Computers & Security 162 (2026) 104762

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

Human-centric security for smart homes: A scoping review

Wanling Cai [a,b,*], Liliana Pasquale [b], Kushal Ramkumar [b], John McCarthy [c], Bashar Nuseibeh [d], Gavin Doherty [a]

[a] Lero @ Trinity College Dublin, Dublin, Ireland
[b] Lero @ University College Dublin, Dublin, Ireland
[c] Lero @ University College Cork, Cork, Ireland
[d] The Open University, Milton Keynes, UK

ARTICLE INFO

Keywords:
Smart homes
Scoping review
Human-centric security
Usable security

ABSTRACT

Smart home technologies, like cameras, door locks, and speakers, are increasingly used in our everyday lives. However, their continuous data collection and internet connectivity pose various security risks. While research on smart home security has mainly focused on technological aspects, human experience and societal factors also play a crucial role. Various human and social factors, such as user experience with smart home devices, security design processes, and government regulations, are intertwined and influence each other, affecting smart home security. It is therefore important to understand and consider these interconnected factors in technology design to secure homes that contain increasingly connected devices. This scoping review provides an overview of current human-centered studies (N = 102) on smart home security, which aims to help researchers and practitioners better navigate this field. We present a conceptual framework that outlines key challenges in ensuring smart home security with a synthesis of insights on contributing human factors. We then summarize general security design principles and map existing user-centred security approaches in smart homes, and highlight research directions for future investigation. Beyond mapping existing studies, the review reveals a growing emphasis on engaging multiple stakeholders, especially smart home users, in shaping human-centered security.

1. Introduction

Smart devices (e.g., smart cameras, smart speakers) have been increasingly used in our home environments to improve home security, energy efficiency, and quality of life (Marikyan et al., 2019; Aldrich, 2003). For example, a smart lock can allow homeowners to remotely control access to the home via a smartphone or tablet; a smart light can automatically adjust its settings based on the presence of people and the time of day; a smart speaker (also called smart personal assistant) can respond to voice commands to manage various services, e.g., music or TV, and other smart home devices, e.g., lights, thermostats, and cameras. According to recent statistics (Thormundsson, 2024), several major companies such as Google, Amazon, Apple, and Xiaomi have driven increased use of smart home devices, primarily through smart speaker products. The number of users of smart homes was anticipated to exceed 400 million in 2024 and reach 785 million by 2028 (Statista, 2023).

However, smart home devices face ongoing security threats, raising concerns for end users (Hammi et al., 2022; Valencia-Arias et al., 2023). Security concerns with smart home devices primarily arise from two main characteristics. First, smart home devices continuously collect data about users' activities. If unauthorized third parties access sensitive data, they could be used for targeted advertising, profiling, and exposing individuals to various risks. Second, smart home devices are constantly connected to the Internet, making them susceptible to hacking. Hackers can potentially take control of smart home devices and control them to cause harm to end users. For example, in 2019, reports indicated that Ring cameras were susceptible to hacking, leading to harassment and threatening behavior towards users (Paul, 2020). As the security of smart home technology significantly influences the willingness of people to adopt these devices (Valencia-Arias et al., 2023), there has been an increasing interest in improving smart home security. To date, most research has focused on technological solutions, ranging from encryption and network security to firmware updates, for mitigating security breaches in smart homes, and this focus is also evident in many reviews that primarily examine technical countermeasures (Lin and Bergmann, 2016; Touqeer et al., 2021; Hammi et al., 2022).

In recent years, efforts to enhance smart home security have extended beyond purely technological solutions to increasingly incorporate human-centered perspectives. As such, an increased proportion of

* Corresponding author.
E-mail address: wanling.cai@ucd.ie (W. Cai).

https://doi.org/10.1016/j.cose.2025.104762
Received 26 May 2025; Received in revised form 30 September 2025; Accepted 12 November 2025
Available online 17 November 2025

smart home research has considered human factors (Zeng et al., 2017; Zeng and Roesner, 2019; Turner et al., 2022b), e.g., exploring users' lived experience with smart home security, their security perceptions and behavior. Previous research has shown that a range of human and social factors, including user awareness and interactions with smart home devices, technology design practices, and government regulations, interact with one another and collectively shape the overall security of smart homes (Haney et al., 2021; Zeng et al., 2017). Given the growing number of human-centered studies on smart home security, it is important to review the literature on human-centered approaches in this domain. In this work, we aim to review the existing human-centered literature on smart home security, offering an overview of current research, summarizing the human factors and security approaches, and highlighting areas that require further investigation. A recent review article provides a survey of user perspectives on security and privacy within home networking environments, summarizing user-centered security and privacy studies, which align with the focus of our review (Pattnaik et al., 2023). Unlike that survey, which broadly addresses user perspectives on security and privacy across various technologies in the home environment, including personal computers, our review focuses specifically on human-centered perspectives on smart home security. We go beyond understanding user perspectives to explore a broader range of human and social factors influencing smart home security. The analysis in our study also examines the interplay between these factors and how they are integrated into the design of security mechanisms for smart homes. It is important to note that while security and privacy are closely related, they do pertain to two distinct issues (Haney et al., 2021); security focuses on protecting systems and data from threats often via cybersecurity measures, whereas privacy involves the control of personal information and individuals' rights regarding how their information is collected, used, and shared. Our study primarily focuses on security issues from a human-centered perspective, as they have been less studied than privacy issues in the smart home context (Pattnaik et al., 2023). However, privacy may also be discussed in contexts where it relates to security, e.g., preventing unauthorized access to personal data is crucial to preserving privacy.

In this work, we conducted a scoping review to map existing human-centric research on smart home security, which is intended to contribute an understanding of (1) what methods are used for human-centered investigation; (2) what human factors which impact smart home security are studied; and (3) what security approaches are being designed to help people secure their smart homes. Our desire is to then identify research challenges and develop a conceptual framework that can inform future research on human-centered security in smart homes. Following the PRISMA-ScR guidelines, we systematically searched three major databases (e.g., ACM Guide to Computing Literature, IEEE Xplore Digital Library, and Scopus) in both 2023 and 2025. After two-step screening (i.e., title and abstract screening, and full-text screening), we included 102 eligible papers for further analysis. The included literature explores smart home security from the perspectives of various stakeholders, e.g., end-users, designers, and security experts, or designs security mechanisms from a human-centered perspective. Using a qualitative analysis approach, we examined the reviewed literature to identify a variety of human factors influencing smart home security and the existing human-centric solutions to secure a smart home. We then introduce a conceptual framework that emphasizes the main challenges in this evolving field, highlighting the key dimensions related to human factors and security approaches identified in the existing studies. We believe this scoping review can provide insights into our current understanding of smart home security and offer guidance for researchers and practitioners interested in human-centered security in smart homes.

In the rest of the paper, we first introduce the background related to this research in Section 2 and our research questions in Section 3. Then, we describe the methodology of this scoping review in Section 4, followed by the results from Sections 5–8 that include the presented conceptual framework in Section 6. Finally, we present our overall discussion in Section 9 and conclusions in Section 10.

2. Background

2.1. Smart home research

What is a smart home? Various approaches and definitions have been used in the literature to describe and conceptualize smart homes (Marikyan et al., 2019). Among them, the definition by Aldrich (2003) encompassed both the technological aspects and the functions and benefits provided to satisfy user needs for living in a home equipped with smart technology. Aldrich (2003) described a smart home as "*a residence equipped with computing and information technology, which anticipates and responds to the needs of the occupants, working to promote their comfort, convenience, security, and entertainment through the management of technology within the home and connections to the world beyond*". Similarly, Ricquebourg et al. (2006) indicated that smart homes are now designed to simplify the lives of their inhabitants by providing comfort and security solutions and supporting energy efficiency. According to a systematic review of the smart home literature (Marikyan et al., 2019), there are four broad areas where smart home devices can offer benefits to users: health-related benefits (e.g., promoting well-being of ageing and vulnerable people), environmental benefits (e.g., reduction of electricity and energy consumption), financial benefits (e.g., affordability of health care and lower costs associated with virtual visits), and psychological benefits (e.g., providing support and enhancing social inclusion). However, these benefits are accompanied by risks and challenges. As shown in another review article (Sovacool and Del Rio, 2020), the top two risks and concerns about smart home technologies are "consumer protection and data security" as well as "technical reliability, warranties, and obsolescence," which may impede user adoption.

2.2. Security of smart home technology

Security issues in smart home technologies typically stem from two main characteristics: the constant collection of user data such as activities, preferences, and even their presence in the home; and the devices' connection to the internet (Batalla et al., 2017; Lee et al., 2014). These two characteristics create the risk of the collected data being stolen, hacked, or misused. If malicious actors gain control of users' devices, they could access users' personal information, use them to spy on residents, or even disrupt their lives. As the security of smart home technology would influence people's adoption of security devices (Sovacool and Del Rio, 2020; Li et al., 2021), there has been an increasing interest in enhancing the security of smart homes, but most past research has focused on the technological aspects (Touqeer et al., 2021). For example, a recent survey (Hammi et al., 2022) provides a summary of the security requirements, challenges, and threats associated with smart homes and discusses the countermeasures, e.g., encryption, authentication, and network security, that can be deployed to mitigate the identified threats. Given the focus on technological aspects, most existing review articles in smart home research are centered on technical security approaches, e.g., (Lin and Bergmann, 2016; Touqeer et al., 2021; Hammi et al., 2022). However, technological solutions alone cannot completely address security issues in smart homes, which are intricate socio-technical systems, blending technology with human and social factors (Zeng et al., 2017; Li et al., 2023). Various human and social factors, such as user awareness and interaction with smart home devices, technology design practices, and government regulations, can interact and influence each other, impacting the overall security of smart homes (Haney et al., 2021). For instance, users may utilize specific smart home devices, such as security cameras, to continuously monitor or surveil individuals within the home (Neilly et al., 2022), which may raise concerns about security and privacy, as well as the ramifications of this technology, e.g., exacerbating patriarchy (Chidziwisano and Jalakasi, 2023). Also, many

smart home devices and platforms lack transparency about their data practices (i.e., how they collect and use consumer data), which makes it difficult for smart home users to understand the potential risks (Tabassum et al., 2019). Furthermore, the lack of standardized policy regulations in the smart home industry may hinder manufacturers from adhering to optimal security practices (Chalhoub et al., 2020). These human and social aspects have increasingly been discussed in recent interdisciplinary research in human-computer interaction (HCI) and security and privacy (Pattnaik et al., 2023; Yao et al., 2023; Grobler et al., 2021).

2.3. Human-centered security research

In the broader field of computer security research, the traditional security research community has identified that many security issues stem from user behavior and has labeled users as the "weak links" in the security chain (Sasse et al., 2001). However, since the 1990s, researchers have increasingly focused on human factors of security systems, shifting the field's perspective from viewing users as 'the enemy' to viewing people as part of the solution (Adams and Sasse, 1999; Dourish et al., 2004; Furnell and Clarke, 2012; Garfinkel and Lipford, 2014; Zimmermann and Renaud, 2019; Borgert et al., 2024). As pointed out in earlier works by Adams and Sasse (1999), as security mechanisms are both designed and used by people, as well as occasionally exploited, it is crucial to consider human factors in the design. Earlier research has also indicated that software developers developing security controls have largely overlooked usability issues; many users of security systems (e.g., authentication management and encryption) have encountered unrealistic requirements and received inadequate support or training, compromising the effectiveness of security measures (Adams and Sasse, 1999; Whitten and Tygar, 1999; Dourish et al., 2004). The past two decades have seen the emergence of a larger community focused on "usable security", with the aim of designing systems that are both usable and secure (Garfinkel and Lipford, 2014; Reuter et al., 2022; Grobler et al., 2021). This community emphasizes improving security mechanisms to enhance usability by aligning with human needs and limitations, incorporating insights and methods from human-computer interaction and psychology (Furnell and Clarke, 2012; Garfinkel and Lipford, 2014; Zimmermann and Renaud, 2019). The major focus of research has been around the topics of user authentication, phishing, Email security, and encryption. Most studies have investigated users' perspectives on security technology, often referred to as "user-centered security"(Garfinkel and Lipford, 2014). In recent years, recognizing that many security incidents result from insecure code (Green and Smith, 2016), research efforts have included software developers as investigated user groups (also known as "developer-centered security"), aiming to provide usable development support and tools to ensure more secure code (Tahaei and Vaniea, 2019). Building on insights from human-centered security research and security concerns in smart homes, this study aims to review human-centered security focused specifically on the smart home context.

3. Research questions

Human-centered research is essential for understanding how people perceive and interact with security-related issues in smart homes and designing security solutions that are both effective and usable, aligning with real-world needs. As previously outlined, the goal of this scoping review is to advance understanding in three key areas: (1) the research methods employed for human-centred investigation; (2) the human factors examined in relation to smart home security; and (3) the security approaches designed to support users in securing their smart homes. Accordingly, we formulate our research questions as follows:

RQ1 [Methods] What research methods (e.g., interviews, surveys, and focus groups) are currently being used to investigate human-centric security for smart homes? By mapping existing approaches, we might identify dominant trends, methodological gaps, and opportunities for more innovative methods in smart home security research.

RQ2 [Human Factors] What human factors (such as user perception, user behavior, and contextual factors) may impact smart home security? Identifying these factors can help uncover users' real-world challenges, such as awareness gaps and contextual issues, which can influence users' security practices.

RQ3 [Security Solutions] What human-centered solutions are being designed to increase smart home security? This investigation can reveal how existing research empowers individuals to secure their smart homes by incorporating their perspectives, and what considerations should guide future design innovations.

4. Methodology

For our research aims, we chose to conduct a scoping review. This thorough and transparent literature review method can synthesize evidence and provide a map or overview of the literature on a research topic (Munn et al., 2018). Examining current research activity on emerging topics and identifying research gaps are common goals in a scoping review (Arksey and O'Malley, 2005), so this review method aligns well with the objective of our study. Guided by the framework proposed by Arksey and O'Malley (2005) and the PRISMA extension for scoping reviews (PRISMA-ScR) checklist and explanations (Tricco et al., 2018), we developed our scoping review protocol, which was pre-registered with the Open Science Framework on October 18, 2023 (Cai et al., 2023). In the following, we briefly describe our methods of conducting this scoping review. For a detailed description, please refer to Appendix A.

4.1. Search and screening

In this review, we conducted our search in the three databases (i.e., ACM Guide to Computing Literature, IEEE Xplore Digital Library, and Scopus) in two rounds: the first on October 27, 2023, and the second on July 3, 2025, with a further update on September 11, 2025, thereby including literature up to that date. Studies were assessed against a set of eligibility criteria, comprising inclusion criteria (IC) and exclusion criteria (EC) described as follows:

IC 1 Include studies that are explicitly concerned with human-related issues in smart homes;

IC 2 Include studies that focus on human-centric approaches to smart home security:
- Are concerned to some extent with the understanding of human factors (including knowledge, attitude, preference, concerns, expectations, and needs regarding security) in smart homes;
- Present security solutions or approaches for smart homes in which they consider human aspects;
- Describe user evaluations (e.g., user studies) of security approaches in smart homes.

EC 1 Exclude studies in which the security aspect was weak or marginal (e.g., studies focusing primarily on user adoption of smart home technologies or exclusively on privacy issues), as this review emphasises security-specific investigations;

EC 2 Exclude studies that solely addressed technological security solutions or conducted purely technical security analyses;

EC 3 Exclude studies conducted in other contexts (e.g., general home computing environments, smart cities, or office settings) if they did not explicitly focus on smart homes;

EC 4 Exclude literature reviews, books, book chapters, and theses;

EC 5 Exclude studies not published as full, peer-reviewed papers;

EC 6 Exclude papers that are not written in English;

EC 7 Exclude papers that are not accessible.

Targeting inclusion criteria (IC 1 and IC2), we searched the three databases for items including the following terms in the title or abstract:

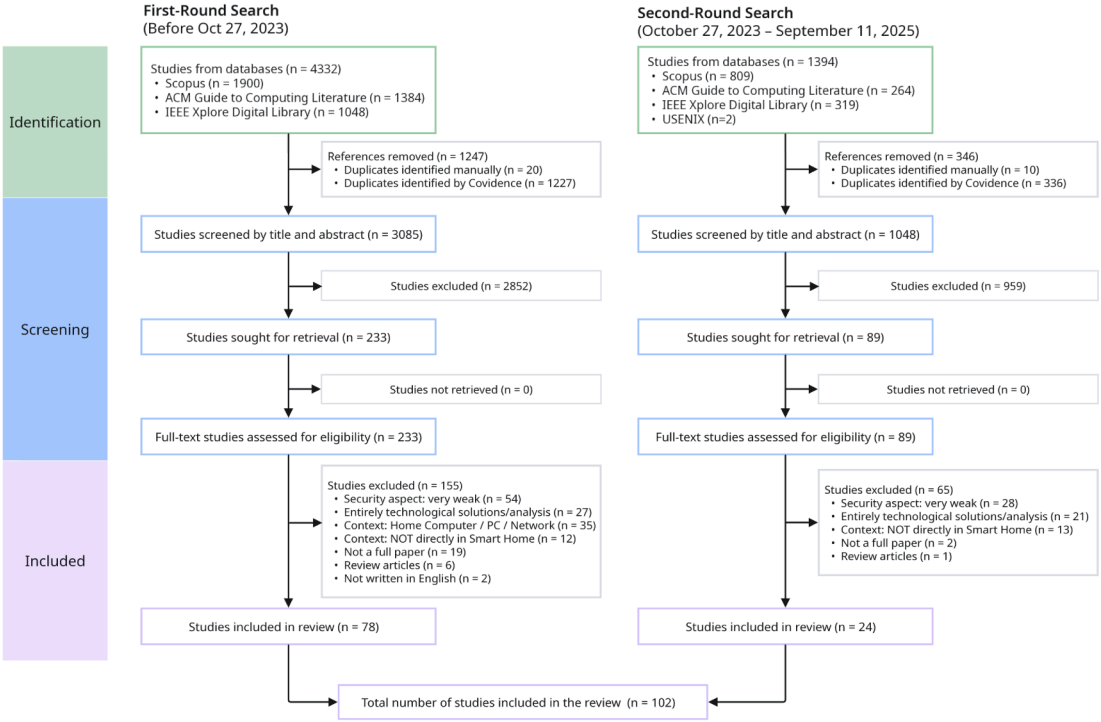

Fig. 1. PRISMA flowchart illustrating the scoping review process..

- **Search Term 1 [Smart Home]** :
  `(Home AND (Smart OR Connected OR Network* OR Comput* OR IoT OR Device)) AND`
- **Search Term 2 [Security]** :
  `(Secur* OR Cybersecurity) AND`
- **Search Term 3 [Human-related]** :
  `((User OR Human OR People OR Person) AND (Cent* OR Factor OR Experience OR Perception OR Feeling OR Sense OR Attitude OR Knowledge OR Awareness OR Concern OR Vulnerab* OR Behavi*))`

The above search terms were adapted from a recent review of user perspectives on security and privacy in home networking environments (Pattnaik et al., 2023). We used the asterisk (*) in several terms to specify a number of unknown characters, e.g., the term secur* will match terms including 'secure' and 'securing' in addition to 'security. During the second round search, we also carried out a separate search in the USENIX database, since not all papers published in USENIX Security Proceedings – though expected to appear in the ACM Guide to Computer Literature – were fully indexed there. The search results were filtered according to EC4 and EC6, using the built-in functions provided by the three databases. We then imported the references of the search results into Covidence[1] (a software system for systematic review management) for duplicate detection and screening.

Following the steps described above, our search of the three databases identified 3085 papers in the first round, and an additional 1048 papers in the second round. We followed a two-step process to screen the identified articles: (1) Title and Abstract Screening: The first and second authors independently reviewed the titles and abstracts to screen papers according to the eligibility criteria. There was 94 % agreement for this screening in the first round. A total of 196 conflicts were then resolved by consensus and discussion between the two authors. This screening resulted in 2852 excluded papers that did not engage with human-related security aspects in smart homes, and 233 papers for full-text review. In the second round, the title and abstract screening tasks were split between the first and second authors. (2) Full-text Screening: The first author then retrieved the full text of the eligible papers, and both the first and second authors independently assessed the eligibility of the remaining articles based on exclusion criteria (EC 1–5) by reviewing the full text and resolved the conflicts via discussion. This process resulted in a final corpus of 102 papers (78 from the first round and 24 from the second) relevant to our research aims (see Fig. 1). See further details of our search and screening process in Appendix A.2.

