time and over again that every technical advancement has certain obstacles and detractors. While there will always be IoT security issues, this shouldn't stop businesses from creating IoT applications. An example of an IoT infrastructure and its tiers are shown in Figure 1 [1].

The Emergence of IoT-enabled Smart Homes With the integration of IoT devices and technology to improve occupant comfort, convenience, and efficiency, smart homes mark a paradigm change in residential life (see Figure 2). These houses include networked appliances, sensors, and gadgets that talk to external networks and one another. This allows for remote control and monitoring via smartphones or other internet-enabled devices. The many features offered by smart home appliances, which range from door locks and thermostats to voice assistants and security cameras, are all designed to make

DOI: https://doi.org/10.37256/cnc.2120244736

daily activities easier and enhance quality of life. The benefits of smart homes include increased security and entertainment options, energy efficiency, and the automation of repetitive jobs. For example, smart lighting systems may be designed to generate ambiance or boost energy efficiency, and smart thermostats can learn the inhabitants' preferences and change the temperature accordingly. Additionally, real-time monitoring and alarms provided by motion sensors and smart security cameras enhance house security and inhabitants' peace of mind [2]. Security and Privacy Challenges in IoT-enabled Smart Homes However, the rapid proliferation of IoT devices in smart homes has exposed vulnerabilities and raised concerns regarding security and privacy. These concerns stem from several factors, including the sheer volume and diversity of connected devices, the decentralized nature of IoT ecosystems, and the often-inadequate security measures implemented by device manufacturers. Consequently, smart homes have become lucrative targets for cybercriminals seeking to exploit vulnerabilities and gain unauthorized access to sensitive data or control over devices.

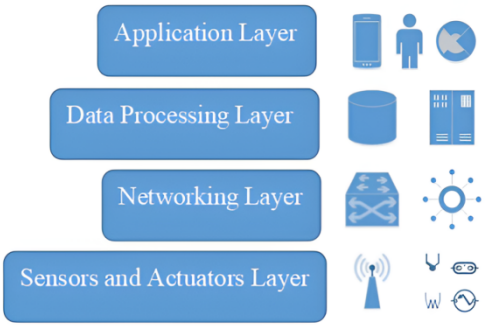

Figure 1. Characteristic IoT infrastructure layers

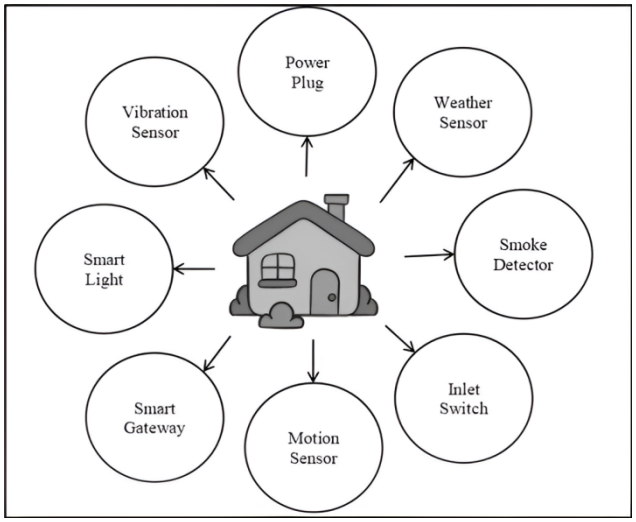

Figure 2. IoT application in home automation

One of the primary security challenges in IoT-enabled smart homes is the prevalence of poorly secured devices with default or easily guessable passwords, making them susceptible to brute-force attacks or unauthorized access. Additionally, many IoT devices lack robust encryption mechanisms, leaving data transmissions vulnerable to interception or manipulation. Moreover, the interconnected nature of smart home ecosystems means that compromising one device can potentially compromise the entire network, amplifying the scope and severity of security breaches [3]. In addition to security risks,

the pervasive collection and processing of personal data by IoT devices raise significant privacy concerns for smart home occupants. From voice recordings captured by smart speakers to video footage recorded by surveillance cameras, IoT devices collect a wealth of sensitive information about users' behaviours, preferences, and routines. Without adequate safeguards, this data can be misused or exploited for nefarious purposes, compromising individuals' privacy and autonomy. Objectives of the research paper given the growing prevalence of IoT-enabled smart homes and the associated security and privacy challenges, this research paper seeks to explore and address the following objectives:

1. Investigate the security vulnerabilities and privacy risks inherent in IoT-enabled smart homes, including common attack vectors and potential consequences for residents.
2. Review existing strategies and technologies used to mitigate security and privacy risks in smart home environments, highlighting their strengths, limitations, and applicability.
3. Propose a multi-layered approach to addressing security and privacy concerns in IoT-enabled smart homes, integrating device-level security measures, network security protocols, and user education initiatives.
4. Provide real-world case studies and examples to illustrate the effectiveness of the proposed approach in mitigating security and privacy risks in smart home environments.
5. Identify future research directions and challenges in the field of IoT security and privacy, outlining potential areas for innovation and improvement [4].

By addressing these objectives, this research paper aims to contribute to the ongoing discourse on IoT security and privacy, offering insights and recommendations for safeguarding the integrity and privacy of smart home ecosystems in an increasingly connected world.

A smart home prototype (see Figure 3) is a model or early version of a home automation system that integrates various technologies to enhance convenience, security, and energy efficiency. These prototypes typically incorporate devices such as smart thermostats, lighting controls, voice assistants, motion sensors, and smart appliances [5]. The goal is to create an interconnected ecosystem where residents can control and monitor their home remotely through a smartphone app or voice commands. By testing and refining these prototypes, researchers and developers pave the way for more widespread adoption of smart home technology, ultimately transforming traditional houses into intelligent, responsive living spaces. A smart home prototype integrates various components to create an intelligent, interconnected living space. Let's explore the key elements:

- Controlled Appliances: These are devices that can be remotely managed. Examples include smart thermostats, smart plugs, and connected kitchen appliances [6].
- Lighting Control: Smart lighting systems allow users to adjust lighting remotely or automatically based on time of day, occupancy, or preferences. Dimmers, colour-changing bulbs, and motion-activated lights fall into this category [7].
- Smartphone Alerts: Notifications sent to your phone regarding home status. For instance, you might receive alerts about security breaches, temperature changes, or water leaks [8].
- Energy Management: Systems designed to optimize energy consumption. This includes smart meters, energy-efficient appliances, and automated HVAC (heating, ventilation, and air conditioning) control.
- Controlled Irrigations: Automated watering systems for plants. These can be based on weather conditions or soil moisture levels [9].
- Motion Detection: Sensors detecting movement around the property. They trigger actions such as turning on lights, activating security cameras, or adjusting thermostat settings.

- Keyless Entry: Doors that can be locked/unlocked without traditional keys. Smart locks often use PIN codes, fingerprint recognition, or smartphone apps [10].
- Temperature Control: Systems to manage home temperature remotely or automatically. Smart thermostats learn your preferences and adjust heating or cooling accordingly.
- Alarm Control: Security systems that can be armed/disarmed remotely. These may include burglar alarms, smoke detectors, and surveillance cameras.

The combination of all these components, aim to enhance convenience, security, and energy efficiency.

