Security and Privacy in Smart Home Systems During Crises and Emergencies: A Systematic Literature Review

Thomas Synaepa-Addison
University of Cincinnati
synaeptq@mail.uc.edu

Jess Kropczynski
University of Cincinnati
jess.kropczynski@uc.edu

ABSTRACT

This systematic literature review (SLR) investigates security and privacy threats, and solutions for Smart Home Systems (SHS) in crises contexts. SHSs are interconnected devices of which a breach of any one component can compromise the entire system. This SLR answers two questions: (RQ1) What are the documented security vulnerabilities and privacy risks associated with smart homes in emergency scenarios like fires or burglaries? and (RQ2) What technical or architectural solutions have been used to enhance the resilience of smart homes against security vulnerabilities and privacy risks? The analysis reports data management risks; (83.33% of articles) are most prevalent threats. Human related factors are less dominant but can jeopardize SHSs. Cryptography is mostly adopted in implementing security and privacy solutions while less studies focus on AI/ML and human practices. This research highlights the gap in crises-focused analysis, as existing studies dwell on general cyber security with no clear-cut solutions for crises.

Keywords

Crises, Privacy, Security, Smart Home System, Systematic Literature Review

INTRODUCTION

SHSs have become common in many households today and can be considered as a necessity for modern living, redefining how households integrate technologies and everyday activities. Poh et al. (2021) defined a SHS as a system of Internet of Things (IoT) devices that are used to improve living conditions in a home environment to enable automation and allow for remote control using mobile phones, tablets or other computing devices. SHS encompass a diverse range of applications such as cameras, thermostats, doorbells, streaming devices, Wireless Fidelity (Wi-Fi) devices, speakers, display monitors, smoke and alarm systems, door locks, lighting, plugs and outlets, home entertainment, vacuums and mops, televisions, pet feeders, and climate control devices (Google 2026; Amazon.com, Inc. 2025; Samsung Electronics Co., Ltd. 2025; Apple Inc. 2025). These systems enhance monitoring of environments to improving safety and security for residents (M. R. Alam et al. 2012). In crises situations, SHSs have become critical nodes as part of the emergency response network structure where signals are sent directly from SHS automatically upon detection of threats and are leading broader conversation on smart and sustainable communities.

Bishop (2003) described security as protection against threats to confidentiality, integrity, and availability of information. In early information-systems literature, privacy is often framed as individual control over personal information (Bélanger and Crossler 2011). However, recent scholarship argues that this view is necessary but not sufficient for datafied and AI-enabled environments. Group privacy highlights risks that emerge at collective levels even when no single individual is directly identified (Floridi 2017). Mühlhoff (2023) further argues that AI and big-data systems create predictive privacy harms at collective levels, requiring collective data-protection approaches beyond individual notice-and-consent models. Relatedly, anonymity and consent can be undermined by inference, linkage, and large-scale analytics (Barocas and Nissenbaum 2014). This broader framing is important for SHSs because data flows across households, platforms, and service ecosystems. Protecting SHSs therefore requires

attention to both individual and collective privacy harms, especially when emergency data sharing is intensified. A critical look at the case for cameras; analog surveillance cameras capture locally and are often isolated from external access, but cloud-connected smart cameras are vulnerable to credential stuffing, unauthorized access, and live-feed manipulation (E. Zeng, Mare, et al. 2017).

Starbuck et al. (1978) framed crises as circumstances that threaten organizational continuity. In residential contexts, fire and burglary are appropriate high-stakes focal scenarios because they are frequent, time-critical, and directly tied to physical safety and property loss. In 2020, U.S. fire departments responded to over one million fire incidents, with more than half in residential settings; internationally, millions of fires continue to be reported annually with substantial injuries and fatalities (International Association of Fire and Rescue Services (CTIF) 2022). U.S. burglary reports similarly indicate large incident volumes and major property losses (Federal Bureau of Investigation 2019). We therefore focus on fires and burglaries as analytically representative crises where SHSs operate as both ally and adversary: they can provide early detection and rapid notification (Karemaker et al. 2021), but they can also fail under attack (for example, alarm suppression, denial of service, credential abuse), leading to delays in emergency response (Sredhar et al. 2024; Mahlous 2023).

Fires and burglaries are not the only crises relevant to smart homes, but they are among the most common and policy-relevant residential emergencies, and they strongly exercise core SHS functions including detection, alerting, access control, and remote monitoring, under severe time pressure (International Association of Fire and Rescue Services (CTIF) 2022; Federal Bureau of Investigation 2019; Karemaker et al. 2021). As a result, they provide a high-contrast test bed for evaluating whether security and privacy controls hold when consequences escalate quickly (Sredhar et al. 2024; Mahlous 2023). We therefore treat them as representative lookout scenarios for household crisis resilience, where findings are expected to transfer most directly to crises with similar characteristics such as heightened vulnerability, high urgency, safety implications, and reliance on device-to-cloud communication (Starbuck et al. 1978; Barbosa et al. 2024).

SHSs are vulnerable to multiple security and privacy threats which are exacerbated during fire and burglary crises. Such threats are comprised of technically complex problems to minor problems. In highly interconnected systems like SHSs, even low-severity issues cannot be taken for granted as a single flaw can cascade the entire system, and compromise security and privacy. Previous studies have recorded threats including access control, poor authentication, data leakage, and intrusion detection (Zheng et al. 2018; Fernandes et al. 2016). Solutions that have been used to address threats to SHSs revolve around technical implementation, organizational governance, and human behaviors. Existing reviews are broad in scope and have not specified peculiar challenges as they relate to smart home systems during crises. A situation of a denial of service attack is known to inconvenience users but the consequences in a fire crises could have dire implications as it could delay or deny notification to emergency responders. This lack of collective, crises focused synthesis represents a research gap and necessitates this SLR to address the research questions giving the pervasive adoption of SHSs and increasing occurrence of crises.

This SLR investigates prior literature in crises contexts of the security and privacy threats, and solutions for SHS. The authors aim to evaluate the security challenges and privacy risks, and solutions that affect SHS during fire and burglary crises situations. The SLR is guided by these research questions:

1. What are the documented security vulnerabilities and privacy risks associated with smart homes in emergency scenarios like fires or burglaries?
2. What technical or architectural solutions have been used to enhance the resilience of smart homes against security vulnerabilities and privacy risks?

By answering these research questions, this study seeks to provide valuable insights into smart home security and privacy threats and solutions during crises. The study analyzes challenges including data management risks, network and communication based attacks, technical and protocol level vulnerabilities, systemic and architectural weaknesses, and human and user-centric factors. For solutions, the study analyzes these: cryptographic mechanisms, resilient system architectures, context-aware and policy based control, AI/ML driven security, and foundation security practices.

RELATED WORKS

To position the SLR, this section synthesizes prior work on: (1) baseline SHS security/privacy challenges, (2) SHS use in crisis and emergency contexts, and (3) human-centered resilience. This narrative review identifies the gap that the systematic review addresses in subsequent sections.

The Smart Home Ecosystem: Functionality and Baseline Challenges

Zeghida et al. (2024) reported that many SHS deployments still depend on weak communication configurations such as insecure transport, creating interception opportunities. Sharif and Tenbergen (2020) showed that always-on devices, especially voice assistants and cameras, continuously collect behaviorally rich data that can be repurposed for profiling and surveillance. Edu et al. (2020) identified concrete privacy concerns including non-transparent sharing of user data with third parties, unclear downstream reuse of data for analytics and marketing, and limited user ability to control retention and deletion of collected data. Girish et al. (2023) further linked insecure communication and poor access control to unauthorized access to sensitive household data, including financial and behavioral information.

Personal data may be shared by such systems with third-party services without explicit user consent, creating risks of secondary use, re-identification, and behavioral profiling (Edu et al. 2020). Ansari et al. (2024) classified smart home system vulnerabilities and emphasized that threats include unauthorized access and leakage of data due to insecure interfaces and misconfigurations. Touqeer et al. (2021) reviewed security challenges across multiple IoT layers within smart home systems and identified that threats affect different aspects at different times and in different situations across both device and network layers. Popoola et al. (2024) noted the combination of IoT and blockchain for healthcare smart home systems in particular introduces some security and privacy threats due to distributed data sharing such as data confidentiality, access control and trust management. Edu et al. (2020) classified security threats of voice-controlled and AI-assistant-powered smart home systems and highlighted privacy concerns in data collection, cloud storage, and inference from interaction logs.

