Radboud Universiteit

Navigating the Complexity of Smart-home Cybersecurity: Insights from a System Dynamics Approach

MASTER THESIS

Student name: R.S. (Ruben) Hoogakker

Student number: S1083925

Program: Business Administration

Specialization: Business Analysis and Modelling

Supervisor: dr. H.A.G.M. Jacobs (Eric)

Second examiner: dr. B.H. Hoorani (Bareerah Hafeez)

Date: June 23, 2023

Acknowledgements

I would like to thank all those who have supported and guided me throughout completing this master's thesis. Firstly, I am grateful to my supervisor, Eric Jacobs, for his guidance and expertise. His insightful feedback has shaped this research and improved its quality. I extend my appreciation to all the participants who participated in the interviews and generously shared their time, expertise, and valuable suggestions that have contributed to the development of the end product of this study. In addition, I am grateful to my friends, family, and girlfriend for their unconditional love, encouragement, and belief in my abilities during this challenging process. Their support throughout this journey has been a constant source of motivation. Lastly, I would like to thank all the researchers whose work laid the foundation for this study. Their efforts have been crucial in shaping the end product of this study and inspired me to pursue this research. While it is impossible to mention everyone individually, I am sincerely grateful to all those who have directly or indirectly contributed to completing this master's thesis. As I reflect upon the demanding and dedicated months that have shaped this research, a quote by Magda Chelly resonates deeply with me as a researcher:

"Cybersecurity is a social responsibility. We all have a role to play."

These words serve as a potent reminder that cybersecurity extends beyond individual efforts. It highlights the collective responsibility we share in safeguarding digital systems and protecting the safety and privacy of society. With this in mind, I dedicate my work to contributing to a safer and more resilient digital world where all share the responsibility for cybersecurity.

Sincerely,

Ruben Hoogakker

Nijmegen, June 23, 2023.

Abstract

In recent years, the growing popularity and accessibility of smart home (SH) devices have raised concerns about emerging cyber threats and vulnerabilities. Existing studies have focused on securing individual devices, neglecting the interconnected nature among different disciplines of the smart home ecosystem (SHES). To address this challenge, we propose a holistic analysis of the interdependencies among SHES components and their contribution to cybersecurity risks (CSRs). A semi-systematic literature review (SSLR) was conducted across multiple disciplines to combine each component from the SHES, extracting variables to develop a causal loop diagram (CLD). Disconfirmatory interviews (DIs) (n = 4) with experts from various fields validated the accuracy of the CLD. The findings revealed four reinforcing and five balancing feedback loops, and other interdependencies that significantly contribute to CSRs, particularly related to human behaviour, the deployment of devices, and interconnected vulnerabilities in the SHES. Overall, the results provide valuable insights for holistic cybersecurity approaches in SHs.

Keywords: *smart home, smart-home ecosystem, cybersecurity risks, causal loop diagram, system dynamics, semi-systematic literature review.*

Index

List of Figures

List of Tables

List of Abbreviations

Abbreviation	Explanation
BN	Bayesian Network
CLD	Causal Loop Diagram
CSR	Cybersecurity Risk
DDoS	Distributed Denial-of-Service
DI	Disconfirmatory Interview
GMB	Group Model Building
IoT	Internet of Things
IT	Information Technology
RIQ	Rigorously Interpreted Quotation
SD	System Dynamics
SH	Smart-Home
SHES	Smart-Home Ecosystem
SSLR	Semi-Systematic Literature Review

1 Introduction

1.1 Research context

The Internet of Things (IoT) introduces new features and services in many domains by connecting physical devices and objects worldwide via the Internet. The smart-home (SH) is an important domain (Chakraborty & Datta, 2017). In recent years, the popularity of SH devices has been increasing, with more consumers integrating these technologies into their living spaces (Ansar et al., 2022). SH devices allow individuals to remotely control and monitor various aspects of their home through a network connection, such as smart-speakers, security cameras, lightbulbs and thermostats. These interconnected devices act as a cohesive whole and comprise a smart-home ecosystem (SHES) (Gajewski et al., 2019). The global number of SH devices is projected to rapidly rise from 307 million in 2022 to an estimated 672 million by 2027, raising concerns about their security (Statista, 2022; Arabo, 2015). A remote intrusion enables the adversary to invade the privacy and safety of SH inhabitants by obtaining personal or sensitive information for personal benefit, controlling the SH device, or even monitoring residents inside the SH (Sivanathan et al., 2017; Ali & Awad, 2018).

The proliferation of interconnected SH devices via the Internet has raised concerns about new cyber threats and potential vulnerabilities that have yet to be discovered (Chen et al., 2020; Gheisari et al., 2021). SH devices are interconnected, often connected to the same network and share data through various means, such as Wi-Fi, cloud-based services, or Bluetooth, enabling seamless information exchange and enhancing user experience (Aheleroff et al., 2020). However, this interdependence also introduces vulnerabilities, as a security breach in one device can potentially compromise the entire system (Kimani et al., 2019).

Consequently, there is a pressing need to comprehensively understand the vulnerabilities and threats to the SH (Abomhara & Køien, 2015). However, identifying and analysing SH devices' potential cybersecurity risks (CSRs) is challenging due to the complex interdependencies within a SHES (Kitchin & Dodge, 2020). The intricate interdependencies among the interconnected devices in a SHES make it challenging to establish a clear defensive boundary or employ static access control methods (Zhou et al., 2018). Furthermore, "*cyberattacks are characterized by inherent complexity, ambiguity and uncertainty as a plethora of contributing variables*" (Khan et al., 2022: 1). These challenges are further

compounded by the unpredictable nature of human behaviour within the SHES (Jose & Malekian, 2017), which plays a significant role in many security incidents, underscoring the importance of considering human factors alongside technical issues when addressing CSRs (Kadena & Gupi, 2021). Hence, to fully understand the vulnerabilities and threats in the SHES, a new approach is needed that transcends the traditional technical perspective and instead focus on the interdependencies among its various components, including the *house, nodes, users, links, data, and policies* (Bugeja et al. 2020; Heiding et al., 2023). Addressing this gap, necessitates conducting a literature review, as it allows for synthesising existing research, identifying cause-effect relationships and mechanisms, and establishing a comprehensive understanding of CSRs within the SHES. Such a literature review will facilitate the integration of both technical and behavioural disciplines among the components within the SHES, providing valuable insights into its interconnectedness.

While several studies have explored CSRs of SH devices, there remains a lack of a comprehensive understanding concerning these CSRs, specifically regarding the interdependencies between different components of the SHES (Zhou et al., 2018). Previous research by Cannizzaro et al. (2020), Li et al. (2021), Shuhaiber & Mashal (2019) and Philip et al. (2023) has focused on the user component in the SHES, emphasizing device adoption and perceived CSRs. However, these studies neglect the interaction between CSRs and other components, thereby overlooking the interdependencies within the SHES. Alternatively, Azam et al. (2022) examined the data component and identified privacy threats in autonomous systems. Nevertheless, their study was limited to exploring threats and vulnerabilities related to data only. Studies by Abdullah et al. (2019), Arabo (2015), Heartfield et al. (2018), Yang & Sun (2022), and Darem et al. (2022) focused specifically on the SH devices (nodes component), investigating vulnerabilities and threats to SHs. However, these studies lack a holistic approach, leaving a comprehensive understanding of CSRs and their interactions within the SHES incomplete. Recent work by Ayavaca-Vallejo & Avila-Pesantez (2023) explored the cybersecurity landscape in SHs and highlighted threats and vulnerabilities faced by devices. However, like the aforementioned studies, they also overlooked the complex interconnected nature of the entire SHES. Therefore, this study aims to bridge this gap by synthesizing the literature, integrating technical and behavioural disciplines and establishing a causal diagram to holistically understand CSRs within the SHES among its individual components.

System dynamics (SD) offers a promising approach to model interconnected systems, enabling the capture of interdependent cause-effect relationships among vulnerabilities and threats in the SHES, which can be challenging to identify using other methods (Hasan &

Foliente, 2015). For example, unlike Bayesian Networks (BNs), a commonly used method used in cybersecurity research to capture cause-effect relationships between risk events and calculate their probabilities (Chockalingham, 2017; Flores et al., 2022). It is not appropriate for studying the CSRs in the SHES, as it does not account for its dynamic and interdependent nature (Punyamurthula & Badurdeen, 2018). Risk analysis methods like BNs focus on quantifying the probability of individual risk events by considering their causal relationships. However, they do not adequately account for the dynamic interactions and feedback loops that can occur within a system (Cheng & Greiner, 2001). In contrast, SD provides a framework in which the interdependencies and dynamic interactions within the system can easily be seen, providing a more comprehensive understanding of its behaviour (Azar, 2012). SD helps understand how the behaviour of a complex system is influenced by its components, shedding light on potential CSRs related to the interdependencies in the SHES (Bloodgood et al., 2015; Kannan, 2017).

SD approaches have proven effective in understanding interdependencies across various fields. For example, Alirzaei et al. (2017) employed SD to examine the connections between road safety, economic factors, and climate change, providing a comprehensive model for policymakers. Similarly, Jahan et al. (2022) employed SD to analyse the interrelations among risk factors and address complexity in construction profitability, providing a holistic perspective on the influencing causal factors. In cybersecurity, SD approaches have also been effectively applied in modelling interactive systems. Khan et al. (2022) developed a CLD, and successfully analysed the system behaviours of unintended consequences of cyberattacks in connected and autonomous vehicles. Tweneboah-Koduah and Buchanan (2018) provide another example where they developed a security risk assessment model based on SD for downstream energy sector infrastructures. Their CLD identified interdependencies and revealed the potential impacts of cyberattacks on the overall system.

These examples highlight the effectiveness of SD and CLDs in cybersecurity research, as they can help identify complex interdependencies and feedback loops that may not be immediately obvious. Gou et al. (2022) further support this notion, by highlighting how SD research on safety and security has helped identify potential threats, further reinforcing the significance of SD as a crucial approach for studying system security.

1.2 Research objective

The goal of this research is to provide insights into the potential CSRs associated with the interdependencies between different components of a SHES to enhance their cybersecurity and

improve the safety and privacy of homeowners. To attain this objective, a causal diagram will be constructed in which the interrelationships between the different components of a SHES will be identified and analysed to understand the system behaviour. The following specific knowledge is required to construct the causal diagram:

- Develop a comprehensive understanding of the key variables and their interrelationships in SHESs that contribute to CSRs;
- Understand the complexity of the SHES by developing a causal diagram of the SHES to capture the interdependencies and interactions between its components.

1.3 Research questions

To achieve the objective of this research, we formulated the central research question as follows:

"To what extent do the interdependencies among the components of a smart-home ecosystem contribute to the cybersecurity risks within the smart-home?"

To answer this central research question, the following sub-questions are presented:

- SQ 1: What are the specific threats and vulnerabilities and their relationships that affect cybersecurity risks in the smart-home ecosystem?
- SQ 2: What are the interdependencies between the different components of a smart-home ecosystem that affect the cybersecurity risks in that system?

Building an SD model serves well to answer the above sub-questions, as this approach aligns with the understanding of interdependencies and relationships between variables.

1.4 Thesis outline

The remaining sections of this thesis include a theoretical background, methodology, construction of the theoretical model, validation of the model, identification and description of feedback loops, and a concluding discussion.

2 Theoretical background

In this section, we will discuss the fundamental concepts of this research. We will begin by defining the SHES and its interdependent structure. Next, we will explore cybersecurity, focusing on its interdisciplinary nature and the associated CSRs SH devices face.

2.1 Smart-home ecosystem

Smart-home ecosystems (SHESs) are systems of interconnected SH devices that provide users with advanced features beyond basic convenience. For example, a SHES might include connected door locks for enhanced home security or water flow sensors to improve energy efficiency (Fernandes et al., 2016). These devices generate data based on user behaviour, which is then used to adapt the SHES to the user's needs (Rasch, 2013).

A SHES consists of several components that interact with each other and create interdependencies that might contribute to potential CSRs. Bugeja et al. (2020) identified six components of a SHES: *house, nodes, users, links, data* and *policies*. The *house* is the physical home where users reside and where the connected devices are typically located, *nodes* are the physical SH devices in the house, *users* are the human occupants that interact with the nodes, *links* are the channels facilitating communication between the users and nodes, as well as between nodes themselves, *data* refers to information that the SHES collects, such as device usage patterns and *policies* are the rules that dictate how data is transmitted between different entities in the SHES (Bugeja et al. 2020; Heiding et al., 2023).

2.2 Cybersecurity

Cybersecurity involves diverse, interconnected discussions and lacks a broadly accepted definition (Cavelty, 2010; Craigen et al., 2014). Breaking down the term cybersecurity provides a better understanding of its relation to cyber and security domains (Craigen et al., 2014).

Cyber refers to the interaction between electronic communication and virtual networks in order to carry out digital tasks (Eling & Schnell, 2016). It is part of a dynamic ecosystem called cyberspace, which encompasses physical infrastructure, software, regulations, ideas, innovations, and interactions. Cyberspace is shaped by a diverse community of contributors and continuously evolves (Deibert & Rohozinski, 2010; Craigen et al., 2014).

Security, on the other hand, has no widely accepted definition and involves various discourses focused on identifying who secures what, for whom, why, with what outcomes and under what conditions (Buzan et al., 1998; Craigen et al., 2014).

Together, cyber and security can be seen as various aspects related to safeguarding electronic communication, virtual networks, and digital information against unauthorized access, data breaches, and cyberattacks (Abomhara & Køien, 2015; Srinivas et al., 2019). Cybersecurity encompasses studies on threat assessments, vulnerabilities, risks, incident response, and strategies to mitigate and manage risks (Jbair et al., 2022). Consequently, cybersecurity can be seen as complex, multidimensional, and continuously evolving in a rapidly changing landscape.

2.2.1 Interdisciplinary nature of cybersecurity

The multidimensionality of cybersecurity is highly variable and often subjective, indicating that its interpretations can differ across various contexts. This subjectivity suggests that individual perspectives and subjective judgments shape how cybersecurity is perceived and approached (Craigen et al., 2014). As a result, diverse disciplines that should be collaborating to address cybersecurity challenges are separated, hindering progress in this field (Craigen et al., 2014; Ramirez, 2017).