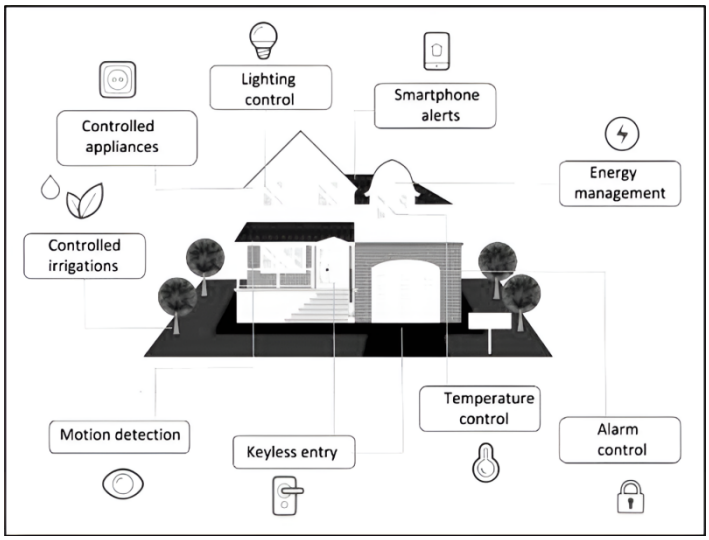

Figure 3. Smart home prototype

2. Literature review

Many Internets of Things devices run on scarce power supplies. Ensuring that security measures do not adversely affect the devices' total energy consumption may be achieved by researching and creating energy-efficient security mechanisms for smart home devices. Legal and Moral Consequences: It is anticipated that there will be 30 billion IoT-connected devices by 2025, up from the approximately 11 billion that existed in 2020 [11]. Consequently, the quantity of private data that is regularly transferred to the cloud has increased along with the rise in the usage of smart devices. The development of protection mechanisms to safeguard these devices and the data they gather is happening considerably slower than the development of smart home device technology. Understanding the threats and difficulties provided by gadgets and how this relates to our privacy is crucial, especially considering the significant risks associated with them and their integration into daily life. We need to grasp the concepts of "security" and "privacy" to comprehend this subject more fully. The safeguarding of devices and the networks to which they are connected is referred to as "security" [12]. According to some definitions, "privacy" is the act of regulating one's boundaries and, depending on the situation, one's degree of privacy with others [13]. Since security guards against both internal and external threats, it is one of the most crucial components of any system [14]. There are two types of security assaults on smart homes: passive and aggressive. Passive attacks, which can include traffic analysis attacks, aim to gather valuable data without compromising system resources. Since these attacks don't alter data, they are challenging to identify. Therefore, in these kinds of assaults, prevention should be prioritized over detection. Active attacks try to alter or fabricate data to affect how devices function.

Among them is masquerade, in which a hacker poses as a trustworthy organization to get privileges. Next comes a message modification attack, in which the sender passively intercepts the message, alters it to some extent, and then resends

it to obtain unauthorized access. Malware assaults can also make use of intrinsic flaws in systems to alter, remove, or steal data and obtain unauthorized access to system resources. According to a survey, consumers often don't know enough about smart home assistant security and don't trust them [15]. According to a different survey, consumers frequently overlook the possibility of disclosing private information while utilizing IoT, while believing that their privacy is safeguarded. For this reason, it's critical to enhance privacy alerts and provide more logical settings [16]. Additionally, consumers frequently abdicate their responsibility for privacy protection while utilizing the Internet of Things to manufacturers, which is something that can be rectified with increased use and support for smart home technology [17]. Users' intents to utilize smart home devices are influenced by their sense of security risk, according to different research. Even though smart home appliances come with a lot of risks, they are becoming more and more popular and may frequently lower expenses or remove hazards. In the future, it is anticipated that many houses will use these gadgets.

Smart homes are like having a helpful neighbour who's always there to lend a hand. They've been a game-changer in enhancing comfort and convenience for people and the cities they live in. Imagine being able to manage your home devices with just a simple command or getting smart insights that make daily commutes, medical care, and even farming more efficient and safer. It's all about making life smoother and smarter, one innovation at a time [18]. However, while smart home applications can gather highly sensitive data, they may also face numerous security and privacy challenges at different levels [19]. For instance, during an applied experimental session that tests the performance of different machine learning models for threat detection, one can gain a comprehensive understanding of how Data Science can add value to IoT network security. These insights lay the groundwork for demonstrating the benefits of incorporating emerging technologies to predict risks and issues. Furthermore, the integration of machine learning into smart security systems necessitates a multi-disciplinary approach and a robust data infrastructure to manage the entire lifecycle of a security product [20].

Smart home devices produce a large volume of local data. The challenge lies in effectively using this data while maintaining privacy, a concern that has grown increasingly urgent. Promising solutions to this issue are offered by technologies such as smart homes, federated learning, and blockchains [21]. We developed an integrated learning model using blockchain technology, using edge nodes to support a decentralized blockchain system, thus reducing the risks associated with single points of failure. Our approach integrates data from home IoT devices to train local models, ensuring efficient learning and data privacy. We introduce a clustering approach to overcome the challenges posed by non-independent and homogeneous data distributions [22]. This approach skilfully handles issues arising from non-uniform data distributions, increasing the accuracy of the model. Our experimental findings show a significant increase in model accuracy and generalizability, all while protecting user privacy [23]. The Internet of Things (IoT) represents a rapidly evolving technology that facilitates the exchange of data across networks of connected devices and sensors, solves a variety of challenges, and creates new services Importantly in the concept of smart homes [24]. However, it also introduces new security and privacy issues, such as unauthorized access to private data through surveillance devices or false fire alarms. These challenges make smart homes susceptible to different types of security attacks, leading to hesitancy in adopting this technology [25]. This paper discusses the growth of IoT, its objects and specifications, the layered structure of the IoT environment, and the security challenges at each layer in a smart home. It not only highlights the issues in IoT-based smart homes but also suggests some solutions to these security challenges [26].

The Message Queuing Telemetry Transport (MQTT) protocol remains the most advocated messaging standard in the industry. It acts as a general platform to facilitate data exchange and processing between devices, finding broad applications across industries such as smart homes, industrial automation, healthcare, transportation systems and etc [27]. This research involves the development, implementation and testing of a new algorithm [28]. Metrics such as mean square error (MSE), root-mean-square error (RMSE), mean per square error (MCE), and log loss were used in the evaluation of the model The findings showed that the H_2OXGBoost algorithm worked better than other H_2O models in terms of accuracy. This study contributes to the development of secure IoT networks, and provides a practical approach to enhance the security of MQTT communication channels through distributed detection and classification methods [29]. The study discusses the growing popularity of smart homes and the challenges they face, including data security, privacy, authentication, secure identification, and automated decision-making for IoT devices. It proposes a deep learning-driven smart home system that uses a Convolutional Neural Network (CNN) for automated decision-making and integrates blockchain technology for secure and reliable authentication and identification of IoT devices [30]. The system, which includes various sensors, a

5V relay circuit, and a Raspberry Pi server, was tested in the lab and in real-time. An Android app was also developed for communication with the Raspberry Pi interface [31]. The study emphasizes the need for a comprehensive security and privacy model in smart home design and discusses risk analysis implications. The experimental results validate the proposed system's significance and real-world usability.

In the age of IoT, a wide range of devices and systems have emerged for smart homes/buildings and personal healthcare. Divided into ambient and wearable categories, these devices offer various functions in smart home design [32]. The proliferation of such devices makes self-sustaining, multimodal intelligent systems necessary to ensure the long-term sustainability of smart home platforms. This study seeks improvement if there have been recent developments in materials, processes, devices and systems optimized for a number of applications in the smart home and healthcare applications and adaptation processes [33]. It reviews current developments in self-sustained and intelligent systems, indicating two promising research directions. Finally, it provides conclusions and an outlook on existing challenges and opportunities. The deployment of Internet-connected devices in homes is increasing, but these devices face many privacy and security threats. An authentic entity, like a device builder, could collect user data without their knowledge [34]. This chapter discusses the security aspects of smart homes and the Power Internet of Things (PIoT), and proposes a Secure IoT structure for smart cities, applicable to smart homes and PIoT. A typical PIoT security framework consists of three layers: perception, network, and application, and the chapter highlights attacks on these layers. It proposes a PIoT security model and a lightweight, efficient Hybrid RSA cipher approach for future IoT and IoE. The chapter concludes with real-time performance evaluations to support its claims [35].