Yang and Sun (2022) found that smart home systems are vulnerable to malware, eavesdropping, and physical attacks. Utomo et al. (2022) similarly showed that IoT-enabled home benefits are accompanied by persistent security and privacy trade-offs. Khawla and Tomader (2018) emphasized weak protocols and physical device insecurity as recurring technical causes. Vardakis et al. (2024) demonstrated that controls effective at one layer (device, network, or data) often fail when threats traverse layers, leaving systemic security gaps. Security analysis by Fernandes et al. (2016) showed that privilege-escalation vulnerabilities can let attackers issue unauthorized commands on smart devices; however, this work did not model emergency conditions where the impact of command abuse is amplified.

Smart Homes in Crisis and Emergency Contexts

The use of smart home systems has gained attention in crisis scholarship. Barbosa et al. (2024) examined smart-home-enabled resilience during COVID-19 in Brazil and explicitly discussed devices such as smart cameras, voice assistants, wearable health monitors, and connected environmental sensors used for remote monitoring, risk signaling, and coordination across household members and care/support networks. K. Mohan et al. (2016) demonstrated that IoT-based emergency evacuation systems in residential buildings can combine sensing, alerting, and mobile guidance to improve evacuation performance. Shahzad et al. (2024) proposed an IoT-based Smart Emergency Response System that integrates home, mobility, and health signals for emergency management. Collectively, these studies indicate that crisis value depends on cross-device reliability and timely data sharing, not only on isolated device intelligence.

Ray et al. (2017) in a survey categorized solutions provided by smart home systems for disaster management into that which provide early warnings, remote monitoring, an coordinated decision to support in crisis situations. Boukerche and Coutinho (2018) proposed smart disaster detection and response system is focused on integrating smart home infrastructure and emergency responders to enable timely data sharing and risk mitigation during crises. F. Zeng et al. (2023) in their systematic review looked at interconnected smart homes devices as important nodes to coordinate in locating individual persons and dissemination of situational awareness to emergency responders during urban disaster management. Alshamaila et al. (2023) developed a framework for disaster response for buildings with smart home systems incorporating multiple technologies including IoT, fog computing, and cloud technologies to produce energy-efficient and faster evacuation of persons. A systematic analysis of smart home systems by Akhtar et al. (2024) identified the current trends and recommended the need for identifying flaws to improve such systems during emergencies.

Human-Centered Security and Resilience in Emergencies

Smart home systems much as other interconnected systems and networked systems are vulnerable to attacks in their normal operations (H. Alam and Tomai 2023). These vulnerabilities are heightened during fire and burglary crises. SHS are both vulnerable during normal states and emergency states (Nandhini and Prakash 2024). Resilient IoT architectures show the redundancy and distributed security frameworks are able to mitigate risks in crises situations but resource limitations of SHS prevent the implementation of such solutions (Castro and Jack 2022).

Barhamgi et al. (2018) proposed an architectural framework that allows users to balance privacy risk with benefits and make informed decisions about how much data to share in a smart home system. Privacy preservation is especially critical during crises because urgency increases data sharing while also increasing exposure to unauthorized access, eavesdropping, and leakage. Chhetri and Genaro Motti (2022) showed that users often rely on default privacy settings because they perceive them as easier and safer under cognitive load, but this reliance can hide meaningful trade-offs in data visibility and control. Zheng et al. (2018) corroborated this pattern, showing that users tend to trust preset configurations from manufacturers and providers while lacking clear understanding of the resulting privacy exposure.

E. Zeng and Roesner (2019) demonstrated that smart homes are multi-user and multi-device systems and explored security and privacy challenges in this context noting that such problems associated here emanate from the other users who may or may not have authorization. The researchers mentioned that the security and privacy challenges with network and embedded systems aspects of smart home systems are exposed by remote attackers but companies and business entities exploit data privacy and surveillance limitations to collect information without users explicit consent which endanger user security and privacy.

In Kafle et al. (2024), the authors discussed the HomeEndorser framework that utilize device states of hardware resources in addition to software prevent malign actors ability to safeguard smart home environments. Smart home systems sensors can allow for limited access to controls to threats when smart home sensors detect an emergency and the primary user does not provide feedback (Agrawal et al. 2020). The Privacy via Anomaly-detection System (PALS) posited by Dutta et al. (2020) uses context sourced from sensed data and user behaviors to make necessary overrides to policies to enable access in different situations. Purohit and Sharan (2024) posited that intrusion detection systems rely on machine learning algorithms to continuously monitor home environments in order to identify inconsistent activities from sensors to trigger counter measures like sounding alarms.

METHODOLOGY

This study follows Keele et al. (2007) as the primary SLR protocol for planning, conducting, and synthesizing evidence. We use PRISMA 2020 (Page et al. 2021) as a reporting framework to transparently document identification, screening, eligibility, and inclusion decisions. We use the work of Keele et al. (2007) to structure the review process, while PRISMA (Page et al. 2021) shows how the process is reported.

Query

We searched ACM Digital Library, IEEE Xplore, and Scopus. The query was built from three keyword categories (Table 1): (1) smart home context, (2) security/privacy, and (3) crisis context. To select the primary studies, a search query was crafted with the keywords (k) in the three categories (c) as shown in Table 1. For each category, denoted as C_i, with i as category number, there was a use of disjunction of keywords, k, to get $C_i = K_1$ OR K_2 OR $...K_n$. The categories are three, C_1, C_2 and C_3. To get the final search query, we combined each of these categories as a conjunction, C_1 AND C_2 AND C_3 which was executed in the databases. The crisis category deliberately included fire- and burglary-related terms because these were the predefined focal crisis types. To reduce the risk of missing burglary studies, we tested additional synonyms such as housebreaking, property theft, and breaking and entering, during pilot searches; these terms did not retrieve additional in-scope records after title/abstract screening and often produced legal or policing studies outside SHS contexts. We therefore retained the final compact query shown in Figure 1.

Table 1. Keywords used in SLR

Category, C	Keywords, K
Smart Home	smart home, iot home, home automation, smart home hub, gateway, iot hub, smart home system, smart home environment, smart home device
Security and Privacy	security, privacy, data protection
Crisis	crisis, emergency, fire, burglary

("smart home" OR "iot home" OR "home automation" OR "smart home hub" OR "gateway" OR "iot hub" OR "smart home system" OR "smart home environment" OR "smart home device")

AND

("privacy" OR "security" OR "data protection")

AND

("cris" OR "emergenc*" OR "burglary" OR "fire")*

Figure 1. Search Query

Inclusion and Exclusion Criteria

After conducting the search across the databases, the results showed multiple publications some of which the researchers considered irrelevant to this systematic literature review due to use of common words as keywords. The research applied the inclusion and exclusion criteria shown in Table 2 to compile a dataset of primary studies. A study is considered a primary study (PS) if it met the inclusion and exclusion criteria stipulated in Table 2.

Table 2. Inclusion and Exclusion Criteria

Inclusion Criteria	Exclusion Criteria
Research articles	Non-English articles
Articles written in English	Theses and Dissertations
Articles published between January 2015 and July 2025	Systematic literature reviews
Articles that have full text available for review	
Articles published in journals	
Articles focused on crises and emergencies	

To ensure inclusion of relevant literature, we restricted the publication period to January 2015–July 2025 and retained peer-reviewed journal and conference articles with full text. Duplicates and non-English records were removed. Title and abstract screening then applied the inclusion/exclusion criteria in Table 2; eligibility checks at full-text stage applied the same criteria plus topical fit to fire or burglary emergency contexts. This process produced 24 primary studies, as shown in Figure 2.

Quality Assurance

Each of the articles was evaluated by review the title, abstract, and keywords to ascertain the relevance to security and privacy of smart home systems in crises and emergency contexts particularly fires or burglaries or both. Out of the 24 selected papers, twenty-three (23) articles representing 95.83% were classified as Highly Focused decisively addressing the research questions. The remaining one (1) article representing 4.17% was classified as Less Focused as it had minor connection to the research question. The quality assurance process followed a quantitative approach to guarantee that the final synthesis reflected relevant and reliable literature. The final dataset was normalized to a value of 100% after which the proportion corresponding to either Highly Focused or Less Focused was derived using the formula:

$$P_i = \left(\frac{n_i}{n_{\text{total}}}\right) \times 100 \tag{1}$$

$$P_{\text{Highly Focused}} = \left(\frac{n_{\text{Highly Focused}}}{n_{\text{total}}}\right) \times 100 \tag{2}$$

$$P_{\text{Less Focused}} = \left(\frac{n_{\text{Less Focused}}}{n_{\text{total}}}\right) \times 100 \tag{3}$$

This quantitative model allows for the final dataset to be sufficiently focused which provided a robust basis for synthesis and analysis. The results from the computation is shown in Table 3.