4.2. Data charting and analysis

Data charting (i.e., data extraction) was intended to extract relevant data from the reviewed papers to better map the literature and answer our research questions on research methods, human factors, and security solutions, as shown in Section 3. The charting factors and the charting process are detailed in Appendix A.3. After charting the data (including categorical data and text snippets), we first performed a descriptive analysis of publication and author details to provide an overview of the corpus (see Section 5.1). Then, the first three authors conducted a qualitative content analysis to categorize the literature according to research motivations, aims, research questions, and methodologies, offering an overall picture of existing studies (see Section 5.2). Furthermore, the first author conducted a reflexive thematic analysis to uncover key concepts and themes concerning human factors using data from the included studies that are understanding-oriented (see Section 7). For included studies that are more design-oriented, the second and third authors performed a qualitative content analysis to categorize them based on the focused security approach and design principles (see Section 8). Based on this review and our analysis, we present a conceptual framework for mapping human-centered security research in the smart home context in Section 6.

5. Findings from the scoping review: an overview

The following section offers an overview of the scoping review corpus, outlining the main features and distribution of the included studies.

[1] https://www.covidence.org/.

Table 1
A Summary of Included Literature based on Research Categories and Aims.

Aims	Primary Research Objectives and Included Studies	Research Methods
Category One: Understanding Human Factors in Smart Home Security		
Aim (a) - Understand Users in General Smart Home (N = 44)		
	In this subset, studies have sought to understand average smart home users' experiences and perspectives on security, such as their concerns and attitudes, e.g., (Zeng et al., 2017; Li et al., 2023; Haney et al., 2021; Vetrivel et al., 2023; Peterson and Mujeye, 2025); and examine the security perspectives of particular groups, including specific demographics (e.g., parents and children (Turner et al., 2022b; Sun et al., 2021)), professions (e.g., journalists (Shere et al., 2020), home care providers (Fayoumi et al., 2022)), vulnerable populations (Chidziwisano and Jalakasi, 2023; Leitão, 2019; He et al., 2025), and less commonly studied geographical locations (Almutairi and Almarhabi, 2021; Patterson et al., 2021). ★★ (Huijts et al., 2023; Brush et al., 2011; Haney et al., 2021; Chalhoub et al., 2021; Turner et al., 2022a; Zimmermann et al., 2018; Zeng et al., 2017; Li et al., 2023; Philip et al., 2023; Tabassum et al., 2019; Barbosa et al., 2020; Klobas et al., 2019; Pospisil et al., 2022; Shuhaiber et al., 2023; George et al., 2021; Seymour et al., 2022; He et al., 2019; McDermott et al., 2019; Taieb and Pelet, 2019; Haney et al., 2020; Park et al., 2018)(Kulyk et al., 2020; Lafontaine et al., 2021; Maiorescu et al., 2021; Douha et al., 2023; Vetrivel et al., 2023; Haney et al., 2025; Keleher et al., 2024; Löbner et al., 2024; Schuster and Habibipour, 2024; Peterson and Mujeye, 2025; Zhang-Kennedy et al., 2025; Protick et al., 2024; Turner et al., 2022b; Fayoumi et al., 2022; Almutairi and Almarhabi, 2021; Benton et al., 2023; Chidziwisano and Jalakasi, 2023; Shere et al., 2020; Leitão, 2019; Patterson et al., 2021; Sun et al., 2021; He et al., 2025; Pattnaik et al., 2024)	surveys, interviews, focus groups, field or ethnographic studies, online data analysis
Aim (b) - Understand User Experience with Specific Devices (N = 13)		
	This subset of studies has examined end users' security perceptions and behavior in terms of particular smart home devices, for example, smart personal assistants (Abdi et al., 2019; Abrokwa et al., 2021; Huang et al., 2020), security cameras (Neilly et al., 2022), and smart locks (Hazazi and Shehab, 2023, 2024). ★★ (Abrokwa et al., 2021; Breve et al., 2023; Abdi et al., 2019; Fruchter and Liccardi, 2018; Neilly et al., 2022; Chhetri and Motti, 2019; Seymour and Such, 2023; Huang et al., 2020; Mols et al., 2022; Hazazi and Shehab, 2023, 2024; Ye et al., 2025; Valero et al., 2023)	surveys, interviews, focus groups, online data analysis
Aim (c) - Understand User Experience with Security Mechanisms (N = 7)		
	This subset has contributed to a better understanding of users' experiences with specific security mechanisms, focusing primarily on authentication (Alam et al., 2021; Ponticello et al., 2021; Prange et al., 2021; Wang et al., 2025) and, to a lesser extent, the management of smart home updates (Haney and Furman, 2023b,a) and diagnositic services (Sasaki et al., 2025). ★★ (Alam et al., 2021; Ponticello et al., 2021; Haney and Furman, 2023b,a; Prange et al., 2021; Wang et al., 2025; Sasaki et al., 2025)	surveys, interviews, focus groups
Aim (d) - Understand Security Issues (N = 6)		
	This subset has analysed specific security risks and issues in smart home environments, which can be introduced through user interaction with various IoT devices (McCarthy et al., 2020; Hodges, 2021; Alghamdi and Furnell, 2023) or home automation systems (Saura et al., 2021; Jacobsson et al., 2014, 2016). ★★ (McCarthy et al., 2020; Saura et al., 2021; Hodges, 2021; Jacobsson et al., 2014, 2016; Alghamdi and Furnell, 2023)	online data analysis, workshop, survey
Aim (e) - Understand Security Design Process and Practices (N = 3)		
	This subset has explored security design practices through interviews with smart home camera designers (Chalhoub et al., 2020), heuristic evaluations of smart home hubs (Mare et al., 2019), and analyses of user manuals and support pages (Blythe et al., 2019), revealing how security design and communication shape security practices. ★★ (Chalhoub et al., 2020; Blythe et al., 2019; Mare et al., 2019)	interview, heuristic evaluation, online data analysis
Category Two: Designing User-Centered Security		
Aim (a) - Design Usable Security Mechanisms (N = 12)		
	This subset has focused on designing or enhancing the usability of security mechanisms, particularly concerning access control (Malkin et al., 2023; Zeng and Roesner, 2019; Goffinet et al., 2021; Jang et al., 2017; Jia et al., 2021) and authentication (George et al., 2019; Yu et al., 2022; Zimmermann et al., 2025; He et al., 2018). ★★ (Malkin et al., 2023; George et al., 2019; Zeng and Roesner, 2019; Goffinet et al., 2021; Jang et al., 2017; Feth et al., 2017; Yao et al., 2019; Yu et al., 2022; Jia et al., 2021; Zimmermann et al., 2025; He et al., 2018; McCall et al., 2023)	online/laboratory experiment, survey, interview workshop/focus group
Aim (b) - Design Mitigation Strategies for End-Users (N = 9)		
	This subset has explored mitigation strategies and security interventions aimed at improving user engagement with security measures through clear communication (Duezguen et al., 2021; Collen et al., 2022), risk assessment support (Windl et al., 2022), and motivation of secure actions (Prange et al., 2022; Morgan et al., 2022). ★★ (Collen et al., 2022; Nurse et al., 2016; Prange et al., 2022; Duezguen et al., 2021; Scott et al., 2022; Windl et al., 2022; Morgan et al., 2022; Vasalou et al., 2025; Alsufyani et al., 2025)	interview, survey, online/laboratory experiment, field experiment
Category Three: Supporting Smart Home Security Education and Research		
Aim (a) - Support Security Education / Training (N = 6)		
	This subset has investigated ways to enhance security education by designing explanations to raise smart home owners' understanding of security issues (Bahrini et al., 2020b,a), developing curricula or workshops to teach cybersecurity concepts (Bailey et al., 2023; Sharevski et al., 2018; Jois et al., 2024), and evaluating education and awareness programs (Plachkinova and Menard, 2022). ★★ (Bahrini et al., 2020b,a; Bailey et al., 2023; Sharevski et al., 2018; Plachkinova and Menard, 2022; Jois et al., 2024)	online/laboratory experiment, workshop curriculum development
Aim (b) - Support Cybersecurity Research (N = 2)		
	In this subset, studies have provided instrumental support for security research in smart homes, including the CySESH scale for assessing cybersecurity self-efficacy (Borgert et al., 2023) and modeling techniques that produce realistic automation scenarios to guide system design and user evaluation (Manandhar et al., 2020). ★★ (Borgert et al., 2023; Manandhar et al., 2020)	literature review, statistical analysis

After ★★, the complete list of included studies for the corresponding subset is provided.

5.1. Overview of the corpus

5.1.1. Publication venues and years

We analyzed the distribution of publication years and venues for the final corpus of 102 papers. The included papers span from 2011 to 2025, with the majority published after 2019. This distribution highlights a growing focus on human-centered research in smart home security in the last seven years. The papers were published in various venues focusing on human-computer interaction (HCI), computer security, or the broader field of computer science, including CHI, SOUPS, USENIX Security, CSCW, IEEE S&P, etc. See further details of publications in Appendix B.1.

5.1.2. Locations

The research institutes, considering all authors, contributing to the corpus are primarily located in the USA (N = 40), the UK (N = 25), and various countries across Europe, with fewer contributions from Asia (N = 6). Details of the distribution are provided in the table in Appendix B.2. This geographic distribution underscores the global interest in this research area, but the concentration of work primarily coming from research centers in North America and Europe suggests that the existing results may be centered around Western cultural perspectives.

5.1.3. Expertise of research teams

When examining the expertise of the researchers contributing to the corpus based on their personal profiles or affiliations, we found that they come from various fields, primarily focusing on usable (or human-centered) security and privacy; some teams have more expertise on cybersecurity while others focus more on HCI. Additionally, researchers from other computer science and information technology fields, such as information systems, mobile computing, machine learning, and IoT, along with researchers with backgrounds in social sciences, psychology, and business, have also contributed their expertise to enrich research in this direction. This multidisciplinary collaboration offers insights into smart home security by addressing both technology design and human factors, contributing to a thorough understanding of the topic.

5.2. Research categories, aims, and methods (RQ1)

To address our three main research questions and provide an overall picture of the review literature, we qualitatively analyzed the research motivations, aims, research questions, and methodologies of the articles. Through the analysis, we identified three main research categories, each addressing different focal areas: (1) understanding human factors in smart home security; (2) designing usable security for smart homes; and (3) supporting smart home security education and research. We summarized the primary *research objectives* and typical *research methods* associated with each category in Table 1 to map out the included literature.

For RQ1, which examines the research methods used in human-centered investigations of smart home security, we identified diverse methodological approaches across three categories: (1) Studies aiming to better understand user experiences and perspectives on smart home security typically employed surveys and interviews (e.g., (Almutairi and Almarhabi, 2021; Maiorescu et al., 2021; Abdi et al., 2019; Tabassum et al., 2019; Hazazi and Shehab, 2023)) to capture users' perceptions, such as risk awareness and security intentions, including several relational studies that examined associations among these factors. Focus groups and design sessions were also commonly used to elicit people's perspectives, e.g., (Chidziwisano and Jalakasi, 2023; Seymour et al., 2022; Prange et al., 2021). Unlike most studies, which used surveys and individual or group interviews conducted at singular time points, a few studies employed an "in-situ" methodology by conducting field studies or ethnographic studies to gain insights into users' lived experiences (Brush et al., 2011; Huijts et al., 2023; Chalhoub et al., 2021; Turner et al., 2022a). Additionally, several studies analyzed online textual data (e.g., consumer reviews, Reddit discussions) (Fruchter and Liccardi, 2018; Chhetri and Motti, 2019; Li et al., 2023; Protick et al., 2024) to understand users' security perspective and practices. (2) For studies that focused on improving the usability of security mechanisms and mitigation strategies, most of them evaluated security approaches through user studies, either via laboratory experiments (George et al., 2019; Yu et al., 2022; Jia et al., 2021) or online experiments (Malkin et al., 2023). Notably, Zeng and Roesner (2019) conducted a month-long in-home user study (i.e., field experiment) to evaluate the design of a mobile app for smart home control. (3) For studies supporting security education, they designed curricula or explanations to teach cybersecurity concepts in workshops or summer camps (Bailey et al., 2023; Sharevski et al., 2018), or evaluated them in online experiments (Bahrini et al., 2020b). These results demonstrate that researchers in this field have employed a variety of methodological approaches tailored to their specific investigations.

6. Conceptual framework for human-centered security in smart home research

Based on our analysis of the contributions, we further organized the reviewed studies into two primary groups to further map the landscape of this research area: one focused on gaining a better understanding of the problem space, especially human factors, and the other centered on designing or improving security and support solutions. Building on this classification, we developed a conceptual framework, which highlights the main challenges, design principles, contributing human factors, and existing security approaches that arise from the reviewed studies (see Fig. 2).

This framework, along with the synthesis of findings in Sections 7 and 8 addressing RQ2 and RQ3, is intended to guide researchers and practitioners in navigating human-centered approaches to smart home security and in identifying key directions for future investigations. For smart home designers, Section 6.1 highlights key human-centred challenges (e.g., complexity of the smart home environment) and Section 6.2 provides general design principles, which can be applied to the design and development of secure devices and systems in smart home contexts. For usable security researchers, Section 7 provides a summary of major findings concerning six key human factor dimensions (e.g., user perception, user behavior, and contextual factors). These insights can be used to guide future empirical investigations (e.g., exploring the security of new devices) or to refine existing security mechanism designs. For security practitioners, incorporating the security design and support approaches outlined in Section 8 may be considered, with the aim of improving these strategies to better align with users' needs and behaviours according to the design principles. Finally, for policymakers in the smart home and IoT field, this framework reveals socio-technical considerations (e.g., in particular the findings of organizational factors in Section 7.6) that might be taken into account for developing guidelines and standards that can support both security and user empowerment. By connecting human factors with security solutions through the identified challenges and design principles, this framework aims to offer an overview of human-centered security in existing smart home research.

In the following sections, we first discuss the four main challenges in human-centered smart home security in Section 6.1, and outline general design principles for designing effective security approaches in Section 6.2.

6.1. Main challenges

Due to its cyber-physical and socio-technical nature, smart home security is a complex and challenging problem. Part of the complexity of security arises from the need to secure both physical spaces (e.g., preventing burglary at home) and digital environments (e.g., protecting multi-device data from cyber threats). From a socio-technical

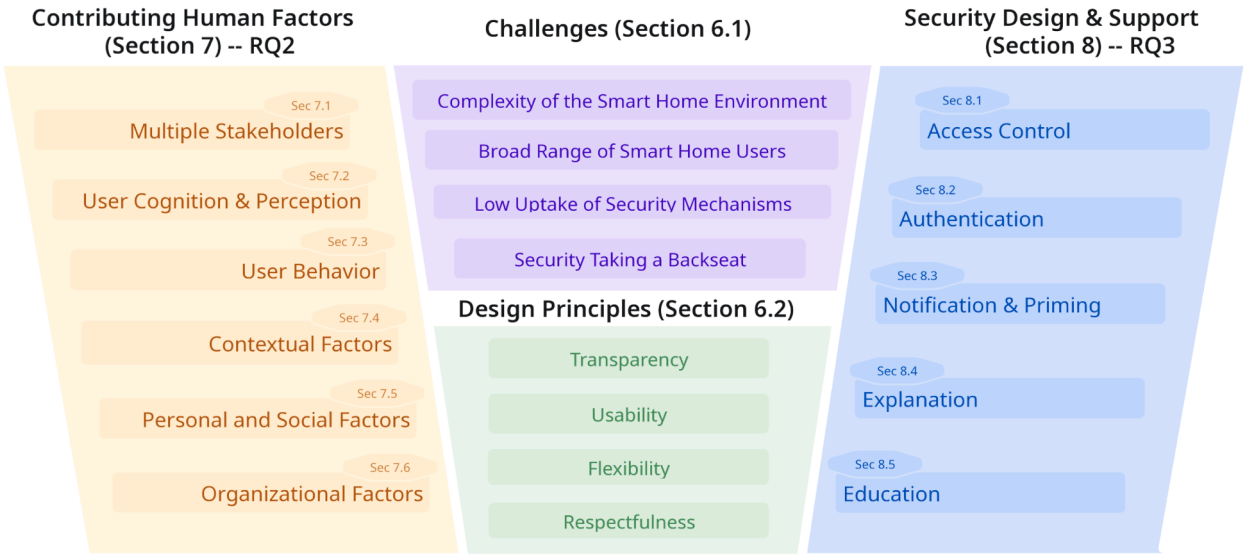

Fig. 2. Conceptual Framework for Human-Centric Security in Smart Home Research.

perspective, diverse user groups and needs, contexts, and social factors add more challenges. Based on insights from all the reviewed studies, we summarize four main human-centered challenges in smart home security research.

6.1.1. *Challenge 1: Complexity of the smart home environment*

The complexity of home contexts mainly stems from the presence of multiple devices and users (Zeng et al., 2017; Haney et al., 2025). Devices in the home can serve various purposes (e.g., cameras and locks used for home security or surveillance (Chalhoub et al., 2021; Neilly et al., 2022; Hazazi and Shehab, 2024, 2023)) and be placed in different locations (Lafontaine et al., 2021), resulting in diverse perceptions and security needs. This highlights the importance of considering diverse contextual requirements when designing security mechanisms, such as authentication and access control (Zeng and Roesner, 2019; Manandhar et al., 2020; Zimmermann et al., 2025; He et al., 2018), to better align with users' needs. Also, variations in power dynamics within a multi-user context create specific contextual requirements for multi-user interaction, which may vary based on their roles (e.g., parents and children, caretakers and caregivers, employers or domestic workers) within the household (Zeng et al., 2017; Turner et al., 2022b; Fayoumi et al., 2022; He et al., 2025; Pattnaik et al., 2024). Therefore, it is essential to identify nuanced requirements for multi-user interactions and varied relationships. An in-depth understanding of these contextual factors (as discussed in Section 7.4) can inform the design of tailored mechanisms for specific home contexts while also guiding the creation of user-friendly designs that facilitate the effortless adoption of necessary protective strategies.

6.1.2. *Challenge 2: Broad range of smart home users*

As smart home IoT devices become increasingly widespread, many users, spanning different ages and countries are incorporating these devices into their daily lives (Park et al., 2018; Kulyk et al., 2020; Douha et al., 2023; Haney et al., 2025). Previous studies have suggested that smart home users have varied mental models (Zeng et al., 2017; Abdi et al., 2019), typically with an incomplete understanding of smart home devices and ecosystems, which impacts their security perceptions and behaviors (see detailed discussion in Section 7.2). In addition, individual differences (e.g., demographics and personal experience) (Breve et al., 2023; Zeng et al., 2017; Löbner et al., 2024) and social factors (such as culture, online reviews, and social media content) (Leitão, 2019; Li et al., 2023; He et al., 2025; Douha et al., 2023; Zhang-Kennedy et al., 2025) can also influence users' security attitudes and behaviors. When designing security mechanisms for such a broad range of smart home users, it is crucial to consider these factors (see Section 7.5) or leverage them to enhance the overall security posture (i.e., to better meet the security requirement).

6.1.3. *Challenge 3: Low uptake of security mechanisms*

In addition to the previously discussed conceptual challenges related to diverse users and the smart home context, a more practical challenge is the low adoption of security mechanisms. As revealed in previous investigations (Haney et al., 2021, 2020; Tabassum et al., 2019; Haney et al., 2025; Sasaki et al., 2025), many users rely on non-technical mitigation strategies (e.g., reducing device use) rather than technical mitigation strategies (e.g., authentication management or applying updates) because of limited knowledge of security and lack of awareness of available options for protection. Another factor contributing to the low adoption of security mechanisms is their usability and trustworthiness (Zeng and Roesner, 2019; He et al., 2018). Users have reported experiencing security fatigue, often due to a lack of control over the mechanisms and a sense of fatalism regarding their effectiveness (Haney et al., 2021). User security behavior is discussed further in Section 7.3.