Cybersecurity was previously seen as a technical subfield of computer science (Craigen et al., 2014). However, in recent years, researchers have recognized the importance of incorporating human factors, such as awareness and proficiency, into CSR models to gain a deeper understanding of the behaviours that contribute to these risks. Therefore, current cybersecurity research challenges the technical-focused definition as it incorporates diverse fields such as social sciences, psychology, and risk and decision science combined with computer science, engineering and information technology (IT) (Craigen et al., 2014; Ramirez, 2017; NIST, 2018; Jeong et al., 2019; Cains et al., 2021).

This increasingly interdisciplinary nature of cybersecurity poses a challenge for stakeholders from diverse disciplines, as they may view cybersecurity through different lenses, influencing their perception of cybersecurity-related terms. This can complicate discussions and efforts to create a unified approach to cybersecurity (Craigen et al., 2014; Cains et al., 2022).

2.2.2 Cybersecurity risks in smart-homes

Failing to provide adequate cybersecurity gives rise to potential risks known as CSRs. In SHs, these risks, encompass the possibility of harm, damage or loss to one of the SHES's components, which varies depending on context (Bugeja, 2021). CSRs emerge from incidents, events, or occurrences, and their severity is determined by the probability of a certain threat exploiting a specific vulnerability and the potential consequences resulting from such an exploit (NIST, 2018).

A comprehensive CSR model typically includes information about the *network infrastructure*, *security settings*, *threats*, *vulnerabilities*, and *risks* (Bastos et al., 2018; Kannan, 2017). In this research, the network infrastructure and security settings belong to the vulnerability category because they are both potential weaknesses or flaws in an SH that attackers can exploit to gain unauthorized access or compromise the SHES's security (Ryoo et al., 2017). Each CSR aspect will be explained below in how it applies to SHs.

Threats refer to any potential action or event that can exploit a vulnerability in the SHES, and is likely to cause damage, harm or loss (Bastos et al., 2018; Abdullah et al., 2019). Adversaries exploit these vulnerabilities to gain control over SH devices and engage in malicious activities, such as malware infections or eavesdropping, to expose valuable and confidential information (Abbas et al., 2021). The severity of threats in SHs surpasses those in other technologies due to their potential impact on the physical world. For instance, when adversaries gain access to the control of a smart-door lock, thereby compromising the physical security of the home (Cannizzaro et al., 2020).

Vulnerabilities are weaknesses or gaps inside the SHES, which adversaries can exploit, providing opportunities to compromise its security and integrity (Bastos et al., 2018; Abdullah et al., 2019). The hardware, network infrastructure, and protocols of systems are the most targeted vulnerabilities (Kadena & Gupi, 2021). An example of a hardware vulnerability is the resource-constrained nature of devices (Abbas et al., 2021). An example of a network infrastructure vulnerability is system accessibility, meaning hackers can exploit attacks remotely (Lin & Bergmann, 2016). Protocol vulnerabilities refer to an interception of communication between different devices or components in a SHES (Chhetri & Motti, 2021). Moreover, human factors also relate to security vulnerabilities (Kadena & Gupi, 2021). Individuals may refuse to adopt security technologies, disregard established security protocols, participate in malicious activities that pose considerable risks and underestimate the likelihood of experiencing a cybersecurity incident (Herath & Rao, 2009; Kadena & Gupi, 2021).

Risks represent the potential harm or loss due to a threat exploited by the system's vulnerability (Bastos et al., 2018). These can range from unauthorized parties gaining access to personal information, psychological dimensions of privacy, financial loss, reputational damage, or even physically breaching privacy by entering an individual's home without permission (Heartfield et al., 2018; Hall et al., 2020).

3 Methodology

This chapter presents the research design, including a detailed description of the semi-systematic literature review (SSLR) and its search strategy. The development of the causal diagram is discussed, followed by an explanation of its validation and the analysis methods used. Finally, research ethics will be addressed.

3.1 Research design

We employed an explanatory qualitative approach to identify and analyse CSRs of SH devices within the SHES. According to Denscombe (2012), explanatory research aims to understand why things happen and uncover their underlying causes. In this study, we built on existing knowledge to identify CSRs associated with the components in the SHES. Subsequently, we constructed and analysed a CLD to explain the mechanisms underlying these CSRs. Additionally, we utilized an inductive approach, as Hayes et al. (2010) suggested, where existing knowledge was used to predict new cases. In this case, we used the inductive approach to conceptualize the CLD by extracting variables and relationships from the SSLR.

3.2 Data collection

The research method consists of (1) a SSLR to extract variables and their relationships from different fields to bridge the disciplinary boundaries and eventually construct a CLD of the SHES, including its components, and (2) disconfirmatory interviews (DIs) (n = 4) to validate the CLD. These two steps are elaborated below.

3.2.1 Semi-systematic literature review

In this research, we employed a SSLR as the primary method. A literature review serves several scientific purposes, including discovering relevant variables, identifying relationships between ideas and practices, gaining methodological insights, establishing the context of the problem, and understanding the structure of the subject (Randolph, 2009). This study aimed to understand CSRs associated with the interdependencies of the components in the SHES, aligning with the goals outlined by Randolph (2009). The SSLR is a well-suited approach for exploring the multidimensional CSRs within the SHES, and addresses concerns Snyder (2019) raised

regarding the comprehensiveness and rigour of traditional literature reviews. By adopting the SSLR, we ensured reliability and credibility by providing a structured and rigorous methodology. Moreover, it allowed for integrating knowledge from various disciplines involved in studying CSRs within the SHES, which are perceived differently and investigated across diverse fields (Snyder, 2019). Conducting the SSLR enabled a comprehensive analysis, identification and integration of key variables and their relationships with CSRs among the components of the SHES, which informed the development of the CLD.

3.2.1.1 Search strategy

We used scientific papers from reputable databases like Scopus and Web of Science as the primary data sources (UOW, 2022; Ahmad & Alsmadi, 2020). A thorough and objective process was followed to ensure reliability and minimize selection bias (Snyder, 2019).

The search strategy was developed based on the research questions and adheres to the three key principles of systematic reviews, outlined in the Cochrane Handbook (Higgins et al., 2019). 1) *High sensitivity*: a variety of spelling variations and terms were considered, including "cybersecurity," "cyber," "security," "cyber security," and "cyber-security,". This approach aimed to capture relevant literature while maintaining high sensitivity. 2) *Avoiding excessive search concepts*: The strategy avoided using too many search concepts. Instead, we combined various search terms within each concept using the "OR" operator. This ensured that studies using different terminology within CSRs and SHs were included. 3) *Using free-text and subject headings*, was adhered to, ensuring studies indexed using standardized terms were not missed. The search query used to identify relevant literature was as follows:

(("cybersecurity" OR "cyber" OR "security" OR "cyber security" OR "cyber-security") AND ("risk" OR "threat" OR "vulnerability" OR "attack") AND ("smart-Home" OR "smart Home" OR "connected household" OR "connected home" OR "smart household" OR "home automation")).

To account for the dynamic nature of CSRs, we have only included sources published in 2019 or later, focusing on open-access papers in English (Calliess & Baumgarten, 2020). Papers written in other languages native to the researchers (German and Dutch) were included, however no relevant research was found. Studies written in any other language than Dutch, German and English were excluded from this study. This resulted in only English written relevant studies. The most cited papers retrieved from the search strategy were given priority

as they are considered seminal or prominent, establishing a strong foundation of knowledge for the study (Etemadi., 2021). The full list of inclusion and exclusion criteria is presented in Table 1.

Table 1

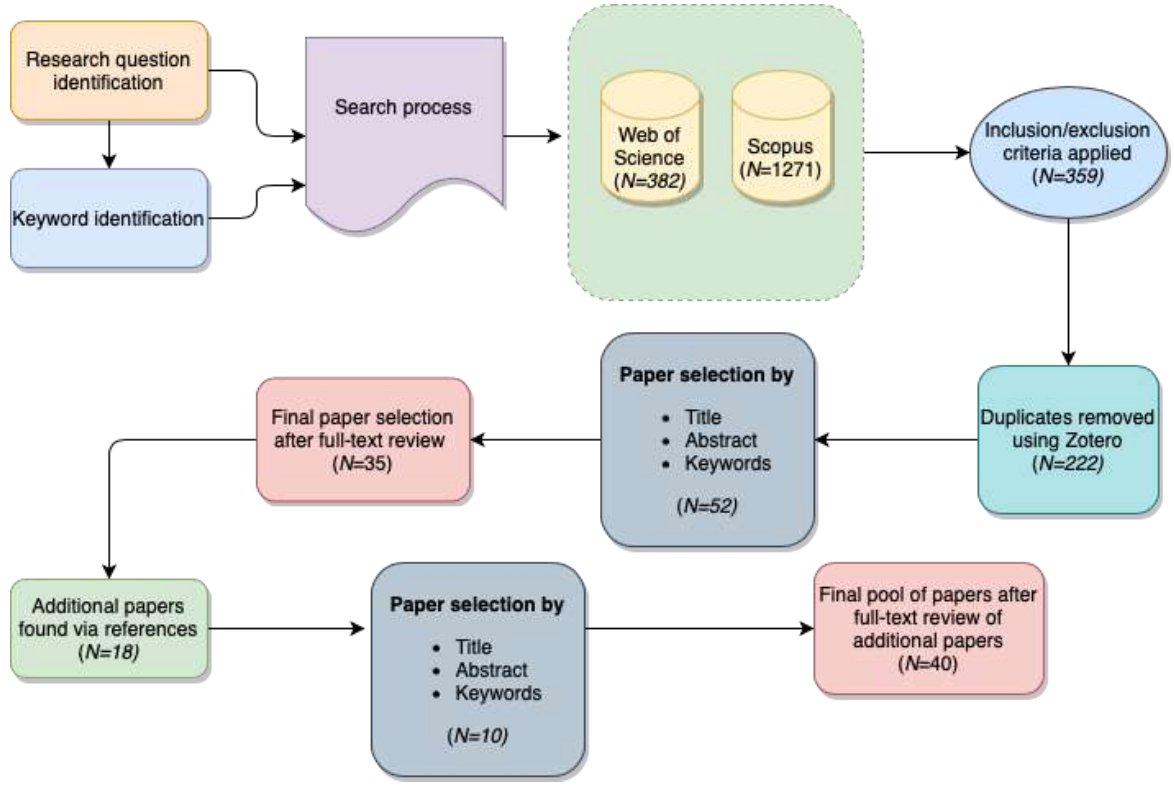
Inclusion/exclusion criteria for the SSLR

Inclusion criteria	Exclusion criteria
Written in English, Dutch or German	Papers written in languages other than English, Dutch or German
Full text available	Research papers containing less than three pages
Peer-reviewed articles	Non-peer-reviewed papers
Published from 2019 onwards	Published before 2019

We removed duplicates after applying the inclusion/exclusion criteria. The relevance of articles was assessed based on their abstracts, titles, and keywords, aligning with the research questions of this study. Full texts of the selected articles were then reviewed to make the final inclusion decision. We scanned the references cited in the selected articles to identify additional relevant articles, following Snyder's suggestion (2019), to which the same selection process and criteria were applied. The SSLR process is illustrated in Figure 1, and continued until we reached saturation, indicating no new variables were obtained from the compiled list of studies (Beaulieu et al., 2022).

Figure 1

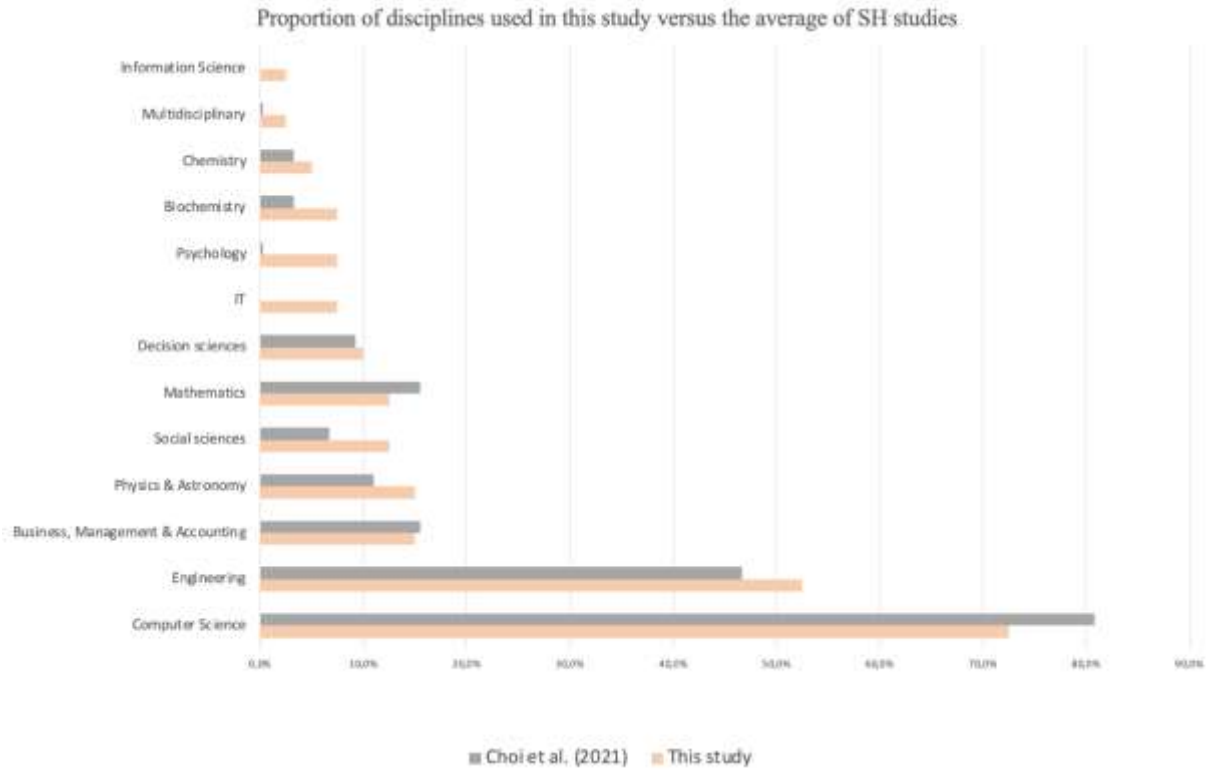
Review process of the semi-systematic literature review



We tried to include more behavioural disciplines in the SSLR, despite their lower representation in the databases compared to technical disciplines. Figure 2 shows the current state of SH literature, which reflects this observation (Choi et al., 2021). However, the SSLR achieved a higher proportion of behavioural disciplines, such as social sciences, decision sciences, and psychology, surpassing the dominant technical distribution in the literature. A complete list of the papers and their disciplines included in the SSLR for the development of the CLD, can be found in Appendix 2.