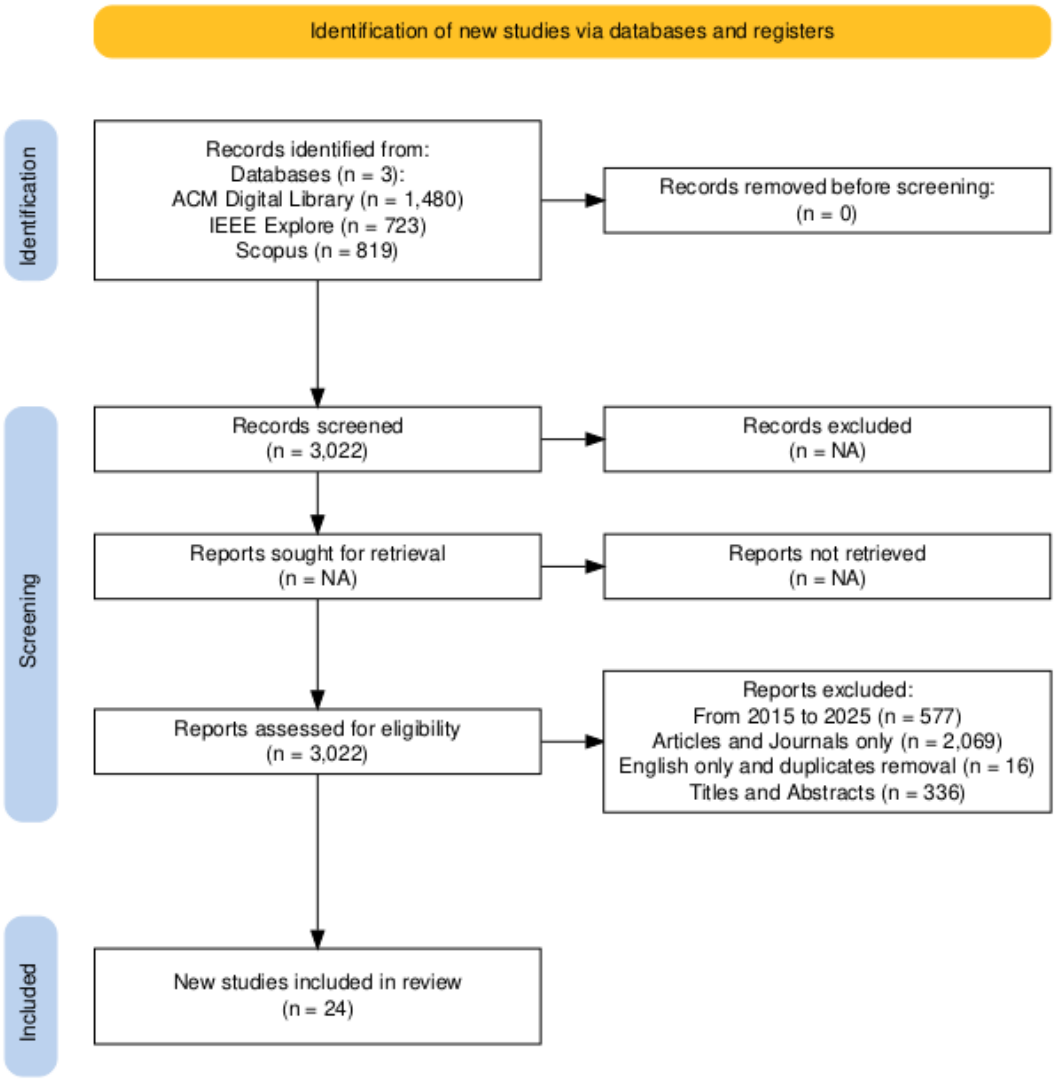

Figure 2. Page et al. (2021) PRISMA flow diagram showing the inclusion and exclusion process

Data Extraction

For data extraction, we used a structured template with thirteen fields aligned to the research questions. SciSpace was used as an assistive summarization and information-retrieval aid but not as a decision maker which was to accelerate initial field population (SciSpace 2022). All extracted entries were then manually checked, corrected, and normalized by the authors against full-text articles.

Table 3. Quality Assurance Criterion

	Highly focused	**Less focused**
What is the degree to which the article addresses fires and burglary scenarios of security and privacy in smart home systems in crises context?	95.83%	4.17%

Data Analysis

Data extracted was analyzed based on the type of information gathered from articles. In some cases, a quantitative count could be generated based data presented in articles. For example, the types of emergency; fire or burglary implemented in the papers may be presented in a quantitative count. However, other types of data extracted were more qualitative in nature, such as the types of privacy challenges that each article addressed. In this case, notes on the types of challenge were gathered in a database of researcher notes. We used Google Gemini with a constrained prompt posited by (Basty et al. 2025) as a secondary coding assistant to propose candidate codes across the 24 studies (Table 6), while human coders performed independent coding in parallel. AI assistance was used to improve coding consistency and auditability, not to replace interpretive judgment. Final themes and sub-themes reported in this paper are human-validated outputs.

RESULTS

This section summarizes the findings from the systematic literature review on security and privacy of SHSs during fire and burglary emergencies. The challenges in relation to security and privacy risks, and the technical or architectural solutions of SHSs identified are categorized.

Security Challenges and Privacy Risks in the Literature (RQ1)

The analysis of security challenges and privacy risks from the literature as shown in Table 4 revealed certain themes across. Management risks in relation to data access, control and governance was most common followed by network and communication based attacks. Technical and protocol-level vulnerability like authentication and implementation flaws together with systematic and architectural weaknesses followed as the common themes. Human and user-centric factors were the least occurring theme across the literature.

Management risks (83.33%, N=20) was the most common type of security challenge and privacy risk. The analysis of this theme revealed further that unauthorized access and data exposure dominated (80.00%, N=16) supporting the assertion that personal data are highly vulnerable to breaches. Just a few studies focused on deficient user control and data governance (20.00%, N=4) suggesting that despite the existence of governance challenges, they are less relevant compared data access.

The second common theme was network and communication based attacks (62.50%, N=15). Within this theme, spoofing and impersonation (40.00%, N=6) were the most commonly reviewed, followed by service disruption and interception (33.33%, N=5), and side channel and traffic analysis (26.67%, N=4). This therefore disclose that there are multiple threats aimed at communication pathways, with impersonation in particular due to the capability to go around trust structures within interconnected environments.

Technical and protocol-level vulnerability (54.17%, N=13) made up the next common theme. Within this theme, weak cryptography and authentication (6.15%, N=6) and software and implementation flaws (46.15%, N=6) had similar distribution in the mentions among the primary studies. Authentication bypass and evasion (7.69%, N=1))was relatively negligible. This allocation insinuate that encryption and software robustness are pressing needs, but specialized attacks that exploit bypasses are less frequent in the literature.

Systematic and architectural weaknesses (54.17%, N=13) was of similar weight as theme specified above. The most frequently reported challenge in this section was ecosystem complexity and fragmentation (38.46%, N=5). The two

other observed challenges reported under this theme were inadequate security and management practices (30.77%, N=4) and device-level constraints (30.77%, N=4). These challenges show that resources limitation of smart devices prevent the deployment of next-level security mechanisms.

The least reported threat by the literature was human and user-centric factors (37%, N=9). Among these are malicious data and deception (22%, N=4), insider and social threats (33%, N=3), and user practices and errors (44.44%, 4). This theme emphasize that end users of smart devices intentionally misuse or through unintentional error are contributors to making smart home systems vulnerable.

Further analysis shows there are different challenges and reveal some patterns. Management risks and attacks on networks are dominant and shows that data management and communication security are core to smart home systems. While human related factors are less dominant, they equally can contribute to the overall shutdown of a system by amplifying technical drawbacks. These findings show that security and privacy challenges in SHSs cover different dimensions from technical implementation to user behavior. The connection between these challenges show that they are not disjointed but interconnected such that a loophole in one can affect the entire architecture.

Technical and Architectural Solutions in the Literature (RQ2)

The thematic analysis of technical and architectural solutions addressed in the literature is shown in Table 5. Cryptographic mechanisms were the most common, followed by resilient system architectures and context-aware/policy-based controls. Artificial intelligence and machine learning driven security, and foundational security practices, appeared with lower frequencies.