6.1.4. *Challenge 4: Security taking a backseat*

The final, yet enduring challenge is that smart home users and involved organizations often do not consider security a primary task (Chalhoub et al., 2020; Blythe et al., 2019; Vetrivel et al., 2023; Zimmermann et al., 2025). Smart home users may typically prioritize convenience, functionality, and affordability when selecting devices, sometimes having to balance or trade-off security for convenience (Li et al., 2023; Keleher et al., 2024). In manufacturing, companies prioritize business value and profitability for smart home devices (Chalhoub et al., 2020). Ideally, smart home companies would incorporate robust and usable security mechanisms like encryption, secure communication protocols, and timely software updates. The incorporated security mechanisms should be visible and user-friendly (i.e., easy to understand and use). However, designing and implementing these features often requires substantial resources, including security experts and user experience designers, and time for collaboration and innovation (Chalhoub et al., 2020). This can be seen as not cost-effective, particularly for start-ups. Therefore, security is sometimes implemented only to satisfy basic regulatory requirements, which may fall short of preventing vulnerabilities that attackers can exploit. Further insights from previous studies are detailed in Section 7.6.

6.2. Design principles

Drawing on all the reviewed literature, we distilled four general design principles that guide the development of security approaches addressing these challenges. Section 8 will then present existing approaches that predominantly reflect these principles.

6.2.1. Transparency

Transparency in smart home security includes clearly communicating the security mechanisms for devices, how security mechanisms work, what data is collected, and how it is used, etc (Blythe et al., 2019). Transparency is widely recognised, by most studies, as essential for bridging the gap between users and systems. Transparent technical design can be beneficial to foster users' security awareness and improve their security knowledge (Zeng and Roesner, 2019; Turner et al., 2022b), enhancing their willingness to adopt security mechanisms and follow secure practices (Hazazi and Shehab, 2023; Schuster and Habibipour, 2024; Wang et al., 2025). For instance, a smart door lock that provides real-time notifications about who accessed the door and how they gained access can ensure users understand system operations and identify potential risks, which may reduce potential security issues (Brush et al., 2011; Morgan et al., 2022). Being transparent in security design can build a foundation of trust and accountability, allowing users to take their informed responsibility and engage with security features (Haney et al., 2021).

6.2.2. Usability

Usability in security involves designing approaches that are simple to use, easy to understand, and seamlessly integrate into daily routines without requiring extensive technical expertise (Zeng and Roesner, 2019; Yu et al., 2022; Jang et al., 2017; He et al., 2018; Zimmermann et al., 2025). Given that the general public often has limited knowledge of security and perceives security as a secondary task (Zeng et al., 2017; Tabassum et al., 2019; Zimmermann et al., 2025), usability should be a primary consideration when designing nearly all security mechanisms for smart home devices (see Section 8). As an example, to address challenges posed for users (e.g., cumbersome password authentication), Zimmermann et al. (2025) suggested embedding authentication within existing primary tasks or replacing it with them, for example, using a unique cleaning routine. Increasing research efforts highlight the importance of designing highly usable security mechanisms, ensuring that security does not hinder users but instead integrates seamlessly into their daily routines.

6.2.3. Flexibility

Flexibility in security approaches means accommodating diverse user needs, preferences, and contexts. Given the challenge of catering to a broad range of users in smart homes, security design should be flexible to adapt to individual users and different user scenarios, ensuring inclusivity and effectiveness across various households and usage patterns (Zeng et al., 2017; Zeng and Roesner, 2019; Kulyk et al., 2020; He et al., 2025). For example, flexibility can be achieved by accommodating users with different levels of expertise, such as offering detailed security configuration options for experienced users while providing simplified setup modes for novices (Vetrivel et al., 2023). Similarly, a parental control feature that enables varying levels of access for different family members exemplifies flexibility, allowing security to be maintained without compromising usability (Zeng and Roesner, 2019). Flexibility can help ensure security approaches (e.g., access control) remain practical for diverse users, fostering broader adoption.

6.2.4. Respectfulness

Respectfulness in security design involves safeguarding user privacy, minimizing unnecessary data collection, and respecting individual choices and autonomy (Jang et al., 2017; Zeng and Roesner, 2019; Hazazi and Shehab, 2023). Studies have shown that some smart home users express concerns about insecure data protection (Haney et al., 2021; Chalhoub et al., 2021; Almutairi and Almarhabi, 2021), respectful design combined with transparency can align with data ethics and help build user trust. For example, a smart thermostat that processes data locally without uploading it to the cloud respects user privacy while maintaining functionality. In addition, respectfulness in multi-user interactions can be supported by preventing one user from controlling or automating devices in ways that might unexpectedly disrupt or surprise others (e.g., through device automation). Such design consideration helps maintain harmony, reduce conflicts, and reinforce each user's sense of agency and respect (Zeng and Roesner, 2019; Pattnaik et al., 2024; Huang et al., 2020).

6.3. Short summary

This section described the multifaceted challenges inherent in smart home security as depicted in our conceptual framework (Fig. 2). Effectively addressing these challenges requires shared responsibilities and coordinated efforts among three main stakeholders: users, manufacturers, and regulators, with researchers playing a crucial role in informing, evaluating, and supporting their practices. We then discussed the four overarching principles, i.e., transparency, usability, flexibility, and respectfulness, that form a basic framework for effective smart home security. Transparency and respectfulness build trust, usability ensures accessibility, and flexibility accommodates diverse user needs, collectively driving the secure and user-friendly design of smart home technologies.

In the next two sections, we will present a detailed synthesis of findings on contributing human factors (Section 7) and five main types of security design and support solutions (Section 8), as illustrated in the left and right modules of our framework.

7. Findings on human factors in smart home security (RQ2)

In this section, we address RQ2, which investigates what human factors may impact smart home security, by synthesising key findings from the included studies that focus on understanding human factors (N = 73). Through our thematic analysis of these studies, we identified six dimensions: *multiple stakeholders*, *user cognition & perception*, *user behavior*, *contextual factors*, *personal and social factors*, and *organizational factors*. Together, these dimensions reveal the complex and socio-technical challenges of securing smart home environments. These insights not only offer an in-depth understanding of human-centric security challenges but also provide a conceptual foundation for researchers and practitioners to integrate these factors into real-world security design in smart home contexts.

In the following, we present key concepts and main themes (see a summary in Table 2), illustrating how various human and social factors relate to smart home security and how these findings have implications for future efforts to secure smart homes. This summary table offers a structured overview and point of reference, aiming to support navigation within this section. Additionally, a summary table of review papers categorised by human factor dimensions is provided in Appendix B.3, allowing access to the complete mapping between studies and factors.

7.1. Multiple stakeholders

7.1.1. Stakeholders

The literature considers three key stakeholder groups in smart home contexts: smart home users, companies, and regulators.

This subset of the corpus explored diverse stakeholders who may directly or indirectly impact smart home security, including: the *end users* who interact with smart home devices, the *organizations* that design smart home technology and products, and *regulators* who ensure and enforce

Table 2
Summary of Human Factors, Major Themes, and Key Concepts in Smart Home Security.

Dimensions	Themes	Concepts	Example Studies
Multiple Stakeholders			
Stakeholders	The literature considers three key stakeholder groups in smart home contexts: smart home users, companies, and regulators.	Smart home end-users, Smart home companies, Regulators, Others	Zeng et al. (2017), Chalhoub et al. (2020)
Responsibilities	All stakeholders share responsibility for ensuring smart home security.	Perceived responsibility	Haney et al. (2021)
User Cognition & Perception			
Security Knowledge	Smart home users have varied mental models, often with an incomplete understanding of smart home devices and ecosystems, impacting their security perceptions and behaviors.	Mental models, Understanding of smart home ecosystems and data practices	Abdi et al. (2019), Zimmermann et al. (2018), Zeng et al. (2017), Tabassum et al. (2019)
	Some smart home users can identify potential threat agents and security attacks, but many still lack knowledge about protective strategies.	Security knowledge, Threats and adversarials	Chalhoub et al. (2021), Abdi et al. (2019), Zeng et al. (2017), Neilly et al. (2022)
Security Perceptions	Smart home users generally have low awareness of security risks, although their levels of concern can vary and may depend on other factors.	Security awareness, Security concerns	Huijts et al. (2023), Kulyk et al. (2020), Fayoumi et al. (2022), Turner et al. (2022a), Löbner et al. (2024)
	Users' security perception consists of several aspects, e.g., perceived severity, vulnerability, and information sensitivity, which can be influenced by personal, social, and contextual factors.	Threat perception, Risk perception, Perceived sensitivity of information, Trust perception	Zeng et al. (2017), Abdi et al. (2019), Huijts et al. (2023)
Security Attitude	Smart home users show varied attitudes towards security, influenced by concerns and considerations such as perceived benefits and effort.	Attitude towards security, Perceived benefits effort	Li et al. (2023), McDermott et al. (2019)
Intention to Secure	User intentions to secure their smart homes are influenced by their attitudes towards security as well as their perceived self-efficacy.	Intention to secure,Attitude towards security, Perceived self-efficacy	Philip et al. (2023)
User Behavior			
Mitigation Strategies	Smart home users leverage security controls and technical mitigation strategies, while some rely on non-technical strategies due to a lack of knowledge of protection measures.	Technical mitigation, Non-technical strategies	Haney et al. (2021), Abdi et al. (2019), Haney et al. (2020), Chhetri and Motti (2019)
Pre-emptive Strategies	In addition to mitigation strategies during device use, other pre-emptive strategies employed to preserve security include device selection and setup, and participation in online discussions.	Device configuration, Device use, Online community	Turner et al. (2022a,b), Haney et al. (2020)
	In real smart home scenarios, identifying attacks can be challenging for users.	Response to attacks	Huijts et al. (2023), Pospisil et al. (2022)
Contextual Factors			
Device as Context	Smart home devices typically influence users' concern levels and attitudes towards security; for instance, security cameras and door locks are perceived as having higher sensitivity.	Security cameras, Smart speakers, Smart door locks	Sun et al. (2021), Chalhoub et al. (2021), Brush et al. (2011), Hazazi and Shehab (2023)
Location as Context	The location of smart home devices can also impact user security perception, particularly when devices are placed in private spaces.	Private & public space	Lafontaine et al. (2021), Haney et al. (2020)
Multi-User and Use Scenarios	In a smart home context, the presence of multiple users raise additional concerns related to varying rights to control devices and access data.	Multi-user control, Technology use scenarios, Sharing practices	Alam et al. (2021), Zeng et al. (2017), Fayoumi et al. (2022), Pattnaik et al. (2024)
Technology Adoption Phase	Users' security concerns and attitudes change depending on their technology adoption phase.	Device purchase, Device installation & use	Patterson et al. (2021), Huijts et al. (2023), Turner et al. (2022a)
Personal and Social Factors			
Personal Factors	Users' perceptions, attitudes, and behavior can be influenced by individual difference, such as demographics and personal experiences	Demographics, Personal experience	Park et al. (2018), Kulyk et al. (2020), Zeng et al. (2017), Breve et al. (2023)
Social Factors	External influences that stem from interactions with others and the broader social contexts can also influence user security attitudes and behaviors in smart home.	Social norms, Online information and media	Shuhaiber et al. (2023), Chidziwisano and Jalakasi (2023), Li et al. (2023), Sun et al. (2021)
Organizational Factors			
Security Design Practice	Smart home companies should be responsible for providing user security support and managing resources to ensure effective security practices.	Security support UX for security design	Chalhoub et al. (2020), Blythe et al. (2019)
Policy Regulation	Policy regulations play a crucial role in ensuring companies adhere to best practices and secure smart homes.	Security practices Data protection	Haney et al. (2021), Philip et al. (2023), Chalhoub et al. (2020)
Security Education	Security education is equally important for raising user awareness and equipping individuals with the knowledge to secure their homes.	Education, Awareness enhancement	Haney et al. (2021), Turner et al. (2022b)

technology compliance with regulations and industry standards. Regarding the end-users, the majority of studies examined the perspective of primary users who would directly interact with smart home devices and are most impacted by them (e.g., Abdi et al., 2019; Huijts et al., 2023; Zeng et al., 2017; Ponticello et al., 2021; Li et al., 2023). Several studies investigated the perspectives of non-primary users, e.g., visitors, bystanders (Zeng et al., 2017; Neilly et al., 2022; Chidziwisano and Jalakasi, 2023; Leitão, 2019), domestic abuse survivors (Leitão, 2019), and domestic workers (He et al., 2025). In addition, some studies explored security knowledge and perceptions through the lens of a family (Turner et al., 2022b). At the organizational level, several studies examined practices in smart home companies by exploring the perspectives of people who work in product design teams, development teams, or who hold expertise in security, e.g., (Chalhoub et al., 2020; Shere et al., 2020; Prange et al., 2021; Jacobsson et al., 2014, 2016). Yet, none of the studies in our corpus has directly examined the perspectives of regulators, even though their role in ensuring smart home security is acknowledged to some extent in most studies.

7.1.2. Responsibility

All stakeholders share responsibility for ensuring smart home security.

As diverse stakeholders are involved, it would be helpful to understand their own responsibilities and how people perceive responsibilities for smart home security. In our corpus, most studies assumed the allocation of these responsibilities, mainly to manufacturers, without addressing issues of responsibility, while one interview study went further to understand users' perceptions of responsibility (Haney et al., 2021). This study investigated how smart home users assign responsibility for the privacy and security of their devices and how their perceptions influence their concerns and mitigation actions. They present a model of perceived relationships between users, manufacturers, and third parties, providing insights to strengthen the interdependent relationships crucial for smart home security. To ensure the security of smart homes, ideally, all three stakeholder groups should take responsibility and collectively contribute to securing the home; smart home users need to ensure secure interaction with smart home devices; companies should ensure the design complies with security policy and design usable and effective security mechanisms for users; and regulators should provide comprehensive security guidance to support companies and users. However, users' perceived responsibilities, attitude, and behavior, and the practices of smart home companies are influenced by many other factors, which will be detailed in the following section.

7.2. User cognition & perception

This section presents the main themes related to users' knowledge, perceptions, attitudes, and intentions regarding smart home security, which play a crucial role in shaping their security behaviors.

7.2.1. Security knowledge

Smart home users have varied mental models, often with an incomplete understanding of smart home devices and ecosystems, impacting their security perceptions and behaviors.

In our corpus, several studies investigated users' mental models of smart home ecosystems or devices, including users' knowledge and understanding of their devices and the associated data practices, as this would influence their understanding of threats (Abdi et al., 2019; Zimmermann et al., 2018; Zeng et al., 2017; Tabassum et al., 2019). Existing empirical studies have indicated that smart home users have varied mental models (Zeng et al., 2017; Tabassum et al., 2019). For example, Zeng et al. (2017) uncovered that users with more advanced mental models are able to describe more technical details, such as smart home networks (e.g., cloud servers, routers, wireless protocols), while users with intermediate level or limited understanding of smart home technology may only understand that smart home devices can communicate with other devices but do not know how; some users even have no awareness of the network or the cloud. These studies also suggest that many smart home users possess incomplete mental models of the devices they used, which can affect their perceptions of data practices and security, hence influencing their behavior (Abdi et al., 2019; Huijts et al., 2023; Zeng et al., 2017; Tabassum et al., 2019).

Some smart home users can identify potential threat agents and security attacks, but many lack knowledge about protective strategies.

Studies in the corpus also examined what users know about security, also called users' *threat models*, in smart homes (Abdi et al., 2019; Zeng et al., 2017), which can again be influenced by users' mental models of smart home ecosystem and device. In these studies of threat models, they investigated what threats or attacks smart home users can identify. Security threats describe potential dangers that may exploit security vulnerabilities, which might lead to unauthorized access, data breaches, or other harmful consequences (Chalhoub et al., 2021). According to the reviewed studies (Abdi et al., 2019; Neilly et al., 2022; Zimmermann et al., 2018; Zeng et al., 2017; Almutairi and Almarhabi, 2021), users mentioned various potential threat agents, such as hackers, malicious actors, data brokers, advertisers, smart home device manufacturers, cloud service providers, third parties, and government agencies. They are aware of some potential security threats, including (1) cybersecurity threats or cyberattacks (Alam et al., 2021; Chalhoub et al., 2021; Haney et al., 2021; Zeng et al., 2017; Haney et al., 2020), e.g., data breaches, insecure Wi-Fi networks, device security, and cloud security; (2) physical security threats (Kulyk et al., 2020; Zimmermann et al., 2018; Zeng et al., 2017; Haney et al., 2020), e.g., financial loss, burglary; and (3) privacy threats (Haney et al., 2021; Chalhoub et al., 2021; Almutairi and Almarhabi, 2021): insecure data protection or concerns about manufacturers. While some smart home users are aware of some threat agents and potential threats, most studies indicated that users' threat models were sparse. For example, Zeng et al. (2017) found that most identified threats related to physical security, such as risks involving smart locks or cameras, which safeguard property from physical dangers like unauthorized access. They also observed that smart home users identified few concrete vulnerabilities that could lead to a security or privacy compromise, and the majority of participants did not identify any potential vulnerabilities. Similarly, Abdi et al. (2019) reported that many smart speaker users have difficulty articulating potential attacks, with unwanted listening being the most commonly identified attack. Furthermore, many smart home users have little knowledge of security and protection strategies (Alam et al., 2021; Abdi et al., 2019; Zeng et al., 2017; Haney et al., 2020; Turner et al., 2022b), e.g., Alam et al. (2021) observed that smart home users have security concerns but they have misconceptions about device and data protection.

Why do some users have limited knowledge of smart home ecosystems and security? This could be influenced by various factors, including (1) personal factors: Users' technical knowledge can impact their mental model as mentioned previously (Zeng et al., 2017), which can influence their threat models, e.g., their assesment of vulnerabilities (Abdi et al., 2019; Chalhoub et al., 2021) ; (2) social factors: Users' understanding may be shaped by security concerns or stories from other domains (e.g., online banking) they come across via social media or news sources (Abdi et al., 2019; Vetrivel et al., 2023; Zhang-Kennedy et al., 2025); (3) contextual factors: For multi-user contexts, users who install and set up smart home devices may be more aware of the associated mechanisms and data practices (Tabassum et al., 2019); (4) organization factors: The information offered by manufacturers can impact users' understanding, e.g., a study found that the information presented to users is often too abstract and not easily understood (Turner et al., 2022a). While these

studies suggest that users may express more security concerns and adopt protective strategies as their security knowledge increases, some users tend to have low security concerns despite being aware of potential adversaries and threats (Zeng et al., 2017). This may be due to factors such as trust in companies to safeguard their data.

7.2.2. Security perceptions

Smart home users generally have low awareness of security risks, although their levels of concern can vary and may depend on other factors.

A common finding was that smart home users often display low awareness of security and privacy risks in smart homes (Huijts et al., 2023; Kulyk et al., 2020; Fayoumi et al., 2022; Turner et al., 2022a,b). This lack of awareness can be attributed to several factors, including a lack of user understanding of potential vulnerabilities of their devices or the associated security implications, as discussed previously. Other factors influencing user awareness include the complexity of security issues and the general lack of clear information about the associated risks (Blythe et al., 2019). Alongside the findings of low security awareness, studies have also indicated that many users exhibit low levels of security and privacy concerns (Huijts et al., 2023; Haney et al., 2021; Zeng et al., 2017; Tabassum et al., 2019; Haney et al., 2020, 2025). The main reasons for users having low concerns are that: (1) some users have trust in manufacturers or regulators to ensure protection (Haney et al., 2021; Zeng et al., 2017; Tabassum et al., 2019; Haney et al., 2025; Löbner et al., 2024); they also often trust researchers who handle their data (Huijts et al., 2023); (2) some users perceive a lower likelihood of cyberattack because they do not believe they are attractive targets (Zeng et al., 2017), perceiving their information as neither valuable nor interesting to others (Haney et al., 2021, 2020); (3) some believe they do not have something to hide (Zeng et al., 2017); (4) some believe their existing mitigations to be sufficient (Huijts et al., 2023; Zeng et al., 2017); and (5) some are willing to accept security and privacy risks in exchange for the functionality and convenience of smart home technology; they may perceive some level of concern, but they perceive the cost of protective measures as high (Zeng et al., 2017; Tabassum et al., 2019; Haney et al., 2020).

Despite generally low security awareness and concerns observed among many smart home users in the existing literature, some users did express concerns about security and privacy (Alam et al., 2021; Haney et al., 2021, 2020). Depending on users' security knowledge, users typically mentioned concerns including data breaches, audio or video access, government access, and exposure of sensitive information such as financial information. Users' security concerns are often context-dependent. For instance, one notable user concern is about the lack of security of their conversations (i.e., audio recording) through smart speakers (Abdi et al., 2019) or smart home hubs (Chhetri and Motti, 2019). More contextual influences will be discussed in Section 7.4. In addition to concerns regarding particular devices, studies also showed that some users also mentioned concerns about security mechanisms (Wang et al., 2025) or home automation (Brush et al., 2011; Breve et al., 2023; He et al., 2019). For example, Brush et al. (2011) noted that users expressed concerns about remote access, believing that this feature could make their homes more vulnerable. He et al. (2019) discussed end-user programming offered by many smart devices, indicating that some users are concerned about potentially breaking the systems by writing their own programs. Furthermore, in contrast to users who tend to trust manufacturers, several studies emphasized that some smart home users have privacy concerns regarding their data and the manufacturers handling it (Haney et al., 2021; Chalhoub et al., 2021; Almutairi and Almarhabi, 2021; Chhetri and Motti, 2019; Kulyk et al., 2020). The above findings indicated users' security concerns vary from person to person, which can be explained by several factors. Next, we will further examine the factors that shape users' security perceptions.