Figure 2

Discipline distribution in this study versus average smart-home studies



3.2.2 Developing a causal loop diagram based on textual data

We constructed a CLD to visually depict the variables extracted from the SSLR in a causal diagram. CLDs are valuable tools for understanding complex systems, revealing feedback structures and interconnectedness (Xia et al., 2021; Kwoun et al., 2013; Agnew et al., 2018). The CLD development process aligned with the data analysis methodology presented by Kim and Andersen (2012), which involved systematic qualitative data coding to identify key variables and their underlying structural relationships. This approach facilitated systems

thinking and enabled the generation of new knowledge through inductive analysis of raw qualitative data (Xia et al., 2021; Charmaz, 2006).

The method by Kim and Andersen (2012) consists of five steps tailored to this study. Step 1, problem articulation, involves clearly understanding the system boundary and key variables (Zhang et al., 2021). The model boundary was based on the research objective in 1.2, and includes the key variables: CSRs and its underlying aspects: *threats, vulnerabilities,* and *risks* outlined in 2.2.2, and the interdependencies among the components that contribute to the CSRs in a SHES, outlined in 2.1 (Sterman, 2000; Meadows 2008). We intentionally omitted external variables outside of the SHES to maintain a clear focus on the modelling purpose, increasing its usefulness (Sterman, 2000). Additionally, we excluded variables that do not bring about behavioural change, as the focus of this research is to understand how the interdependencies among the components contribute to CSR. These variables do not provide insights on the system behaviour under investigation (Xia et al., 2020). This clear model boundary allowed for effective analysis of CSRs and their underlying causes within the SHES.

Step 2 involved identifying all key variables and their causal relationships, by marking data segments in the articles. The selection was based upon the subsequent criteria, 1) the text is related to one of the components of the SHES, 2) the text relates to CSRs, i.e., *vulnerabilities, threats or risks*, and 3) it is a contributing factor to CSR, rather than a mitigating factor. The marked data segments, indicated the cause-and-effect relationship between each variable. Once we read each article, step 3 followed, wherein we outlined the identified variables, their causal relationships, and polarities in a cause-effect diagram in Excel. This sequence of steps, namely steps 2 and 3, were then repeated for each article in the analysis.

In step 4, we generalized individual cause-effect diagrams to merge system structures into a comprehensive CLD, addressing variations in variable names across articles (Kim & Andersen, 2012). Axial coding was applied to establish connections between categories (Myers, 2019), resulting in an aggregated CLD developed using Vensim, a tool for dynamic feedback models (Xia et al., 2021). In order to integrate all the available data into the aggregated model, we introduced three intermediate variables and one assumed relationship. To ensure accuracy, we carefully studied these assumptions and verified them through expert interviews, mitigating potential biases (Kim & Andersen, 2012). Our assumptions are documented in Appendix 5, providing transparency regarding the basis for these assumptions.

Finally, in step 5, we documented each variable and its relationship to the data source in a column alongside the cause-effect diagrams.

3.2.3 Validating the causal loop diagram

To confirm our accuracy of the analysis and mitigate biases, validating interviews were conducted (Buchbinder, 2011). Models are simplified representations of the real world, necessitating a validation process to increase its confidence (Pala et al., 1999; Lane, 2015). Validation aims to establish the soundness and usefulness of the model for its intended purpose (Barlas, 1996), and includes structural and behavioural tests (Pala et al., 1999). Given the qualitative nature of our model, behavioural tests were not applicable as they involve simulation and output behaviour generation. Instead, we employed DIs to validate the structural components and assumptions of the CLD. DIs focus on uncovering discrepancies and challenging the model's validity by comparing the model's structure with the interviewees' perception of reality (Andersen et al., 2012).

Three of the four interviews were conducted online via Microsoft Teams video conferencing software due to the geographical dispersion of the selected experts. Screen sharing capabilities provided by the software were essential for visual presentation and shared model viewing during the interviews (Gray et al., 2020). The online format facilitated in-depth discussions and informed feedback. One expert, located nearby, participated in a face-to-face interview, allowing for a more personalized interaction.

To establish trust and obtain reliable responses, we took steps to familiarize ourselves with the participants and show genuine interest in their expertise, gathering preliminary information through LinkedIn (Bowden & Galindo-Gonzales, 2015; Darbi & Hall, 2014). Creating a comfortable atmosphere and building rapport before the interviews further enhanced trust-building (Andersen et al., 2012).

3.2.3.1 Interview sample

A holistic view is crucial to obtain a comprehensive understanding of cybersecurity's interdisciplinary nature, integrating multiple stakeholder perspectives (Vennix, 1996; Ryan et al., 2021). For this purpose, we recruited a diverse group of participants (n = 4) for the interviews, considering cybersecurity's interdisciplinary nature, as outlined in section 2.2.1. Each expert represents a different discipline related to cybersecurity, including Psychology, IT, Engineering, and Cybersecurity itself. LinkedIn was used to identify and invite potential experts by searching for keywords such as "smart-home" and "psychology." We contacted suitable experts and invited them to participate. Further details about the interviews and the interviewees can be found in Table 2.

Table 2

Conducted interviews and interviewee details

Interviewee	Discipline	Role	Language	Length	Format
P1	*Psychology*	PhD Psychology with experience in risk perception and human technology interaction.	English	78 min.	Teams
IT1	*IT*	Application manager with five years of experience in managing SHs.	Dutch	57 min.	Face-to-face
E1	*Engineering*	PhD candidate in Systems Engineering with six years of working experience as a privacy and security specialist in the IoT department of an electronics company.	English	75 min.	Teams
C1	*Cybersecurity*	Cybersecurity expert with seven years of working experience and specialized in IoT.	English	88 min.	Teams

3.2.3.2 Interview setup

We obtained consent from participants for recording the interview and assured them of their anonymity throughout the process. Additionally, we informed them about their voluntary participation rights, emphasizing their freedom to withdraw consent without the obligation to provide a reason.

As the CLD served as a boundary object, structuring the interview process, we gave a presentation about SD to familiarize experts with the approach and facilitate understanding (Diker, 2003; Andersen et al., 2012). Subsequently, the CLD was presented and explained step by step, while encouraging interruptions and feedback from the interviewees (Diker, 2003; Andersen et al., 2012). We decomposed the CLD into three separate models to facilitate comprehension, simplifying the interpretation for experts without SD experience (Andersen et al., 2012). To ensure clarity, textual information alongside diagrams is necessary. Therefore, we had transformed the feedback loops into statements, which were presented to the

interviewees. We asked them to confirm or falsify the statements and explain their choices (Luna-Reyes, 2004; Andersen et al. 2012).

Finally, we discussed the implications for the model structure, following validation criteria from Burns and Musa (2001). The discussion covered various aspects of the model, including clarity, causality existence, cause insufficiency, logic, additional variables, tautology, and the inclusion of intermediate variables. Specific questions guiding this discussion can be found in Appendix 1.3.

3.2.3.3 Analysis of interviews

We recorded the DIs and transcribed them using Microsoft Teams' transcribing function, with a double-check for consistency (Creswell, 2014). Following transcription, we employed the rigorously interpreted quotation (RIQ) method for analysing the DIs (Tomoaia-Cotisel et al., 2022). This method offers a formal and purposeful text analysis approach to enhance CLDs in late-stage conceptualization. By employing the RIQ method, we ensured a structured assessment of the accuracy of the findings, thereby improving both the validity and reliability of the analysis (Tomoaia-Cotisel et al., 2022). Relevant text from the DIs was extracted to an Excel table for ease of processing, encompassing columns for the expert abbreviation, their quotation, our interpretation, the causal chain (including arrow direction and polarity between variables), and an optional column for our interpretive notes. Phrases in the quotation that were deemed significant for the CLD were underlined. We ensured reliability through a consistent and transparent process (Tomoaia-Cotisel et al., 2022). Interview reports, including CLD modifications, were sent to the interviewees for member checking, ensuring the accuracy and validity of the processed results (Birt et al., 2016), which allowed for replication (Yin, 2009). Appendix 1 contains the complete interview guide.

3.2.4 Analysis of the causal loop diagram

The CLD analysis examined variables within the model based on their connections represented by positive (+) or negative (-) arrows, indicating cause-and-effect relationships (Meadows, 2008). Positive links signify that an increase (or decrease) in the cause variable leads to a corresponding increase (or decrease) in the effect variable, while negative links indicate an inverse relationship (Meadows, 2008). The final CLD was examined to identify feedback loops, revealing the system's behaviour (Egerer, 2021). These feedback loops are either reinforcing (R) or balancing (B). Reinforcing loops showed continuous increases or decreases within the

system, while balancing loops aimed to counteract changes and maintain stability (Xia et al., 2021). Analysing the CLD and its feedback loops gave a deeper understanding of the complex dynamics and interactions among CSRs in the SHES.

3.3 Research ethics

The research ethics, including details on preventing harm to participants, obtaining voluntary consent, and maintaining scientific integrity, can be found in Appendix 3.

4 Model construction

This chapter introduces the theoretical model constructed from the SSLR, accompanied by visual representations in the CLD. The refined model derived from the DIs is then discussed, followed by identifying and explaining the feedback loops.

4.1 Theoretical model

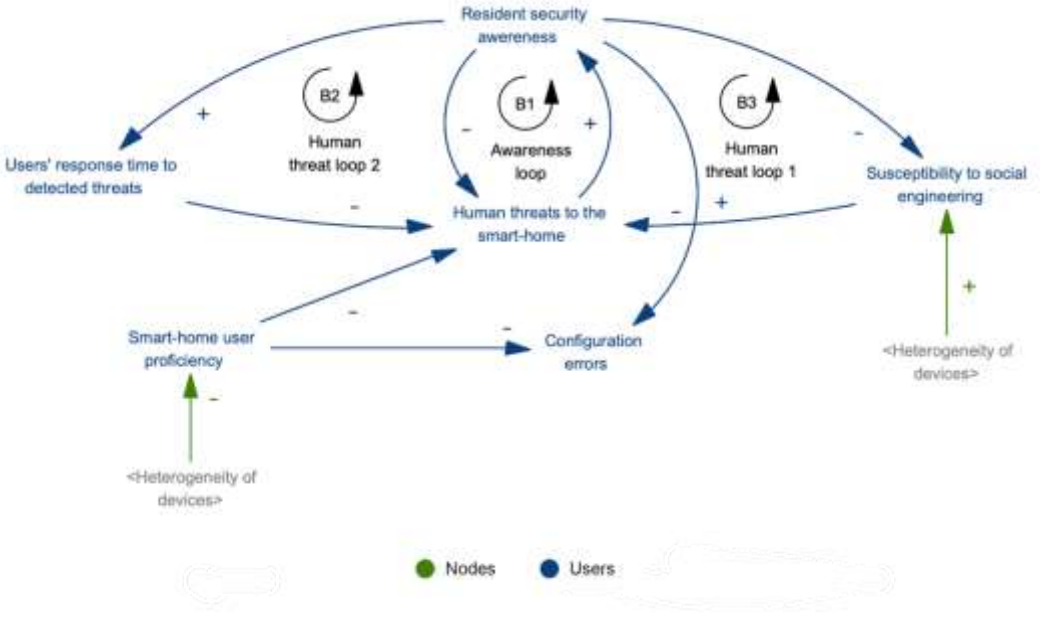
This section will explain all the elements of the theoretical model we have found in scientific papers and aggregated into an overall model. Each variable encompassing CSRs among the components of the SHES in the model will be explained, along with how it relates to other variables within the system. To aid understanding, distinct colours have been assigned to the components included in the legend of each figure.

4.1.1 Human behaviour in the smart-home

Human behaviour in the SH brings a challenge in ensuring security, as they are the weakest link in the security chain (Plachkinova & Menard, 2022). According to IBM (2015), over 95% of the security breaches in the SH can be attributed to human error. Users often lack the skills and knowledge to securely manage the SH (Douha et al., 2022). It is, therefore, crucial to address their influence on CSRs in the SHES. The human behaviour part of the theoretical model is shown in Figure 3 and will be explained in the subsequent paragraph.

Figure 3

Human behaviour in the smart-home



When users personally encounter human-like threats, it triggers a heightened sense of awareness regarding the importance of security measures and practices within their SHs (Li et al., 2023). This motivates users to become more proactive and informed about potential risks, contributing to an overall improvement in resident security awareness. The latter is critical in mitigating human threats to the SHES (Plachkinova & Menard, 2022). However, when users lack awareness regarding security in SHs, they are more likely to make assumptions, such as underestimating the likelihood of becoming a victim of a cyberattack, and, therefore failing to follow security protocols, increasing the human-like threats to the SH in the future (Kuyucu et al., 2019; Kadena & Gupi, 2021).

The lack of security awareness increases the susceptibility to successful social engineering attacks (Iqbal et al., 2020; Pillai & Helberg, 2021), in which humans instead of networks are targeted. In these attacks, adversaries try to manipulate humans psychologically in order to extract sensitive information (Haseeb-ur-Rehman et al., 2022). The heterogeneity of devices causes easier exploitation of social engineering attacks, as the wide variety of SH devices with different purposes and user profiles provides adversaries a higher attack vector (Yang & Sun, 2022). When people become susceptible to social engineering, human threats to the SH will increase as the potential for unauthorized access increases.

The level of security in the SHES is influenced by users timely updating their devices in response to detected threats. This proactive action mitigates human threats to the SH (Batalla & Gonciarz, 2019). When users are more aware of potential security threats, it is assumed that they will respond more quickly to detected threats, as they are better informed about the risks, which results in proactive behaviour (Plachkinova & Menard, 2022).