Cryptographic mechanisms (33.33%, N=7) was the most frequently occurring theme. This suggests that there is a huge dependence on encryption and secure authentication protocols as seen in the literature as solutions to security and privacy. The next most frequently occurring themes include Resilient System Architectures (19.00%, N=4) and Context-Aware and Policy-Based Control (19.00%, N=4). Resilient system architectures theme was further divided into hardware-software co-design (9.50%, N=2) and decentralized and zero-trust models (9.50%, N=2). This supports the position that security solutions are incorporated into the physical components of smart home systems. This also suggests that solutions take into consideration the dynamic and changing context of situations.

The next most frequently discussed theme was Artificial Intelligence (AI) and Machine Learning (ML) driven security (14.30%, N=3). The higher research theme within this is anomaly and threat detection (9.50%, N=2) while the least is biometric authentication (4.80%, N=1). This indicates that there is a growing interest in exploring systems being able to identify attacks addressing common adversaries. The least common identified theme across the studies was foundational security practices (14.30%, N=3). This theme focuses on best practices adopted by end users and tools for maintaining, monitoring, and recovery of systems.

These findings reveal a pattern where complex technical problems are more addressed. Cryptography is widely adopted in providing solutions to address security and privacy threats of data management and communication (Yusoff et al. 2024; Sharma and Dhiman 2024). Cryptography is adopted in privacy preservation and data anonymization of sensitive user data collected by smart home devices (Abu-Tair et al. 2020). The focus on human factors, extensive applications of AI/ML and system management as solutions are less researched.

In conclusion, these findings show that research focusing on solutions to security and privacy of smart home systems are inclined towards technical threats that are address particularly by cryptography. Other solutions that are more focused on human factors, AI/ML and system management are less researched and this creates a research gap in solutions for smart home system security and privacy threats.

Table 4. Thematic Analysis of Security Challenges and Privacy Risks

Theme and Sub-theme(s)	Definition
Theme 1:Data Management Risks (83.33%, N=20)	**The compromise of personal and sensitive information through improper handling, storage, and access control.**
1.1 Unauthorized Access and Data Exposure (80%, N=16)	The illicit viewing, theft, or leakage of sensitive user data, including personal identifiers, credentials, and private activities.
1.2 Deficient User Control and Data Governance (20%, N=4)	This includes issues related to users' inability to manage their data, insecure data life cycle management, and opaque system processes.
Theme 2: Network and Communication Based Attacks (62.50%, N=15)	**Threats that target the data in transit between smart devices, gateways, cloud services, and user applications**
2.1 Service Disruption and Interpretation (33.33%, N=5)	The malicious actions aimed at making services unavailable (Denial of Service) or secretly listening to communications.
2.2 Spoofing and Impersonation (40.00%, N=6)	The attacks where and adversary masquerades as a legitimate device, user, or network component to gain unauthorized access.
2.3 Side-Channel and Traffic Analysis (26.67%, N=4)	The techniques that exploit indirect information leakage (for example power usage, data packet timing) to infer sensitive information or user activities.
Theme 3: Technical and Protocol Level Vulnerability (54.17%, N=13)	**These include the flaws within the fundamental software, hardware, and cryptographic implementations of smart home systems.**
3.1 Weak and Cryptography and Authentication (46.15%, N=6)	These are vulnerabilities from poorly implemented encryption, authentication mechanisms, and key management practices.
3.2 Software and Implementation Flaws (46.15%, N=6)	These are the security gaps from design flaws, insecure configurations in device operating systems, firmware and applications.
3.3 Authentication Bypass and Evasion (7.69%, N=1)	These are methods used by attackers to bypass identity verification systems that may rely of biometrics.
Theme 4: Systemic and Architectural Weaknesses (54.17%, N=13)	**These are the high level and structural problems in the broader smart home ecosystem that create a permissive environment for threats.**
4.1 Ecosystem Complexity and Fragmentation (38.36%, N=5)	These are the security challenges from the diverse and incompatible nature of devices and platforms, creating large and inconsistent attack surface.
4.2 Inadequate Security and Management Practices (30.77%, N=4)	This includes the failure to implement dynamic, context-aware security policies and updates that leave systems vulnerable to evolving threats.
4.3 Device-Level Constraints (30.77%, N=4)	These are inherent limitation of IoTs including low computational power, physical vulnerability, low memory that hinder robust security.
Theme 5: Human and User-Centric Factors (37.50%, N=9)	**These are the vulnerabilities introduced by the actions, behaviors, and social context of people interacting with smart home systems**
5.1 User Practices and Error (22.22%, N=2)	These are security risks created by users including using weak passwords, misconfiguration of devices, or placing undue trust in manufacturers settings.
5.2 Insider and Social Threats (33.33%, N=3)	These are threats from legitimate or former users, including malicious insiders or issues arising from the transfer of devices to new owners.
5.3 Malicious Data and Deception (44.44%, N=4)	These include the injection of false information into the system to mislead its logic or trigger incorrect responses.

Table 5. Thematic Analysis of Technical and Architectural Solutions

Theme and Sub-theme(s)	Definition
Theme 1: Cryptographic Mechanisms (33.33%, N=7)	**The application of encryption, hashing, key exchange protocols, and other cryptographic primitives to secure data in transit and at rest, and to ensure the authenticity of communication parties.**
Theme 2: Resilient System Architectures (19.00%, N=4)	**Fundamental design patterns and hardware-level modifications to build inherently secure and private smart home systems from the group up.**
2.1 Hardware-Software Co-design (9.50%, N=2)	The integration of security features at the hardware level (for example physical unclonable functions, network-on-chip interconnects) in conjunction with software to create a robust security foundation.
2.2 Decentralized and Zero-Trust Models (9.50%, N=2)	The shifts from centralized, implicit trust models to architectures where data control is user-centric (decentralized) or no entity is trusted by default (Zero Trust), requiring strict verification.
Theme 3: Context-Aware and Policy-Based Control (19.00%, N=4)	**The utilization of environmental context, system state, user behavior, and predefined rule of logic to make dynamic security and data-sharing decisions, enabling adaptive protection.**
Theme 4: Artificial Intelligence and Machine Learning Driven Security (14.30%, N=3)	**This involves the use of artificial intelligence and machine learning models for sophisticated security purposes such as threat detection and advanced authentication**
4.1 Anomaly and Threat Detection (9.50%, N=2)	The use of machine learning algorithms such as hidden Markov Model and federated learning to identify unusual patterns, malicious behavior, or specific attacks like distributed denial-of-service attacks.
4.2 Biometric Authentication (4.80%, N=1)	The use of neural networks and other artificial intelligence models for user verification through unique biological traits like facial features or voice patterns.
Theme 5: Foundational Security Practices (14.30%, N=3)	**This includes established best practices and tools for system maintenance, monitoring, vulnerability management, and recovery to ensure ongoing operational resilience.**

DISCUSSION

Documented Security and Privacy Vulnerabilities (RQ1)

The findings of this systematic literature review show the current state of the security and privacy in smart homes research during emergencies. The findings show the progress made so far in developing secure smart home systems and the important gaps that exist in addressing specific emergency contexts for fire and burglary emergencies. The documented vulnerabilities identified include, data management risks, network and communication based attacks, technical and protocol level vulnerabilities, systemic and architectural weaknesses, and human and user-centric factors.

Data management risks accounted for the highest portion of identified challenges. The compromise of personal and sensitive information through improper access control, processing and storage dominated the risks. The studies reported situations of theft, leakage and misuse of data including, and personal identifiable information. The others include authentication credentials and private records of home activities all of which endanger users' security and privacy. The inability of users themselves to control their data reflecting in insecure data management life cycle management and inconsistent or non-existent management practices add to this challenge (Wazid et al. 2019; Mexis et al. 2021; Nguyen et al. 2025). These limitations of the security of SHSs does not only negate technical measures but also leads to the fading of user trust.

The documented challenges show that attacks on data-in-transit between devices, gateways, cloud services, and applications are central to SHS risk, and this risk is amplified in crises situations where decisions are highly time-sensitive. Denial-of-service attacks can make devices unavailable at precisely the moment alerts are needed, delaying emergency response in fire and burglary events. Eavesdropping, interception, impersonation, and traffic analysis can expose occupancy patterns and routines that support cyber-enabled crime planning, including burglary attempts and this aligns with cyber-enabled crime literature showing how digital data are operationalized to facilitate offline offenses (Kalnoor and Gowrishankar 2022; Sikder et al. 2021; Jose and Malekian 2017; Hodges 2021).

These findings reinforce the need for robust communication-channel protection to keep SHS data secure, private, and available under crisis conditions.