Users' security perception consists of several aspects, e.g., perceived severity, vulnerability, and information sensitivity, which can be influenced by personal,social, and contextual factors.

Some of the literature investigates user security perceptions (or threat perceptions), including how an individual evaluates threats in a smart home, and indicates users' perceptions may impact users' concerns or fears (Li et al., 2023). Several studies refer to Protection Motivation Theory (PMT), which is a socio-cognitive model that includes two pathways (threat appraisal and coping appraisal) linking perceptions to behavior (Boer and Seydel, 1996). Threat appraisal refers to the evaluation of an individual's perception of a threat, which typically consists of the perceived severity (perceived degree of harm from the insecure behavior) and perceived vulnerability (perceived probability that one will experience threats). Coping appraisal refers to an evaluation of one's ability to deal with the threat. Several studies indicate that users' perceptions of the sensitivity of information collected by smart home devices can influence their willingness to share it (Alam et al., 2021; Zeng et al., 2017). In addition, user perceptions of the trustworthiness of manufacturers are linked to their threat perceptions (Zeng et al., 2017; Abdi et al., 2019; Huijts et al., 2023), and the relationship between user trust perception and threat perception can be bi-directional. For example, some users who trust manufacturers to protect their data tend to have low perceptions of vulnerability (Abdi et al., 2019); but users concerned that manufacturers can access and monitor their data may perceive higher threats (Almutairi and Almarhabi, 2021). Furthermore, researchers have also indicated that users' security perceptions are influenced by contextual, personal, and social factors (see Sections 7.4 and 7.5). For example, Park et al. (2018) found that user security perceptions of IoT-based home energy management are influenced by individual differences such as acceptance of new technology and sensitivity to electricity price changes. Also, users' security perceptions can be influenced by the stage of technology adoption; Huijts et al. (2023) indicated that users' perception of risks become less salient when they get used to the presence of the devices.

7.2.3. Security attitude

Smart home users show varied attitudes towards security, influenced by concerns and considerations such as perceived benefits and effort.

In addition to different concerns and considerations, smart home users demonstrate different attitudes towards security. Among our corpus, Li et al. (2023) analyzed online comments in Reddit, categorizing the five major categories of user attitudes toward security and privacy, each combining the users' degree of security and privacy (S&P) concerns and their level of incorporation of protective strategies: (1) "dismissiveness of S&P concerns"; (2) "exploration of possible concerns and protective strategies"; (3) "resignation to incorporating S&P protective strategies"; (4) "positive pragmatism in terms of incorporating protective strategies that balance cost and benefit tradeoffs"; (5) "devotion to incorporating protective strategies". Again, this study also suggested user attitudes towards security and privacy are context-dependent and change according to their contexts (e.g., device factors and adoption phases), and their considerations may evolve as some users may proactively seek related information. They also noted that individual differences (users' prior experience or preconceptions about a smart home device) can shape their attitude, influencing their assessment. In another study, Haney et al. (2021) observed an inconsistent relationship between user concerns, user attitudes towards accepting personal responsibility, and user behavior; people with security and privacy concerns did not always accept their personal responsibility, and sometimes people with low levels of concern accept responsibility and take mitigative actions for ensuring security and privacy. In terms of the relationship between user attitude and user behavior, while it is common to

believe that users with a positive attitude towards protective behavior will take mitigative action, McDermott et al. (2019) found that many users who show interest in protecting their privacy rarely perform actual behaviors. Regarding security, few studies sought to understand the relationship between security attitude and security behavior intentions, as discussed next.

7.2.4. Intention to secure

User intentions to secure their smart homes are influenced by their attitudes towards security as well as their perceived self-efficacy.

Regarding user intentions to secure their smart home (i.e., how likely a user plans or intends to take protective strategies), studies showed user considerations are multi-dimensional and depend on the interplay with other factors such as context Li et al. (2023), Philip et al. (2023). Philip et al. (2023) empirically analyzed the factors driving smart home users' security intentions and the relationships among those factors, based on theory of planned behavior (TPB) and rational choice theory (RCT). In line with TPB, they examined three main factors that drive users intentions to secure a smart home, including *attitude towards securing*, *normative beliefs* (i.e., subjective norm and normative norm), and *security behavior self-efficacy*. Attitude and self-efficacy are shown to be positively correlated to users' intentions. As theoretically supported by RCT, they also found the two broad categories of factors, "cost of securing or not securing" (e.g., life impediment, price, effort) and "benefit of securing" (e.g., intrinsic benefit), can form users' beliefs of security implications and drive users' attitudes towards security, which thereby affect users' intention to secure their smart homes. Regarding self-efficacy (or perceived self-efficacy), the study further shows that users are more likely to feel able to secure their devices if the provided interaction allows sufficient control. These findings suggest that reinforcing factors such as the benefits of security, reduced cost of securing, and improved self-efficacy in security behavior collectively contribute to positive user beliefs and attitudes toward security practices, which may drive user intentions to engage in security behavior.

7.3. User behavior

7.3.1. Mitigation strategies

Smart home users leverage security controls and technical mitigation strategies, while some rely on non-technical strategies due to a lack of knowledge of protection measures.

The existing literature has also investigated what mitigation strategies users adopt for protecting their device or data (Chalhoub et al., 2021; Haney et al., 2021, 2025, 2020; Tabassum et al., 2019; Zeng et al., 2017). These are typically categorized into two main categories: technical mitigation strategies and non-technical mitigation strategies. For technical mitigation strategies, studies showed that (1) some smart home users describe their strategies related to authentication management, such as changing passwords frequently, using strong passwords and two-factor authentication (Tabassum et al., 2019); (2) some users would limit access to devices and their apps, e.g., limiting the information they share with visitors and service providers (Haney et al., 2020); (3) some mentioned using a password to protect their Wi-Fi, and some discuss more sophisticated security mitigations, e.g., segmenting their home network, or monitoring network traffic (Haney et al., 2021; Tabassum et al., 2019; Haney et al., 2020); (4) some configured device options (e.g., disabling some default functionality like ordering for virtual assistants (Haney et al., 2021, 2020)); (5) some mentioned smart home updates or upgrades for mitigation purposes (Haney et al., 2020).

Rather than technical mitigation strategies, studies revealed that smart home users often rely on non-technical strategies due to limited knowledge of security and protective strategies (Haney et al., 2021; Abdi et al., 2019; Haney et al., 2020; Chhetri and Motti, 2019; Tabassum et al., 2019). Users may choose to limit audio and video exposure in certain places, e.g., avoiding placing cameras and smart speakers in more private rooms; some users may use certain devices offline to limit internet access to their data; some may limit the amount of information disclosed to the device; some may avoid the use of certain device functionality; some turn off smart speakers or delete the history data when possible; for smart cameras, some mention covering the camera lens with a sticker.

7.3.2. Pre-emptive strategies

In addition to mitigation strategies during device use, other pre-emptive strategies employed to preserve security include device selection and setup, and participation in online discussions.

Studies have also indicated that some smart home users would take pre-emptive considerations to prevent security issues before purchasing or adopting a device, such as reading online customer reviews that consider security and privacy (Turner et al., 2022a,b; Haney et al., 2020; Vetrivel et al., 2023). Also, users typically consider security and privacy and device management during the installation of devices (Turner et al., 2022a). After setting up the device following the suggested practices, consideration of device security rarely comes up again (Huijts et al., 2023). Moreover, some users would engage in security discussions either within their households (e.g., family discussions involving children (Sun et al., 2021) or in online forums such as Reddit (Li et al., 2023; Protick et al., 2024; Vetrivel et al., 2023). However, users with low concerns or even those with concerns may not take these actions. Users mentioned various reasons for inaction, some of which are due to low levels of concern, such as perceived low risks or low vulnerability. Additional reasons are that users are not aware of available options for protection, and users indicated security fatigue due to fatalism and a lack of control (Haney et al., 2021).

In real smart home scenarios, identifying attacks can be challenging for smart home users.

Regarding how people would respond to security attacks, in our corpus, Huijts et al. (2023) conducted a field experiment to investigate how people would respond to simulated security attacks, finding that simulated attacks had little impact on their participants, as people often did not notice any security risks. They also suggested that it is difficult for most smart home users to identify simulated attacks, and attack-related irregularities correctly were often ignored or mistaken for technical issues. Pospisil et al. (2022) surveyed users about cyberattack experiences, and found that very few respondents (3 %) reported unauthorized access to their smart home devices, with even fewer (2 %) experiencing disruption or blocking, unauthorized reconfiguration, or changes to device settings. However, it was found that participants informed about simulated attacks showed improved awareness and better ability to identify them, and some even developed rules to distinguish between random irregularities and simulated attacks (Huijts et al., 2023).

7.4. Contextual factors

Thus far, we have looked at how smart home user perceptions and behavior to secure their smart home. In this section, we examine how contextual factors influence these perceptions and behaviors.

7.4.1. Device as context

Smart home device types influence users' concern levels and attitudes towards security; for instance, security cameras and door locks are perceived as having higher sensitivity.

In our corpus, studies indicated that the types of smart home devices can influence how users perceive the sensitivity of information (Alam et al., 2021), their security concerns (Brush et al., 2011), and their privacy perceptions (Chalhoub et al., 2021). The devices most often studied are door locks (Brush et al., 2011; Alam et al., 2021; Sun et al., 2021; Hazazi and Shehab, 2023, 2024), cameras (including security cameras and smart display cameras) (Brush et al., 2011; Chalhoub et al., 2021), and voice-enabled devices such as smart speakers and smart displays (Zeng et al., 2017; Valero et al., 2023). For example, Alam et al. (2021) found that some users were skeptical about the data and control aspects of smart locks, envisioning serious physical consequences if compromised. In contrast, Hazazi and Shehab (2023) revealed that despite such concerns, many users still preferred smart locks, perceiving traditional locks as more vulnerable. In a household study, Brush et al. (2011) also found that door locks and cameras raise more security concerns. Regarding smart home cameras, users expressed more concerns about monitoring and surveillance. For example, Sun et al. (2021) indicated that most parents with concerns about cloud-based security cameras expressed worries about cameras being hacked and exposing their children to surveillance by strangers. Another phenomenon is that smart home cameras are frequently repurposed for surveillance (or parenting) and entertainment (Chalhoub et al., 2021), although they are originally designed to protect the household from burglary. Due to this repurposing, some users expressed privacy concerns and a feeling of intrusiveness, and some mentioned feeling a loss of control over their personal data.

In terms of smart speakers, Sun et al. (2021) showed that some smart home users are aware of privacy risks linked to smart speakers, but they expressed tolerance to such risks. Some users also raised concerns about the safety implications of automated control via smart speakers, as speakers are often used as smart home hubs; e.g., an automated garage door could be controlled by smart speakers. Abdi et al. (2019) found that users did not make the most of the shopping capabilities of smart speakers due to a lack of trust, security, and privacy concerns. This lack of trust is influenced by several factors: "products (visibility, comparisons, and mistakes), vendors, security of the connection, and privacy of the orders (e.g., other people may hear about the order)." That study also suggested that if the configuration of voice recognition is properly set up for users, it might serve as an easy and straightforward authentication method, potentially increasing user trust in smart speakers (Abdi et al., 2019).

7.4.2. Location as context

The location of smart home devices can impact user security perception, particularly when devices are placed in private spaces.

Studies also suggest that the location of the device can also influence user security perception. For example, Lafontaine et al. (2021) investigated users' comfort level when interacting with home IoT devices in different locations and showed that many users are comfortable using their devices in various locations and settings, particularly in private settings. However, some users are reluctant to interact with IoT devices in public spaces, which depends on individual differences (e.g., personal privacy concerns). Another study showed that users would limit their audio and video exposure to manufacturers or authorized users by strategically placing cameras and speakers, avoiding private areas of the home (Haney et al., 2020).

7.4.3. Multi-User, use scenarios

The presence of multiple users raises additional concerns related to varying rights to control smart home devices and access data.

Two other major contextual factors would be the presence of multiple users in the home context and the diversity of use scenarios and purposes of smart home devices. For multiple users in the home context, studies considered different categories, such as primary users and non-primary users (e.g., home owners and guests, visitors, other residents, or tenants), expert users and non-expert users, parents and children within a family, care-receivers, and care-providers. Regarding how the multi-user context influences user preferences and security perceptions, studies showed diverse user preferences, posing questions for future research on multi-user control. For instance, Alam et al. (2021) showed that some people expressed a preference for allowing family members to perform security-related tasks such as authentication, while some would not, as trust in family members varies. Zeng et al. (2017), He et al. (2025), and Pattnaik et al. (2024) discussed the differences in power and control within a multi-user context, indicating that non-primary users typically have less access and interest in smart homes, potentially resulting in the primary user (either intentionally or unintentionally) holding more control over other residents. Their study also found that incidental users tend to have simpler mental models, lower awareness of security and privacy, and weaker threat models. These results showed that "homes with multiple users pose unique security and privacy challenges, especially when the primary user has greater knowledge and control of the system than incidental users (Zeng et al., 2017)."

In addition, technology use scenarios may influence user concerns. Studies found varying user concerns in different scenarios, such as using devices for shopping, device management, social situations, and home care (Abdi et al., 2019; Kulyk et al., 2020; Ponticello et al., 2021; Fayoumi et al., 2022). For example, Kulyk et al. (2020) showed that users mentioned more concerns about using devices for health purposes, e.g., home care providers are concerned about the use of technology, exposure of the patients' personal information, and the potential for third parties to use the data (Fayoumi et al., 2022).

7.4.4. Technology adoption phase

Users' security concerns and attitudes change depending on their technology adoption phase.

Technology adoption phases, or users' experience of smart home technology, can also impact users' security perceptions, such as risk perception. For example, Patterson et al. (2021) highlighted risks linked to various phases of the IoT lifecycle, from device purchase, usage, the point when the device is no longer supported, and its eventual decommissioning (and possible rehoming). From a user perspective, Turner et al. (2022a) showed that device security questions typically occur when setting up the device, and occur less after installation. Similarly, Huijts et al. (2023) indicated that when smart home users get used to the presence of their device, the risks become less noticeable. This may be due to familiarity with the device increasing comfort levels of users. This familiarity and comfort with devices may also influence user preferences for locations to place their devices (Lafontaine et al., 2021).

7.5. Personal and social factors

7.5.1. Personal factors

Users' perceptions, attitudes, and behavior can be influenced by individual differences, such as demographics and personal experiences.

Studies also explore individual differences in user perceptions and behaviors regarding security in smart homes. Investigated factors typically include demographics (such as age, gender, and countries), education, expertise, and propensity to accept new technology, which yielded mixed results. For example, Park et al. (2018) found that users' risk perceptions of IoT-based home energy management are influenced by age, gender, and education. Their results indicated that older people tend to perceive lower risks; women tend to perceive higher risks than men; and people with higher education tend to have higher risk perceptions.

(Klobas et al., 2019) demonstrated the influence of personal factors on the decision to purchase smart home devices, showing that older and more educated people are more likely to consider security risks in their decision-making. A cross-country study (Kulyk et al., 2020) yielded contrasting results, showing gender did not make a significant difference and age had a small influence. However, they found a significant difference between three countries in terms of user awareness of security and privacy, with Germans being more concerned about security and privacy issues compared to users in Spain and Romania. In addition, a family-focused study (Turner et al., 2022b) showed that older participants are more inclined to discuss cyber security-strategies with their children than younger participants (Park et al., 2018).

Also, personal background and expertise are shown to impact security perceptions and behavior (Zeng et al., 2017; McDermott et al., 2019; Breve et al., 2023; Abrokwa et al., 2021). For example, security experts typically have more sophisticated mental models and can articulate more specific threats and mention more security concerns, which may not be shared by the general population with limited security expertise (Zeng et al., 2017). Also, people with a computer science background are more aware of potential risks and harms if sensitive information were disclosed (Breve et al., 2023). Moreover, people who self-identified with more technical knowledge tend to have a higher ability to detect an infected device (McDermott et al., 2019). Most of them have aligned results, showing that increased tech-savviness may lead to increased risk perceptions, which might also correlate with positive attitudes toward security (Abrokwa et al., 2021). In addition to users' technical knowledge, willingness to accept new technology can also influence risk perceptions.

7.5.2. Social factors

External factors stemming from interactions with others and the broader social context can influence user security attitudes and behaviors in smart homes.

The literature also indicates that social factors can influence users' security perceptions, and hence influence their trust in smart homes and their behavior (Shuhaiber et al., 2023). Social factors, such as influence of family members, culture, online reviews, and social media contents, can impact people's attitudes and behaviors towards security. In two studies that investigated security perceptions and discussion within families, parents with children tend to perceive a higher risk of data collection than people without children (Maiorescu et al., 2021). Also, when discussing cybersecurity at home, families tend to discuss risks and threats relating to online safety issues (Turner et al., 2022b). Moreover, several studies considered the influence of social contextual factors by examining particular user groups (Benton et al., 2023; Chidziwisano and Jalakasi, 2023; Leitão, 2019; He et al., 2025). Leitão (2019) examined intimate partner abuse survivors and support worker perspectives, showing their worries about the intricate security and privacy issues brought about by: (1) the shared use of smart home devices and accounts; (2) access to past usage logs containing information about all residents; and (3) the ability to remotely view live video streams inside the house. Chidziwisano and Jalakasi (2023) investigated how social norms of patriarchal societies shape the utilization of smart home technologies in Malawian homes. It emphasized women's rights and technology use by revealing the often-overlooked perspectives of marginalized women in designing smart home security systems suited to their specific needs. Benton et al. (2023) investigated the perspective of social housing tenants' on smart devices used in their rented homes, and He et al. (2025) explored the security and privacy challenges of Chinese domestic workers. Compared with general findings, tenants and domestic workers expressed higher concerns about security and privacy risks, which typically relate to three aspects: intimate spaces (e.g., avoiding bedroom recordings), social responsibility (e.g., not recording visitors or particular household members), and surveillance concerns (e.g., not wanting to feel constantly watched).

Online sources such as online reviews and social media can influence users' security perceptions and behavior Li et al. (2023), Vetrivel et al. (2023), Protick et al. (2024), Zhang-Kennedy et al. (2025). As stated by Li et al. (2023), "discourse in an online forum fulfills users' information and social needs despite their varied attitudes". In that study, they also identified different interactions in online communities (i.e., Reddit), e.g., users share strategies to resolve ambiguity issues related to security and privacy, and social interaction may contribute to the development of users' security attitudes. Also, these online resources allowed users to gain more knowledge of security threats and raise their awareness and concerns (Chalhoub et al., 2021; Turner et al., 2022a,b; Vetrivel et al., 2023; Protick et al., 2024). On the other hand, these studies also indicated the information gap in online platforms, e.g., users rarely "refer to reputable and understandable information sources" about the security and privacy of smart home devices when discussing the associated issues (Li et al., 2023; Protick et al., 2024).

7.6. Organizational factors

In this section, we will take a look at organizational factors that relate to practices in smart home companies, policy and regulators, and education, which also play a key role in maintaining smart home security.

7.6.1. Security design practice

Smart home companies should be responsible for providing user security support and managing resources to ensure effective security practices.

The security design employed by smart home companies, including device manufacturers, can impact user interaction experiences with regard to security, affecting user intentions to adopt the smart home device and their security perceptions and behaviors (Li et al., 2023; Philip et al., 2023). For example, smart home users tend to purchase devices that comply with security and privacy regulations and provide relevant security information (Li et al., 2023). Also, the design of security mechanisms can also influence users' security behavior; e.g., Abdi et al. (2019) showed that when a new security approach, such as voice authentication to prevent impersonation, is designed with greater usability, it encourages user adoption.