The SH network is typically installed and understood by a single resident, leading to a lack of proficiency among other residents (Piasecki et al., 2021). This knowledge gap increases human threats to the SH, as addressing security issues, performing updates, or responding to threats becomes challenging when the knowledgeable resident is unavailable. Consequently, the SH system becomes more vulnerable to unauthorized access, breaches, and misuse by malicious individuals (Piasecki et al., 2021). The heterogeneity of devices further reduces SH user proficiency, as users may struggle to locate and navigate controls (Philip et al., 2023). This decrease in proficiency contributes to configuration errors, which are mistakes or issues that occur during network setup or device configuration (Batalla & Gonciarz, 2019; Widjaja et al., 2022). Resident security awareness plays a role in mitigating configuration errors, yet users often lack awareness and are more prone to make such errors (Widjaja et al., 2022). Common

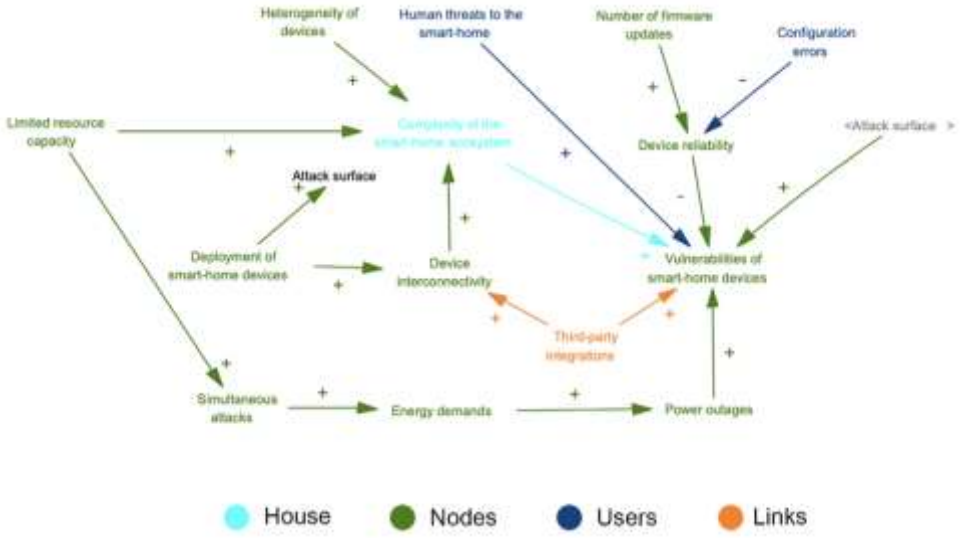
configuration errors include using default passwords, infrequent password changes, or neglecting software updates (Allifah & Zualkernan, 2022).

4.1.2 Vulnerabilities in the smart-home

Vulnerabilities in the SH can arise directly from six factors and are shown in Figure 4 below. Each variable and its relationship will be explained in the subsequent paragraph.

Figure 4

Vulnerabilities in the smart-home



First, the SHES's complexity, resulting from interconnectivity and deploying numerous interconnected devices with limited resources and high heterogeneity, contributes to these vulnerabilities. The limited resource capacity, encompassing factors such as low computational power or memory storage, introduces challenges in managing and securing the devices (Abbas et al., 2021; Shaukat et al., 2021). Additionally, SH devices are heterogeneous regarding hardware, software and protocols (Anthi et al., 2019), as manufacturers use their own standards to produce SH devices, resulting in high fragmentation (Yang & Sun, 2022). Furthermore, the variety of appliances and products with different purposes also give rise to a high degree of heterogeneity (Kuyucu et al., 2019), due to the multiple architectures (Yu et al., 2020). Finally, the last variable influencing the SHES's complexity is the increased deployment of devices. This gives rise to more interconnectivity, which is also amplified by the integration of third-party services, of various devices, services, and platforms through seamless communication, which creates intricate relationships and dependencies (Anthi et al., 2019; Yamauchi et al., 2020; Kavallieratos et al., 2019).

The latter is the second contributor to vulnerabilities, as third-party integrations introduce additional vulnerabilities due to the potential for security weaknesses in the integrated services (Lyu et al., 2019; Allifah & Zualkernan, 2022).

The third contributor is an increased attack surface due to the exponential deployment of devices which gives adversaries more entry points for their malicious activities (Yamauchi et al., 2020), and raises the likelihood of vulnerabilities within the system (Kavallieratos et al., 2019).

Fourth, the device reliability affects the SH device vulnerabilities, as unreliable devices are prone to vulnerabilities, influenced by the frequency of firmware updates and configuration errors. Insufficient firmware updates expose devices to unpatched vulnerabilities, allowing ongoing exploitation of security weaknesses (Huraj et al., 2020; Abbas et al., 2021). Configuration errors also increase vulnerabilities, for instance due to weak credentials (Widjaja et al., 2022).

The fifth factor is power outages, caused by distributed denial-of-service (DDoS) attacks, which the devices are vulnerable to due to the limited resource capacity (Huraj et al., 2020). DDoS attacks involve a simultaneous and overwhelming flood of requests or traffic, which can exhaust the devices and disrupt their normal functioning. In SHs, these attacks can have further implications, as they can cause sudden spikes in energy demands, potentially overloading the power supply systems, resulting in power outages (Yamauchi et al., 2020). Consequently, these power outages can disrupt the regular operation of SH devices, affecting their functionality and making them temporarily unusable, leading to potential vulnerabilities in the SH (Subhita et al., 2023).

And sixth, the number of human-like threats increase the overall vulnerabilities in SH devices. An example is the earlier mentioned susceptibility to social engineering attacks that increase human threats to the SH as users inadvertently disclose sensitive information, which adversaries exploit for malicious purposes (Haseeb-ur-Rehman et al., 2022).

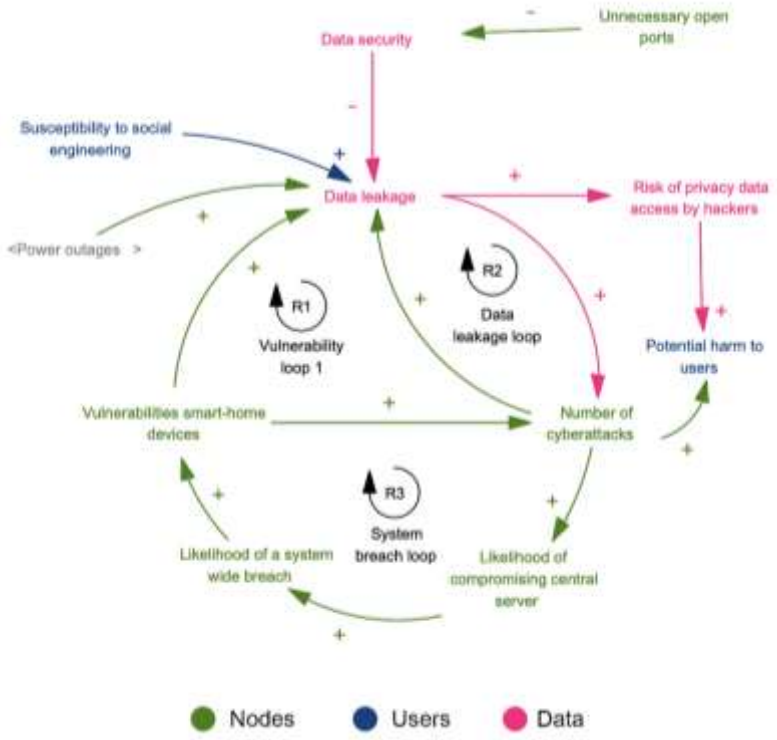
4.1.3 Threats in the smart-home

All the above-described factors contributing to vulnerabilities can be exploited by adversaries, thereby creating threats and increasing the potential for cyberattacks (Iqbal et al., 2020). The SHES is vulnerable to a wide range of various cyber threats, including unauthorized access, malware infiltration, impersonation, and data breaches. These are collectively described as *cyberattacks* to keep the model readable and maintain its usefulness. However, social

engineering and DDoS attacks are considered separately due to their frequent occurrence in the literature and the association of social engineering with the user component. The threats in the SH are shown below in Figure 5, and subsequently their behaviour is explained.

Figure 5

Threats in the smart-home



Besides vulnerabilities in SH devices, hackers can also exploit data leakage to launch cyberattacks. Data leakage results from four factors, including vulnerabilities, human factors, power outages and poor data security. First, data leakage resulting from vulnerabilities in SH devices (Park et al., 2019), enable adversaries to exploit for various cyberattacks. For instance, side-channel attacks can lead to additional data leakage through various channels within the system, enabling adversaries to exploit the leaked data and uncover meaningful patterns of correlation between events and communication nodes (Hameed et al., 2022; Nassiri Abrishamchi et al., 2022). This can result in adversaries obtaining sensitive private data for malicious purposes. For example, if a side-channel attack manages to obtain a SH's internal temperature data and operational parameters of the lighting system, this information could be used to deduce the presence of occupants, presenting a risk of burglary (Wang & Zhang, 2021). Second, human factors contribute to data leakage via the susceptibility to social engineering attacks. Third, power outages can result in data loss as devices may shut down abruptly, causing

data corruption or loss (Liu et al., 2021). And fourth, poor data security causes data loss. Since the SHES hold personal information about their residents, it is critical to have good data security to prevent data from leaking (Park et al., 2019). The presence of unnecessary open ports within the SHES can undermine data security by extracting or manipulating sensitive information (Eze et al., 2022). When data gets leaked, the risk of privacy information access increases, eventually resulting in potential harm to residents (Park et al., 2019).

Furthermore, the centralized nature of SHs makes the central server a potential target for cyberattacks. The more cyberattacks are launched, the higher the probability the central server gets compromised (Arif et al., 2020). This interconnected nature of the devices to the central server makes the SH only "*as strong as its weakest link*" (Morgan et al., 2022: 2). When the central server gets compromised, the likelihood of a system-wide breach increases because all devices are connected to the central server and, are, therefore, susceptible to cyberattacks on different devices. A system-wide breach may reveal additional vulnerabilities in the devices, reinforcing the existence of vulnerabilities in SH devices (Arif et al., 2020).

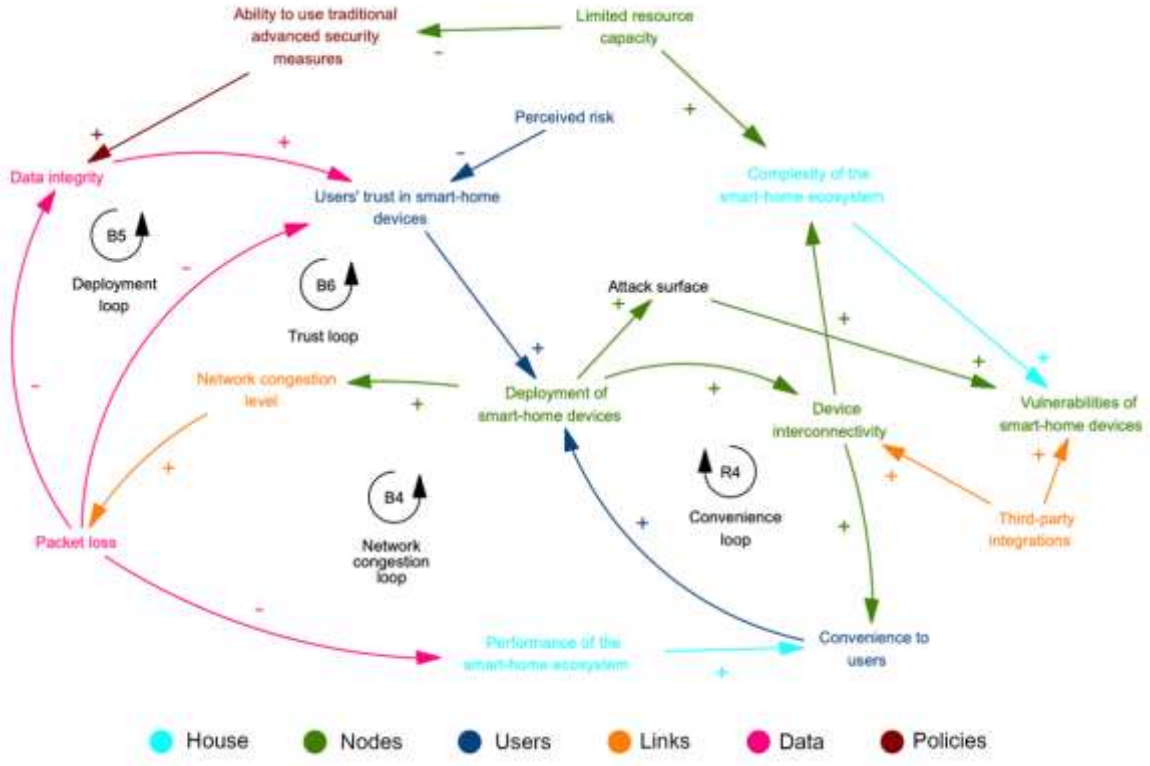
The consequences of all these cyberattacks can impact residents lives in various ways. These attacks pose various risks, including hardware damage, psychological impacts on privacy, financial losses, reputational damage, and even physical breaches of privacy by unauthorized entry into individuals' homes (Hall et al., 2020; Huraj et al., 2020; Abbas et al., 2021).

4.1.4 Deployment of smart-home devices

The relationship between the number of SH devices in use and the number of vulnerabilities and threats in the SH is interconnected. The relationships between the variables influencing the deployment part are shown below in Figure 6. Subsequently their behaviour will be explained.

Figure 6

Deployment of smart-home devices



The interrelationships between the variables: deployment of SH devices, interconnectivity, vulnerabilities, limited resource capacity, and attack surface have been previously addressed in sub-section 4.1.2. A detailed repetition of these discussions will not be provided here to avoid redundancy.

Due to the interconnectivity, users will experience more convenience (Flores et al., 2022), which influence their intention to expand their SH network with more devices (Shuhaiber & Mashal, 2019). However, the proliferation of devices within SHs can result in network congestion and subsequent packet loss (Liping & Liding, 2020; Sharma et al., 2023). Packet loss occurs when some data packets during transmission between devices within the SH network do not reach their intended destination (Sharma et al., 2023). This can lead to lower performance in the SH, a decrease in data integrity and lower user trust in SH devices. First, missing or incomplete data packets disrupt the smooth flow of communication and result in delays, errors, or inconsistencies in device operations and interactions (Liping & Liding, 2020), decreasing the overall SHES performance (Guan & Choi, 2021), thereby leading to inconvenience to the user. Second, as packet loss potentially leads to inaccuracies or distortions

in the received information, it undermines the assurance that the transmitted data accurately reflects the intended content as intended by the user, decreasing the integrity of the data (Minoli, 2020). Third, packet loss also influences users' trust in SH devices as it creates a perception of unreliability, raising concerns about the overall dependability of the devices (Lo & Niang, 2020).

Additionally, the limitations in computational power and storage capacities of devices, makes it difficult to implement traditional advanced network security measures (Nandy et al., 2019; Batalla & Gonciarz, 2019; Arif et al., 2020; Cvitic et al., 2022; Allifah & Zualkernan, 2022), which compromises the integrity of the data in the SH (Salimitari et al., 2020).