The findings show that there are some risks in SHSs that are as a result of issues with software and hardware configurations allowing for easy targeting of devices. Weak authentication mechanisms and poor use of encryption leave systems vulnerable and attackers take advantage of this to break into systems and compromise data. This means systems can accept false commands from unauthorized entities, which is especially dangerous in crises because responders and residents depend on the integrity of alerts and automated actions. Insecure operating system and firmware settings, applications and design errors are another concern. These can allow intruders exploit devices that are mandated to protect homes. For instance, in the event of a firmware compromise, fire alarms may be prevented from going off at the right time of which the effects can be chaotic. Biometric systems such as fingerprint are able to gain access as a result of poor encryption to access a home; in crisis terms, this can convert a protective system into an attack-enabling infrastructure for burglary (Mosenia et al. 2017; Sikder et al. 2021; Saxena and Varshney 2021; Hodges 2021). These show that technical and protocol level flaws are risks to smart homes.

The findings show that systemic weaknesses can cause threats to smart home systems. Incompatibly of devices and platforms can make SHSs prone to attacks. As SHSs components are sources from multiple suppliers, the different standards applied by different companies open SHSs to exploitation. With no clearly defined standards and policy to address different contexts for SHSs, vulnerabilities in relation to emergencies are unavoidable. The possible lack of a schedule to periodically update firmware and other adaptive measures in different situation mean that SHSs will continue to be vulnerable to attacks. With SHSs having limited access to resources for storage and processing, there is a ceiling on the kind of robustness to security implementations (Mahlous 2023; Rhujittawiwat et al. 2022; Garcia et al. 2024). These findings suggest that in addressing such threats, researchers must not only focus on one device or platform but explore approaches that take into account the interoperability and multi platforms and standards phenomena of SHSs.

It is evident from the study that human and user focused factors affect smart home security and privacy. Some security risks are as a result of users using weak passwords and intentionally or unintentionally refusing to update passwords. Users tend to wholly trust manufacturers hence do not change the manufacturers default passwords and in some instances tend to wrongly configure devices while setting up. This reflects a situation for the trust paradox where users depend on SHSs for safety and therefore assume default privacy and security settings are sufficient, yet those same defaults can leave systems exposed at the exact moment crisis protection is most needed. End users knowingly or unknowingly may provide wrong information and this can deceive the logic of a system leading to bad actors leveraging such occurrence to cause havoc. With no way to know what is real or not real as input from a user in an emergency scenario can be dangerous as this may either cause a delay or no response (Yao et al. 2019; Khoa et al. 2020; Sikder et al. 2021). In crisis situations, this paradox can amplify harm as over-trust in defaults may delay corrective action, while under stress users may have limited time to verify alerts, permissions, and device states. What emerges from the analysis is that human action and inaction cannot be relegated to later stages. Interface design, anomaly detection and flexible controls should be implemented to account for changing contexts.

Technical and Architectural Solutions to Enhancing Resilience of Smart Home (RQ2)

The results reveal the state of security and privacy of solution research in smart homes systems during emergencies. The documented solutions include cryptographic mechanisms, resilient system architectures, context-aware and policy based control, AI/ML driven security, and foundational security practices.

The examination of the data from the literature that cryptographic mechanisms are the most dominant technical solution for securing smart homes with several studies positing lightweight real-time authentication algorithms and symmetric key authentication. The SHA-256 algorithm is identified as one of the algorithms used to ensure data integrity and improve security against attacks (Rababah et al. 2022; Nyangaresi et al. 2022; Khoa et al. 2020). There is however a major challenge with the reliance on cryptography as a means of safeguarding smart homes systems given their resource constraint nature. Lightweight cryptography is used to address SHSs security vulnerabilities (Alaba et al. 2017; Al Salami et al. 2016; J. Mohan and Rajesh 2021; Zhang 2024; Dey and Hossain 2019). The fact that several studies report the use of cryptographic mechanisms in solving security and privacy threats suggest that they make marginal improvements rather than transformative approaches to addressing problems.

It is evident from the data determined that solutions take into consideration hardware and software components of SHSs. The study elucidates that zero-trust models are implemented to ensure resilience of systems. Effective security must be integrated across the entire system wholistically rather than being device or platform dependent (Almuhaideb et al. 2021; Mexis et al. 2021; Garcia et al. 2024). This is imperative in SHSs as their architectural structure of multiple connected devices and systems add extra layers of end-to-end protection. Decentralized

systems distributes responsibilities, and control access to individual components to enhance resilience and improve security .

The findings demonstrated that there are solutions which take into account situational factors of the SHS. These context-aware and policy-based framework solutions adjust access controls and authentication based on for example user's location (Sikder et al. 2021; Nguyen et al. 2025; Jose and Malekian 2017). Such adjustments are crucial in fire or burglary emergencies, where strict protocols can either delay or fail to offer timely assistance to changing threats. Considering the number of studies found to support this approach, it suffices to say research is yet to fully leverage contextual intelligence to achieve SHS security and usability in emergencies.

The review highlights AI/ML driven security where anomaly detection and biometric authentication show the possibility to add to known methods by allowing for suggestive and adaptive responses to attacks. With AI/ML approaches, unusual patterns can be identified in case of an attack and biometric authentication will offer stronger identity assurance over passwords (Kalnoor and Gowrishankar 2022; Patel et al. 2024; Saxena and Varshney 2021). With the relatively small number of the literature reporting this, it suggests this is not widely researched.

The analysis suggests what can be considered as foundational security practices such as regularly updating firmware and software, or routinely changing passwords, or securely configuring devices during set up (Norris et al. 2022; Aldahmani et al. 2023; Hodges 2021) as solutions documented to provide security and privacy in SHSs. These measures though basic, their limited presence in the literature suggests research is biased toward more advanced and technical concepts. This may be problematic as there will not be enough evidence to substantiate the effects such practices have on the overall security and privacy of smart home systems.

Implication of Results

Critical Challenges

The dominating challenges are data management risks, insecure data handling, and communication-based attacks. In crisis settings, these are not abstract technical weaknesses; they directly affect whether sensors trigger, alarms reach users and responders, and locks behave safely during fire and burglary events. This means the core implication is operational: security failures become emergency-response failures.

Research Gap

The majority of studies focused on fire-related emergencies and technical solutions, particularly cryptography. Burglary-focused emergencies, cross-crisis comparisons, and human-centered approaches remain less researched. This implies relatively limited evidence on how user action and inaction, household coordination, and stress-driven decision-making shape smart home security outcomes during emergencies.

Future Solutions

The findings show partial alignment between identified challenges and proposed solutions. There is strong alignment where communication and data risks are matched by encryption, authentication, and resilient architectures. However, alignment is weak for crisis-specific challenges linked to usability, trust, multi-user coordination, and real-time decision support. In other words, the literature proposes many controls that protect systems in principle, but fewer solutions that ensure those controls remain usable and reliable when households are under emergency pressure. Future solution design should therefore pair technical hardening with human-centered crisis workflows, transparent privacy controls, and mechanisms that support fast and accurate action under stress.

Limitations and Future Works

This review focused on smart home systems particularly in the context of fire and burglary emergencies. This may not reflect all situations of crises and emergencies as other types of cases may have different results. The limited number of primary studies (24) restricts the generalization of these findings. The analysis also centered majorly on the technical and architectural solutions, possibly underestimating the relevance of other factors including human factors, user awareness, policy and legal angles of mitigating these challenges and risks.

Future studies will need to be done from the adversarial perspective where exploration of ways in which malicious actors behave are examined when they exploit smart home systems in crises scenarios. Another perspective will be to look at the resilience between smart home systems and external emergency services during an emergency situation. New works should extend and focus on exploring in detail fire and burglary crises and other forms of crises including but not limited to natural disasters or technological crises such as widespread power outages or medical crises likes pandemics.These will guide on which aspects of SHSs must be critically evaluated when deploying in situations where there can be high potential of crises.

CONCLUSION

This review clarifies what we now know about IoT devices particularly SHSs in times of crisis. SHSs can support safety during fires and burglaries, but the same connectivity that enables rapid alerts also creates attack paths that can disrupt, delay, or distort emergency response. The evidence across the included studies shows that crises expose weaknesses that may appear manageable in routine conditions but become high-impact when decisions must be made in seconds.

For RQ1, the literature consistently documents vulnerabilities across data management, network communication, architecture, and user practices, with unauthorized access and data exposure reported most often. In the practical terms, this means attackers can misuse household data, infer occupancy patterns, interfere with device communication, and exploit weak configurations at moments when residents are most vulnerable.