However, only two studies have explicitly investigated design practices in smart home companies. Blythe et al. (2019) investigated the information provided by manufacturers (including device manuals and support pages) for encouraging consumers to protect their devices and reduce their risk of cybercrime. They found that manufacturers provide limited security information (e.g., only 10 % of devices discussed security updates and 10 % provided security hygiene advice, placing the responsibility for device security on poorly informed consumers. Another study by Chalhoub et al. (2020) investigated UX designer practices in smart home companies, uncovering several UX challenges in security design, e.g., impractical regulations and conflicting priorities between security and UX teams. They also highlighted key incompatibilities, such as unclear team ownership of security features (e.g., the information security team or the design team), security design being a low priority, security being viewed as a purely technical issue, limited security expertise among design teams, and security considerations arising only during implementation. These observations suggest the need for further research to explore the relationship between UX and security and improve security communication within and outside companies.

7.6.2. Policy regulation

Policy regulations play a crucial role in ensuring companies adhere to best practices for securing smart homes.

Policy regulations can guide and ensure that manufacturers properly implement security and privacy measures. As suggested in the previous

sections, smart home users may perceive manufacturers to be responsible for following security practices to protect their data and security, but in practice this is not the case; some manufacturers may not know how to effectively implement security and privacy, as they might be new to developing smart device products (Haney et al., 2021). One of the challenges here is that there are no agreed-upon standards or guidelines regarding smart home privacy and security; manufacturers may sell their devices in a global market, and individual governments may have their own guidance or regulations for manufacturers (Haney et al., 2021). Although our corpus did not include studies that specifically examined security policy in smart homes, many studies offer recommendations and discuss smart home security issues with a focus on policy. For example, Philip et al. (2023) pointed out that security policies should "revisit access policies to include the possibility of the smart home network as another facet of the attack surface". Chalhoub et al. (2020) suggested that data protection legislation should explicitly address security user experience, as manufacturers have little incentive to invest extra effort into improving the UX of security. Several studies also highlight that policy should pay more attention to consumer protection and security information disclosure (Blythe et al., 2019; Turner et al., 2022b). These studies indicate that consumer policy requires greater research, as user behavior is also influenced by the policy and legislative environment (Patterson et al., 2021).

7.6.3. Security education

Security education is equally important for raising user awareness and equipping individuals with the knowledge to secure their homes.

In line with the low levels of security awareness and knowledge among smart home users discussed previously, studies suggested the critical role of education in enhancing security in smart homes. Haney et al. (2021) emphasized the need for consumer education to provide users with resources on smart home security and privacy and provide them with actionable tips during the configuration and use. Philip et al. (2023) and Douha et al. (2023) suggested that security awareness training should be given by organizations to employees working from home or citizens to protect smart homes. For family-focused studies, e.g. (Turner et al., 2022b), they indicated that neither adults nor children had an opportunity to learn about cybersecurity, suggesting the need to have appropriate ways to teach such information to either adults or children.

8. Findings on security approaches (RQ3)

In this section, we address RQ3, which examines what human-centered solutions are being designed to enhance smart home security, by focusing on existing security approaches studied from a human-centered perspective (N = 29). To assist smart home users in better securing their smart homes, prior research has explored five major categories of approaches: *Access Control*, *Authentication*, *Notification and Priming*, *Explanation*, and *Education*. These include efforts to improve the design of security mechanisms such as access control, and to develop security interventions like notifications or explanations that encourage users' security behavior. These investigations illustrate emerging directions for integrating human factors into security design and highlight opportunities for future research to design and improve these approaches in real-world contexts, ultimately fostering more usable and trustworthy smart home security systems. Below, we describe the design principles and specific methods for each category.

8.1. Access control

Smart homes are often occupied by multiple residents with complex social relationships and power dynamics (e.g., children, guests, roommates, and domestic workers) (Zeng and Roesner, 2019). Family members or guests might misuse their access to smart home devices or change their settings in harmful ways, posing security threats (Jang et al., 2017). Hence, it is necessary to design access control mechanisms that limit the actions or operations residents can perform, preventing activities that could compromise security (Yao et al., 2019). An access control rule typically determines whether access should be granted or denied to specific resources (e.g., data and services) based on criteria like user identity, role, or location. An access control policy refers to the complete set of access control rules. Since a smart home is managed by its users, access control mechanisms are typically provided to users to establish an access control policy. However, this could be a cognitively challenging task for some users who may have limited knowledge about access control rules. Also, in some circumstances, access control may not be necessary, for example, when residents trust each other enough not to be concerned about device misuse or when devices are placed in shared areas for communal use (Zeng and Roesner, 2019; He et al., 2018). Therefore, to better align with users' needs, studies have enhanced access control mechanisms to provide more user-friendly assistance. Below we will describe the general design principles and existing implementations of access control mechanisms.

8.1.1. Design principles

- *Transparency (TP)* . As smart home automation and applications may malfunction, engage in malicious behavior (Fernandes et al., 2016; Surbatovich et al., 2017), invade the privacy of unaware users, or cause confusion for those who have not configured properly (Zeng and Roesner, 2019), access control should **transparently display smart home activities** to relevant users.
- *Usability (UP)*. Access control should be **easy to configure**. Defining access control policies (Manandhar et al., 2020) and installing and using access control applications should require minimum effort (Zeng and Roesner, 2019).
- *Flexibility (FP)*. Access control should **accommodate various relationships** among residents, such as children, roommates, guests, couples, and domestic workers. It should also be configurable depending on **contextual factors** such as location, time of the day, and the device to be controlled (Zeng and Roesner, 2019; He et al., 2018).
- *Respectfulness (RP)*. Given the potential for tensions and conflicts among smart home users (Geeng and Roesner, 2019; Zeng and Roesner, 2019), access control solutions should **promote respectful usage** by minimizing sources of conflict, e.g., making it more difficult for one user to remotely control devices in a way that might surprise or disturb others.

8.1.2. Access control mechanisms

The design principles discussed in the previous section have guided the implementation of different access control mechanisms. The majority have more explicitly aimed to improve the *flexibility* (FP) and *usability* (UP) of access control by enabling users to configure access more effectively based on contextual factors such as their role, device, and time. For example, *role-based* access controls associate permissions with roles and assign users to appropriate roles, allowing the flexible management of social relationships among smart home tenants. For instance, tenants can be assigned roles like admin, guest, and child, with only admins having the ability to make changes such as modifying access control policies and adding new users (Zeng and Roesner, 2019). Parents can use this form of access control to prevent undesired use of devices by children, or device owners can prevent other tenants (e.g., family members) from changing device configuration, automation, and access control policies (Zeng and Roesner, 2019). Moreover, *device-based* access control manages access to specific devices differently from other devices because some may be security-critical or should only be accessed in particular situations (Zeng and Roesner, 2019). For example, voice assistants are usually given unrestricted access to smart home devices. This may allow a malicious user to bypass the access control rules that

apply to another specific device by sending a command through a voice assistant. Hence, remote access to voice assistants is typically restricted. Recently, He et al. (2018) suggested using *capabilities-based access control* instead of device-based control, as this approach may better match users' expectations, given that different capabilities (such as those of voice assistants and door locks) involve different levels of sensitivity. Furthermore, *time-based* access control can be used to grant guests access to devices or resources or for a limited amount of time (Zeng and Roesner, 2019), and *supervisory* access control allows a user to control a device only if another authorized user is nearby. This mechanism addresses the need for parental control, where children should be allowed to use smart home devices only when a parent is at home and able to supervise (Zeng and Roesner, 2019).

Some access control mechanisms have been designed with a stronger emphasis on *transparency* (TP) while simultaneously supporting other principles. For example, *reactive access control* allows users to request access to a device they do not have permission to use by seeking approval from a more privileged user in real-time (Mazurek et al., 2011). This access control transparently displays access requests to privileged users while also supporting flexibility and usability by avoiding static access control policies. Furthermore, *optimistic access control* allows users to gain the level of access they consider appropriate while ensuring adequate observability so that any inappropriate access can be detected by other household members (Malkin et al., 2023). Similarly to reactive access control, it prevents the user from manually configuring access control rules. The awareness that others may discover misuse, along with the potential consequences, could serve as a sufficient deterrent, discouraging users from exceeding their authorization without a good reason and encouraging mutual respect among users.

Another access control mechanism with more focus on *respectfulness* (RP) is *location-based* access control, which restricts users from controlling device capabilities unless they are physically near the device or at home. For example, the house owner may restrict access to physical areas or digital devices for visitors (e.g., guests and domestic workers) when they are not home (Zeng and Roesner, 2019). It can also prevent users from remotely controlling devices (e.g., lights) when other people are in the room.

8.2. Authentication

A critical initial step to access control is verifying users' identities through identification and authentication. The social relationships and power dynamics in households with multiple users sharing devices necessitate the implementation of authentication mechanisms, which enable users to seamlessly switch between profiles (Jang et al., 2017) while safeguarding the privacy of each family member (Yao et al., 2019).

8.2.1. Design principles

Besides the need for security (protecting against unauthorised users, such as those attempting imitation or brute force attacks) (Yu et al., 2022), multi-user authentication must adhere to usability and respectfulness principles to be adopted in practice.

- *Usability (UP).* Authentication should be **convenient for frequent use** (Yu et al., 2022; Zimmermann et al., 2025; He et al., 2018). If it is not effortless, users may become frustrated and choose to bypass authentication (Jang et al., 2017). Additionally, authentication must be fast (with low latency) (Yu et al., 2022) and lightweight (requiring minimal resources) (Yu et al., 2022).
- *Respectfulness (RP).* Authentication should **respect privacy**, avoiding exposure of private information (Jang et al., 2017).

8.2.2. Authentication methods

Prior research has shown that various methods are used for authentication in smart home devices. Similar to authentication in the broader security domain (Shah and Kanhere, 2019), these methods can be classified into three main categories according to the underlying factors of authentication, i.e., knowledge factor (something you know), inherence factor (something you are), and possession factor (something you have). For the knowledge factor, the typical method is the use of passwords and Personal Identification Numbers (PINs) (Jang et al., 2017). However, this mechanism requires users to create strong passwords to prevent exploitation by hackers. This makes it challenging for users to maintain a strong and unique password for each device. The second category, the inherence factor, generally leverages physical or behavioral biometrics. In some smart homes, a user can authenticate to a device with a camera, like a smart lock, through face recognition or custom hand gestures. Users can use hand gestures recognized by sensor signals collected by a smartwatch to authenticate and control commands to smart home devices. Even basic finger gestures, like the victory sign, can provide reliable identification results (Windl et al., 2022). Facial recognition offers hands-free access, while hand gestures enable quick authentication. Smart locks and doorbells can also use facial recognition to manage individual profiles for household members and grant guests access to the home during designated time periods (Jang et al., 2017). Also, a user can authenticate to a device recording their voice using a microphone. The device can identify the user with voice recognition algorithms or personalized voice commands, with the latter providing a quick, hands-free authentication method (Jang et al., 2017; Yao et al., 2019). Face and voice recognition technologies can be ideal for use on security-critical devices (Jang et al., 2017). However, voice recognition mechanisms can be fooled by voice recordings (Chen et al., 2020). The third category, the possession factor, requires some form of hardware (e.g., smartphone or wearable devices) to be possessed by the legitimate user. For instance, a user can authenticate to the smart home devices in their proximity using the Bluetooth signal of their smartphone or wearable device. This form of authentication is more usable and faster than those adopting biometric information (i.e. fingerprint, voice, and face) (Jang et al., 2017). To better align authentication with user needs and the home context, Zimmermann et al. (2025) recently proposed using everyday objects and routine household tasks (e.g., cleaning the kitchen) as part of the authentication process, exploring how authentication could be integrated into daily routine as a primary and effortless task.

8.3. Notification & priming

A notification is a message or alert that informs users about an event, update, or status change in the smart home. Notifications can serve as security interventions to improve transprency, increase awareness of security and privacy risks in smart home devices and empower users to make informed security decisions (Goffinet et al., 2021). Priming is a type of notification that subtly influences users by activating mental representations, which could stimulate user awareness and encourage secure behavior (Morgan et al., 2022). Priming can be explicit and intentionally draw attention to itself (e.g., highlighting words and phrases) or implicit and unobtrusive; both have been demonstrated to influence user behavior.

8.3.1. Design principles

- *Usability (UP).* To avoid overwhelming users, smart home notifications should be **minimally intrusive**. For example, users should be able to turn off notifications for individual devices or receive notifications only from nearby devices (Goffinet et al., 2021). Users should be able to filter notifications depending on certain criteria (e.g., the security risk level not exceeding a given threshold) (Collen et al., 2022). Also, notifications should be **easy to understand**.

8.3.2. Notification & priming methods

Notifications have been implemented differently, depending on their purpose. For instance, notifications displaying the status of nearby devices (Zeng and Roesner, 2019) have been implemented as persistent notifications in a mobile app, including action buttons to toggle the discovered devices. To reduce intrusiveness, these notifications are silent

and displayed at the bottom of the notification tray (Zeng and Roesner, 2019) (UP). Notifications providing information about the behavior of smart home devices display the device name, the state change, and the user or process responsible for causing the change (Zeng and Roesner, 2019). They allow users to identify undesired behaviors and configure access control rules (Zeng and Roesner, 2019).

Notifications providing information about security decisions made by a system (e.g., drop network packets in a specific flow, block a device) include a simplified description of the security interventions required and justify these interventions based on a decision tree workflow (Collen et al., 2022). Notifications that provide reports about the security and privacy vulnerabilities of the users' smart home appliances can convey the severity of a vulnerability using a traffic light metaphor to facilitate understanding (UP) (Windl et al., 2022); e.g., a green light means that no new vulnerability report or only reports older than one year are available, and a yellow light indicates that reports less than one-year-old are available. Since merely informing users about existing vulnerabilities may lead to frustration, notifications should also give specific recommendations on how to fix the vulnerabilities (UP) (Patil et al., 2015; Colnago et al., 2020).

Concerning priming, previous work (Morgan et al., 2022) has examined the effect of explicit and implicit priming in designing trigger-action-rules created to personalize the behavior of smart home devices. For example, a user may create a rule to trigger an action (e.g., "play a podcast") when a specific event (e.g., "When I turn off the alarm") happens. In this study (Morgan et al., 2022), explicit primes show users the importance of maximizing security and privacy in their homes (e.g., to prevent burglaries and protect personal details from outsiders). Implicit primes prompt users to consider home security and privacy by asking them to identify which house is more vulnerable to burglary based on characteristics, e.g., location and garden presence. Prompting users to prioritize security using both explicit and implicit priming results in a noticeable reduction in the number of rules they enable, indicating increased cognitive control over their decisions (Morgan et al., 2022).

8.4. Explanation

Previous work has also considered providing explanations about security and privacy risks in the smart home (Bahrini et al., 2020a; Duezguen et al., 2021) to support users in identifying cyber-attacks and taking actions to secure the smart home (Plachkinova and Menard, 2022; Vasalou et al., 2025).

8.4.1. Design principles

- *Transparency (TP)*. Explanations should promote transparency by addressing biases and misconceptions. For instance, explanations about security and privacy risks in smart homes should reduce misconceptions about manufacturers (Duezguen et al., 2021). Although some users recognize manufacturers as potential adversaries, they may still trust them and believe their security measures are sufficient (Zeng et al., 2017). These misconceptions may lead users to avoid taking protective measures in smart homes.
- *Usability (UP)*. To effectively raise risk awareness and motivate users to secure their smart home, explanations should be **clear and accessible to a wide audience**. For instance, they should break down complex security concepts using simple language (Duezguen et al., 2021) and use visuals or other indicators that are **easy to understand** (Vasalou et al., 2025).

8.4.2. Explanation method

When designing explanations about security and privacy risks, the main aspects considered are the explanation content and its style. Previous work (Duezguen et al., 2021) has designed explanations including those which aim to reduce user misconceptions regarding manufacturers, risks and their consequences. Explanations included smart home device manufacturers' motivation for potential data leaks, and shortcuts they take to protect their users (Duezguen et al., 2021) (TP). To raise risk awareness and motivate smart home users to protect themselves, explanations also included both abstract risks and specific negative consequences. To reach a broader audience, explanations of security risks typically cover a wide range of use cases, such as physical, social, psychological, legal, career, and freedom-related consequences. Note that people tend to better understand common risks and those related to the physical world (e.g., burglaries), viewing them as more dangerous (Garg and Camp, 2012), which encourages users to relate to potential victims and take action.

Concerning the explanation style, previous work has considered the use of infographics (e.g., recognizable comics and images) to help smart home owners become familiar with security issues and risks (Bahrini et al., 2020a), or leveraged multimodal indicators (combining visual and textual cues) integrated into AI-enabled deviced to raise awareness of cyber-attacks. Such visual approaches to communicating security information have been shown to better capture users' attention, and increase their interest, enjoyment and perceived competence (UP). Also, message framing (gain- and loss-framed) techniques have been explored to appeal to an audience with different pre-existing security concerns (Plachkinova and Menard, 2022). Gain-framed explanations feature language emphasizing positive outcomes from the performance of security interventions, while loss-framed explanations focus on negative outcomes resulting from the failure to perform security interventions. Loss-framed explanations were more effective for users with lower pre-existing smart home security concerns, while gain-framed explanations worked better for those with higher pre-existing concerns.

8.5. Education

Our corpus reveals a lack of studies dedicated to designing education and training programs specifically for smart home users (Sharevski et al., 2018; Bailey et al., 2023; Jois et al., 2024). The educational approaches discussed below have mainly used Internet of Things (IoT) devices commonly found in smart homes to explain security concepts for educational purposes. The design principles align with general educational principles (e.g., increase engagement, tailor to students' needs, and foster student collaboration).

Previous work has presented two educational examples: the Secure Design course and the GenCyber FACS Summer Camp, both of which applied their programs to smart home IoT products. The Secure Design course is an undergraduate, interdisciplinary course in cybersecurity and interaction design (Sharevski et al., 2018). It integrates disciplines to equip future professionals with the ability to address security challenges in product design. The course also extends cybersecurity awareness to students designing IoT smart home products, interfaces, and communication materials, empowering users to understand and adopt cybersecurity protocols as essential parts of their daily tasks. Regarding GenCyber FACS Summer Camp (Bailey et al., 2023), it aims to involve females (e.g., African American women) in the field of cybersecurity. Students engaged in group activities, exploring smart home use cases to demonstrate their understanding by exploiting and defending home automation devices.

9. Discussion and future directions

In this scoping review, we outline four main human-centered challenges in ensuring the security of smart homes in the conceptual framework presented in Section 6.1, with a detailed synthesis of insights of six contributing human factors that relate to smart home security. We also summarize four general principles for security design and provide an overview of existing security approaches from a human-centered perspective. Based on the provided conceptual framework and the synthesised findings, we identified two major directions that require further investigation to ensure smart home security: (1) *improving security understanding and awareness*; and (2) *designing user-centered security mech-*

anisms for smart homes. In addition, for this interdisciplinary research area, *broadening the range of research methodologies used*, e.g., participatory design, may help tackle the human-centered security challenges in smart homes. We discuss these directions below to inform and guide researchers and practitioners in their future work.

9.1. Improving security understanding and awareness

Ensuring the security of smart homes is intuitively a shared responsibility among multiple stakeholders; however, the distribution of responsibility for security is often ambiguous (Haney et al., 2021). As discussed in the results of human factors in Section 7, many smart home users possess limited security knowledge related to smart homes (Zeng et al., 2017; Abdi et al., 2019; Tabassum et al., 2019). This lack of understanding often leads to varied attitudes toward security and different perceptions of responsibility (Haney et al., 2021; Li et al., 2023). Additionally, various factors, e.g., environmental and organizational factors, can affect the implementation of security practices (Nurgalieva et al., 2023). For instance, manufacturers and their employees (e.g., product design teams) ask for clear guidance about security information disclosure and implementation of security features (Chalhoub et al., 2020; Blythe et al., 2019; Haney et al., 2021). For sustainable security in the future (Pasquale et al., 2024), it is essential to enhance the security understanding of all key stakeholders and encourage them to take informed actions in securing their smart homes. For users to take informed responsibility for securing their smart homes, they need to be provided with clear and accessible security information and supported by usable security features and appropriate educational resources (Philip et al., 2023). For manufacturers to implement effective security practices, clear guidance and well-defined user expectations should be articulated and communicated before the design process begins. Drawing on the synthesized findings from this scoping review, we propose practical directions for future research below.