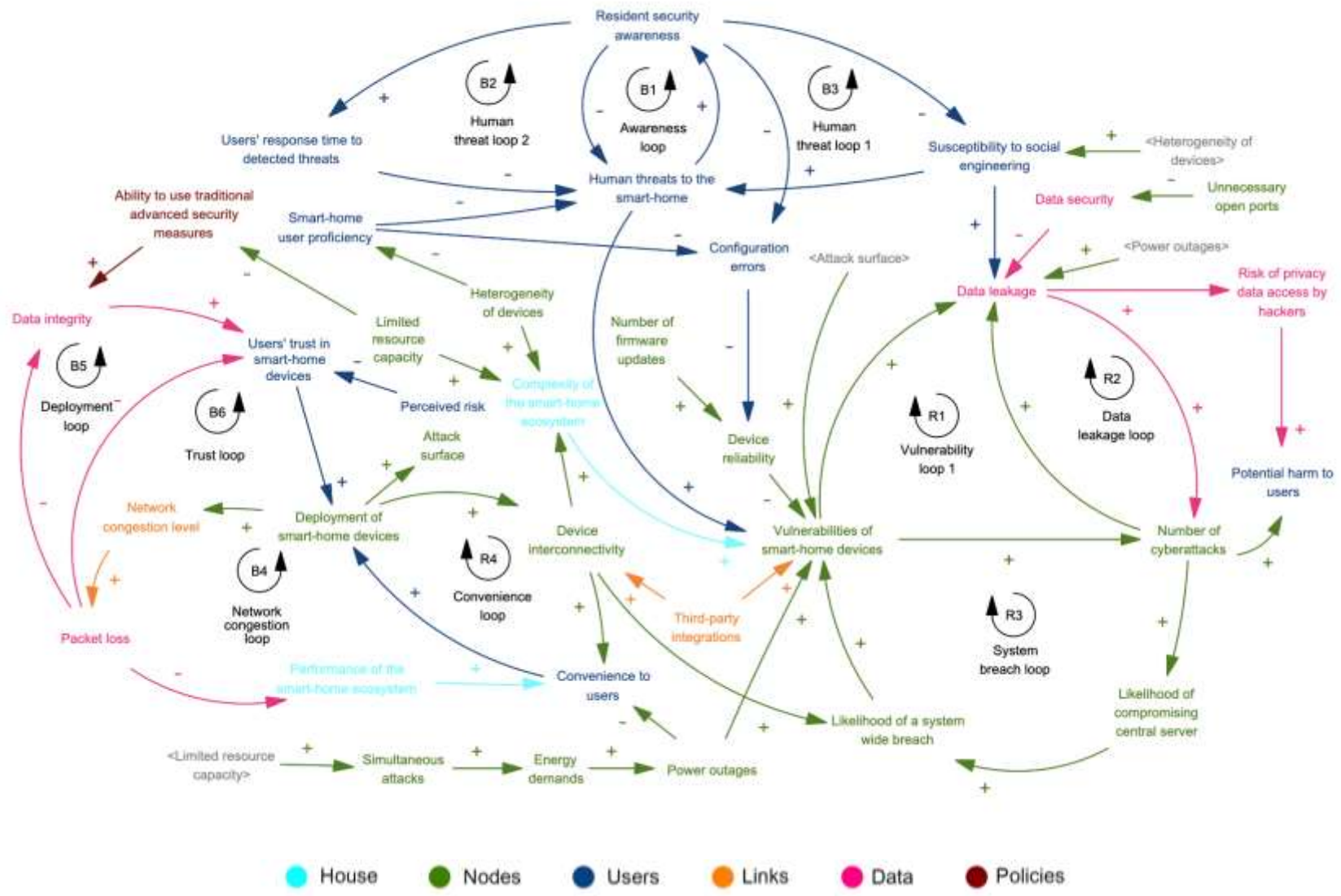
Moreover, the perceived security and privacy risks significantly impact users' trust in SH devices, and subsequently influences their intention to deploy fewer SH devices (Shuhaiber & Mashal, 2019; Cannizzaro et al. 2020; Li et al., 2021).

4.1.5 Aggregated theoretical model

The comprehensive model in Figure 7 integrates all the previously discussed elements of the theoretical model and integrates each component of the SHES.

Figure 7

Aggregated theoretical model



4.2 Refined model after validation and modification

This chapter presents the refined model validated through the DIs. The modifications made in the model are associated with specific experts, represented by abbreviations for easy referencing: P1 (Psychologist), C1 (Cybersecurity Expert), E1 (Engineer), and IT1 (Application Manager).

4.2.1 Shifting human threats to human vulnerabilities

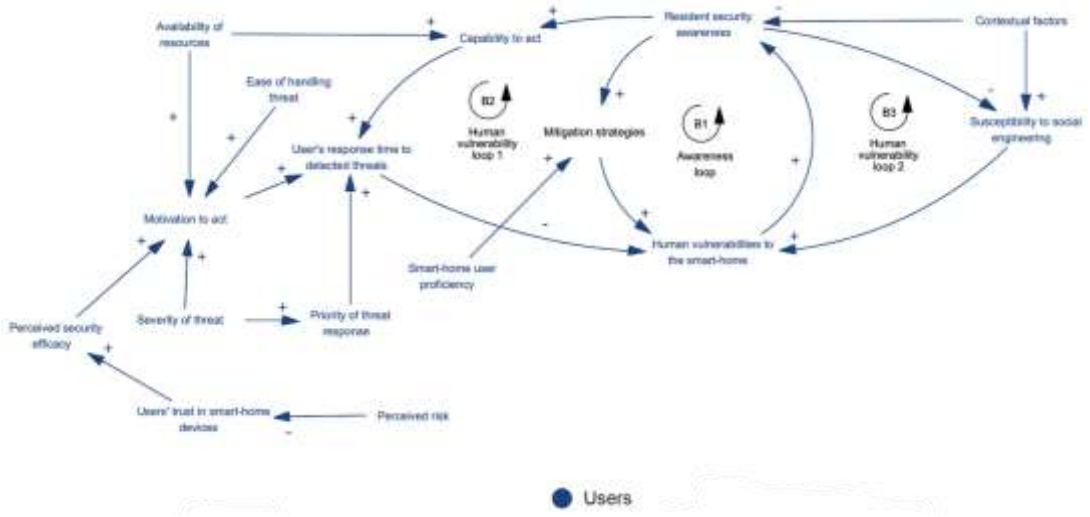
According to IT1, the term *human threats to the smart-home* may not accurately reflect the nature of the issue. Considering the example of user response time to detected threats, it became apparent that *human vulnerabilities to the smart-home* is more appropriate in this context. By not reacting promptly to potential threats, the vulnerabilities of human behaviour increase. This indicates that it is not necessarily the presence of human threats but rather the existence of human vulnerabilities that are more relevant in the CLD. As a result, we have substituted *human threats* for *human vulnerabilities to the SH*.

4.2.2 Human factors influencing users' motivation to act

After undergoing validation, the human behaviour aspect of the model revealed the absence of certain crucial variables. As a result, we have refined the structure of the model, as illustrated in Figure 8. The subsequent section will explain each modification.

Figure 8

Refined human behaviour part of the model



While recognizing human vulnerabilities to the SH is an essential first step, it does not guarantee the motivation to take appropriate action, as noted by all respondents. The presence of intermediate variables crucial for effective mitigation were lacking. One important variable is the relationship between awareness and mitigation strategies, as highlighted by E1. When users are aware of potential vulnerabilities, they are more likely to seek ways to mitigate them and apply appropriate strategies. Therefore, this increases the capability to act, as noted by P1. However, these strategies' effectiveness depends on the user's proficiency in managing the SH. If users lack the necessary knowledge or understanding to apply these strategies, their ability may be limited, as mentioned by E1.

P1 highlighted that the motivation to act depends on factors such as the ease with which the threat can be addressed and the convenience of taking action. It is also influenced by the availability of appropriate tools and resources, according to P1 and IT1, including those provided by third-party entities like manufacturers. In some instances, manufacturers may fail to release necessary updates to counter detected threats or even provide the ability to get insights into a threat, thereby limiting the ability to take action effectively.

Additionally, P1 mentioned other contributing factors such as the priority assigned to the task. For instance, if someone is working from home and already occupied with specific responsibilities, their response to a detected threat may not be immediate. Similarly, if individuals perceive the detected threat as less severe, they are likely to prioritize other tasks over responding to the threat, decreasing their motivation to act.

Furthermore, P1 highlighted that a lack of trust towards SH devices leads to a diminished sense of security and reliability associated with SH devices. When users lack trust, they tend to question the effectiveness of the security measures implemented by the devices and manufacturers. This can result in a lack of motivation to proactively engage in security behaviours or follow recommended security practices they are taught to. Therefore, this can slow down the response time to detected threats, eventually increasing the human vulnerabilities to the SH.

In light of this feedback, we have added the following variables and relationships to the model: *mitigation strategies, capability to act, availability of resources, ease of handling threat, severity of threat, priority of threat response, motivation to act* and *perceived security efficacy.*

For the susceptibility to social engineering techniques, P1, C1, and IT1 made evident that various contextual factors come into play, affecting both resident security awareness and susceptibility to social engineering tactics. It is essential to acknowledge that, at times, avoiding social engineering attempts can be very hard. Even if an individual possesses awareness, factors

such as fatigue or a high workload can lower their vigilance, consequently impacting their ability to apply previously acquired knowledge and avoid falling prey to malicious tactics. In light of this feedback, we have added *contextual factors* to the model. This variable stands symbolically as an umbrella term incorporating influential elements, such as fatigue and inadvertence, which impact an individual's capacity to recognize and resist social engineering.

4.2.3 Classification of cyberattacks

During the interviews, several types of attacks were discussed. The model initially considered three types of attack variables: the umbrella term *cyberattacks*, *social engineering attacks*, and *simultaneous attacks* (DDoS attacks). However, it should be noted that numerous other cyberattacks cannot all be individually included in the model due to the sheer number of types of attacks. Therefore, we have omitted the *simultaneous attacks* variable. To ensure equal representation and avoid minimizing any specific cyberattacks, it was advised by P1 to categorize all cyberattacks under the variable *number of cyberattacks*. This approach eliminates the potential for downplaying or overshadowing any type of cyberattack, except for social engineering attacks, which we kept treating as a distinct category. This separation is necessary because social engineering attacks involve the active participation of users, who are considered an independent component within the system.

4.2.4 Perceived usefulness

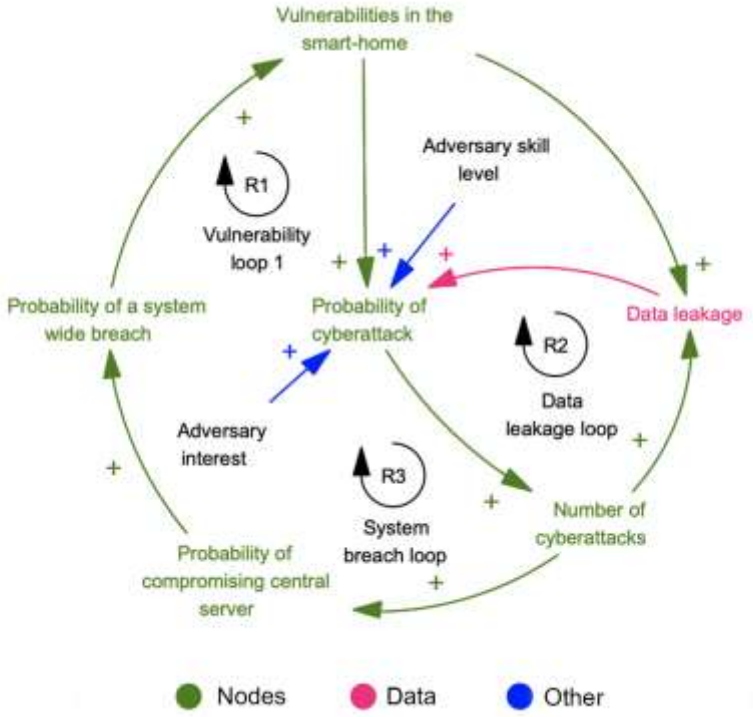
In response to P1's advice, replaced the variable *convenience* with *perceived usefulness*. This change in perspective highlights the subjective perception of the benefits and value provided by SH devices, rather than solely emphasizing convenience. By considering perceived usefulness, we acknowledge the importance of users' evaluation of the usefulness of SH devices, which influences intention to deploy more devices.

4.2.5 Adversary behaviour

In response to the advice of P1, we have decided to include adversary behaviour in the model. Despite not belonging directly to one of the components, it was strongly advised because of its significant impact on the system. The new structure influencing the threat part of the model is shown below in Figure 9, and, subsequently, its modification will be explained.

Figure 9

Refined vulnerabilities part of the model including adversary behaviour



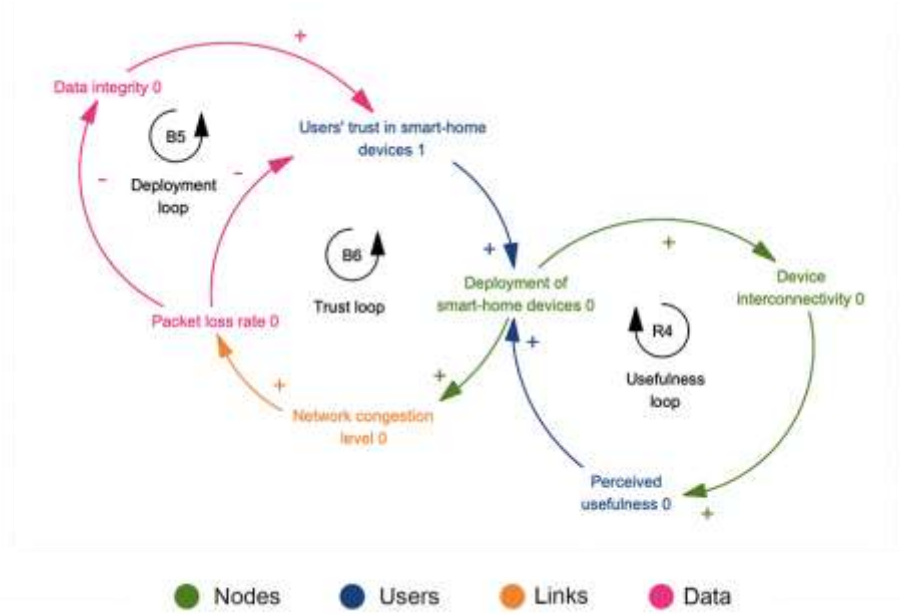
Adversary behaviour, characterized by opportunism, plays an important role in exploiting vulnerabilities, leading to increased attacks. It is important to note that vulnerabilities alone do not necessarily increase attacks. Moreover, the opportunistic nature of attackers is further influenced by the presence of hype surrounding a particular attack, which can increase the attractiveness for adversaries. If adversaries know that there is an increase in the use of specific SH devices, this will increase their interest. Similarly, the experience of the adversary increases the probability of a cyberattack. To capture this dynamic, it was advised to incorporate a probability variable before the actual cyberattack variable, as factors influence this probability. However, if the probability is zero, it signifies that no cyberattacks will occur. To address these insights, we have added the following variables to the model: *probability of a cyberattack, adversary skill level* and *adversary interest.*

4.2.6 Performance of the smart-home ecosystem

In response to E1's and IT1's insights, we have adjusted the model by deleting the performance of the SHES variable to enhance the focus of the analysis. The new structure is shown below in Figure 10, and, subsequently, the reasons for omission are explained.