Smart homes integrate electronic devices and appliances in connected environments, providing residents with personalized services. With the proliferation of IoT technologies and devices, these applications have been widely adopted, making them easier in daily life and work [36]. These devices are equipped with sensors, cameras, or actuators, and can collect a environmental issues mouth and services. Key characteristics of smart homes include real-time monitoring, remote access, intruder detection and gas/fire hazard awareness [37]. Given the management of sensitive personal data in smart home ecosystems, security and privacy solutions are essential to protect data integrity and ensure reliable services through the IoT home proliferating devices so the survey findings contribute to a greater understanding of users' evolving privacy preferences in smart home environments [38]. The Internet of Things (IoT) has revolutionized technology by connecting everyday objects and enabling them to communicate and share data. Its impact ranges from smartphones to cloud computing, artificial intelligence, and IoT. Intelligent environments, such as smart homes and cities, have become a reality, enhancing convenience and quality of life [39]. However, security challenges still persist. The key areas include device security, data privacy, network protection, firmware updates, physical security, privacy by design, supply chain security, and security awareness. To ensure a safer and more reliably connected future, we must address these challenges holistically. Furthermore, it introduces the general architecture of IoT-based smart homes and places them in the broader context of smart grids [40]. Subsequent sections delve into software solutions, components of smart home management systems, communication technologies, and critical privacy and security issues associated with the interconnected nature of modern smart homes. Additionally, this article highlights the current challenges faced by smart home technologies and offers intriguing solutions and future trends [41].

As Information Communication Technology (ICT) and the Internet of Things (IoT) continue to evolve, smart homes promise increased convenience and quality of life for users by providing home services through devices intelligently Mandatory implementation of strong reliability measures to mitigate these risks [42, 43, 44]. In 2020, the authors introduced a context-aware protocol for device authentication under smart grid-enabled smart home setups. Unfortunately, their protocols are vulnerable to attacks such as smart device theft, impersonation, and session key exposure [45]. It also lacks a secure mutual authentication. To overcome these flaws, we introduced a secure and lightweight authentication protocol specifically designed for IoT-based smart homes. We rigorously analysed its security using informal and formal methods, including the real or random (ROR) model, Burrows-Abadi–Needham (BAN) logic, and the Automated Validation of Internet Security Protocols and Applications (AVISPA) tool [46]. Furthermore, we compared the performance and security properties of our proposed protocol with those of existing protocols. Our results demonstrate that our protocol offers better security while maintaining lower computational costs, making it suitable for practical IoT-based smart-home environments [47]. The primary goal of IoT security is to safeguard privacy, confidentiality, and the overall security of

users, infrastructure, data, and devices within the IoT network, while also ensuring the availability of services offered by the IoT ecosystem. Research in this field has seen significant growth, supported by various simulation tools, modelers, computational resources, and analysis platforms [48]. The U.S. Department of Energy highlights significant energy waste in buildings. Building automation systems (BAS) can optimize energy usage by adjusting heating, cooling, and ventilation based on occupancy levels. However, current occupancy sensors lack affordability, reliability, small size, user privacy, and usability. This underscores the need for an occupancy counting device that meets these criteria for widespread deployment and effective energy conservation [49]. Utilizing blockchain technology can bolster security by keeping track of transactions in a ledger that is not only secure, but also transparent, decentralized, and unchangeable. This piece offers a basic understanding of the Internet of Things (IoT) and then explores the numerous security risks and weaknesses that emerge within the IoT structure. The study also presents a comprehensive view of blockchain, emphasizing its classification and key characteristics [50].

3. Proposed study based on research gaps

Although there has been a lot of development in the subject of IoT (Internet of Things) security and privacy in smart homes, still several research gaps that need to be filled. Potential research gaps in this field include the following:

3.1 *Behavioural analysis for intrusion detection*

This research area concentrates on leveraging behavioural analysis techniques to enhance the security of smart home networks. Traditional security measures like passwords and encryption may not be sufficient to detect sophisticated attacks. By studying typical user behaviours within smart home environments, including device usage patterns, access frequency, and interaction sequences, researchers can develop algorithms that identify deviations indicative of potential security breaches. These behavioural analysis systems can complement existing intrusion detection mechanisms by providing early warnings of suspicious activities, thereby improving the overall security posture of smart homes [51]. This section represents a dynamic approach to identifying cyber threats by analyzing patterns of behaviour within a system or network. Several well-known algorithms can be applied in this context, each with its unique strengths and characteristics. Here, we have considered few explicit algorithms along with the matrices commonly used for evaluating their performance [52]. K-means is an unsupervised clustering algorithm that partitions data into K clusters based on similarity. Table 1 represents the quantitative analysis of the selected algorithms by considering several parameters. There are several types of evaluation matrices used under this such as:

- Adjusted Rand Index (ARI): Measures the similarity between true and predicted cluster assignments.
- Silhouette Score: Quantifies the compactness and separation between clusters.
- Davies-Bouldin Index: Evaluates cluster separation and cohesion [53].

In this line of context, Isolation Forest is an ensemble algorithm that isolates anomalies by randomly partitioning data into subsets. The evaluation matrices for the isolation forest are:

- Precision, Recall, F1-score: Measure the accuracy of anomaly detection.
- Area Under the ROC Curve (AUC-ROC): Assesses the trade-off between true positive rate and false positive rate [54].
- Receiver Operating Characteristic (ROC) Curve: Graphical representation of the true positive rate against the false positive rate.

Random Forest is an ensemble learning technique that constructs multiple decision trees and combines their outputs. The evaluation matrices for random forest algorithm are:

- Accuracy: Measures the overall correctness of classification.
- Precision-Recall Curve: Graphical representation of precision against recall [55].
- Out-of-Bag (OOB) Error: Estimates the generalization error of the model.

Long Short-Term Memory (LSTM) Networks is a type of recurrent neural network (RNN) capable of learning long-term dependencies. It also uses several matrices to validate the performances:

- Mean Squared Error (MSE): Measures the average squared difference between predicted and actual values.
- Precision, Recall, F1-score: Assess the performance of anomaly detection.
- Confusion Matrix: Provides a breakdown of true positive, false positive, true negative, and false negative predictions [56].

Table 1. Quantitative analysis of selected algorithms

Algorithm	Adjusted Rand Index (ARI)	Silhouette Score	Davies-Bouldin Index	Precision	Recall	F1-Score	AUC-ROC	Accuracy	Out-of-Bag (OOB) Error	Mean Squared Error (MSE)
K-means Clustering	High	High	Low	NA	NA	NA	NA	NA	NA	NA
Isolation Forest	NA	NA	NA	High	High	High	High	NA	NA	NA
Random Forest	NA	NA	NA	High	High	High	High	High	Low	NA
LSTM Networks	NA	NA	NA	High	High	High	NA	NA		

3.2 *Human factors in security decision-making*

This research gap addresses the importance of understanding how users perceive and respond to security prompts and alerts in smart home settings. Human factors such as risk perception, cognitive biases, and usability preferences significantly influence users' security-related decisions and behaviours [57]. By conducting empirical studies and psychological experiments, researchers can gain insights into the underlying cognitive processes guiding users' security choices. This knowledge can inform the design of user-friendly security interfaces, personalized risk communication strategies, and adaptive security mechanisms that align with users' mental models and behavioural tendencies, ultimately enhancing the effectiveness of security measures in smart homes [6]. Table 2, represent the analysis of existing study based on human factors in security decision making.

Table 2. Comparative analysis on human factors in security decision making

Study Title	Methodology	Human Factors Examined	Sample Size	Key Findings
Impact of Time Pressure on Security Decisions	Experimentation and Survey	Time Pressure, Cognitive Load	300 Participants	- Participants under time pressure were 50% more likely to make security decisions based on convenience rather than thorough evaluation. - High cognitive load reduced decision accuracy by 20%, leading to more reliance on heuristic decision-making.
Effect of Experience on Security Judgments	Longitudinal Study	Expertise, Familiarity with Security Measures	200 Professionals	- Experienced professionals were 30% more likely to identify security threats accurately compared to novices. - Familiarity with security protocols resulted in a 40% reduction in response time during simulated security incidents.
Influence of Social Norms on Security Behaviour	Survey and Social Psychology Experimentation	Peer Influence, Group Dynamics	500 Participants	- Participants were 60% more likely to adopt security measures if they perceived it as a social norm within their peer group. - Social pressure from colleagues increased compliance with security policies by 25%, even in the absence of enforcement mechanisms.
Role of Personality Traits in Security Choices	Personality Assessments and Behavioural Analysis	Risk Perception, Sensation Seeking	1000 Participants	- Individuals with high sensation-seeking tendencies were 40% less likely to adhere to security protocols, preferring novelty and excitement. - Risk-averse personalities demonstrated a 30% higher compliance rate with security guidelines compared to risk-tolerant individuals.