9.1.1. Transparent security communication

Smart home devices often have security vulnerabilities (Hammi et al., 2022), but manufacturers rarely disclose information concerning the security vulnerabilities in the devices they produce and their management of security and privacy (Zeng and Roesner, 2019; Yao et al., 2019; Blythe et al., 2019). Better security information disclosure may encourage users to adopt more risk-averse security behaviors. For instance, user manuals or informed consents can clearly communicate the types of user data that individual smart home devices, as well as the overall smart home system, collect, infer, share, and use. To further raise users' awareness of security threats and promote the adoption of protective measures, innovative approaches to communicating security risks (such as contextual notifications and explanations (Goffinet et al., 2021; Windl et al., 2022; Vasalou et al., 2025)) could be further explored to improve users' understanding of security controls and interventions, and motivate their security behaviours. In addition, online review forums present valuable venues for sharing security-related information (Protick et al., 2024; Vetrivel et al., 2023; Li et al., 2023), where security risks and potential solutions can be highlighted or matched to specific device issues, enabling both experienced and novice users to stay informed and make more secure choices. For these communications, manufacturers and online platforms should verify the accuracy of the information they communicate, as misleading details about security risks might create a false sense of security for smart home users (Windl et al., 2022).

9.1.2. Policy guidance

Currently, there is limited guidance on the required level of security or the duration for which smart home devices should maintain security after they are produced. Government and regulatory policymakers have a crucial role to play in ensuring that manufacturers maintain satisfactory security standards throughout the product lifecycle, including post-production (Haney et al., 2021; Blythe et al., 2019; Chalhoub et al., 2020). Although security and privacy laws exist, such as the NIS2 directive and the GDPR, they are framed at a high level and do not provide actionable and concrete guidance to smart home manufacturers (Yao et al., 2019; Chalhoub et al., 2020). Therefore, clear guidelines should be established for integrating robust security and privacy features, as well as preventing vulnerabilities and risky security behaviors. Some of the reviewed studies also emphasise that policy should place greater focus on consumer protection and the disclosure of security information (Blythe et al., 2019; Turner et al., 2022b). Another key aspect that policies and regulations should address is the responsibility and liability of device manufacturers regarding security breaches in smart homes. This includes establishing clear and well-defined security responsibilities for both manufacturers and users (Yao et al., 2019; Blythe et al., 2019; Patterson et al., 2021). Given the limited attention to regulators' perspectives in existing research, future studies should address the gap by engaging with regulators to understand their roles and challenges, and explore how policies can better align with user needs and industry practices, e.g. through interviews, focus groups, or participatory design workshops. Also, given the complexity of regulations and in line with recent research on developer-centered security (Tahaei and Vaniea, 2019), further exploration of tools to assist designers and developers in security design for smart homes would be beneficial.

9.1.3. Security education and training

Our review also indicates that smart homes represent a practical case study for several cybersecurity training and education programs (Sharevski et al., 2018; Bailey et al., 2023). However, there is a lack of specialized education and training for smart home users. Unlike workplaces, many homes lack people with the necessary skills to manage smart home networks and devices securely (Philip et al., 2023). Also, in the home environment, people of all ages, including children and older adults with relatively low digital literacy, interact with smart home devices. As smart home devices become more widespread and security threats constantly evolve, it is desirable to provide consumer education on smart home security and privacy, along with actionable tips for configuration and use (Turner et al., 2022b). Similar to cybersecurity training offered in organisational settings to ensure employees follow secure practices (Prümmer et al., 2024), future research may explore how to embed consumer-oriented education at home to help users develop the knowledge to manage and protect their smart home environments effectively.

9.2. Designing user-Centered security mechanisms for smart homes

Another key research direction is to design mechanisms that allow users to manage their smart home devices, understand security risks, and mitigate them effectively (Haney et al., 2021; Zeng and Roesner, 2019). As discussed in user perception and user behavior in Section 7, in current practices, smart home users often adopt non-technical strategies or experience fatigue with security mechanisms (Zeng et al., 2017). Their behavior may be impacted by personal, social, or contextual factors. To better support users in adopting security mechanisms, previous research has explored user-centred approaches to access control and authentication (see Section 8). However, the intricate nature of the smart home environment requires more user-centered research to identify effective ways to support users in securing their smart homes when action by the user is required. This research may consider reducing the cognitive load on users and fostering greater user intention to secure their homes. Below, we highlight three areas that are worth further investigation.

9.2.1. Personalized security mechanisms

Considering that personal factors (e.g., age, gender, personal background) may affect users' device usage and their security perception and behavior (as shown in Section 7.5), it is beneficial to consider critical factors when designing security mechanisms, as this might help minimize the effort required from users to adopt them. For instance, when

a device is used by an older adult for health monitoring, it may be appropriate to inquire whether they consent to their children accessing private data, as this is likely a common scenario. To achieve personalization, it can be useful to identify the key factors that can influence security behavior within a smart home and then use these insights to create *smart home security personas* (McDermott et al., 2019). Such security personas can be helpful for designing personalized user interfaces tailored to the specific needs of each persona. For example, access control or notifications about device information and security threats could be customized based on a user's technical proficiency and device ownership (Goffinet et al., 2021). Moreover, we can predict security risks specific to each persona, based on which we can implement targeted measures to strategically support users who are more likely to engage in insecure behaviors in their homes.

9.2.2. Protecting users in smart homes

The complexity of the home environment, with its multiple users and diverse roles, leads to varied user behaviors that can impact security and privacy (see discussion about contextual factors in Section 7.4 and social factors in Section 7.5). Previous studies, e.g., (Chidziwisano and Jalakasi, 2023; Leitão, 2019), also suggest that smart homes might exacerbate or facilitate harm in adversarial living situations, such as households experiencing domestic abuse or in rental arrangements. For example, a malicious administrator could misuse their privileges to prevent victims from controlling the home or bypass safeguards against remote harassment. Addressing this issue is complex, as many security features serve dual purposes. A key challenge for future design is to develop smart home access controls and monitoring systems that safeguard users from abuse while also supporting legitimate and benign use cases (Zeng and Roesner, 2019). For example, Xiao et al. (2023) used a digital twin to reason about possible malicious behaviors that existing access control policies can enable in a smart home. For multi-user security and privacy issues, leveraging social norms in the design of security interventions can be helpful (Zeng and Roesner, 2019). Encouraging positive norms could help minimize friction in typically cooperative households, where conflicts and tension may stem from a lack of understanding about how actions impact others. Therefore, designing "nudges" that encourage positive behaviours by smart home users may be beneficial. Nudges can be displayed when a user's action violates a social norm, prompting them to reconsider before disturbing others.

9.2.3. AI For security support

To tackle the complex challenges in smart home security, an *AI security assistant* may provide an adaptable approach for smart home users to manage the security in their homes. It can be designed with AI (e.g., machine learning techniques) to understand the context of user actions and adjust security mechanisms accordingly (Yao et al., 2019). For instance, integrating device and people detection with automated risk assessment can help identify scenarios that require activating security mechanisms and notifying users if necessary, e.g., disabling voice recording during private conversations or triggering notifications when a recording device (such as a smart toy) is co-located in the same space as the relevant user. Also, an AI assistant could offer personalized, real-time security adjustments based on contextual factors like time of day and device usage. It could also send security notifications or explanations (e.g., updating firmware, changing passwords) (Prange et al., 2022; Vasalou et al., 2025) at appropriate times and tailor them to users' technical proficiency, fostering secure behavior, or even providing proactive threat detection. By learning from user behavior and continuously improving, the assistant may reduce users' cognitive load, encourage secure practices, and ensure that security is maintained without overwhelming users (Malkin et al., 2023; Abdi et al., 2019). This could be a promising solution to help users manage smart home security. Future efforts could explore smart home users' perspectives, examine potential security implications, and investigate the appropriate design of such an AI security assistant.

9.3. Broadening the range of research methodologies and populations

This scoping review reveals that the majority of understanding-oriented studies focus on understanding user perceptions and behavior mainly through surveys and interviews (see Section 5.2). Only a few authors have conducted field studies or ethnographic studies to explore users' lived experiences (Huijts et al., 2023; Chalhoub et al., 2021). Further research can examine the lived experiences of smart home users regarding security, providing valuable insights and validating design approaches. Regarding design-oriented studies, they typically follow user-centered approaches to design a specific security mechanism based on the identified user needs (Zeng and Roesner, 2019; Malkin et al., 2023). A recent study engaged smart home users in focus group workshops to co-design authentication mechanisms (Zimmermann et al., 2025), providing a practical example of how a participatory approach can help develop usable security solutions that better align with users' expectations. Moreover, ensuring smart home security requires active collaboration among multiple stakeholders; in addition to smart home users, other stakeholders, such as companies (including security experts and designers) and regulators, may have varying priorities and concerns, so it is also interesting to understand their perspectives and see how different values, such as usability, feasibility, autonomy, security, privacy, and safety, could be considered in the design process. This is essential, not only for developing security mechanisms but also for improving security communication, shaping policies, and designing effective security education and training programs. Participatory design approaches and value-oriented frameworks may facilitate the exploration of diverse perspectives and values, and help design smart home devices that better align with all stakeholders' interests (Sanders, 2002).

The review also highlights a predominant focus on western populations (see Section 5.1), with only a few recent studies considering more diverse user groups (Almutairi and Almarhabi, 2021; Patterson et al., 2021; He et al., 2025; Sasaki et al., 2025). Given that security perceptions and practices can vary across cultural contexts and social norms (He et al., 2025; Kulyk et al., 2020), current research may limit the diversity of perspectives represented. To address this, future work could employ more inclusive and cross-cultural approaches, such as cross-cultural comparative studies and participatory engagement with underrepresented groups (e.g., (He et al., 2025; Chidziwisano and Jalakasi, 2023)) to gain a deeper understanding of diverse cultural contexts. These efforts would help develop a more comprehensive understanding of users' experiences and insights into smart home security.

10. Conclusion

Smart home technology brings both convenience and security challenges due to its constant connectivity and data collection. While past research has largely focused on technical solutions to security, this review has highlighted the importance of considering human and social factors in ensuring smart home security. By synthesizing existing human-centered research, this review mapped the landscape of current studies, including their aims, methodologies, and insights into human factors and security approaches. We also presented a conceptual framework for human-centered security in smart home research, identifying key challenges and design principles and emphasizing the need for designing and supporting smart home security from a human-centered perspective. As the adoption of smart home technologies continues to grow, addressing these human and social factors will be essential for maintaining sustainable security in smart homes. We believe this review will be helpful for future studies that explore smart home security.

CRediT authorship contribution statement

Wanling Cai: Writing – review & editing, Writing – original draft, Visualization, Validation, Project administration, Methodology, Investigation, Formal analysis, Data curation, Conceptualization; **Liliana**

Pasquale: Writing – review & editing, Writing – original draft, Validation, Methodology, Investigation, Funding acquisition, Formal analysis, Data curation, Conceptualization; **Kushal Ramkumar:** Writing – review & editing, Validation, Methodology, Investigation, Formal analysis, Data curation; **John McCarthy:** Writing – review & editing, Supervision, Methodology, Conceptualization, Funding acquisition; **Bashar Nuseibeh:** Writing – review & editing, Supervision, Methodology, Funding acquisition, Conceptualization; **Gavin Doherty:** Writing – review & editing, Supervision, Methodology, Funding acquisition, Conceptualization, Investigation.

Data availability

No data was used for the research described in the article.

Declaration of competing interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests:

Wanling Cai reports financial support was provided by Lero, the Science Foundation Ireland Research Centre for Software. If there are other authors, they declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

This work was supported with the financial support of the Science Foundation Ireland grant 13/RC/2094_P2 and co-funded under the European Regional Development Fund through the Southern & Eastern Regional Operational Programme to Lero - the Science Foundation Ireland Research Centre for Software.

Appendix A. Detailed Methodology for Our Scoping Review

Our scoping review was guided by the framework proposed by Arksey and O'Malley (Arksey and O'Malley, 2005), and the PRISMA extension for scoping reviews (PRISMA-ScR) checklist and explanations (Tricco et al., 2018).

A.1. Protocol design and development

To develop our scoping review protocol, we performed preliminary searches in the ACM Digital Library to evaluate the feasibility of the review based on various eligibility criteria. Moreover, to ensure thorough charting of key information from the literature, the first author piloted a data charting procedure by extracting data from 7 papers. The protocol for this review was developed iteratively through individual and group meetings involving all authors. We pre-registered the protocol with the Open Science Framework on October 18, 2023 (Cai et al., 2023).

A.2. Search and screening

In this review, we conducted our search in two rounds: the first on October 27, 2023, and the second on July 3, 2025, with a further update on September 11, 2025, thereby including literature up to that date.

A.2.1. Eligibility criteria

Studies were assessed against a set of eligibility criteria, comprising inclusion criteria (IC) and exclusion criteria (EC) described as follows:

IC 1 Include studies that are explicitly concerned with human-related issues in smart homes;

IC 2 Include studies that focus on human-centric approaches to smart home security:

- Are concerned to some extent with the understanding of human factors (including knowledge, attitude, preference, concerns, expectations, and needs regarding security) in smart homes;
- Present security solutions or approaches for smart homes in which they consider human aspects;
- Describe user evaluations (e.g., user studies) of security approaches in smart homes.

EC 1 Exclude studies in which the security aspect was marginal (e.g., studies focusing primarily on user adoption of smart home technologies or exclusively on privacy issues), as this review emphasises security-specific investigations;

EC 2 Exclude studies that solely addressed technological security solutions or conducted purely technical security analyses;

EC 3 Exclude studies conducted in other contexts (e.g., general home computing environments, smart cities, or office settings) if they did not explicitly focus on smart homes;

EC 4 Exclude literature reviews, books, book chapters, and theses;

EC 5 Exclude studies not published as full, peer-reviewed papers;

EC 6 Exclude papers that are not written in English;

EC 7 Exclude papers that are not accessible.

A.2.2. Information sources & search terms

The review sources included the three databases: ACM Guide to Computing Literature, IEEE Xplore Digital Library, and Scopus. Targeting IC 1 and 2, we searched the three databases for items that include the following search terms in either the title or the abstract:

- **Search Terms 1 [Smart Home]**

```
(Home AND (Smart OR Connected OR Network* OR
 Comput* OR IoT OR Device)) AND
```

- **Search Terms 2 [Security]**

```
(Secur* OR Cybersecurity) AND
```

- **Search Terms 3 [Human-related]**

```
((User OR Human OR People OR Person) AND
(Cent* OR Factor OR Experience OR Perception OR
 Feeling OR Sense OR Attitude OR
 Knowledge OR Awareness OR Concern
 OR Vulnerab* OR Behavi*))
```

The above search terms were adapted from search terms used for a recent review of user perspectives on security and privacy in home networking environments (Pattnaik et al., 2023). We used the asterisk (*) in several terms (e.g., Network*, Secur*) to specify a number of unknown characters, e.g., the term seucr* will match terms including 'secure' and 'securing' in addition to 'security'. During the second round search, we also carried out a separate search in the USENIX database, since not all papers published in USENIX Security Proceedings – though expected to appear in the ACM Guide to Computer Literature – were fully indexed there. Targeting EC 4 and 6, search results were then filtered to exclude papers that are not written in English, books, book chapters, and theses, using the built-in functions provided by the three databases. The references of the search results (N = 4332) were exported as BIB files. We computationally parsed them into RIS files, which were then imported into Covidence[2] (i.e., a software designed to organise and streamline literature reviews while supporting collaboration) for screening. After removing 1227 duplicates detected by Covidence, the remaining articles (N = 3105) proceeded for screening.

A.2.3. Screening & selection process

We followed a two-step process to screen the remaining articles: (1) Title and Abstract Screening: The first and second authors independently

[2] https://www.covidence.org/.

reviewed the titles and abstracts to screen papers according to the eligibility criteria. There was 94 % agreement for this screening in the first round. A total of 196 conflicts were then resolved by consensus and discussion between the two authors. Disagreements typically centered on whether the paper was related to security (instead of solely focusing on privacy, health, or safety) and whether it constituted adequate human-centered research. The title and abstract screening resulted in 2852 excluded papers, 20 duplicates, and 233 papers for full-text review. In the second round, the title and abstract screening tasks were split between the first and second authors, which resulted in 959 excluded papers, 10 duplicates, and 89 papers for full-text review. (2) Full-text Screening: The first author then retrieved the full text of the eligible papers, and both the first and second authors independently reviewed them based on exclusion criteria (EC 1–5). There was 76 % agreement in the full review. Conflicts identified during screening (57 in the first round and 22 in the second) were discussed in group meetings and resolved via discussion among the two reviewers. Across both rounds, the full-text review process resulted in the exclusion of 220 papers. Specifically, we excluded 82 papers that only briefly mention the security aspects without further engaging with the topic (e.g., papers mainly focusing on users)" intention to adopt smart home technology and users' perspective on home automation; 48 papers that are purely technology solutions or analyses without considering human aspects; 35 papers that addressed general home computers or personal computers rather than smart homes; 25 papers that focused on IoT devices in general contexts (e.g., smart cities) instead of IoT devices in a smart home environment; 21 papers that are research proposals rather than full papers; 7 review articles; and 2 papers that are not written in English.

A.3. Data charting

For our scoping review, we extracted relevant data from the reviewed papers regarding the three main aspects:

- Research Methods
  - Research study design (e.g., qualitative or quantitative research)
  - Concrete research methods (e.g., interview, survey, laboratory experiment)
  - A short description of research methodology
  - Research theories applied (if any)
  - Evaluation approaches (if any)
- Human Factors
  - Stakeholders considered in the study (e.g., primary users, designers)
  - Characterisation of human factors investigated (e.g., user perception, user behavior, contextual factors)
  - A short description of human factors investigated
- Security Solutions
  - Design objectives (e.g., motivate users to take action, sustain user engagement)
  - Security features/mechanism (e.g., authentication, security update)
  - Human-centric approach (e.g., usability testing)
  - Human factors considered in the security design
  - Design principles / rationales

To better map the literature, we also extracted general information about the papers (including title, authors, publication venues and years, locations of research institutes, expertise of research teams), research motivations and aims (including their research questions if they are explicitly mentioned), key findings and contributions, and design implications from the reviewed papers. The charting factors, including categorical data and text snippets, were detailed in our scoping review protocol (Cai et al., 2023). It should be noted that our data charting is to code the explicit content in the paper, avoiding inferences or interpretations of the charted data. We used Covidence to build and perform data extraction forms in the charting process. The corpus was distributed among authors 1–3 for data charting. To ensure consistency, an initial subset of 9 papers was first extracted. Each author extracted data from 6 papers out of the initial subset, with every paper being reviewed by two authors. Each pair of authors extracted 3 papers in common. Then, all three authors compared the extracted data from the initial subset and discussed discrepancies and the level of detail for each charting factor. After reaching a consensus, the remaining papers for data charting were distributed among the three authors.

A.4. Data analysis

We converted categorical data and short text snippets into binary or nominal categories for descriptive analysis. For unconstrained text snippets (mainly for human factors and security solutions), we performed qualitative analyses, including reflexive thematic analysis and content analysis, to inductively identify concepts, categories, or themes from the extracted data. To be more specific, we performed a descriptive analysis of publication and author details to provide an overview of the corpus (see Section 5.1). The first three authors conducted a qualitative content analysis to categorise the literature according to research motivations, aims, research questions, and methodologies, offering an overall picture of existing studies (see Section 5.2). The first author conducted a reflexive thematic analysis to uncover key concepts and themes concerning human factors using data from the included studies that are understanding-oriented (see Section 7). For included studies that are more design-oriented, the second and third authors performed a qualitative content analysis to categorise them based on the focused security approach and design principles (see Section 8).

A.5. Positionality statement

Our interdisciplinary team brings together expertise from the fields of human-computer interaction, cybersecurity, software engineering, and psychology. We are currently working on a "sustainable adaptive security" project, and we incorporate a sustainability perspective into our discussions in this scoping review. We are convinced that human and social aspects are crucial in ensuring security within technological contexts such as smart home environments. Understanding and considering these aspects will provide a sustainable way to maintain security in future smart homes with an increasing number of connected devices. During the review process, two authors with HCI and cybersecurity backgrounds screened and selected articles to mitigate bias based on our backgrounds. Three authors of diverse genders and HCI and security backgrounds worked together to chart data from the included literature and perform data analysis, allowing us to consider different perspectives. All team members engaged in collective discussions to review and revise the scoping review.

Appendix B. Additional Detailed Results of Our Scoping Review

B.1. Publication venues and years

In our corpus, the included papers span from 2011 to September 2025, with the majority published after 2019. This distribution highlights a growing focus on human-centered research in smart home security in the last seven years.