Figure 10

Refined deployment part of the model



The relationship between the deployment part of the model, and security/privacy, which interviewee E1 did not recognize, has been considered. Consequently, we have omitted the variable *performance of the smart-home ecosystem*, as it does not directly influence behavioural changes that contribute to cybersecurity risks, which IT1 also mentioned. Moreover, its exclusion was also based on the assumption of its structure, explained in Appendix 5.

Despite E1's perspective that there is no relationship between *convenience* and security, we have decided to retain the variable convenience in the model. This decision is based on the recognition that both convenience and the new variable *perceived usefulness* contribute to a reinforcing loop that ultimately increases the attack surface, making it a significant contributor to CSRs.

Additionally, feedback loops B5 and B6, associated with the deployment of devices, have been maintained in the model. These loops are crucial as they cause behavioural changes that contribute to CSRs, particularly within the human behavioural aspects of the model.

4.2.7 Interoperability challenges

IT1 suggested that the *heterogeneity of devices* does not directly create complexity. It is argued that different device protocols and functionalities lead to interoperability challenges. These challenges, in turn, contribute to the overall complexity of the SHES. Therefore, we have added

interoperability challenges between device heterogeneity and system complexity according to IT1's perspective.

4.2.8 Open ports increase the attack surface

Based on the advice of IT1, we have changed the relationship of unnecessary open ports from data security to the attack surface. An open port on the Internet serves two key purposes: it acts as an entry point for external devices to connect with one's own devices within the SH, and it also serves as an entry point for adversaries. As a result, the impact of unnecessary open ports is more closely associated with the attack surface rather than directly affecting data security.

4.2.9 Data security principles

Initially, data security was considered as a mitigating factor for data leakage. However, based on the clarification provided by C1, *data security* is an overarching term of the CIA triad, which includes *data confidentiality*, *integrity*, and *availability*. In light of this feedback, we have replaced data security with data confidentiality, aligning it with our intended use. Regarding data availability, which ensures uninterrupted access to required data for authorized users, it was initially included in the model as an intermediate variable between packet loss and the performance of the SHES. However, following the omission of the performance of the SHES variable based on IT1's and E1's feedback, we have also excluded data availability from the model. Data integrity was already included in the model and has remained unchanged.

4.3 Suggested modifications outside the model boundary

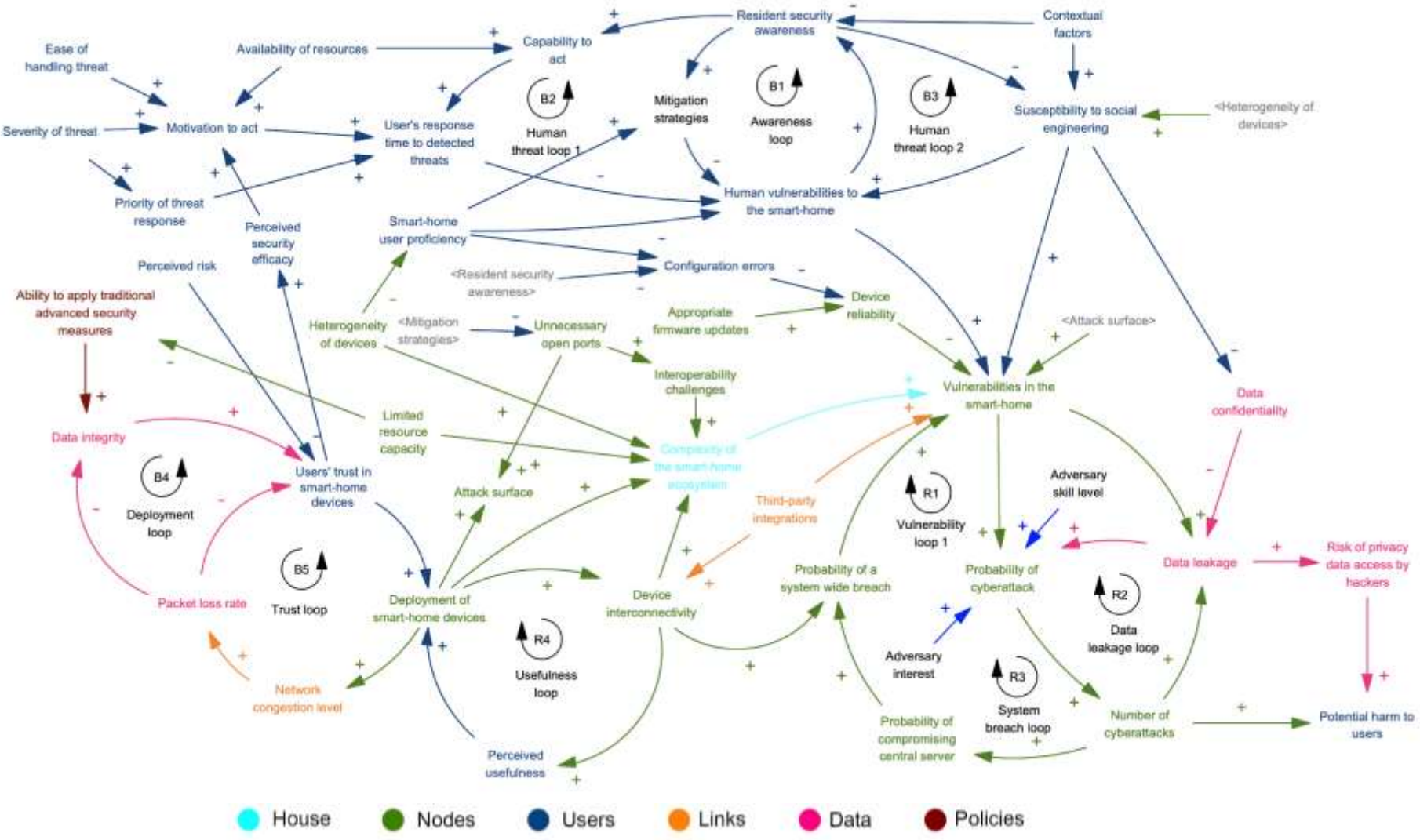
It is important to note that we have only incorporated modifications within the model's boundary, with one exception as described in 4.2.5. The suggestions from experts that have been omitted can be found in Appendix 4.

4.4 Final model

Figure 11 represents the final validated model after undergoing the validation process.

Figure 11

Final model after interviews



4.5 Loop identification

The final model contains five balancing and four reinforcing loops. The loops including its behaviour and their significant effect on CSRs in the SHES are thoroughly explained in Appendix 6.

5 Conclusion

This chapter discusses the interpretation of the results to address the central research question, research limitations, a reflection on the researchers' role, the contribution of the findings to existing knowledge, and ultimately the practical implications.

5.1 Interpretation of the results

The study aimed to identify and analyse CSRs in the SHES by building a CLD. We have gathered initial input through a SSLR, and subsequently conducted DIs with experts from different disciplines to validate and modify the theoretical model. Sub-questions were addressed in the model construction Chapter 4, to answer the central question:

'To what extent do the interdependencies among the components of a smart-home ecosystem contribute to the cybersecurity risks within the smart-home?'

Four main contributing factors to CSRs in the model were found. First, human behaviour was identified as an important contributing factor to CSRs. Security unawareness has severe consequences, as it is linked to three balancing loops (B1, B2 & B3), increasing the human vulnerabilities to the SHES. Security unawareness interacts with the capability to act, susceptibility social engineering and mitigation strategies, and can lead to data leakage, vulnerabilities, and subsequent cyberattacks, exposing users to the potential harm of these attacks. Users become susceptible to social engineering attacks through unawareness, the heterogeneity of devices and contextual factors, like fatigue. The motivation to act is important because it dictates the response time to detected threats and is mainly influenced by cognitive aspects, such as the ease of handling a threat and the perceived severity of the threat.

The deployment aspect of the model in the SHES involves two balancing loops (B4 & B5) and one reinforcing loop (R4), which indirectly contribute to CSRs. These loops negatively impact users' trust, reducing the perceived efficacy of security measures and diminishing the motivation to respond promptly to threats. As a result, adversaries find opportunities to exploit the compromised SH environment due to a lack of effective barriers. The reinforcing loop leads to an increased number of deployed devices driven by the perceived usefulness of

interconnectivity, which in turn, increases the attack surface and provides more entry points for adversaries.

Furthermore, seven interconnected variables were identified to directly contribute vulnerabilities within the SHES, enabling exploitable threats for adversaries. These threats primarily stem from vulnerabilities but also exploit data leakage. Adversaries' behaviour, such as their interest and skill level, further reinforces these threats. The increasing number of cyberattacks heightens the likelihood of a system-wide breach by compromising the central server, exposing threats to all SH devices connected to the central server and amplifying vulnerabilities. This behaviour is reinforced by three reinforcing loops (R1, R2, & R3), emphasizing the need for proactive security measures.

The analysis of the final CLD revealed the significant role of interdependencies among the components of a SHES in contributing to CSRs within the system. This study challenged the conventional technical perspective on SH cybersecurity and demonstrated the effectiveness of SD in capturing interdependencies and understanding CSRs among the components in SHESs, by integrating technical and behavioural disciplines. While the empirical examination focused on validating the CLD rather than establishing empirical links, the study underscores the importance of a comprehensive approach to protect SH users' privacy and security. Understanding the interconnected factors influencing CSRs enables the development of effective strategies to mitigate risks and promote a secure SHES.

5.2 Knowledge contribution

As indicated in Chapters 1 and 2, there was a noticeable lack of comprehensive understanding regarding the interdependencies among different components of SHESs that contribute to CSRs. Given that CSRs involve a multitude of interconnected variables that influence one another (Khan et al., 2022), it became evident that a new approach considering the interconnected nature of the SHES was necessary (Bugeja et al., 2020; Heiding et al., 2023). While several studies were conducted examining CSRs in SHs, they focused on singular devices or individual components, instead of giving a complete picture of how the interrelated components interact with one another (Abdullah et al., 2019; Darem et al., 2022). This study addressed this gap in the literature by constructing a CLD to provide a thorough understanding of the CSRs resulting from interdependencies among the components within the SHES. The CLD proved to be a valuable tool for unravelling the complex dynamics and feedback loops that impact CSRs in SHs. Additionally, this study made a significant contribution by adopting

an interdisciplinary approach that integrated all SHES components into a unified model. The model was subsequently validated through collaboration with disciplines such as psychology, IT, engineering, and cybersecurity, confirming the accuracy. This interdisciplinary approach bridges gaps between disciplinary boundaries and recognizes the importance of human behaviour, system design, and technological vulnerabilities in shaping CSRs within the SH environment. These findings align with the notion by Ye et al. (2020) that integrating multiple disciplines is crucial for effectively addressing CSR challenges in SHESs, as they illustrate how the interconnected components collectively contribute to CSRs.

5.3 Practical/managerial implications

From a practical perspective, the findings of this study have implications for various stakeholders involved in the design, development, deployment, and management of SH systems. Raising awareness among SH users about CSRs and promoting best practices for secure behaviour can mitigate vulnerabilities stemming from human behaviour. To achieve this, user-friendly interfaces, clear instructions, and educational resources should be provided, empowering and motivating users to make well-informed decisions and appropriately safeguard their SHES. Manufacturers also play a crucial role by acknowledging the interconnected nature of devices and prioritizing security measures that address the identified vulnerabilities. Policymakers hold the responsibility to establish clear guidelines and regulations on SHES security, which may include mandatory security standards for manufacturers to adhere to, ensuring that security measures across different devices are more generalizable and can be built upon.

5.4 Reflection on my role as a researcher

One important consideration was creating a comfortable and open atmosphere during the DIs, which aimed to build trust and encourage interviewees to provide reliable and insightful responses. From my perspective, trust was successfully established during the interviews, allowing for a more reliable exchange of information. Furthermore, regarding the subject of study, it is important to acknowledge that this was not within the researcher's domain expertise, this may have led to the unintentional omission of relevant information during the SSLR.

6 Discussion

6.1 Limitations

In this research, our initial goal was to validate the theoretical model through Group Model Building (GMB) sessions. These sessions would have allowed active participation from multiple stakeholders, across diverse disciplines within the cybersecurity field, to integrate their perspectives and generate consensus about the causes of CSRs in SHESs, which are subject to different interpretations across disciplines (Vennix, 1996; Eker & Zimmerman, 2018). Instead of conducting individual DIs, our intention was to bring together representatives from various disciplines simultaneously, fostering more discussions between them (Vennix, 1996). Unfortunately, due to logistical constraints, we were unable to conduct GMB sessions, resulting in the inability to gather input from experts simultaneously, potentially limiting the validity and confidence in the CLD.

The second limitation arises from the number of respondents for the DIs. Although we have tried recruiting additional participants, the small sample size of four participants ($n = 4$) limits the findings' reliability. It is important to acknowledge that prioritization of diverse voices is more important than solely focusing on the number of interviews (Myers, 2019). This study addressed this concern by integrating experts from four different disciplines. However, not all disciplines interrelated with cybersecurity were integrated in the DIs.