For RQ2, current solutions are concentrated in cryptographic protections, authentication improvements, and resilient architectures. These are necessary and valuable, but they are not sufficient on their own for crisis performance. The review finds fewer studies that test whether solutions remain understandable, trustworthy, and usable for households under stress, or whether they integrate effectively with emergency-response workflows.

Overall, the results suggest a clear direction proposing that the next generation of smart home security must be designed for emergency conditions and heightened vulnerability, not only for normal operation. A central implication is that the human-practices gap is also a crisis-analysis gap such that if we do not study how residential users interpret alarms, share access, trust automation, and make decisions under stress, we cannot reliably evaluate whether technical protections will work when stakes are highest. Research and practice should therefore align technical protection with human-centered crisis use, so that IoT home devices do not merely resist attacks, but continue to provide reliable and timely support when crises actually occur.

REFERENCES

Abu-Tair, M., Djahel, S., Perry, P., Scotney, B., Zia, U., Carracedo, J. M., and Sajjad, A. (2020). "Towards secure and privacy-preserving IoT enabled smart home: architecture and experimental study". In: *Sensors* 20.21, p. 6131.

Agrawal, D., Bhagwat, R., Bandopadhyay, R., Kunapareddi, V., Burden, E., Halse, S., Wisniewski, P., and Kropczynski, J. (2020). "Enhancing smart home security using co-monitoring of IoT devices". In: *Companion Proceedings of the 2020 ACM International Conference on Supporting Group Work*, pp. 99–102.

Akhtar, A. et al. (2024). "Systematic analysis of smart homes: Current trends and future recommendations". In: *Cogent Engineering*.

Al Salami, S., Baek, J., Salah, K., and Damiani, E. (2016). "Lightweight Encryption for Smart Home". In: *2016 11th International Conference on Availability, Reliability and Security (ARES)*, pp. 382–388.

Alaba, F. A., Othman, M., Hashem, I. A. T., and Alotaibi, F. (2017). "Internet of Things security: A survey". In: *Journal of Network and Computer Applications* 88, pp. 10–28.

Alam, H. and Tomai, E. (2023). "Security attacks and countermeasures in smart homes". In: *International Journal on Cybernetics & Informatics (IJCI)* 12.12, p. 109.

Alam, M. R., Reaz, M. B. I., and Ali, M. A. M. (2012). "A review of smart homes—Past, present, and future". In: *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)* 42.6, pp. 1190–1203.

Aldahmani, A., Ouni, B., Lestable, T., and Debbah, M. (2023). "Cyber-Security of Embedded IoTs in Smart Homes: Challenges, Requirements, Countermeasures, and Trends". In: *IEEE Open Journal of Vehicular Technology* 4, pp. 281–292.

Almuhaideb, A. M., Alotaibi, N. M., Wang, H., and Aldossary, S. (2021). "ZTA-IoT: A Novel Architecture for Zero-Trust in IoT Systems and an Ensuing Usage Control Model". In: *IEEE Access* 9, pp. 146297–146312.

Alshamaila, Y., Papagiannidis, S., Alsawalqah, H., and Aljarah, I. (2023). "Effective Use of Smart Cities in Crisis Cases: A Systematic Review of the Literature". In: *International Journal of Disaster Risk Reduction* 85, p. 103521.

Amazon.com, Inc. (2025). *Smart home devices*. https://www.amazon.com/smart-home-devices/b?node=6563140011.

Ameer, S., Praharaj, L., Sandhu, R., Bhatt, S., and Gupta, M. (2024). "Zta-iot: A novel architecture for zero-trust in iot systems and an ensuing usage control model". In: *ACM Transactions on Privacy and Security* 27.3, pp. 1–36.

Ansari, A. M., Nazir, M., and Mustafa, K. (2024). "Smart homes app vulnerabilities, threats, and solutions: a systematic literature review". In: *Journal of Network and Systems Management* 32.2, p. 29.

Apple Inc. (2025). *Buy Smart Home Devices & Accessories – Apple*. https://www.apple.com/shop/smart-home/accessories.

Barbosa, S. et al. (2024). "Smart resilience through IoT-enabled natural disaster management: A COVID-19 response in São Paulo state". In: *IET Smart Cities*.

Barhamgi, M., Perera, C., Ghedira, C., and Benslimane, D. (2018). "User-centric Privacy Engineering for the Internet of Things". In: *IEEE Cloud Computing* 5.5, pp. 47–57.

Barocas, S. and Nissenbaum, H. (2014). "Big Data's End Run around Anonymity and Consent". In: *Privacy, Big Data, and the Public Good: Frameworks for Engagement*. New York, NY: Cambridge University Press, pp. 44–75.

Basty, R., Kropczynski, J., and Halse, S. (2025). "Exploring Higher Education Faculty Insights on Generative AI in Creative Courses". In: *Journal of Information Technology Education: Research* 24, p. 018.

Bélanger, F. and Crossler, R. E. (2011). "Privacy in the digital age: a review of information privacy research in information systems". In: *MIS quarterly*, pp. 1017–1041.

Bishop, M. (2003). "What is computer security?" In: *IEEE Security & Privacy* 1.1, pp. 67–69.

Boukerche, A. and Coutinho, R. W. L. (2018). "Smart Disaster Detection and Response System for Smart Cities". In: *2018 IEEE Symposium on Computers and Communications (ISCC)*. IEEE, pp. 1107–1112.

Castro, H. and Jack, C. (2022). *Blockchain for Secure Fire Alarm Systems: Enhancing Reliability and Safety*. https://www.researchgate.net/publication/388198470.

Chhetri, C. and Genaro Motti, V. (Nov. 2022). "User-Centric Privacy Controls for Smart Homes". In: *Proc. ACM Hum.-Comput. Interact.* 6.CSCW2.

Dey, S. and Hossain, A. (2019). "Session-Key Establishment and Authentication in a Smart Home Network Using Public Key Cryptography". In: *IEEE Sensors Letters* 3.4, pp. 1–4.

Dutta, S., Chukkapalli, S. S. L., Sulgekar, M., Krithivasan, S., Das, P. K., and Joshi, A. (2020). "Context sensitive access control in smart home environments". In: *2020 IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing,(HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*. IEEE, pp. 35–41.

Edu, J. S., Such, J. M., and Suarez-Tangil, G. (Dec. 2020). "Smart Home Personal Assistants: A Security and Privacy Review". In: *ACM Comput. Surv.* 53.6.

Federal Bureau of Investigation (2019). *Burglary, Crime in the U.S. 2019*. URL: https://ucr.fbi.gov/crime-in-the-u.s/2019/crime-in-the-u.s.-2019/topic-pages/burglary (visited on 09/05/2025).

Fernandes, E., Jung, J., and Prakash, A. (2016). "Security analysis of emerging smart home applications". In: *2016 IEEE symposium on security and privacy (SP)*. IEEE, pp. 636–654.

Floridi, L. (2017). "Group Privacy: A Defence and an Interpretation". In: *Group Privacy: New Challenges of Data Technologies*. Cham: Springer International Publishing, pp. 83–100.

Garcia, K., Vontobel, J., and Mayer, S. (June 2024). "A Digital Companion Architecture for Ambient Intelligence". In: *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 8.2.

Girish, A., Hu, T., Prakash, V., Dubois, D., Matic, S., Huang, D. Y., Egelman, S., Reardon, J., Tapiador, J., Choffnes, D., et al. (2023). "In the Room Where It Happens: Characterizing Local Communication and Threats in Smart Homes". In: *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security (CCS '23)*.

Google (2026). *Smart Homes start with Google Nest - Google Store*. https://store.google.com/category/connected_home?hl=en-US.

Hodges, D. (2021). "Cyber-enabled burglary of smart homes". In: *Computers & Security* 110, p. 102418.

Hutchinson, S., Stanković, M., Ho, S., Houshmand, S., and Karabiyik, U. (2023). "Investigating the Privacy and Security of the SimpliSafe Security System on Android and iOS". In: *Journal of Cybersecurity and Privacy* 3.2, pp. 145–165.

International Association of Fire and Rescue Services (CTIF) (2022). *World Fire Statistics Report 2022*. URL: https://www.ctif.org/world-fire-statistics (visited on 09/05/2025).

Jose, A. C. and Malekian, R. (2017). "Improving Smart Home Security: Integrating Logical Sensing Into Smart Home". In: *IEEE Sensors Journal* 17.13, pp. 4269–4286.