The papers in our corpus were published in various venues focusing on human-computer interaction, computer security, or the broader field of computer science. The most common publication venues were ACM SIGCHI Conference on Human Factors in Computing Systems (CHI) (N = 12, (Brush et al., 2011; Chalhoub et al., 2021; Borgert et al., 2023; Turner et al., 2022a; Fruchter and Liccardi, 2018; Neilly et al., 2022; Yao et al., 2019; Huang et al., 2020; Lafontaine et al., 2021; He et al., 2025; Ye et al., 2025; Zhang-Kennedy et al., 2025)), Symposium on Usable Privacy and Security (SOUPS) (N = 9, (Chalhoub et al., 2020; Abrokwa et al., 2021; Abdi et al., 2019; Zeng et al., 2017; Ponticello et al., 2021;

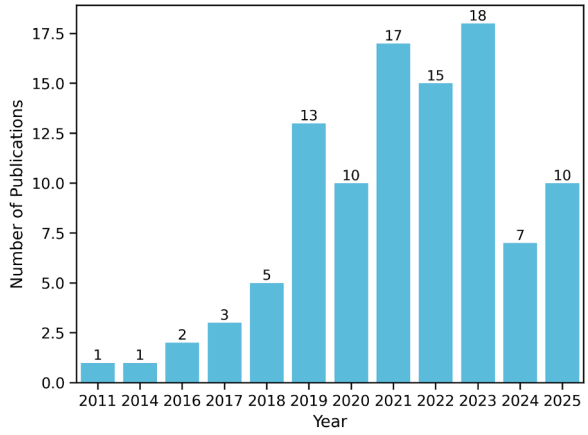

Fig. B.3. Distribution of papers by year of publication.

Tabassum et al., 2019; Barbosa et al., 2020; Hazazi and Shehab, 2023; McCall et al., 2023)), USENIX Security Symposium (N = 5, (Haney et al., 2021; Zeng and Roesner, 2019; Vetrivel et al., 2023; He et al., 2018; Sasaki et al., 2025)), ACM SIGCHI Conference on Computer-Supported Cooperative Work & Social Computing (CSCW) (N = 4, (Turner et al., 2022b; Seymour and Such, 2023; Sun et al., 2021; Pattnaik et al., 2024)), IEEE Symposium on Security and Privacy (IEEE S&P) (N = 4, (Malkin et al., 2023; Li et al., 2023; Haney and Furman, 2023b; Manandhar et al., 2020)). Notably, other publication venues that emphasized interdisciplinary approaches to security include: International Conference on Human-Computer Interaction (HCII) - HCI for Cybersecurity, Privacy and Trust (N = 4, (Alam et al., 2021; Haney and Furman, 2023a; Haney et al., 2020, 2025)), International Conference on Human Aspects of Information Security, Privacy, and Trust (N = 2, (Nurse et al., 2016; Feth et al., 2017)); European Workshop on Usable Security (N = 2, (Shere et al., 2020; Hazazi and Shehab, 2024)); other HCI publication venues include but not limited to: ACM Conference on Designing Interactive Systems (N = 3, (Benton et al., 2023; Chidziwisano and Jalakasi, 2023; Leitão, 2019)), Computers in Human Behavior (N = 1, (Philip et al., 2023)), and International Journal of Human - Computer Studies (IJHCS) (N = 1, (Morgan et al., 2022)); other top-tier computer security venues included Computer & Security (N = 3, (Hodges, 2021; Klobas et al., 2019; Vasalou et al., 2025)), and ACMConference on Computer and Communications Security (CCS) (N = 1, (Jia et al., 2021)).

Table B.3
Distribution of Papers by Research Institution Countries.

Country	#Paper
USA	40
UK	25
Germany	16
Canada	5
Netherlands	5
China	3
Sweden	3
Switzerland	3
Belgium	2
Romania	2
Saudi Arabia	2
Spain	2
Janpan	2
Australia	1
Austria	1
Denmark	1
Finland	1
France	1
Iran	1
Italy	1
New Zealand	1
South Korea	1
The United Arab Emirates (UAE)	1

B.2. Distribution of review papers by research institution countries

To understand the global research landscape on human-centric smart home security, we analysed the distribution of the included review papers according to the countries of the authors' affiliated research institutions (see Table B.3). Each paper was assigned to one or multiple countries based on the affiliations of all authors.

B.3. A Summary Table of papers based on addressed human factor dimensions

A summary table below is provided to present the review papers that address different human factor dimensions.

Table B.4
Summary of Papers Based on Addressed Human Factor Dimensions.

References	# Papers	Cognition & Perception	Behavior	Personal & Social	Contextual	Organizational
(Ponticello et al., 2021; Benton et al., 2023; Neilly et al., 2022; Huang et al., 2020; Hazazi and Shehab, 2023; Haney et al., 2025; Hazazi and Shehab, 2024; Wang et al., 2025)	8	●	●	-	●	-
(Fruchter and Liccardi, 2018; Barbosa et al., 2020; George et al., 2021; Seymour et al., 2022; Haney and Furman, 2023a; Keleher et al., 2024)	6	●	-	-	-	-
(Breve et al., 2023; Chidziwisano and Jalakasi, 2023; Shuhaiber et al., 2023; Park et al., 2018; Protick et al., 2024)	5	●	-	●		-
(Zimmermann et al., 2018; Philip et al., 2023; Klobas et al., 2019; Taieb and Pelet, 2019; Seymour and Such, 2023)	5	●	-	○	-	-
(Turner et al., 2022a; Tabassum et al., 2019; Pospisil et al., 2022)	3	●	●	○	-	-
(Huijts et al., 2023; Alam et al., 2021; Haney et al., 2020)	3	●	●	-	○	-
(Almutairi and Almarhabi, 2021; Peterson and Mujeye, 2025; Sasaki et al., 2025)	3	●	●	-	-	-
(Brush et al., 2011; Prange et al., 2021; Patterson et al., 2021)	3	●	-	-	○	-
(Chalhoub et al., 2020; Blythe et al., 2019; Mare et al., 2019)	3	-	-	-	-	●
(Shere et al., 2020; Vetrivel et al., 2023)	2	●	●	●	-	◐
(Zeng et al., 2017; Ye et al., 2025)	2	●	●	◐	◐	-
(Li et al., 2023; Pattnaik et al., 2024)	2	●	◐	●	●	-
(Leitão, 2019; Zhang-Kennedy et al., 2025)	2	●	-	●	◐	-
(Kulyk et al., 2020; Lafontaine et al., 2021)	2	●	-	●	○	-
(Maiorescu et al., 2021; Schuster and Habibipour, 2024)	2	●	-	◐	-	-
(Sun et al., 2021)	1	●	●	◐	○	
(Turner et al., 2022b)	1	●	●	◐	-	◐
(Abdi et al., 2019)	1	●	●	○	●	○
(Chalhoub et al., 2021)	1	●	●	○	◐	-
(Löbner et al., 2024)	1	●	●	-	-	◐
(McDermott et al., 2019)	1	●	◐	○	-	-
(Haney and Furman, 2023b)	1	●	◐	-	○	-
(Haney et al., 2021)	1	●	◐	-	-	●
(Chhetri and Motti, 2019)	1	●	◐	-	-	-
(He et al., 2025)	1	●	○	●	●	◐
(McCarthy et al., 2020)	1	●	○	-	●	-
(He et al., 2019)	1	●	○	-	○	-
(Douha et al., 2023)	1	●	-	●	-	◐
(Abrokwa et al., 2021)	1	●	-	◐	-	●
(Mols et al., 2022)	1	●	-	○	●	-
(Fayoumi et al., 2022)	1	●	-	-	◐	-

We illustrated the inclusion of this complexity in the reviewed papers using the following specific graphic symbols:
● (substantial coverage) - representing that the paper has a primary focus on this human factor dimension;
◐ (partial coverage) - indicating that the paper devotes some sections to discussing the dimension;
○ (light touch) - indicating that the dimension is only briefly mentioned in the paper.

References

Abdi, N., Ramokapane, K.M., Such, J.M., 2019. More than smart speakers: security and privacy perceptions of smart home personal assistants. In: Fifteenth USENIX Conference on Usable Privacy and Security (SOUPS'19), p. 451–466.

Abrokwa, D., Das, S., Akgul, O., Mazurek, M.L., 2021. Comparing security and privacy attitudes among {US}. users of different smartphone and {Smart-Speaker} platforms. In: Seventeenth Symposium on Usable Privacy and Security (SOUPS'21), pp. 139–158.

Adams, A., Sasse, M.A., 1999. Users are not the enemy. Commun. ACM 42 (12), 40–46.

Alam, A., Molyneaux, H., Stobert, E., 2021. Authentication management of home iot devices. In: International Conference on Human-Computer Interaction. Springer, pp. 3–21.

Aldrich, F.K., 2003. Smart homes: past, present and future. In: Inside the Smart Home. Springer, pp. 17–39.

Alghamdi, S., Furnell, S., 2023. Assessing security and privacy insights for smart home users. In: International Conference on Information Systems Security and Privacy (ICISSP 2023), pp. 592–599.

Almutairi, O., Almarhabi, K., 2021. Investigation of smart home security and privacy: consumer perception in saudi arabia. Int. J. Adv. Comput. Sci. Appl. 12 (4).

Alsufyani, A.A., Rana, O., Perera, C., 2025. Enabling collaborative anomaly exploration in smart homes: eliciting user requirements and security scenarios. Proc. ACM on Interact., Mobile, Wearable Ubiquitous Technol. 9 (3), 1–34.

Arksey, H., O'Malley, L., 2005. Scoping studies: towards a methodological framework. Int. J. Soc. Res. Methodol. 8 (1), 19–32.

Bahrini, M., Zargham, N., Pfau, J., Lemke, S., Sohr, K., Malaka, R., 2020a. Enhancing game-based learning through infographics in the context of smart home security. In: Entertainment Computing–ICEC 2020: 19th IFIP TC 14 International Conference, ICEC 2020, Xi'an, China, November 10–13, 2020, Proceedings 19. Springer, pp. 18–36.

Bahrini, M., Zargham, N., Pfau, J., Lemke, S., Sohr, K., Malaka, R., 2020b. Good vs. evil: investigating the effect of game premise in a smart home security educational game. In: Extended Abstracts of the 2020 Annual Symposium on Computer-Human Interaction in Play, pp. 182–187.

Bailey, D., Kornegay, M., Partlow, L., Bowens, C., Gareis, K., Kornegay, K., 2023. Utilizing culturally responsive strategies to inspire african american female participation in cybersecurity. J. Pre-Coll. Eng. Educ. Res. (J-PEER) 13 (2), 8.

Barbosa, N.M., Zhang, Z., Wang, Y., 2020. Do privacy and security matter to everyone? quantifying and clustering {User-Centric} considerations about smart home device adoption. In: Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020), pp. 417–435.

Batalla, J.M., Vasilakos, A., Gajewski, M., 2017. Secure smart homes: opportunities and challenges. ACM Comput. Surv. (CSUR) 50 (5), 1–32.

Benton, L., Vasalou, A., Turner, S., 2023. Location, location, security? exploring location-based smart device security concerns and mitigations within low-rent homes. In: Proceedings of the 2023 ACM Designing Interactive Systems Conference, pp. 1060–1077.

Blythe, J.M., Sombatruang, N., Johnson, S.D., 2019. What security features and crime prevention advice is communicated in consumer iot device manuals and support pages? J. Cybersecur. 5 (1), tyz005.

Boer, H., Seydel, E.R., 1996. Protection motivation theory. In: Predicting Health Behaviour: Research and Practice with Social Cognition Models. Eds. Mark Conner, Paul Norman. Open University Press, pp. 95–120.

Borgert, N., Jansen, L., Böse, I., Friedauer, J., Sasse, M.A., Elson, M., 2024. Self-efficacy and security behavior: results from a systematic review of research methods. In: Proc. CHI 2024, pp. 1–32.

Borgert, N., Reithmaier, O.D., Jansen, L., Hillemann, L., Hussey, I., Elson, M., 2023. Home is where the smart is: development and validation of the cybersecurity self-efficacy in smart homes (cySESH) scale. In: Proc. CHI 2023, pp. 1–15.

Breve, B., Cimino, G., Desolda, G., Deufemia, V., Elefante, A., 2023. On the user perception of security risks of TAP rules: a user study. In: International Symposium on End User Development. Springer, pp. 162–179.
Brush, A.J.B., Lee, B., Mahajan, R., Agarwal, S., Saroiu, S., Dixon, C., 2011. Home automation in the wild: challenges and opportunities. In: Proc. CHI 2011, pp. 2115–2124.
Cai, W., Pasquale, L., Ramkumar, K., McCarthy, J., Nuseibeh, B., Doherty, G., 2023. Human-centric security for smart homes: Scoping review. Registered: October 18, 2023. https://osf.io/pj347.
Chalhoub, G., Flechais, I., Nthala, N., Abu-Salma, R., 2020. Innovation inaction or in action? the role of user experience in the security and privacy design of smart home cameras. In: Sixteenth Symposium on Usable Privacy and Security (SOUPS'20), pp. 185–204.
Chalhoub, G., Kraemer, M.J., Nthala, N., Flechais, I., 2021. "It did not give me an option to decline": a longitudinal analysis of the user experience of security and privacy in smart home products. In: Proc. CHI 2021, pp. 1–16.
Chen, Y., Yuan, X., Zhang, J., Zhao, Y., Zhang, S., Chen, K., Wang, X., 2020. Devil's whisper: a general approach for physical adversarial attacks against commercial black-box speech recognition devices. In: 29Th USENIX Security Symposium (USENIX Security 20). USENIX Association, pp. 2667–2684.
Chhetri, C., Motti, V.G., 2019. Eliciting privacy concerns for smart home devices from a user centered perspective. In: Information in Contemporary Society: 14th International Conference, iConference 2019, Washington, DC, USA, March 31–April 3, 2019, Proceedings 14. Springer, pp. 91–101.
Chidziwisano, G.H., Jalakasi, M., 2023. Understanding women's perspectives on smart home security systems in patriarchal societies of malawi. In: Proceedings of the 2023 ACM Designing Interactive Systems Conference, pp. 1078–1092.
Collen, A., Szanto, I.-C., Benyahya, M., Genge, B., Nijdam, N.A., 2022. Integrating human factors in the visualisation of usable transparency for dynamic risk assessment. Information 13 (7), 340.
Colnago, J., Feng, Y., Palanivel, T., Pearman, S., Ung, M., Acquisti, A., Cranor, L.F., Sadeh, N., 2020. Informing the design of a personalized privacy assistant for the internet of things. In: Proc. CHI 2020, pp. 1–13.
Douha, N. Y.-R., Renaud, K., Taenaka, Y., Kadobayashi, Y., 2023. Smart home cybersecurity awareness and behavioral incentives. Inf. Comput. Security 31 (5), 545–575.
Dourish, P., Grinter, R.E., Delgado De La Flor, J., Joseph, M., 2004. Security in the wild: user strategies for managing security as an everyday, practical problem. Pers. Ubiquitous Comput. 8, 391–401.
Duezguen, R., Mayer, P., Berens, B., Beckmann, C., Aldag, L., Mossano, M., Volkamer, M., Strufe, T., 2021. How to increase smart home security and privacy risk perception. In: 2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). IEEE, pp. 997–1004.
Fayoumi, A., Sobati-Moghadam, S., Rajaiyan, A., Oxley, C., Montero, P.F., Dahmani, A., 2022. The cybersecurity risks of using internet of things (iot) and surveys of end-users and providers within the domiciliary care sector. In: 2022 Sixth International Conference on Smart Cities, Internet of Things and Applications (SCIoT). IEEE, pp. 1–7.
Fernandes, E., Jung, J., Prakash, A., 2016. Security analysis of emerging smart home applications. In: 2016 IEEE Sym posium on Security and Privacy (SP). IEEE, pp. 636–654.
Feth, D., Maier, A., Polst, S., 2017. A user-centered model for usable security and privacy. In: Human Aspects of Information Security, Privacy and Trust: 5th International Conference, HAS 2017, Held as Part of HCI International 2017, Vancou ver, BC, Canada, July 9-14, 2017, Proceedings 5. Springer, pp. 74–89.
Fruchter, N., Liccardi, I., 2018. Consumer attitudes towards privacy and security in home assistants. In: Extended Abstracts of CHI 2018, pp. 1–6.
Furnell, S., Clarke, N., 2012. Power to the people? the evolving recognition of human aspects of security. Comput. Security 31 (8), 983–988.
Garfinkel, S., Lipford, H.R., 2014. Usable security: History, themes, and challenges. Morgan & Claypool Publishers.
Garg, V., Camp, J., 2012. End user perception of online risk under uncertainty. In: 2012 45th Hawaii International Conference on System Sciences. IEEE, pp. 3278–3287.
Geeng, C., Roesner, F., 2019. Who'S in control? interactions in multi-User smart homes. In: Proc. CHI 2019, pp. 1–13.
George, C., Khamis, M., Buschek, D., Hussmann, H., 2019. Investigating the third dimension for authentication in immersive virtual reality and in the real world. In: 2019 IEEE Conference on Virtual Reality and 3D User Interfaces. IEEE, pp. 277–285.
George, J.F., Chen, R., Yuan, L., 2021. Intent to purchase iot home security devices: fear vs privacy. PLoS One 16 (9), e0257601.
Goffinet, S., Schmitz, D., Zavalyshyn, I., Legay, A., Riviere, E., 2021. Controlling security rules using natural dialogue: an application to smart home care. In: Adjunct Proceedings of the 2021 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2021 ACM International Symposium on Wearable Computers, pp. 194–197.
Green, M., Smith, M., 2016. Developers are not the enemy!: the need for usable security APIs. IEEE Security Privacy 14 (5), 40–46.
Grobler, M., Gaire, R., Nepal, S., 2021. User, usage and usability: redefining human centric cyber security. Front. Big Data 4, 583723.
Hammi, B., Zeadally, S., Khatoun, R., Nebhen, J., 2022. Survey on smart homes: vulnerabilities, risks, and countermeasures. Comput. Security 117, 102677.
Haney, J., Acar, Y., Furman, S., 2021. " it's the company, the government, you and i": User perceptions of responsibility for smart home privacy and security. In: 30th USENIX Security Symposium (USENIX Security 21), pp. 411–428.
Haney, J.M., Acar, Y., Li, A., Haney, F., 2025. Smart home users' security and privacy perceptions and actions differ by device category: results from a US survey. In: International Conference on Human-Computer Interaction. Springer, pp. 188–207.
Haney, J.M., Furman, S.M., 2023a. Smart home device loss of support: consumer perspectives and preferences. In: International Conference on Human-Computer Interaction. Springer, pp. 492–510.
Haney, J.M., Furman, S.M., 2023b. User perceptions and experiences with smart home updates. In: 2023 IEEE Symposium on Security and Privacy (SP)). IEEE, pp. 2867–2884.
Haney, J.M., Furman, S.M., Acar, Y., 2020. Smart home security and privacy mitigations: consumer perceptions, practices, and challenges. In: HCI for Cybersecurity, Privacy and Trust: Second International Conference, HCI-CPT 2020. Springer, pp. 393–411.
Hazazi, H., Shehab, M., 2023. Exploring the usability, security, and privacy of smart locks from the perspective of the end user. In: Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023), pp. 559–577.
Hazazi, H., Shehab, M., 2024. Exploring end users' perceptions of smart lock automation within the smart home environment. In: Proceedings of the 2024 European Symposium on Usable Security, pp. 112–124.
He, S., Zhan, X., Lei, Y., Liu, Y., Abu-Salma, R., Such, J., 2025. Exploring the privacy and security challenges faced by migrant domestic workers in chinese smart homes. In: Pro ceedings of the 2025 CHI Conference on Human Factors in Computing Systems, pp. 1–18.
He, W., Golla, M., Padhi, R., Ofek, J., Dürmuth, M., Fernandes, E., Ur, B., 2018. Rethinking access control and authentication for the home internet of things (IoT). In: 27th USENIX Security Symposium (USENIX Security 18). USENIX Association, Baltimore, MD, pp. 255–272.
He, W., Martinez, J., Padhi, R., Zhang, L., Ur, B., 2019. When smart devices are stupid: negative experiences using home smart devices. In: 2019 IEEE Security and Privacy Workshops (SPW). IEEE, pp. 150–155.
Hodges, D., 2021. Cyber-enabled burglary of smart homes. Comput. Security 110, 102418.
Huang, Y., Obada-Obieh, B., Beznosov, K., 2020. Amazon vs. my brother: how users of shared smart speakers perceive and cope with privacy risks. In: Proc. CHI 2020, pp. 1–13.
Huijts, N., Haans, A., Budimir, S., Fontaine, J., Loukas, G., Bezemskij, A., Oostveen, A., Filippoupolitis, A., Ras, I., IJsselsteijn, W., et al., 2023. User experiences with simulated cyber-physical attacks on smart home iot. Pers. Ubiquitous Comput. 27 (6), 2243–2266.
Jacobsson, A., Boldt, M., Carlsson, B., 2014. On the risk exposure of smart home automation systems. In: 2014 International Conference on Future Internet of Things and Cloud. IEEE, pp. 183–190.
Jacobsson, A., Boldt, M., Carlsson, B., 2016. A risk analysis of a smart home automation system. Future Gen. Comput. Syst. 56, 719–733.
Jang, W., Chhabra, A., Prasad, A., 2017. Enabling multi-user controls in smart home devices. In: Proceedings of the 2017 Workshop on Internet of Things Security and Privacy, pp. 49–54.
Jia, Y., Yuan, B., Xing, L., Zhao, D., Zhang, Y., Wang, X., Liu, Y., Zheng, K., Crnjak, P., Zhang, Y., et al., 2021. Who'S in control? on security risks of disjointed iot device management channels. In: Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security, pp. 1289–1305.
Jois, T.M., Pavlovich, T., McCarron, B.M., Kotz, D., Pierson, T.J., 2024. Smart use of smart devices in your home: a smart home security and privacy workshop for the general public. In: Proceedings of the 55th ACM Technical Symposium on Computer Science Education v. 1, pp. 611–617.
Keleher, M., Barrera, D., Chiasson, S., 2024. Balancing security and longevity: benefits of modular iot infrastructure. In: Proceedings of the New Security Paradigms Workshop, pp. 20–34.
Klobas, J.E., McGill, T., Wang, X., 2019. How perceived security risk affects intention to use smart home devices: a reasoned action explanation. Comput. Security 87, 101571.
Kulyk, O., Reinheimer, B., Aldag, L., Mayer, P., Gerber, N., Volkamer, M., 2020. Security and privacy awareness in smart environments–a cross-country investigation. In: Financial Cryptography and Data Security: FC 2020 International Workshops, AsiaUSEC, CoDeFi, VOTING, and WTSC, Kota Kinabalu, Malaysia, February 14, 2020, Revised Selected Papers 24. Springer, pp. 84–101.
Lafontaine, E., Sabir, A., Das, A., 2021. Understanding people's attitude and concerns towards adopting iot devices. In: Extended Abstracts of CHI 2021, pp. 1–10.
Lee, C., Zappaterra, L., Choi, K., Choi, H.-A., 2014. Securing smart home: technologies, security challenges, and security requirements. In: 2014 IEEE Conference on Communications and Network Securit. IEEE, pp. 67–72.
Leitão, R., 2019. Anticipating smart home security and privacy threats with survivors of intimate partner abuse. In: Proceedings of the 2019 on Designing Interactive Systems Conference, pp. 527–539.
Li, J., Sun, K., Huff, B.S., Bierley, A.M., Kim, Y., Schaub, F., Fawaz, K., 2023. "It's up to the consumer to be smart": understanding the security and privacy attitudes of smart home users on reddit. In: 2023 IEEE Symposium on Security and Privacy (SP). IEEE, pp. 2850–2866.
Li, W., Yigitcanlar, T., Erol, I., Liu, A., 2021. Motivations, barriers and risks of smart home adoption: from systematic literature review to conceptual framework. Energy Res. Soc. Sci. 80, 102211.
Lin, H., Bergmann, N.W., 2016. Iot privacy and security challenges for smart home environments. Information 7 (3), 44.
Löbner, S., Tronnier, F., Miller, L., Lindemann, J., 2024. An in-depth analysis of security and privacy concerns in smart home iot devices through expert user interviews. In: IFIP World Conference on Information Security Education. Springer, pp. 97–110.
Maiorescu, I., Gabudeanu, L., Vîlcea, A.-L., Sabou, G.-C., Dârdală, M., 2021. Intrusiveness and data protection in iot solutions for smart homes. Amfiteatru Econ. 23 (57), 429–447.
Malkin, N., Luo, A.F., Poveda, J., Mazurek, M.L., 2023. Optimistic access control for the smart home. In: 2023 IEEE Sym posium on Security and Privacy (SP). IEEE, pp. 3043–3060.