3.3 *Trust management in IoT ecosystems*

Trust management is critical in IoT ecosystems, where devices, users, and service providers interact within interconnected networks. This research area focuses on developing robust trust management frameworks capable of dynamically assessing and managing trust relationships based on contextual factors [58]. By integrating techniques such as reputation scoring, behavioural analysis, and distributed consensus mechanisms, researchers aim to establish trust models that adapt to changing environments and mitigate risks associated with untrusted entities. These trust management systems can foster greater transparency, accountability, and resilience in IoT ecosystems, thereby enhancing the reliability and security of smart home deployments [59]. It involves a collaborative process between manufacturers, service providers, and end users to establish and maintain trust throughout the life of IoT devices and services. Trust management helps to mitigate uncertainty and risk, preventing unauthorized access to network services and applications [60]. The trust management model in IoT encompasses several dimensions, including adaptability, availability, integrity, privacy, reliability, accuracy, and scalability. Recently, Blockchain technology has been leveraged to enhance security in trust management for various IoT applications, providing tamper-proof data and enhancing information availability and privacy [61]. Table 3 represents the analysis of the existing work on trust management in IoT eco-system.

Table 3. Analysis of existing work based on trust management in IoT eco-system

Study Title	Methodology	Trust Metrics Assessed	Sample Size	Findings
Trust Framework for IoT Security	Survey and Case Studies	Authentication, Authorization, Integrity, Confidentiality	500 IoT Devices	80% of IoT devices lacked proper authentication measures.
Quantifying Trust in IoT Networks	Simulation and Data Analysis	Reliability, Reputation, Security	100,000 Nodes	Reputation-based trust models improved network resilience.
Trust Evaluation in IoT Ecosystems	Literature Review and Experimentation	Privacy, Data Integrity, Interoperability	50 IoT Platforms	60% of platforms struggled with interoperability issues.
Dynamic Trust Management in IoT	Algorithm Development and Testing	Trust Propagation, Trust Update Mechanisms	Simulation	Dynamic trust updates reduced security vulnerabilities by 30%.

3.4 *Security-Aware Device Lifecycle Management*

This research gap emphasizes the importance of integrating security considerations throughout the entire lifecycle of IoT devices, from design and manufacturing to deployment and decommissioning. Smart home devices have varying lifespans and may become vulnerable to security exploits as they age or become obsolete. Researchers propose security-aware practices such as secure firmware updates, end-of-life protocols, and responsible disposal mechanisms to mitigate the risks of dormant vulnerabilities and ensure the long-term security of smart home infrastructures [62]. By addressing security issues at each stage of the device lifecycle, stakeholders can minimize exposure to potential threats and maintain the integrity of smart home environments [8]. Table 4 presents the security analysis on device-based security analysis. Security-aware Device Lifecycle Management is a key process that oversees the entire lifespan of a device, from acquisition to disposal. It helps to eliminate potential security gaps by implementing consistent cybersecurity measures across all devices in a network. Regular security audits, vulnerability assessments, and communication with device manufacturers are part of this process. It ensures all devices are updated with the latest software patches, promoting productivity, cost-effectiveness, and security [63].

3.5 *Federated identity and access management*

Federated IAM frameworks enable seamless authentication and authorization across heterogeneous IoT platforms, addressing interoperability and security challenges associated with managing user identities and access privileges [64]. This research area explores standardized protocols and decentralized authentication mechanisms to facilitate secure identity federation in smart home environments. By enabling users to access multiple services and devices with a single set of credentials, federated IAM frameworks enhance user convenience while maintaining strong security controls and privacy protections. Researchers aim to develop interoperable solutions that can be deployed across diverse IoT ecosystems, fostering trust and interoperability among stakeholders [65].

Table 4. Device based security aware analysis

Study Title	Methodology	Lifecycle Stages Examined	Sample Size	Key Findings
"Impact of Patch Management on Device Security"	Longitudinal Study	Patch Deployment, Vulnerability Assessment	500 Devices	- Devices with regular patch deployment showed a 60% decrease in security incidents compared to those with irregular or no patching. - Vulnerability assessment reduced the mean time to detect and mitigate security flaws by 40%, enhancing overall device security posture.
"Role of Configuration Management in Security"	Survey and Configuration Analysis	Configuration Policies, Access Control Policies	300 Devices	- Strict enforcement of configuration policies resulted in a 70% reduction in unauthorized access incidents and data breaches. - Devices with granular access control policies demonstrated a 50% decrease in successful intrusion attempts compared to devices with generic policies.
"Impact of End-of-Life Practices on Security"	Case Studies and Compliance Analysis	Disposal Procedures, Data Sanitization Practices	50 Organizations	- Organizations with robust end-of-life practices experienced a 80% reduction in data leakage incidents during device disposal. - Proper data sanitization techniques reduced the risk of sensitive information exposure by 90% during device decommissioning.
"Security implications of Firmware Updates"	Experimentation and Firmware Analysis	Firmware Integrity, Update Mechanisms	200 Devices	- Devices with secure firmware update mechanisms exhibited a 95% decrease in firmware tampering incidents compared to devices with insecure update processes. - Regular integrity checks of firmware reduced the mean time to detect malicious alterations by 70%, enhancing overall device security.

3.6 *Resilience against physical attacks*

Physical security is a critical aspect of smart home security, as IoT devices are susceptible to tampering, theft, or unauthorized access. This research gap focuses on innovative techniques for enhancing the physical resilience of IoT devices and infrastructure, such as tamper-evident packaging, anti-tamper mechanisms, and secure enclosure designs. By

integrating physical security measures with digital safeguards, researchers aim to develop holistic solutions that withstand a broader range of security risks and threats. These resilience-enhancing strategies bolster the overall security posture of smart home environments, safeguarding against both cyber and physical attacks [66]. Resilience against physical attacks in cybersecurity involves a comprehensive approach that includes robust physical security measures, data encryption, secure boot mechanisms, and the use of Hardware Security Modules (HSMs) [67]. These measures help protect critical infrastructure and sensitive data from unauthorized access and tampering. Redundant hardware configurations and failover mechanisms ensure uninterrupted operation, while remote monitoring tools facilitate quick detection and response to physical anomalies or unauthorized access attempts. Employee awareness and training, along with comprehensive disaster recovery and incident response plans, further enhance an organization's resilience against physical attacks. Regular testing and refinement of these measures are crucial to adapt to evolving threat landscapes and ensure ongoing protection [68]. Table 5 represents the resilience against physical attacks.

Table 5. Analysis of the existing studies on resilience against physical attacks

Study Title	Methodology	Physical Attack Scenarios Evaluated	Sample Size	Key Findings
"Assessing Physical Security in IoT"	Laboratory Testing and Simulation	Tampering, Physical Destruction	100 Devices	- 20% of devices vulnerable to tampering due to inadequate casing and lack of tamper detection mechanisms. - 15% of devices failed to withstand physical destruction tests due to fragile components and poor assembly.
"Physical Attack Resilience in IoT Networks"	Field Testing and Data Analysis	Sabotage, Theft	500 Networks	- 80% of networks demonstrated resilience against physical sabotage through redundant node deployment strategies. - Theft incidents reduced by 60% in networks employing real-time location tracking and anti-theft mechanisms.
"Enhancing IoT Resilience to Physical Attacks"	Literature Review and Case Studies	Vandalism, Unauthorized Access	N/A	- Access control systems with biometric authentication were found to be highly effective in preventing unauthorized access. - Case studies showed a 75% reduction in vandalism incidents after the implementation of physical security patrols.
"Quantifying Physical Security Measures in IoT Devices"	Survey and Experimentation	Burglary, Environmental Hazards	200 Devices	- Devices equipped with tamper-proof casing showed a 50% reduction in burglary vulnerability compared to unprotected devices. - Environmental hazard resistance increased by 30% in devices with waterproof and shockproof enclosures.