Additionally, during one of these DIs, expert E1 had to leave abruptly due to time constraints, resulting in an incomplete interview. The CLD was presented and discussed, but the remaining statements and questions were not addressed. To ensure the completeness of the data, we sent the outstanding statements and questions E1 via email, as per their request, due to a busy schedule. This would have allowed the continuation of the interview process, although it would have introduced a limitation in capturing social cues that contribute to a complete understanding of the participant’s perspective (Hawkins, 2018; Fritz & Vandermause, 2017). Unfortunately, we did not receive a response from E1, potentially leading to missed insights on the engineering aspects of the CLD.

Furthermore, as a model boundary has to limit the scope of the model to keep it useful (Sterman, 2000), the focus of this study was specifically on CSRs and the interactions between the components of the SHES. However, some external factors are involved in the contribution to CSRs, such as laws and regulations and the broader socio-political environment. This is

another limitation, as the study did not consider these external factors and their influence on CSRs in the SHES.

Although this study has encountered some limitations, it is noteworthy as the first comprehensive exploration of the CSRs related to the components in the SHES. While the results should be interpreted cautiously, they offer valuable insights and serve as a solid foundation for further investigation.

6.2 Future research directions

A promising avenue for future researchers lies in validating the final model through GMB sessions involving experts from various disciplines interrelated with cybersecurity. This collaborative approach allows for the elicitation of additional information from stakeholders with diverse backgrounds, enhancing the comprehensiveness and validity of the model (Eker & Zimmerman, 2018). To gain a further understanding of the SHES's dynamic behaviour in different scenarios, future studies can quantify the final CLD, or the validated CLD from the potential GMB sessions, enabling simulation and analysis for the development of robust strategies (Vennix, 1996). However, some of the variables in the final CLD are hard to measure, such as SH complexity, perceived usefulness, and contextual factors due to their multidimensional characteristics that encompass various interrelated aspects. In such cases, simulating specific parts of the CLD can serve as a reference mode of behaviour, aiding experts in policy development, ideally during GMB sessions (Vennix, 1996). Furthermore, researchers have the opportunity to refine the CLD by further examining specific aspects and breaking down components into smaller fragments. For example, conducting an independent study on human factors in SHES cybersecurity can offer a more detailed understanding of the cognitive and behavioural aspects that shape human behaviour in this context. This deeper understanding can aid in designing user-centric security measures. By creating a separate CLD that specifically examines the cause-effect relationships related to the user component, valuable insights into the complexity of human behaviour can be gained, thereby complementing the existing CLD.

References

Abbas, S. G., Vaccari, I., Hussain, F., Zahid, S., Fayyaz, U. U., Shah, G. A., Bakhshi, T., & Cambiaso, E. (2021). Identifying and Mitigating Phishing Attack Threats in IoT Use Cases Using a Threat Modelling Approach. *Sensors*, 21(14). https://doi.org/10.3390/s21144816

Abdullah, T. A., Ali, W., Malebary, S., & Ahmed, A. A. (2019). A review of cyber security challenges attacks and solutions for Internet of Things based Smart Home. *Internet Journal of Computer Science and Network Security* 19(9), 139.

Abomhara, M., & Køien, G. M. (2015). Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security and Mobility*, 65-88.

Agnew, S., Smith, C., & Dargusch, P. (2018). Causal loop modelling of residential solar and battery adoption dynamics: a case study of Queensland, Australia. *Journal of Cleaner Production*, 172, 2363–2373. https://doi.org/10.1016/j.jclepro.2017.11.174

Aheleroff, S., Xu, X., Lu, Y., Aristizabal, M., Velásquez, J. P., Joa, B., & Valencia, Y. (2020). IoT-enabled smart appliances under industry 4.0: A case study. *Advanced engineering informatics*, 43, 101043.

Ahmad, R., & Alsmadi, I. (2021). Machine learning approaches to IoT security: A systematic literature review. *Internet of Things*, 14, 100365.

Ali, B., & Awad, A. I. (2018). Cyber and physical security vulnerability assessment for IoT-based SHs. *Sensors*, 18(3), 817.

Alirezaei, M., Onat, N. C., Tatari, O., & Abdel-Aty, M. (2017). The climate change-road safety-economy nexus: a system dynamics approach to understanding complex interdependencies. *Systems*, 5(1), 6.

Allifah, N. M., & Zualkernan, I. A. (2022). Ranking Security of IoT-Based Smart Home Consumer Devices. *IEEE Access*, 10, 18352-18369. https://doi.org/10.1109/ACCESS.2022.3148140

Andersen, D. L., Luna-Reyes, L. F., Diker, V. G., Black, L., Rich, E., & Andersen, D. F. (2012). The disconfirmatory interview as a strategy for the assessment of system dynamics models: D. L. Andersen et al.: The Disconfirmatory Interview. *System Dynamics Review*, 28(3), 255-275. https://doi.org/10.1002/sdr.1479

Ansar, S. A., Jaiswal, K., Aggarwal, S., Shukla, S., Yadav, J., & Soni, N. (2022, May). Smart Home Personal Assistants: Fueled by Natural Language Processor and Blockchain Technology. *In 2022 Second International Conference on Interdisciplinary Cyber Physical Systems* (ICPS) (pp. 113-117). IEEE.

Anthi, E., Williams, L., Slowinska, M., Theodorakopoulos, G., & Burnap, P. (2019). A Supervised Intrusion Detection System for Smart Home IoT Devices. IEEE *Internet of Things Journal*, 6(5, SI), 9042-9053. https://doi.org/10.1109/JIOT.2019.2926365

Arabo, A. (2015). Cyber security challenges within the connected home ecosystem futures. *Procedia Computer Science*, 61, 227-232.

Arif, S., Khan, M. A., Rehman, S. U., Kabir, M. A., & Imran, M. (2020). Investigating Smart Home Security: Is Blockchain the Answer? *IEEE Access*, 8, 117802-117816. https://doi.org/10.1109/ACCESS.2020.3004662

Ayavaca-Vallejo, L., & Avila-Pesantez, D. (2023). Smart Home IoT Cybersecurity Survey: A Systematic Mapping. *In 2023 Conference on Information Communications Technology and Society (ICTAS)* (pp. 1-6). IEEE.

Azam, N., Michala, L., Ansari, S., & Truong, N. B. (2022). Data Privacy Threat Modelling for Autonomous Systems: A Survey from the GDPR's Perspective. *IEEE Transactions on Big Data*.

Azar, A. T. (2012). System dynamics as a useful technique for complex systems. *International Journal of Industrial and Systems Engineering*, 10(4), 377-410.

Bastos, D., Shackleton, M., & El-Moussa, F. (2018). Internet of things: A survey of technologies and security risks in SH and city environments.

Barlas, Y. (1996). Formal aspects of model validity and validation in system dynamics. System Dynamics Review: *The Journal of the System Dynamics Society*, 12(3), 183-210.

Batalla, J. M., & Gonciarz, F. (2019). Deployment of Smart Home management system at the edge: Mechanisms and protocols. *Neural Computing and Applications*, 31(5), 1301-1315. https://doi.org/10.1007/s00521-018-3545-7

Beaulieu, E., Spanjaart, A., Roes, A., Rachet, B., Dalle, S., Kersten, M. J., ... & Jalali, M. S. (2022). Health-related quality of life in cancer immunotherapy: a systematic perspective, using causal loop diagrams. *Quality of life research*, 31(8), 2357-2366.

Birt, L., Scott, S., Cavers, D., Campbell, C., & Walter, F. (2016). Member checking: a tool to enhance trustworthiness or merely a nod to validation? *Qualitative health research*, 26(13), 1802-1811.

Bloodgood, J. M., Hornsby, J. S., Burkemper, A. C., & Sarooghi, H. (2015). A system dynamics perspective of corporate entrepreneurship. *Small business economics*, 45, 383-402.

Bowden, C., & Galindo-Gonzalez, S. (2015). Interviewing when you're not face-to-face: The use of email interviews in a phenomenological study. *International Journal of Doctoral Studies*, 10, 79.

British Sociological Association. (2017). Statement of Ethical Practice. https://www.britsoc.co.uk/media/24310/bsa_statement_of_ethical_practice.pdf

Buchbinder, E. (2011). Beyond checking: Experiences of the validation interview. Qualitative Social Work, 10(1), 106-122.

Bugeja, J. (2021). On privacy and security in smart connected homes.

Bugeja, J., Jacobsson, A., & Davidsson, P. (2020). A privacy-centered system model for smart connected homes. In 2020 *IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)* (pp. 1-4). IEEE.

Burns, J. R., & Musa, P. (z.d.). Structural Validation of Causal Loop Diagrams.

Buzan, B., Wæver, O., Wæver, O., & De Wilde, J. (1998). Security: A new framework for analysis. *Lynne Rienner Publishers*.

Cains, M. G., Flora, L., Taber, D., King, Z., & Henshel, D. S. (2022). Defining cyber security and cyber security risk within a multidisciplinary context using expert elicitation. *Risk Analysis*, 42(8), 1643-1669.

Calliess, C., & Baumgarten, A. (2020). Cybersecurity in the EU the example of the financial sector: a legal perspective. *German Law Journal*, 21(6), 1149-1179.

Cannizzaro, S., Procter, R., Ma, S., & Maple, C. (2020). Trust in the Smart Home: Findings from a nationally representative survey in the UK. *PLoS ONE*, 15(5). https://doi.org/10.1371/journal.pone.0231615

Cavelty, M. D. (2010). Cyber-security. In *The Routledge handbook of new security studies* (pp. 154-162). Routledge.

Chakraborty, T., & Datta, S. K. (2017). Home automation using edge computing and internet of things. *In 2017 IEEE International Symposium on Consumer Electronics (ISCE)* (pp. 47-49). IEEE.

Charmaz, K. (2006). *Constructing grounded theory: A practical guide through qualitative analysis*. sage.

Chen, D., Wawrzynski, P., & Lv, Z. (2021). Cyber security in smart cities: a review of deep learning-based applications and case studies. *Sustainable Cities and Society*, 66, 102655.

Cheng, J., & Greiner, R. (2001). Learning bayesian belief network classifiers: Algorithms and system. In *Advances in Artificial Intelligence: 14th Biennial Conference of the Canadian Society for Computational Studies of Intelligence, AI 2001 Ottawa, Canada, June 7–9, 2001 Proceedings 14* (pp. 141-151). Springer Berlin Heidelberg.

Chhetri, C., & Motti, V. (2021). Identifying vulnerabilities in security and privacy of Smart Home devices. In National Cyber Summit (NCS) Research Track 2020 (pp. 211-231). *Springer International Publishing.*

Chockalingam, S., Pieters, W., Teixeira, A., & van Gelder, P. (2017). Bayesian network models in cyber security: a systematic review. In *Secure IT Systems: 22nd Nordic Conference, NordSec 2017, Tartu, Estonia, November 8–10, 2017*, Proceedings 22 (pp. 105-122). Springer International Publishing.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, 4(10).

Creswell, J. W. (2014). *Research Design: Qualitative, Quantitative, and Mixed Methods* Approaches (4th ed.). Thousand Oaks, CA: Sage Publications, Inc.

Cvitic, I., Perakovic, D., Gupta, B. B., & Choo, K. R. (2022). Boosting-Based DDoS Detection in Internet of Things Systems. *IEEE Internet of Things Journal*, 9(3), 2109-2123. https://doi.org/10.1109/JIOT.2021.3090909

Darbi, W. P. K., & Hall, C. M. (2014). Elite interviews: critical practice and tourism. *Current Issues in Tourism*, 17(9), 832-848.

Darem, A., Alhashmi, A. A., & Jemal, H. A. (2022). Cybersecurity Threats and Countermeasures of the Smart Home Ecosystem. *IJCSNS*, 22(3), 303.

Deibert, R., & Rohozinski, R. (2010). Liberation vs. control: The future of cyberspace. *Journal of Democracy*, 21(4), 43-57. ISO 690

Denscombe, M. (2012). *Research Proposals: A practical guide*. Maidenhead Berkshire: McGraw-Hill Education.

DHS. (2014). A Glossary of Common Cybersecurity Terminology. National Initiative for Cybersecurity Careers and Studies: Department of Homeland Security. October 1, 2014.

Diker, V. (2003). Toward a dynamic theory of open online collaboration communities. *AMCIS 2003 Proceedings*, 48.

Douha, N. Y.-R., Bhuyan, M., Kashihara, S., Fall, D., Taenaka, Y., & Kadobayashi, Y. (2022). A survey on blockchain, SDN and NFV for the SH security. *Internet of Things*, 20, 100588. https://doi.org/10.1016/j.iot.2022.100588

Egerer, S., Cotera, R. V., Celliers, L., & Costa, M. M. (2021). A leverage points analysis of a qualitative system dynamics model for climate change adaptation in agriculture. *Agricultural Systems*, 189, 103052.

Eker, S., & Zimmermann, N. (2016). Using textual data in system dynamics model conceptualization. *Systems*, 4(3), 28.

Eling, M., & Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance? *The Journal of Risk Finance*, 17(5), 474-491.

Etemadi, N., Borbon-Galvez, Y., Strozzi, F., & Etemadi, T. (2021). Supply Chain Disruption Risk Management with Blockchain: A Dynamic Literature Review. *Information* 2021, 12, 70.

Eze, K. G., Akujuobi, C. M., Hunter, S., Alam, S., Musa, S., & Foreman, J. (2022). A Blockchain-based Security Architecture for the Internet of Things. *WSEAS Transactions on Information Science and Applications*, 19, 12-22. https://doi.org/10.37394/23209.2022.19.2

Fernandes, E., Jung, J., & Prakash, A. (2016). Security analysis of emerging Smart Home applications. In 2016 *IEEE symposium on security and privacy* (SP) (pp. 636-654). IEEE.

Flores, M., Heredia, D., Andrade, R., & Ibrahim, M. (2022). Smart Home IoT Network Risk Assessment Using Bayesian Networks. *Entropy*, 24(5). https://doi.org/10.3390/e24050668

Fritz, R. L., & Vandermause, R. (2017). Data collection via in-depth email interviewing: Lessons from the field. *Qualitative Health Research*, 1-10. doi: https://doi.org/10.1177/1049732316689067

Gajewski, M., Batalla, J. M., Mastorakis, G., & Mavromoustakis, C. X. (2019). A distributed IDS architecture model for Smart Home systems. *Cluster Computing*, 22, 1739-1749.

Gheisari, M., Najafabadi, H. E., Alzubi, J. A., Gao, J., Wang, G., Abbasi, A. A., & Castiglione, A. (2021). OBPP: An ontology-based framework for privacy-preserving in IoT-based smart city. *Future Generation Computer Systems*, 123, 1-13.