Manandhar, S., Moran, K., Kafle, K., Tang, R., Poshyvanyk, D., Nadkarni, A., 2020. Towards a natural perspective of smart homes for practical security and safety analyses. In: 2020 IEEE Symposium on Security and Privacy (SP). IEEE, pp. 482–499.

Mare, S., Girvin, L., Roesner, F., Kohno, T., 2019. Consumer smart homes: where we are and where we need to go. In: Proceedings of the 20th International Workshop on Mobile Computing Systems and Applications, pp. 117–122.

Marikyan, D., Papagiannidis, S., Alamanos, E., 2019. A systematic review of the smart home literature: a user perspective. Technol. Forecast. Soc. Change 138, 139–154.

Mazurek, M., Klemperer, P., Shay, R., Takabi, H., Bauer, L., Cranor, L., 2011. Exploring reactive access control. In: Proc. CHI 2011, pp. 2085–2094.

McCall, M., Zeng, E., Shezan, F.H., Yang, M., Bauer, L., Bichhawat, A., Cobb, C., Jia, L., Tian, Y., 2023. Towards usable security analysis tools for {Trigger-Action} programming. In: Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023), pp. 301–320.

McCarthy, A., Gaster, B.R., Legg, P., 2020. Shouting through letterboxes: a study on attack susceptibility of voice assistants. In: 2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security). IEEE, pp. 1–8.

McDermott, C.D., Isaacs, J.P., Petrovski, A.V., 2019. Evaluating awareness and perception of botnet activity within consumer internet-of-things (iot) networks. In: Informatics. Vol. 6. MDPI, p. 8.

Mols, A., Wang, Y., Pridmore, J., 2022. Household intelligent personal assistants in the netherlands: exploring privacy concerns around surveillance, security, and platforms. Convergence 28 (6), 1841–1860.

Morgan, P.L., Collins, E.I.M., Spiliotopoulos, T., Greeno, D.J., Jones, D.M., 2022. Reducing risk to security and privacy in the selection of trigger-action rules: implicit vs. explicit priming for domestic smart devices. Int. J. Hum. Comput. Stud. 168, 102902.

Munn, Z., Peters, M. D.J., Stern, C., Tufanaru, C., McArthur, A., Aromataris, E., 2018. Systematic review or scoping review? guidance for authors when choosing between a systematic or scoping review approach. BMC Med. Res. Methodol. 18, 1–7.

Neilly, H.T., Richmond, Y.W., Desjardins, A., Sean, A.M., Pierce, J., 2022. Monitoring pets, deterring intruders, and casually spying on neighbors: everyday uses of smart home cameras. In: Proc. CHI 2022, pp. 1–25.

Nurgalieva, L., Frik, A., Doherty, G., 2023. A narrative review of factors affecting the implementation of privacy and security practices in software development. ACM Comput. Surv. 55 (14s), 1–27.

Nurse, J. R.C., Atamli, A., Martin, A., 2016. Towards a usable framework for modelling security and privacy risks in the smart home. In: Human Aspects of Information Security, Privacy, and Trust: 4th International Conference, HAS 2016, Held as Part of HCI International 2016, Toronto, on, Canada, July 17, 2016, Proceedings 4. Springer, pp. 255–267.

Park, C., Kim, Y., Jeong, M., 2018. Influencing factors on risk perception of iot-based home energy management services. Telemat. Informatics 35 (8), 2355–2365.

Pasquale, L., Ramkumar, K., Cai, W., McCarthy, J., Doherty, G., Nuseibeh, B., 2024. The rocky road to sustainable security. IEEE Security Privacy 22 (5), 82–86.

Patil, S., Hoyle, R., Schlegel, R., Kapadia, A., Lee, A.J., 2015. Interrupt now or inform later? comparing immediate and delayed privacy feedback. In: Proc. CHI 2015, pp. 1415–1418.

Patterson, L., Chard, S., Ng, B., Welch, I., 2021. Internet of things (iot) privacy and security: a user-focused study of aotearoa new zealand home users. In: Proceedings of the 54th Hawaii International Conference on System Sciences, pp. 4404–4413.

Pattnaik, N., Li, S., nurse, J. R.C., 2023. A survey of user perspectives on security and privacy in a home networking environment. ACM Comput. Surv. 55 (9), 1–38.

Pattnaik, N., Li, S., nurse, J. R.C., 2024. Security and privacy perspectives of people living in shared home environments. Proc. ACM Hum.-Comput. Interact. 8 (CSCW2), 1–39.

Paul, K., 2020. Dozens sue amazon's ring after camera hack leads to threats and racial slurs. https://www.theguardian.com/technology/2020/dec/23/amazon-ring-camera-hack-lawsuit-threats.

Peterson, E., Mujeye, S., 2025. Addressing iot vulnerabilities in smart homes. In: Proceedings of the 2025 8th International Conference on Software Engineering and Information Management, pp. 116–121.

Philip, S.J., Luu, T.J., Carte, T., 2023. There'S no place like home: understanding users' intentions toward securing internet-of-things (iot) smart home networks. Comput. Human Behav. 139, 107551.

Plachkinova, M., Menard, P., 2022. An examination of gain-and loss-framed messaging on smart home security training programs. Inf. Syst. Front. , 1–22.

Ponticello, A., Fassl, M., Krombholz, K., 2021. Exploring authentication for {Security-Sensitive} tasks on smart home voice assistants. In: Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021), pp. 475–492.

Pospisil, B., Sauter, T., Treytl, A., Huber, E., Seböck, W., 2022. Cyber security at home-what really matters to people. In: 2022 IEEE 31st International Symposium on Industrial Electronics (ISIE). IEEE, pp. 1208–1213.

Prange, S., George, C., Alt, F., 2021. Design considerations for usable authentication in smart homes. In: Proceedings of Mensch Und Computer 2021. Gesellschaft für Informatik eV, pp. 311–324.

Prange, S., Thiem, N., Fröhlich, M., Alt, F., 2022. "Secure settings are quick and easy¡'–motivating end-users to choose secure smart home configurations. In: Proceedings of the 2022 International Conference on Advanced Visual Interfaces, pp. 1–9.

Protick, T.I., Sabir, A., Abhinaya, S., Bartlett, A., Das, A., 2024. Unveiling users' security and privacy concerns regarding smart home iot products from online reviews. ACM J. Comput. Sustain. Soc. 2 (4), 1–41.

Prümmer, J., van Steen, T., van den Berg, B., 2024. A systematic review of current cybersecurity training methods. Comput. Security 136, 103585.

Reuter, C., Iacono, L.L., Benlian, A., 2022. A quarter century of usable security and privacy research: transparency, tailorability, and the road ahead.

Ricquebourg, V., Menga, D., Durand, D., Marhic, B., Delahoche, L., Loge, C., 2006. The smart home concept: our immediate future. In: 2006 1st IEEE International Conference on E-learning in Industrial Electronics. IEEE, pp. 23–28.

Sanders, E. B.-N., 2002. From user-centered to participatory design approaches. In: Design and the Social Sciences. CRC Press, pp. 18–25.

Sasaki, T., Inazawa, T., Yamaguchi, Y., Parkin, S., van Eeten, M., Yoshioka, K., Matsumoto, T., 2025. Am i infected? lessons from operating a large-scale iot security diagnostic service. arXiv preprint arXiv:2501.07326.

Sasse, M.A., Brostoff, S., Weirich, D., 2001. Transforming the 'weakest link'-a human/computer interaction approach to usable and effective security. BT Technol. J. 19 (3), 122–131.

Saura, J.R., Palacios-Marqués, D., Ribeiro-Soriano, D., 2021. Using data mining techniques to explore security issues in smart living environments in twitter. Comput. Commun. 179, 285–295.

Schuster, F., Habibipour, A., 2024. Users' privacy and security concerns that affect iot adoption in the home domain. Int. J. Hum.–Comput. Interact. 40 (7), 1632–1643.

Scott, E., Panda, S., Loukas, G., Panaousis, E., 2022. Optimising user security recommendations for AI-powered smart-homes. In: 2022 IEEE Conference on Dependable and Secure Computing (DSC). IEEE, pp. 1–8.

Seymour, V., Xenitidou, M., Timotijevic, L., Hodgkins, C., Ratcliffe, E., Gatersleben, B., Gilbert, N., Jones, C.R., 2022. Incorporating the public perspective into the future design of smart home living'. In: International Conference on Human-Computer Interaction. Springer, pp. 362–367.

Seymour, W., Such, J., 2023. Ignorance is bliss? the effect of explanations on perceptions of voice assistants. Proc. ACM on Hum.-Comput. Interact. 7 (CSCW1), 1–24.

Shah, S.W., Kanhere, S.S., 2019. Recent trends in user authentication–a survey. IEEE Access 7, 112505–112519.

Sharevski, F., Trowbridge, A., Westbrook, J., 2018. Novel approach for cybersecurity workforce development: a course in secure design. In: 2018 IEEE integrated STEM education conference (ISEC). IEEE, pp. 175–180.

Shere, A. R.K., nurse, J. R.C., Flechais, I., 2020. " Security should be there by default": investigating how journalists perceive and respond to risks from the internet of things. In: 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). IEEE, pp. 240–249.

Shuhaiber, A., Alkarbi, W., Almansoori, S., 2023. Trust in smart homes: the power of social influences and perceived risks. In: Intelligent Sustainable Systems: Selected Papers of WorldS4 2022, Volume 1. Springer, pp. 305–315.

Sovacool, B.K., Del Rio, D. D.F., 2020. Smart home technologies in europe: a critical review of concepts, benefits, risks and policies. Renewable Sustainable Energy Rev. 120, 109663.

Statista, 2023. Number of users of smart homes worldwide 2019–2028. https://www.statista.com/forecasts/887613/number-of-smart-homes-in-the-smart-home-market-in-the-world.

Sun, K., Zou, Y., Radesky, J., Brooks, C., Schaub, F., 2021. Child safety in the smart home: parents' perceptions, needs, and mitigation strategies. Proc. ACM on Hum.-Comput. Interact. 5 (CSCW2), 1–41.

Surbatovich, M., Aljuraidan, J., Bauer, L., Das, A., Jia, L., 2017. Some recipes can do more than spoil your appetite: analyzing the security and privacy risks of IFTTT recipes. In: Proceedings of the 26th International Conference on World Wide Web, pp. 1501–1510.

Tabassum, M., Kosinski, T., Lipford, H.R., 2019. " I don't own the data": end user perceptions of smart home device data practices and risks. In: Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019), pp. 435–450.

Tahaei, M., Vaniea, K., 2019. A survey on developer-centred security. In: 2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). IEEE, pp. 129–138.

Taieb, B., Pelet, J.-É., 2019. The user's attitude and security of personal information depending on the category of iot. In: World Conference on Information Systems and Technologies. Springer, pp. 431–437.

Thormundsson, B., 2024. Smart home - statistics & facts. https://www.statista.com/topics/2430/smart-homes/#editorsPicks.

Touqeer, H., Zaman, S., Amin, R., Hussain, M., Al-Turjman, F., Bilal, M., 2021. Smart home security: challenges, issues and solutions at different iot layers. J. Supercomput. 77 (12), 14053–14089.

Tricco, A., Lillie, E., Zarin, W., O'Brien, K., Colquhoun, H., Levac, D., Moher, D., Peters, M.D.J., Horsley, T., Weeks, L., et al., 2018. Prisma extension for scoping reviews (prisma-scr): checklist and explanation. Ann. Intern. Med. 169 (7), 467–473.

Turner, S., nurse, J. R.C., Li, S., 2022a. "It was hard to find the words": using an autoethnographic diary study to understand the difficulties of smart home cyber security practices. In: Extended Abstracts of CHI 2022, pp. 1–8.

Turner, S., Pattnaik, N., nurse, J. R.C., Li, S., 2022b. " You just assume it is in there, i guess": understanding UK families' application and knowledge of smart home cyber security. Proc. ACM Hum.-Comput. Interact. 6 (CSCW2), 1–34.

Valencia-Arias, A., Cardona-Acevedo, S., Gómez-Molina, S., Gonzalez-Ruiz, J.D., Valencia, J., 2023. Smart home adoption factors: a systematic literature review and research agenda. PLoS One 18 (10), e0292558.

Valero, C., Pérez, J., Solera-Cotanilla, S., Vega-Barbas, M., Suarez-Tangil, G., Alvarez-Campana, M., López, G., 2023. Analysis of security and data control in smart personal assistants from the user's perspective. Future Gen. Comput. Syst. 144, 12–23.

Vasalou, A., Benton, L., Serta, A., Gauthier, A., Besevli, C., Turner, S., Gill, R., Payler, R., Roesch, E., McAreavey, K., et al., 2025. Doing cybersecurity at home: a human-centred approach for mitigating attacks in AI-enabled home devices. Comput. Security 148, 104112.

Vetrivel, S., Van Harten, V., Gañán, C.H., Van Eeten, M., Parkin, S., 2023. Examining consumer reviews to understand security and privacy issues in the market of smart home devices. In: 32nd USENIX Security Symposium (USENIX Security 23), pp. 1523–1540.

Wang, H., Chen, Y.-P., Bista, D., Calvo, R., Regmi, N., Zhang, X., Neal, T., Ruiz, J., Anthony, L., 2025. 'Over time everyone's gonna be open to it': user attitudes towards security and privacy in continuous authentication for smart homes. IEEE Access.

Whitten, A., Tygar, J.D., 1999. Why johnny can't encrypt: a usability evaluation of PGP 5.0. In: USENIX Security Symposium. Vol. 348, pp. 169–184.

Windl, M., Hiesinger, A., Welsch, R., Schmidt, A., Feger, S.S., 2022. Saferhome: interactive physical and digital smart home dashboards for communicating privacy assessments to owners and bystanders. Proc. ACM Hum.-Comput. Interact. 6 (ISS), 680–699.

Xiao, Y., Jia, Y., Hu, Q., Cheng, X., Gong, B., Yu, J., 2023. Commandfence: a novel digital-Twin-Based preventive framework for securing smart home systems. IEEE Trans. Depend. Secure Comput. 20 (3), 2450–2465. https://doi.org/10.1109/TDSC.2022.3184185

Yao, Y., Basdeo, J., Kaushik, S., Wang, Y., 2019. Defending my castle: a co-design study of privacy mechanisms for smart homes. In: Proc. CHI 2019, pp. 1–12.

Yao, Y., Huang, L., He, Y., Ma, Z., Xu, X., Mi, H., 2023. Reviewing and reflecting on smart home research from the human-centered perspective. In: Proc. CHI 2023, pp. 1–21.

Ye, J., de Carné de Carnavalet, X., Zhao, L., Wu, L., Zhang, M., 2025. Understanding home router configuration habits & attitudes. In: Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems, pp. 1–12.

Yu, X., Zhou, Z., Zhang, L., Li, X.-Y., 2022. Thumbup: secure smartwatch controller for smart homes using simple hand gestures. IEEE Trans. Mob. Comput. 23 (1), 865–878.

Zeng, E., Mare, S., Roesner, F., 2017. End user security and privacy concerns with smart homes. In: Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017), pp. 65–80.

Zeng, E., Roesner, F., 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), pp. 159–176.

Zhang-Kennedy, L., Valiquette, M., Chen, A.B., Hadan, H., Suh, S., 2025. Folk tales of iot: understanding the impact of stories on users' positive and negative perceptions of smart home iot devices. In: Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems, pp. 1–18.

Zimmermann, V., Bennighof, M., Edel, M., Hofmann, O., Jung, J., von Wick, M., 2018. 'Home, smart home'–exploring end users' mental models of smart homes. In: Proceedings of Mensch Und Computer 2018. Gesellschaft für Informatik eV.

Zimmermann, V., Renaud, K., 2019. Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset. Int. J. Hum. Comput. Stud. 131, 169–187.

Zimmermann, V., Schäfer, S., Dürmuth, M., Marky, K., 2025. Authenticate as you go: from exploring smart home authentication with daily objects to authenticating with primary tasks. ACM Trans. Comput.-Hum. Interact. 32 (2), 1–69.