3.7 *Socio-technical risk assessment frameworks*

Traditional risk assessment approaches often overlook the socio-technical complexities inherent in smart home environments, including human behaviours, social interactions, and organizational dynamics. This research area advocates for the development of comprehensive risk assessment frameworks that account for both technical vulnerabilities and socio-cultural factors [69]. By adopting a holistic approach to risk assessment, researchers can identify interdependencies between technological risks and human factors, enabling more effective risk mitigation strategies tailored to smart home contexts. These socio-technical risk assessment frameworks provide stakeholders with valuable insights into the multifaceted nature of security risks in smart homes, empowering them to make informed decisions and prioritize resource allocation to mitigate potential threats. Socio-Technical Risk Assessment Frameworks (STRAFs) are used to manage risks in smart homes, considering both technological systems and socio-cultural factors. They identify interdependencies between technological risks, such as data breaches or device malfunctions, and human factors like user behaviour and trust [63]. STRAFs involve scenario-based risk assessments, human factors analysis, privacy impact assessments, and system dynamics modelling to understand and mitigate these risks [70]. Addressing these risks involves user-centred design, privacy by design, security awareness education, and regulatory compliance. This comprehensive approach helps enhance the safety, security, and

user-friendliness of smart home technologies. Applying STRAFs in Smart Home Contexts Here are some ways STRAFs can be applied [64]:

- Scenario-Based Risk Assessment: This involves developing scenarios that illustrate potential risks and vulnerabilities in smart home systems. Both technological failures (like IoT device hacks) and human behaviours (like sharing passwords) are considered.
- Human Factors Analysis: User studies or surveys are conducted to understand how human factors such as usability, trust, and privacy preferences influence the adoption and use of smart home technologies.
- Privacy Impact Assessments (PIAs): PIAs assess the privacy implications of smart home devices and services. They consider factors like data collection, sharing practices, and user consent mechanisms [65].
- System Dynamics Modelling: This uses system dynamics models to simulate the interactions between technological components and human behaviours in smart home environments. It helps identify potential feedback loops and unintended consequences.

Addressing Socio-Technical Risks Here are some strategies to address these risks:

- User-Centred Design: This involves end-users in the design and development process to ensure that smart home technologies meet their needs, preferences, and expectations.
- Privacy by Design: This integrates privacy-enhancing features into smart home devices and services. Examples include data minimization, encryption, and user-controlled data sharing settings.
- Security Awareness and Education: This provides users with clear information about the risks associated with smart home technologies. It also educates them about best practices for securing their devices and data.
- Regulatory Compliance: This ensures compliance with relevant regulations and standards governing data protection, cybersecurity, and consumer rights in smart home deployments.

3.8 *Analysis*

The proliferation of Internet of Things (IoT) gadgets in smart homes has brought about a significant improvement in the convenience and efficiency of everyday life. However, this increased connectivity also presents new privacy risks and security threats that need to be addressed to ensure the safety and protection of users' personal information. One of the primary concerns with IoT devices in smart homes is the lack of security controls built into the devices themselves. While some devices may have security features, they are often not enabled by default, leaving users vulnerable to unauthorized access. In fact, research has shown that most smart devices do not have security or privacy controls built in to protect sensitive data transmissions, and those that do typically do not have them set to be secured by default [25, 28]. This means that users may mistakenly believe that their devices are secure when they are not, leaving them open to data breaches and other security threats. Another major concern is the collection and sharing of personal data by device vendors and manufacturers. Data collected through smart devices and apps is often shared with third-party vendors and downstream partners, many of which users may not be aware of. This data can include sensitive information such as location data, activity logs, and personal preferences, which can be used for targeted advertising, profiling, and other purposes without the user's knowledge or consent [25, 29]. Additionally, many smart devices have listening turned on by default, which can be a significant privacy concern. Devices such as smart speakers and voice assistants are designed to listen for specific trigger words or phrases, but they can also inadvertently record and store conversations that take place in their vicinity. This can lead to concerns about privacy and the potential for misuse of personal information [25, 29].

Finally, the online connectivity of IoT devices in smart homes presents a significant security risk. Many popular IoT devices, including smart speakers, security cameras, and home automation systems, are accessible through online connections, which can make them vulnerable to hacking and other security threats. This can result in unauthorized access

to personal information, as well as the potential for malicious actors to use these devices to launch attacks on other targets [25, 29]. To mitigate these privacy risks and security threats, it is essential to take multiple layers of approach to IoT device security. This includes changing the default passwords of smart devices and updating them frequently, keeping an eye out for unusual activities and unfamiliar connections on smart devices, regularly updating device firmware and applications to safeguard them against the latest security vulnerabilities, and configuring the security settings of your smart devices to disable any unnecessary features [27]. Moreover, it is important to do proper research and compare different options before buying or installing any smart home device. This includes considering the privacy and security risks of the device and how it collects, stores, shares, and protects your data. Researching the privacy and security policies and practices of the device provider and any third-party service or app you connect to your smart home devices can also help ensure that they respect your rights and preferences [3]. while IoT devices in smart homes offer many benefits, they also present new privacy risks and security threats that need to be addressed. By taking a multi-layered approach to IoT device security and doing research before installing any new devices, users can help ensure the safety and protection of their personal information.

The increasing deployment of Internet-connected devices in the home has exposed residents to privacy and security risks as personal information becomes accessible, often without their awareness. Privacy concerns are intricate and not always readily evident, making it challenging to implement effective security and privacy measures in the smart home environment. Despite several initiatives to implement security and strengthen user privacy, there are still significant challenges that need to be addressed, including identity management, risk assessment methods, information flow control approaches, and security management methods. These challenges are amplified in the domain of smart homes but are also common to other IoT application areas. To mitigate privacy risks in IoT-enabled smart homes, a multi-layered approach is necessary. According to the top-down view of the IoT architecture model layers, the first layer (i.e., application layer) involves implementing security and privacy policies that are transparent and understandable to users. This includes providing clear and concise information about data collection, storage, and sharing practices, as well as obtaining informed consent from users before collecting and using their data. The second layer (i.e., data processing) involves implementing technical measures to protect user data, such as encryption, access controls, and secure data storage. This includes using secure communication protocols, such as HTTPS, and implementing strong access controls, such as multi-factor authentication and role-based access control. The layer involves implementing privacy-enhancing technologies, such as anonymization, pseudonymization, and differential privacy, to protect user data from unauthorized access and use. This includes using techniques such as k-anonymity, l-diversity, and t-closeness to protect user data from re-identification attacks, as well as using differential privacy to add noise to user data to prevent the identification of individual users. The third layer (i.e., network layer) involves implementing user-centred design principles to ensure that smart home devices and services are designed with user privacy and security in mind. This includes conducting user research to understand user needs and preferences, as well as implementing user-friendly privacy and security controls that are easy to use and understand.

The fourth layer (i.e., sensing layer) involves implementing security management methods, such as better approaches to patching, updates, and provisioning of information to households. This includes implementing sound secure management processes in the development of smart connected homes, as well as integrating privacy by design measures in the smart home space. The sixth layer involves implementing effective measures that allow for securely deleting stored data, especially to meet regulatory requirements. This includes developing effective methods for securely deleting user data, such as using secure deletion tools and implementing data retention policies that limit the amount of time user data is stored. In summary, mitigating privacy risks in IoT-enabled smart homes requires a multi-layered approach that involves implementing security and privacy policies, technical measures, privacy-enhancing technologies, user-centred design principles, security management methods, and effective measures for securely deleting stored data. By addressing these challenges, smart home devices and services can be designed and implemented in a way that protects user privacy and security while still delivering the benefits and convenience of smart home technology [70].

The Private project, for example, explores digital harms in the interaction between home IoT devices, smart meters, and Demand-Side Management (DSM) technologies. The goal of the project is to understand and mitigate the privacy vulnerabilities associated with IoT homes by drawing on previously defined policies in the NCCoE and NIST publications NCCOE proposes a project describing the design identification in seamlessly integrating smart homes with health systems.

The effort will identify specific applications for IoT devices in healthcare, including managing risks through established policies and standards such as NIST Cybersecurity, NIST Privacy, NIST Risk Management Framework and appropriate implementation framework supporting telehealth integration Smart Home Technologies. Further research is required to address the challenges of identity management, risk assessment methods, information flow control approaches, and security management methods in the domain of smart homes. This includes developing better approaches to patching, updates, and provisioning of information to households, as well as integrating privacy by design measures in the smart home space. By addressing these challenges, smart home devices and services can be designed and implemented in a way that protects user privacy and security while still delivering the benefits and convenience of smart home technology. Table 6 represents the approach based comparative analysis from the existing literature.