Kafle, K., Jagtap, K., Ahmed-Rengers, M., Jaeger, T., and Nadkarni, A. (2024). "Practical integrity validation in the smart home with homeendorser". In: *Proceedings of the 17th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, pp. 207–218.

Kalnoor, G. and Gowrishankar, S. (2022). "A model for intrusion detection system using hidden Markov and variational Bayesian model for IoT based wireless sensor network". In: *International Journal of Information Technology* 14.4, pp. 2021–2033.

Karemaker, M., Ten Hoor, G. A., Hagen, R. R., Schie, C. H. van, Boersma, K., and Ruiter, R. A. (2021). "Elderly about home fire safety: A qualitative study into home fire safety knowledge and behaviour". In: *Fire safety journal* 124, p. 103391.

Keele, S. et al. (2007). *Guidelines for performing systematic literature reviews in software engineering*. Tech. rep. Technical report, ver. 2.3 ebse technical report. ebse.

Khawla, M. and Tomader, M. (2018). "A survey on the security of smart homes: issues and solutions". In: *Proceedings of the 2nd International Conference on Smart Digital Environment*, pp. 81–87.

Khoa, T. A., Nhu, L. M. B., Son, H. H., Trong, N. M., Phuc, C. H., Phuong, N. T. H., Dung, N. V., Nam, N. H., Chau, D. S. T., and Duc, D. N. M. (2020). "Designing Efficient Smart Home Management with IoT Smart Lighting: A Case Study". In: *Wireless Communications and Mobile Computing* 2020, p. 8896637.

Lv, Z., Qiao, L., Singh, A. K., and Wang, Q. (July 2021). "AI-empowered IoT Security for Smart Cities". In: *ACM Trans. Internet Technol.* 21.4.

Mahlous, A. R. (2023). "Threat model and risk management for a smart home IoT system". In: *Informatica* 47.1.

Mexis, N., Anagnostopoulos, N. A., Chen, S., Bambach, J., Arul, T., and Katzenbeisser, S. (June 2021). "A Lightweight Architecture for Hardware-Based Security in the Emerging Era of Systems of Systems". In: *J. Emerg. Technol. Comput. Syst.* 17.3, pp. 1–25.

Mohan, J. and Rajesh, R. (2021). "Enhancing home security through visual cryptography". In: *Microprocessors and Microsystems* 80, p. 103355.

Mohan, K., Mahesh, A., Vasudevan, A., Panchagnula, K., et al. (2016). "IoT based Emergency Evacuation System". In: *International Journal of Engineering Research & Technology* 4.29.

Mosenia, A., Sur-Kolay, S., Raghunathan, A., and Jha, N. K. (2017). "DISASTER: Dedicated Intelligent Security Attacks on Sensor-Triggered Emergency Responses". In: *IEEE Transactions on Multi-Scale Computing Systems* 3.4, pp. 255–268.

Mühlhoff, R. (2023). "Predictive privacy: Collective data protection in the context of artificial intelligence and big data". In: *Big Data & Society* 10.1, p. 20539517231166886.

Nandhini, P. K. and Prakash, F. (2024). "Securing smart homes: Challenges and solutions in IoT cybersecurity". In: *International Journal of Science, Engineering and Technology* 12.2, pp. 510–517.

Nguyen, P., Nguyen, H.-H., Phung, P., Truong, H.-L., and Cheung, T. (Apr. 2025). "Advanced Context-Sensitive Access Management for Edge-Driven IoT Data Sharing as a Service". In: *ACM Trans. Internet Technol.* 25.2.

Norris, M., Celik, Z. B., Venkatesh, P., Zhao, S., McDaniel, P., Sivasubramaniam, A., and Tan, G. (July 2022). "IoTRepair: Flexible Fault Handling in Diverse IoT Deployments". In: *ACM Trans. Internet Things* 3.3.

Nyangaresi, V. O., Abduljabbar, Z. A., Mutlaq, K. A.-A., Ma, J., Honi, D. G., Aldarwish, A. J. Y., and Abduljaleel, I. Q. (2022). "Energy Efficient Dynamic Symmetric Key Based Protocol for Secure Traffic Exchanges in Smart Homes". In: *Applied Sciences* 12.24, p. 12688.

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., et al. (2021). "The PRISMA 2020 statement: an updated guideline for reporting systematic reviews". In: *BMJ* 372, n71.

Patel, A. N., Srivastava, G., Maddikunta, P. K. R., Murugan, R., Yenduri, G., and Gadekallu, T. R. (2024). "A Trustable Federated Learning Framework for Rapid Fire Smoke Detection at the Edge in Smart Home Environments". In: *IEEE Internet of Things Journal* 11.23, pp. 37708–37717.

Poh, G. S., Gope, P., and Ning, J. (2021). "PrivHome: Privacy-Preserving Authenticated Communication in Smart Home Environment". In: *IEEE Transactions on Dependable and Secure Computing* 18.3, pp. 1095–1102.

Popoola, O., Rodrigues, M., Marchang, J., Shenfield, A., Ikpehai, A., and Popoola, J. (2024). "A critical literature review of security and privacy in smart home healthcare schemes adopting IoT & blockchain: problems, challenges and solutions". In: *Blockchain: Research and Applications* 5.2, p. 100178.

Purohit, A. and Sharan, V. (2024). "Enhancing Smart Home Security Using IoT-Based Intrusion Detection Systems". In: *International Journal of Scientific Research in Engineering and Management (IJSREM)* 8.12, pp. 1–6.

Rababah, H. A., Alhusenat, A. Y., and Mahafzah, K. A. (2022). "A novel smart home lightweight authentication protocol using IoT applications". In: *WSEAS Transactions on Systems and Control* 17.10.37394, pp. 23203–2022.

Rahman, Z., Yi, X., Billah, M., Sumi, M., and Anwar, A. (2022). "Enhancing AES Using Chaos and Logistic Map-Based Key Generation Technique for Securing IoT-Based Smart Home". In: *Electronics* 11.7, p. 1083.

Ray, P. P., Mukherjee, M., and Shu, L. (2017). "Internet of Things for Disaster Management: State-of-the-Art and Prospects". In: *IEEE Access* 5, pp. 18818–18835.

Rhujittawiwat, T., Anderson, C., Keen, D., Miles, C., Farkas, C., Smiles, S., Wells, N., Roginski, J., Frederick, S., and Banik, S. (2022). "Making Smart Platforms Smarter: Adding Third Party Applications to Home Automation Platforms". In: *Journal of Computing Sciences in Colleges* 38.2, pp. 43–53.

Samsung Electronics Co., Ltd. (2025). *SmartThings – Samsung US*. https://www.samsung.com/us/smartthings/.

Saxena, N. and Varshney, D. (2021). "Smart Home Security Solutions using Facial Authentication and Speaker Recognition through Artificial Neural Networks". In: *International Journal of Cognitive Computing in Engineering* 2, pp. 154–164.

SciSpace (2022). *SciSpace: An AI-powered platform for academic research*.

Shahzad, F. et al. (2024). "IoT based smart emergency response system (SERS) for monitoring vehicle, home and health status". In: *Discover Internet of Things*.

Sharif, K. and Tenbergen, B. (2020). "Smart Home Voice Assistants: A Literature Survey of User Privacy and Security Vulnerabilities". In: *Computer Science and Information Technologies* 24.24, pp. 15–30.

Sharma, N. and Dhiman, P. (2024). "Lightweight privacy preserving scheme for IoT based smart home". In: *Recent Advances in Electrical & Electronic Engineering (Formerly Recent Patents on Electrical & Electronic Engineering)* 17.8, pp. 763–777.

Sikder, A. K., Babun, L., and Uluagac, A. S. (Feb. 2021). "AEGIS+: A Context-aware Platform-independent Security Framework for Smart Home Systems". In: *Digit. Threat.: Res. Pract.* 2.1.

Sredhar, A., Khan, A., Gilal, A. R., Alsughayyir, A., Alshanqiti, A., and Talpur, B. A. (2024). "Assessing and Mitigating Network Vulnerabilities in Philips Hue and Nest Protect Smart Home Devices." In: *International Journal of Advanced Computer Science & Applications* 15.2.

Starbuck, W. H., Greve, A., and Hedberg, B. (1978). "Responding to Crises". In: *Journal of Business Administration* 9.2, pp. 111–137.

Tan, B., Biglari-Abhari, M., and Salcic, Z. (Sept. 2017). "An Automated Security-Aware Approach for Design of Embedded Systems on MPSoC". In: *ACM Trans. Embed. Comput. Syst.* 16.5s.