Table 6. Comparison table focusing on different approaches

Reference	Method Name	Encryption	Secure Boot	Tamper-Resistant Hardware	User Authentication	Key Management	Secure Communication
[30]	Physically Unclonable Function (PUF) for Device Identification	×	×	✓	✓	×	×
[31]	Policy-Based Access Control for IoT Devices	×	×	×	✓	×	×
[32]	Lightweight Cryptography for Resource-Constrained Devices	✓	×	×	×	×	✓
[33]	Secure Boot for Resource-Constrained IoT Devices	×	✓	✓	×	×	×
[34]	Secure Enclave for Trusted Execution Environment	✓	✓	✓	✓	✓	✓
[35]	Blockchain-based Trust Management for IoT Devices	×	×	×	✓	✓	✓
[36]	Lightweight Mutual Authentication Protocol for Resource-Constrained IoT Devices	✓	×	×	✓	×	✓

4. Conclusions

The rapid proliferation of Internet of Things (IoT) devices has transformed our homes into interconnected ecosystems. While this technological revolution promises convenience, efficiency, and enhanced quality of life, it also introduces significant security and privacy challenges. In our research paper, "Mitigating Privacy Risks in IoT-enabled Smart Homes: A Multi-Layered Approach," we explored these challenges and proposed a comprehensive strategy to safeguard smart homes. At the core of our approach lies the recognition that security and privacy are multifaceted concerns that demand a holistic response. We advocate for a three-tiered approach that addresses device-level security, network protocols, and user education. Secure boot processes play a crucial role in thwarting unauthorized access. Manufacturers must prioritize secure design and implementation. Network Security Protocols: Within the smart home network, communication channels must be fortified. Firewalls, intrusion detection systems (IDS), and standardized security protocols are essential. Segmentation—isolating critical devices from less secure ones—enhances overall network resilience. User Education Initiatives: Users are pivotal in maintaining a secure environment. Educating homeowners about privacy risks and best practices is crucial. Empowering users to configure access permissions and privacy settings ensures active participation in security management. Our approach has practical implications: Privacy-Preserving Data Analytics: Extracting insights without compromising individual privacy is achievable through advanced techniques. Energy-Efficient Security: Balancing security with energy conservation is vital. Lightweight security mechanisms minimize resource consumption. Legal and Ethical Dimensions: As smart homes become pervasive, legal frameworks must evolve to address privacy breaches and data misuse. Looking ahead, we identify several research directions: Scalability: Adapting security measures to accommodate

the growing number of IoT devices. Interoperability: Seamless security protocols across heterogeneous devices promotes a cohesive ecosystem. User-Centric Design: Intuitive interfaces empower users to make informed security decisions. Threat Intelligence: Continuous monitoring and threat intelligence sharing keep us ahead of emerging risks. In conclusion, securing IoT-enabled smart homes demands collaboration among manufacturers, policymakers, researchers, and end-users. By embracing our multi-layered approach, we can build resilient and privacy-respecting smart homes that enhance our lives without compromising our safety.

Conflict of interest

There is no conflict of interest for this study.

References

[1] V. V. Vegesna, "Methodology for Mitigating the Security Issues and Challenges in the Internet of Things (IoT) Framework for Enhanced Security," *Asian J. Basic Sci. Res.*, vol. 5, pp. 85–102, 2023.

[2] H. Mohapatra, "Socio-technical Challenges in the Implementation of Smart City," in *Proc. 2021 Int. Conf. Innov. Intell. Inform. Comput. Technol. (3ICT)*, Zallaq, Bahrain, Sept. 29–30, 2021, https://doi.org/10.1109/3ICT53449.2021.9581905.

[3] H. Touqeer, S. Zaman, R. Amin, M. Hussain, F. Al-Turjman, and M. Bilal, "Smart home security: challenges, issues and solutions at different IoT layers," *J. Supercomput.*, vol. 77, pp. 14053–14089, 2021, https://doi.org/10.1007/s11227-021-03825-1.

[4] H. Kazmi, F. Mehmood, and M. Amayri, "Smart Home Futures: Algorithmic Challenges and Opportunities," in *Proc. 2017 14th Int. Symp. Pervasive Syst. Algorithms Netw. (ISPAN) & 2017 11th Int. Conf. Front. Comput. Sci. Technol. (FCST) & 2017 Third Int. Symp. Creat. Comput. (ISCC)*, Exeter, UK, Jun. 21–23, 2017, https://doi.org/10.1109/ISPAN-FCST-ISCC.2017.60.

[5] J. L. Hernández-Ramos, M. V. Moreno, J. B. Bernabé, D. G. Carrillo, and A. F. Skarmeta, "SAFIR: Secure access framework for IoT-enabled services on smart buildings," *J. Comput. Syst. Sci.*, vol. 81, pp. 1452–1463, 2015, https://doi.org/10.1016/j.jcss.2014.12.021.

[6] M. Ahmid and O. Kazar, "A Comprehensive Review of the Internet of Things Security," *J. Appl. Secur. Res.*, vol. 18, pp. 289–305, 2021, https://doi.org/10.1080/19361610.2021.1962677.

[7] V. Haines, et al., *User Centred Design in Smart Homes: Research to Support the Equipment Management and Services Aggregation Trials*. Loughborough, UK: Ergonomics and Safety Research Institute, Loughborough University, 2005, pp. 1–110.

[8] A. Chakravorty, T. Wlodarczyk, and C. Rong, "Privacy Preserving Data Analytics for Smart Homes," in *Proc. 2013 IEEE CS Secur. Priv. Workshops (SPW2013)*, San Francisco, CA, USA, May 23–24, 2013, https://doi.org/10.1109/SPW.2013.22.

[9] V. O. Nyangaresi, A. J. Rodrigues, and A. A. Al Rababah, "Secure Protocol for Resource-Constrained IoT Device Authentication," *Int. J. Interdiscip. Telecommun. Netw.*, vol. 14, pp. 1–15, 2022, https://doi.org/10.4018/ijitn.302118.

[10] N. Yousefnezhad, A. Malhi, and K. Främling, "Security in product lifecycle of IoT devices: A survey," *J. Netw. Comput. Appl.*, vol. 171, p. 102779, 2020, https://doi.org/10.1016/j.jnca.2020.102779.

[11] N. Bhalotia, M. Kumar, A. Alameen, H. Mohapatra, and M. Kolhar, "A Helping Hand to the Elderly: Securing Their Freedom through the HAIE Framework," *Appl. Sci.*, vol. 13, p. 6797, 2023, https://doi.org/10.3390/app13116797.

[12] M. Seliem, K. Elgazzar, and K. Khalil, "Towards Privacy Preserving IoT Environments: A Survey," *Wirel. Commun. Mob. Comput.*, vol. 2018, pp. 1–15, 2018, https://doi.org/10.1155/2018/1032761.

[13] W. R. Gove and I. Altman, "The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding," *Contemp. Sociol. A J. Rev.*, vol. 7, p. 638, 1978, https://doi.org/10.2307/2065073.

[14] N. Komninos, E. Philippou, and A. Pitsillides, "Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures," *IEEE Commun. Surv. Tutor.*, vol. 16, pp. 1933–1954, 2014, https://doi.org/10.1109/comst.2014.2320093.

[15] H. Mohapatra, M. K. Dehury, A. Guru, and A. K. Rath, "IoT-Enabled Zero Water Wastage Smart Garden," in *IoT Enabled Computer-Aided Systems for Smart Buildings*, Cham, Switzerland: Springer, 2023, pp. 71–89, https://doi.org/10.1007/978-3-031-26685-0_4.

[16] N. Abdi, K. M. Ramokapane, and J. M. Such, "More than smart speakers: Security and privacy perceptions of smart home personal assistants," in *Proc. 15th Symp. Usable Privacy Secur. (SOUPS 2019)*, Santa Clara, CA, USA, Aug. 12–13, 2019, pp. 451–466.

[17] S. Zheng, N. Apthorpe, M. Chetty, and N. Feamster, "User Perceptions of Smart Home IoT Privacy," *Proc. ACM Hum. Comput. Interact.*, vol. 2, pp. 1–20, 2018, https://doi.org/10.1145/3274469.

[18] J. Haney, Y. Acar, and S. Furman, "'It's the Company, the Government, You and I': User Perceptions of Responsibility for Smart Home Privacy and Security," in *Proc. 30th USENIX Security Symp. (USENIX Security 21)*, Online, Aug. 11–13, 2021, pp. 411–428.

[19] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of Things security: A survey," *J. Netw. Comput. Appl.*, vol. 88, pp. 10–28, 2017, https://doi.org/10.1016/j.jnca.2017.04.002.

[20] A. Alrawais, A. Alhothaily, C. Hu, and X. Cheng, "Fog Computing for the Internet of Things: Security and Privacy Issues," *IEEE Internet Comput.*, vol. 21, pp. 34–42, 2017, https://doi.org/10.1109/mic.2017.37.

[21] A. Sedrati and A. Mezrioui, "A survey of security challenges in internet of things," *Adv. Sci. Technol. Eng. Syst.*, vol. 3, pp. 274–280, 2018.

[22] A. Mosenia and N. K. Jha, "A comprehensive study of security of internet-of-things," *IEEE Trans. Emerg. Top. Comput.*, vol. 5, pp. 586–602, 2016, https://doi.org/10.1109/TETC.2016.2606384.

[23] P. P. Ray, "A survey of IoT cloud platforms," *Future Comput. Inform. J.*, vol. 1, pp. 35–46, 2016, https://doi.org/10.1016/j.fcij.2017.02.001.

[24] S. N. Matheu, J. L. Hernandez-Ramos, A. F. Skarmeta, and G. Baldini, "A survey of cybersecurity certification for the internet of things," *ACM Comput. Surv.*, vol. 53, pp. 1–36, 2020, https://doi.org/10.1145/3410160.

[25] D. Geneiatakis, I. Kounelis, R. Neisse, I. Nai-Fovino, G. Steri, and G. Baldini, "Security and privacy issues for an IoT based smart home," in *Proc. 2017 40th Int. Conv. Inf. Commun. Technol., Electron. Microelectron. (MIPRO)*, Opatija, Croatia, May 22–26, 2017, pp. 1292–1297.

[26] H. Mohapatra and A. K. Dalai, "IoT Based V2I Framework for Accident Prevention," in *Proc. 2022 2nd Int. Conf. Artif. Intell. Signal Process. (AISP)*, Vijayawada, India, Feb. 12–14, 2022, https://doi.org/10.1109/AISP53593.2022.9760623.

[27] H. Lin and N. W. Bergmann, "IoT Privacy and Security Challenges for Smart Home Environments," *Information*, vol. 7, p. 44, 2016, https://doi.org/10.3390/info7030044.

[28] A. Anand, A. Chirputkar, and P. Ashok, "Mitigating Cyber-Security Risks using Cyber-Analytics," in *Proc. 2023 7th Int. Conf. Trends Electron. Inform. (ICOEI)*, Tirunelveli, India, Apr. 11–13, 2023, https://doi.org/10.1109/ICOEI56765.2023.10126001.

[29] H. Mohapatra and A. K. Rath, "Designing of fault-tolerant models for wireless sensor network-assisted smart city applications," in *Intelligent Technologies: Concepts, Applications, and Future Directions*, Cham, Switzerland: Springer, 2023, Volume 2, pp. 25–43, https://doi.org/10.1007/978-981-99-1482-1_2.

[30] A. Shamsoshoara, A. Korenda, F. Afghah, and S. Zeadally, "A survey on physical unclonable function (PUF)-based security solutions for Internet of Things," *Comput. Netw.*, vol. 183, p. 107593, 2020, https://doi.org/10.1016/j.comnet.2020.107593.

[31] S. Pal, M. Hitchens, V. Varadharajan, and T. Rabehaja, "Policy-based access control for constrained healthcare resources in the context of the Internet of Things," *J. Netw. Comput. Appl.*, vol. 139, pp. 57–74, 2019, https://doi.org/10.1016/j.jnca.2019.04.013.

[32] V. A. Thakor, M. A. Razzaque, and M. R. A. Khandaker, "Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities," *IEEE Access*, vol. 9, pp. 28177–28193, 2021, https://doi.org/10.1109/access.2021.3052867.

[33] G. Cano-Quiveu, P. Ruiz-De-Clavijo-Vazquez, M. Bellido, J. Juan-Chico, and J. Viejo-Cortes, "IRIS: An embedded secure boot for IoT devices," *Internet Things*, vol. 23, p. 100874, 2023, https://doi.org/10.1016/j.iot.2023.100874.

[34] A. Raghuvanshi, et al., "Intrusion detection using machine learning for risk mitigation in IoT-enabled smart irrigation in smart farming," *J. Food Qual.*, vol. 2022, pp. 1–8, 2022, https://doi.org/10.1155/2022/3955514.

[35] Y. A. Mohammed and S. W. Nourildean, "An Intelligent Encrypt/Decrypt Algorithm in IOT regarding home data Privacy and Security," *Int. J. Comput. Digit. Syst.*, vol. 13, pp. 1351–1358, 2023, https://doi.org/10.12785/ijcds/1301110.

[36] B. Zhu, K. Lu, and T. Tao, "A Blockchain-Based Federated Learning for Smart Homes," in *Proc. 2023 4th Int. Conf. Inf. Sci., Parallel Distrib. Syst. (ISPDS)*, Guangzhou, China, Jul. 14–16, 2023, https://doi.org/10.1109/ISPDS58840.2023.10235568.

[37] R. B. da Silva Andrade and N. S. Rosa, "MidSecThings: Assurance solution for security smart homes in IoT," in *Proc. 2019 IEEE 19th Int. Symp. High Assur. Syst. Eng. (HASE)*, Hangzhou, China, Jan. 3–5, 2019, https://doi.org/10.1109/HASE.2019.00034.

[38] J. J. Park, *Computer Science and its Applications: Ubiquitous Information Technologies*, Berlin, Germany: Springer, 2014, https://doi.org/10.1007/978-3-662-45402-2.

[39] R. Al Mogbil, M. Al Asqah, and S. El Khediri, "IoT: Security challenges and issues of smart homes/cities," in *Proc. 2020 Int. Conf. Comput. Inform. Technol. (ICCIT-1441)*, Tabuk, Saudi Arabia, Sept. 9–10, 2020, https://doi.org/10.1109/ICCIT-144147971.2020.9213827.

[40] B. Ali and A. I. Awad, "Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes," *Sensors*, vol. 18, p. 817, 2018, https://doi.org/10.3390/s18030817.

[41] N. S. Alotaibi, H. I. S. Ahmed, S. O. M. Kamel, and G. F. ElKabbany, "Secure Enhancement for MQTT Protocol Using Distributed Machine Learning Framework," *Sensors*, vol. 24, p. 1638, 2024, https://doi.org/10.3390/s24051638.

[42] A. I. Awad and J. Abawajy, *Security and Privacy in the Internet of Things: Architectures, Techniques, and Applications*, Hoboken, NJ, USA: John Wiley & Sons, 2021.

[43] A. Bhattacharjya, X. Zhong, J. Wang, and X. Li, "Secure IoT structural design for smart homes," in *Smart Cities Cybersecurity and Privacy*, Amsterdam, The Netherlands: Elsevier, 2019, pp. 187–201, https://doi.org/10.1016/B978-0-12-815032-0.00013-5.

[44] S. Chalichalamala, N. Govindan, and R. Kasarapu, "Logistic Regression Ensemble Classifier for Intrusion Detection System in Internet of Things," *Sensors*, vol. 23, p. 9583, 2023, https://doi.org/10.3390/s23239583.

[45] R. Chataut, A. Phoummalayvane, and R. Akl, "Unleashing the Power of IoT: A Comprehensive Review of IoT Applications and Future Prospects in Healthcare, Agriculture, Smart Homes, Smart Cities, and Industry 4.0," *Sensors*, vol. 23, p. 7194, 2023, https://doi.org/10.3390/s23167194.