Touqeer, H., Zaman, S., Amin, R., Hussain, M., Al-Turjman, F., and Bilal, M. (2021). "Smart home security: Challenges, issues and solutions at different IoT layers." In: *Journal of Supercomputing* 77.12.

Utomo, I. S., Pranoto, C. M., Moniaga, J. V., Jabar, B. A., et al. (2022). "A systematic literature review of privacy, security, and challenges on applying IoT to create smart home". In: *2022 International Conference on Electrical and Information Technology (IEIT)*. IEEE, pp. 154–159.

Vardakis, G., Hatzivasilis, G., Koutsaki, E., and Papadakis, N. (2024). "Review of smart-home security using the internet of things". In: *Electronics* 13.16, p. 3343.

Wazid, M., Das, A. K., Hussain, R., Succi, G., and Rodrigues, J. J. (2019). "Authentication in cloud-driven IoT-based big data environment: Survey and outlook". In: *Journal of Systems Architecture* 97, pp. 185–196.

Yang, J. and Sun, L. (2022). "A Comprehensive Survey of Security Issues of Smart Home System: "Spear" and "Shields," Theory and Practice". In: *IEEE Access* 10, pp. 124167–124200.

Yao, Y., Basdeo, J. R., McDonough, O. R., and Wang, Y. (2019). "Privacy Perceptions and Designs of Bystanders in Smart Homes". In: *Proceedings of the ACM on Human-Computer Interaction* 3.CSCW, Article 59, 1–24.

Yusoff, Z. Y. M., Ishak, M. K., Rahim, L. A., and Asaari, M. S. M. (2024). "Improving Smart Home Security via MQTT: Maximizing Data Privacy and Device Authentication Using Elliptic Curve Cryptography." In: *Computer Systems Science & Engineering* 48.6.

Zeghida, H., Boulaiche, M., and Chikh, R. (2024). "Security of MQTT Protocol: A Brief Overview". In: *CEUR-WS.org* 3973.

Zeng, E., Mare, S., and Roesner, F. (July 2017). "End User Security and Privacy Concerns with Smart Homes". In: *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. Santa Clara, CA: USENIX Association, pp. 65–80.

Zeng, E. and Roesner, F. (Aug. 2019). "Understanding and Improving Security and Privacy in Multi-User Smart Homes: A Design Exploration and In-Home User Study". In: *28th USENIX Security Symposium (USENIX Security 19)*. Santa Clara, CA: USENIX Association, pp. 159–176.

Zeng, F., Pang, C., and Tang, H. (2023). "Sensors on the Internet of Things Systems for Urban Disaster Management: A Systematic Literature Review". In: *Sensors* 23.17, p. 7475.

Zhang, E. (2024). "Enhancing Smart Home Security with Cryptographic Key Exchange Protocols". In: *American Journal Of Cryptography And Network Security* 5.6, pp. 13–18.

Zheng, S., Apthorpe, N., Chetty, M., and Feamster, N. (Nov. 2018). "User Perceptions of Smart Home IoT Privacy". In: *Proc. ACM Hum.-Comput. Interact.* 2.CSCW.

ACKNOWLEDGMENTS

The authors employed Google Gemini for thematic analysis of qualitative data extracted from literature as documented in the methods section of this paper. However, the analytical framework and thematic interpretations were conceived and developed by the authors. All AI-generated content was meticulously reviewed and revised to guarantee its consistency with the authors' original thought and academic rigor.

APPENDICES

Primary Studies

Table 6. Primary Studies on Security and Privacy in Smart Homes in Crisis Context

Paper ID	Title	Citation
P1	A Digital Companion Architecture for Ambient Intelligence	Garcia et al. 2024
P2	A Lightweight Architecture for Hardware-Based Security in the Emerging Era of Systems of Systems	Mexis et al. 2021
P3	A model for intrusion detection system using hidden Markov and variational Bayesian model for IoT based wireless sensor network	Kalnoor and Gowrishankar 2022
P4	A Novel Smart Home Lightweight Authentication Protocol using IoT Applications	Rababah et al. 2022
P5	A Trust Federated Learning Framework for Rapid Fire Smoke Detection at the Edge in Smart Home Environments	Patel et al. 2024
P6	Advanced Context-Sensitive Access Management for Edge-Driven IoT Data Sharing as a Service	Nguyen et al. 2025
P7	AEGIS+: A Context-aware Platform-independent Security Framework for Smart Home Systems	Sikder et al. 2021
P8	AI-empowered IoT Security for Smart Cities	Lv et al. 2021
P9	An Automated Security-Aware Approach for Design of Embedded Systems on MPSoC	Tan et al. 2017
P10	Authentication in cloud-driven IoT-based big data environment: Survey and outlook	Wazid et al. 2019
P11	Cyber-enabled burglary of smart homes	Hodges 2021
P12	Cyber-Security of Embedded IoTs in Smart Homes: Challenges, Requirements, Countermeasures, and Trends	Aldahmani et al. 2023
P13	Designing Efficient Smart Home Management with IoT Smart Lighting: A Case Study	Khoa et al. 2020
P14	DISASTER: Dedicated Intelligent Security Attacks on Sensor-Triggered Emergency Responses	Mosenia et al. 2017
P15	Energy Efficient Dynamic Symmetric Key Based Protocol for Secure Traffic Exchanges in Smart Homes	Nyangaresi et al. 2022
P16	Enhancing AES Using Chaos and Logistic Map-Based Key Generation Technique for Securing IoT-Based Smart Home	Rahman et al. 2022
P17	Improving Smart Home Security: Integrating Logical Sensing Into Smart Home	Jose and Malekian 2017
P18	Investigating the Privacy and Security of the SimpliSafe Security System on Android and iOS	Hutchinson et al. 2023
P19	IoTRepair: Flexible Handling in Diverse IoT Deployments	Norris et al. 2022
P20	Making Smart Platforms Smarter: Adding Third Party Applications to Home Automation Platforms	Rhujittawiwat et al. 2022
P21	Privacy Perceptions and Designs of Bystanders in Smart Homes	Yao et al. 2019
P22	Smart Home Security Solution using Facial Authentication and Speaker Recognition through Artificial Neural Networks	Saxena and Varshney 2021
P23	Threat Model and Risk Management for a Smart Home IoT System	Mahlous 2023
P24	ZTA-IoT: A Novel Architecture for Zero-Trust in IoT Systems and an Ensuing Usage Control Model	Ameer et al. 2024

Gemini Prompt for Thematic Analysis

Conduct a thematic analysis of the following notes from articles in a systematic literature review, which were focused on answering the following research question: [Research Question Entered Here]

Goal: To systematically perform an inductive thematic analysis to understand documented security vulnerabilities and privacy risks associated with smart homes during emergency situations in order to inform future system development that directly addresses these challenges in the future.

Analysis Process:
1. Familiarization: Begin by carefully reading through all data from each of the 24 articles to gain a comprehensive understanding of the data. Each new line represents data from a different one of the 24 articles. If data are removed, please state the rationale before the analysis.

2. Inductive Coding: Identify initial codes that capture recurring ideas, concepts, and patterns related to challenges and proposed solutions. Focus on capturing both semantic meaning (what is said) and latent meaning (what is implied). Do not limit coding to the provided research question; allow for unexpected themes to emerge from the data.

3. Theme Development: Organize the initial codes into potential themes and sub-themes. Ensure themes are relevant to the research question, but also allow for themes that highlight unexpected implications for the design of solutions. Consider the relationships between themes, identifying overarching themes and their related sub-themes.

4. Theme Definition and Refinement: Develop clear and concise definitions for each theme and sub-theme. Review the themes against the data to ensure they accurately capture the nuances and complexities of the responses. Refine themes as needed to improve clarity and accuracy.

5. Exemplification: For each theme and sub-theme, select a few representative quotes that illustrate its essence. Choose quotes that are diverse and capture the range of perspectives within the theme.

6. Quantification: Analyze the frequency of each theme and sub-theme across the data gathered from articles. Calculate the percentage of responses that each theme represents.

7. Presentation: Present the thematic analysis in a clear and organized manner, using a table or other visual aid to summarize: Theme/sub-theme names and definitions Representative notes on the article Frequency and percentage of occurrence

Quality Assurance:
Thoroughness: Ensure all data points are analyzed in detail.
Nuance: Capture the subtleties, contradictions, and complexities within the data.
Objectivity: Maintain an objective and unbiased approach throughout the analysis.
Clarity: Present the findings in a clear, concise, and easily understandable manner.
Data: [Notes Extracted from SLR Entered Here]