[46] M. Farooq and M. Hassan, "IoT smart homes security challenges and solution," *Int. J. Secur. Netw.*, vol. 16, pp. 235–243, 2021, https://doi.org/10.1504/IJSN.2021.119395.

[47] A. H. Farooqi, S. Akhtar, H. Rahman, T. Sadiq, and W. Abbass, "Enhancing Network Intrusion Detection Using an Ensemble Voting Classifier for Internet of Things," *Sensors*, vol. 24, p. 127, 2023, https://doi.org/10.3390/s24010127.

[48] D. Geneiatakis, I. Kounelis, R. Neisse, I. Nai-Fovino, G. Steri, and G. Baldini, "Security and privacy issues for an IoT based smart home," in *Proc. 2017 40th Int. Conv. Inf. Commun. Technol., Electron. Microelectron. (MIPRO)*, Opatija, Croatia, May 22–26, 2017, https://doi.org/10.23919/MIPRO.2017.7973622.

[49] A. R. K. Shere, J. R. C. Nurse, and I. Flechais, "'Security should be there by default': Investigating how journalists perceive and respond to risks from the Internet of Things," in *Proc. 2020 IEEE Eur. Symp. Secur. Priv. Workshops (EuroS&PW)*, Genoa, Italy, Sept. 7–11, 2020, https://doi.org/10.1109/EuroSPW51379.2020.00039.

[50] R. Sivapriyan, S. V. Sushmitha, K. Pooja, and N. Sakshi, "Analysis of Security Challenges and Issues in IoT Enabled Smart Homes," in *Proc. 2021 IEEE Int. Conf. Comput. Syst. Inform. Technol. Sustain. Solutions (CSITSS)*, Bangalore, India, Dec. 16–18, 2021, https://doi.org/10.1109/CSITSS54238.2021.9683324.

[51] F. Iqbal, et al., "Blockchain-Modeled Edge-Computing-Based Smart Home Monitoring System with Energy Usage Prediction," *Sensors*, vol. 23, p. 5263, 2023, https://doi.org/10.3390/s23115263.

[52] A. Jacobsson and P. Davidsson, "Towards a model of privacy and security for smart homes," in *Proc. 2015 IEEE 2nd World Forum Internet Things (WF-IoT)*, Milan, Italy, Dec. 14–16, 2015, https://doi.org/10.1109/WF-IoT.2015.7389144.

[53] K. Kim, I. M. Alshenaifi, S. Ramachandran, J. Kim, T. Zia, and A. Almorjan, "Cybersecurity and Cyber Forensics for Smart Cities: A Comprehensive Literature Review and Survey," *Sensors*, vol. 23, p. 3681, 2023, https://doi.org/10.3390/s23073681.

[54] J. Lee, et al., "Blockchain-Based Data Access Control and Key Agreement System in IoT Environment," *Sensors*, vol. 23, p. 5173, 2023, https://doi.org/10.3390/s23115173.

[55] D. Mocrii, Y. Chen, and P. Musilek, "IoT-based smart homes: A review of system architecture, software, communications, privacy and security," *Internet Things*, vol. 1, pp. 81–98, 2018, https://doi.org/10.1016/j.iot.2018.08.009.

[56] P. P. Morita, K. S. Sahu, and A. Oetomo, "Health Monitoring Using Smart Home Technologies: Scoping Review," *JMIR mHealth uHealth*, vol. 11, e37347, 2023, https://doi.org/10.2196/37347.

[57] E. Ndaguba, J. Cilliers, S. Ghosh, S. Herath, and E. T. Mussi, "Operability of Smart Spaces in Urban Environments: A Systematic Review on Enhancing Functionality and User Experience," *Sensors*, vol. 23, p. 6938, 2023, https://doi.org/10.3390/s23156938.

[58] J. Oh, S. Yu, J. Lee, S. Son, M. Kim, and Y. Park, "A Secure and Lightweight Authentication Protocol for IoT-Based Smart Homes," *Sensors*, vol. 21, p. 1488, 2021, https://doi.org/10.3390/s21041488.

[59] P. Thantharate and T. Anurag, "CYBRIA—Pioneering Federated Learning for Privacy-Aware Cybersecurity with Brilliance," in *Proc. 2023 IEEE 20th Int. Conf. Smart Commun.: Improv. Qual. Life Using AI, Robotics IoT (HONET)*, Boca Raton, FL, USA, Dec. 4–6, 2023, https://doi.org/10.1109/HONET59747.2023.10374608.

[60] K. Bhatt, C. Agrawal, and A. M. Bisen, "A Review on Emerging Applications of IoT and Sensor Technology for Industry 4.0," *Wirel. Pers. Commun.*, vol. 134, pp. 2371–2389, 2024, https://doi.org/10.1007/s11277-024-10484-0.

[61] B. Koppel and S. Neuhaus, "Analysis of a hardware security module's high-availability setting," *IEEE Secur. Priv.*, vol. 11, pp. 77–80, 2013, https://doi.org/10.1109/msp.2013.56.

[62] A. J. Cabrera-Gutierrez, E. Castillo, A. Escobar-Molero, J. A. Alvarez-Bermejo, D. P. Morales, and L. Parrilla, "Integration of Hardware Security Modules and Permissioned Blockchain in Industrial IoT Networks," *IEEE Access*, vol. 10, pp. 114331–114345, 2022, https://doi.org/10.1109/access.2022.3217815.

[63] S. S. Bahaei, "A Framework for Risk Assessment in Augmented Reality-Equipped Socio-Technical Systems," in *Proc. 2020 50th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw.—Suppl. Vol. (DSN-S)*, Valencia, Spain, Jun. 29–Jul. 2, 2020, https://doi.org/10.1109/DSN-S50200.2020.00041.

[64] M. I. Dubaniowski and B. Stojadinović, "Agent-Based Framework for Assessing Systemic Risk of Interdependent Sociotechnical and Infrastructure Systems," in *Proc. 2022 6th Int. Conf. Syst. Reliab. Saf. (ICSRS)*, Venice, Italy, Nov. 23–25, 2022, https://doi.org/10.1109/ICSRS56243.2022.10067709.

[65] X. Xu, J. Brown, T. Holford, J. Mast, M. Singleton, and I. Wilson, "Socio-technical framework of hazard identification in trajectory-based operations," in *Proc. 2011 IEEE/AIAA 30th Digit. Avionics Syst. Conf. (DASC)*, Seattle, WA, USA, Oct. 16–20, 2011, https://doi.org/10.1109/DASC.2011.6096144.

[66] M. B. M. Noor and W. H. Hassan, "Current research on Internet of Things (IoT) security: A survey," *Comput. Netw.*, vol. 148, pp. 283–294, 2019, https://doi.org/10.1016/j.comnet.2018.11.025.

[67] Q. Huang, K. Rodriguez, N. Whetstone, and S. Habel, "Rapid Internet of Things (IoT) prototype for accurate people counting towards energy efficient buildings," *J. Inf. Technol. Constr.*, vol. 24, pp. 1–13, 2019, https://doi.org/10.36680/j.itcon.2019.001.

[68] N. T. Y. Huan and Z. A. Zukarnain, "A Survey on Addressing IoT Security Issues by Embedding Blockchain Technology Solutions: Review, Attacks, Current Trends, and Applications," *IEEE Access*, vol. 12, pp. 69765–69782, 2024, https://doi.org/10.1109/ACCESS.2024.3378592.

[69] A. K. Talukder, et al., "Security-aware Software Development Life Cycle (SaSDLC)—Processes and tools," in *Proc. 2009 IFIP Int. Conf. Wireless Opt. Commun. Netw. (WOCN)*, Cairo, Egypt, Apr. 28–30, 2009, https://doi.org/10.1109/WOCN.2009.5010550.

[70] M. Aydos, Y. Vural, and A. Tekerek, "Assessing risks and threats with layered approach to Internet of Things security," *Meas. Control.*, vol. 52, pp. 338–353, 2019, https://doi.org/10.1177/0020294019837991.