Gou, X., Liu, H., Qiang, Y., Lang, Z., Wang, H., Ye, D., ... & Wang, H. (2022). In-depth analysis on safety and security research based on system dynamics: A bibliometric mapping approach-based study. *Safety science*, 147, 105617.

Gray, L. M., Wong-Wylie, G., Rempel, G. R., & Cook, K. (2020). Expanding qualitative research interviewing strategies: Zoom video communications. *The qualitative report*, 25(5), 1292-1301.

Guan, Y., & Choi, B. J. (2021). Design, Implementation and verification of topology network architecture of smart home tree. *CMC-Computers Materials & Continua*, 68(2), 2399-2411.

Hall, F., Maglaras, L., Aivaliotis, T., Xagoraris, L., & Kantzavelou, I. (2020). Smart Homes: security challenges and privacy concerns. *arXiv preprint arXiv*:2010.15394.

Hameed, K., Garg, S., Amin, M. B., Kang, B., & Khan, A. (2022). A context-aware information-based clone node attack detection scheme in Internet of Things. *Journal of Network and Computer Applications*, 197. https://doi.org/10.1016/j.jnca.2021.103271

Hasan, S., & Foliente, G. (2015). Modeling infrastructure system interdependencies and socioeconomic impacts of failure in extreme events: emerging R&D challenges. Natural Hazards, 78(3), 2143-2168.

Haseeb-ur-rehman, R. M. A., Liaqat, M., Aman, A. H. M., Almazroi, A. A., Hasan, M. K., Ali, Z., & Ali, R. L. (2022). LR-AKAP: A Lightweight and Robust Security Protocol for Smart Home Environments. *Sensors*, 22(18). https://doi.org/10.3390/s22186902

Hawkins, J. E. (2018). The practical utility and suitability of email interviews in qualitative research. *The Qualitative Report*, 23(2).

Hayes, B. K., Heit, E., & Swendsen, H. (2010). Inductive reasoning. Wiley interdisciplinary reviews: *Cognitive science*, 1(2), 278-292.

Heartfield, R., Loukas, G., Budimir, S., Bezemskij, A., Fontaine, J. R., Filippoupolitis, A., & Roesch, E. (2018). A taxonomy of cyber-physical threats and impact in the SH. *Computers & Security*, 78, 398-428.

Heiding, F., Süren, E., Olegård, J., & Lagerström, R. (2023). Penetration testing of connected households. Computers & Security, 126, 103067.

Herath, T. and Rao, H. R. (2009). 'Protection motivation and deterrence: a framework for security policy compliance in organizations', *European Journal of Information Systems*, 18(2), pp. 106-125. DOI: 10.1057/ejis.2009.6.

Higgins, J. P., Thomas, J., Chandler, J., Cumpston, M., Li, T., Page, M. J., & Welch, V. A. (Eds.). (2019). *Cochrane handbook for systematic reviews of interventions*. John Wiley & Sons.

Huraj, L., Simon, M., & Horak, T. (2020). Resistance of IoT Sensors against DDoS Attack in Smart Home Environment. *Sensors*, 20(18). https://doi.org/10.3390/s20185298

Iqbal, W., Abbas, H., Daneshmand, M., Rauf, B., & Bangash, Y. A. (2020). An In-Depth Analysis of IoT Security Requirements, Challenges, and Their Countermeasures via Software-Defined Security. *IEEE Internet of Things Journal*, 7(10), 10250-10276. https://doi.org/10.1109/JIOT.2020.2997651

Jahan, S., Khan, K. I. A., Thaheem, M. J., Ullah, F., Alqurashi, M., & Alsulami, B. T. (2022). Modeling Profitability-Influencing Risk Factors for Construction Projects: A System Dynamics Approach. *Buildings*, 12(6), 701.

Jbair, M., Ahmad, B., Maple, C., & Harrison, R. (2022). Threat modelling for industrial cyber physical systems in the era of smart manufacturing. *Computers in Industry*, 137, 103611.

Jeong, J., Mihelcic, J., Oliver, G., & Rudolph, C. (2019). Towards an improved understanding of human factors in cybersecurity. In 2019 IEEE 5th *International Conference on Collaboration and Internet Computing (CIC)* (pp. 338-345). IEEE.

Jose, A. C., & Malekian, R. (2017). Improving smart home security: Integrating logical sensing into smart home. *IEEE Sensors Journal*, 17(13), 4269-4286.

Kadena, E., & Gupi, M. (2021). Human Factors in Cybersecurity: Risks and Impacts. *Security science journal*, 2(2), 51-64.

Kannan, U. (2017). Cyber Security System Dynamic Modeling (Doctoral dissertation, Auburn University).

Kavallieratos, G., Chowdhury, N., Katsikas, S., Gkioulos, V., & Wolthusen, S. (2019). Threat Analysis for SHs. *Future Internet*, 11(10). https://doi.org/10.3390/fi11100207

Khan, S. K., Shiwakoti, N., & Stasinopoulos, P. (2022). A conceptual system dynamics model for cybersecurity assessment of connected and autonomous vehicles. *Accident Analysis & Prevention*, 165, 106515.

Kim, H., & Andersen, D. F. (2012). Building confidence in causal maps generated from purposive text data: mapping transcripts of the Federal Reserve. *System Dynamics Review*, 28(4), 311-328.

Kimani, K., Oduol, V., & Langat, K. (2019). Cyber security challenges for IoT-based smart grid networks. *International journal of critical infrastructure protection*, 25, 36-49.

Kitchin, R., & Dodge, M. (2020). The (in) security of smart cities: Vulnerabilities, risks, mitigation, and prevention. *In Smart Cities and Innovative Urban Technologies* (pp. 47-65). Routledge.

Kuyucu, M. K., Bahtiyar, S., & Ince, G. (2019). Security and Privacy in the Smart Home: A Survey of Issues and Mitigation Strategies. 2019 4th *International Conference on Computer Science and Engineering (UBMK)*, 113-118. https://doi.org/10.1109/UBMK.2019.8907037

Kwoun, M.-J., Lee, S.-H., Kim, J.-H., & Kim, J.-J. (2013). Dynamic cycles of unsold new housing stocks, investment in housing, and housing supply-demand. *Mathematical and Computer Modelling*, 57(9-10), 2094-2105. https://doi.org/10.1016/j.mcm.2011.08.005

Lane, D. C. (2015). Validity is a matter of confidence-but not just in system dynamics. *Systems Research & Behavioral Science*, 32(4), 450-458.

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 *IEEE Symposium on Security and Privacy (SP)(SP)* (pp. 380-396). Los Alamitos, CA: IEEE Computer Society.

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 Research & Social Science*, 80, 102211.

Lin, H., & Bergmann, N. W. (2016). IoT privacy and security challenges for Smart Home environments. Information, 7(3), 44.

Liping, W., & Liding, L. (2020). Research on Data Integrity Detection Method Based on Security Perception Layer of Internet of Things Architecture. 2020 *International Conference on Robots & Intelligent System (ICRIS)*, 199-202. https://doi.org/10.1109/ICRIS52159.2020.00057

Liu, Y., Zhao, S., Chen, W., Ge, X., Liu, F., Li, S., & Xiao, N. (2021). NVM Storage in IoT Devices: Opportunities and Challenges. *Computer Systems Science & Engineering*, 38(3).

Lo, N., & Niang, I. (2020) A Survey on QoS-based communication protocols for IoT systems. *In Proceedings of the 3rd International Conference on Networking, Information Systems & Security* (pp. 1-9).

Luna-Reyes, L. F., & Andersen, D. L. (2003). Collecting and analyzing qualitative data for system dynamics: methods and models. *System Dynamics Review*, 19: 271-296.

Lyu, Q., Zheng, N., Liu, H., Gao, C., Chen, S., & Liu, J. (2019). Remotely access "my" SH in private: An anti-tracking authentication and key agreement scheme. *IEEE Access*, 7, 41835-41851.

Meadows, D. H. (2008). *Thinking in Systems: A Primer*. (D. Wright, Ed.) Chelsea Green Publishing.

Minoli, D. (2020). Positioning of blockchain mechanisms in IOT-powered SH systems: A gateway-based approach. *Internet of Things*, 10, 100147. https://doi.org/10.1016/j.iot.2019.100147

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. *International Journal of Human Computer Studies*, 168. https://doi.org/10.1016/j.ijhcs.2022.102902

Mulcahy, R., Letheren, K., McAndrew, R., Glavas, C., & Russell-Bennett, R. (2019). Are households ready to engage with Smart Home technology? *Journal of Marketing Management*, 35(15-16), 1370-1400.

Myers, M. D. (2019). *Qualitative research in business and management*. Qualitative research in business and management, 1-364.

Nandy, T., Idris, M. Y. I. B., Md Noor, R., Mat Kiah, M. L., Lun, L. S., Annuar Juma'At, N. B., Ahmedy, I., Abdul Ghani, N., & Bhattacharyya, S. (2019). Review on Security of Internet of Things Authentication Mechanism. *IEEE Access*, 7, 151054-151089. https://doi.org/10.1109/ACCESS.2019.2947723

Nassiri Abrishamchi, M. A., Zainal, A., Ghaleb, F. A., Qasem, S. N., & Albarrak, A. M. (2022). Smart Home Privacy Protection Methods against a Passive Wireless Snooping Side-Channel Attack. *Sensors*, 22(21), 8564. https://doi.org/10.3390/s22218564

National Institute of Standards and Technology (NIST). (2018). Framework for improving critical infrastructure cybersecurity. Version 1.1. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Pala, O., Vennix, J. A., & Kleijnen, J. (1999). Validation in soft OR, hard OR and system dynamics: A critical comparison and contribution to the debate.

Park, M., Oh, H., & Lee, K. (2019). Security risk measurement for information leakage in IoT-based SHs from a situational awareness perspective. *Sensors* (Switzerland), 19(9). https://doi.org/10.3390/s19092148

Piasecki, S., Urquhart, L., & McAuley, P. D. (2021). Defence against the dark artefacts: Smart Home cybercrimes and cybersecurity standards. *Computer Law and Security Review*, 42. https://doi.org/10.1016/j.clsr.2021.105542

Pillai, M. M., & Helberg, A. (2021). Improving Security in Smart Home Networks through user-defined device interaction rules. 2021 *IEEE Africon*, 1-6. https://doi.org/10.1109/AFRICON51333.2021.9570969

Plachkinova, M., & Menard, P. (2022). An Examination of Gain- and Loss-Framed Messaging on Smart Home Security Training Programs. *Information Systems Frontiers*, 24(5), 1395-1416. https://doi.org/10.1007/s10796-019-09970-6

Punyamurthula, S., & Badurdeen, F. (2018). Assessing production line risk using bayesian Belief networks and system dynamics. *Procedia Manufacturing*, 26, 76-86.

Ramirez, R. B. (2017). Making cyber security interdisciplinary: recommendations for a novel curriculum and terminology harmonization (Doctoral dissertation, Massachusetts Institute of Technology).

Randolph, J. (2009). A guide to writing the dissertation literature review. Practical assessment, research, and evaluation, 14(1), 13.

Rasch, K. (2013). Smart assistants for Smart Homes (Doctoral dissertation, KTH Royal Institute of Technology).

Ryan, E., Pepper, M., & Munoz, A. (2021). Causal Loop Diagram Aggregation Towards Model Completeness. *Systemic Practice and Action Research*, 34(1), 37-51. https://doi.org/10.1007/s11213-019-09507-7

Ryoo, J., Kim, S., Cho, J., Kim, H., Tjoa, S., & DeRobertis, C. (2017). IoE security threats and you. In 2017 *International Conference on Software Security and Assurance (ICSSA)* (pp. 13-19). IEEE.

Salimitari, M., Chatterjee, M., & Fallah, Y. P. (2020). A survey on consensus methods in blockchain for resource-constrained IoT networks. *Internet of Things*, 11, 100212.

Sharma, O., Rathee, G., Kerrache, C. A., & Herrera-Tapia, J. (2023). Two-Stage Optimal Task Scheduling for Smart Home Environment Using Fog Computing Infrastructures. *Applied Sciences*, 13(5), 2939. https://doi.org/10.3390/app13052939

Shaukat, K., Alam, T. M., Hameed, I. A., Khan, W. A., Abbas, N., & Luo, S. (2021). A review on security challenges in internet of things (IoT). *In 2021 26th international conference on automation and computing* (ICAC) (pp. 1-6). IEEE.

Shuhaiber, A., & Mashal, I. (2019). Understanding users' acceptance of Smart Homes. *Technology in Society*, 58, 101110. https://doi.org/10.1016/j.techsoc.2019.01.003

Sivanathan, A., Loi, F., Gharakheili, H. H., & Sivaraman, V. (2017). Experimental evaluation of cybersecurity threats to the Smart Homes. In 2017 *IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)* (pp. 1-6). IEEE.

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of business research*, 104, 333-339.

Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future generation computer systems*, 92, 178-188.

Statista. (2022). Number of Smart Homes worldwide from 2022 to 2027. https://www.statista.com/outlook/dmo/SH/worldwide#SHs

Sterman, J. D. (2000). *Business dynamics. Systems thinking and modeling for a complex world*. Boston, MA: McGraw-Hill.

Subhita, Divya, & Kavita. (2023). Scalable and Secure Architecture for SH using Blockchain with data analysis for security risk. 2023 *IEEE 8th International Conference for Convergence in Technology* (I2CT), 1-8. https://doi.org/10.1109/I2CT57861.2023.10126122

Tomoaia-Cotisel, A., Allen, S. D., Kim, H., Andersen, D., & Chalabi, Z. (2022). Rigorously interpreted quotation analysis for evaluating causal loop diagrams in late-stage conceptualization. *System Dynamics Review*, 38(1), 41-80.

Tweneboah-Koduah, S., & Buchanan, W. J. (2018). Security risk assessment of critical infrastructure systems: A comparative study. *The Computer Journal*, 61(9), 1389-1406.

Vennix, J.A.M. (1996). *Group Model Building. Facilitating Team Learning using System Dynamics*. Chichester: John Wiley and Sons.

Wang, J., & Zhang, Y. C. (2021). A Review on Internet of Things Based SH. 2021 *International Conference on Culture-Oriented Science & Technology (ICCST)*, 273-277. https://doi.org/10.1109/ICCST53801.2021.00065

Waterlander, W. E., Singh, A., Altenburg, T., Dijkstra, C., Luna Pinzon, A., Anselma, M., ... & Stronks, K. (2021). Understanding obesity-related behaviors in youth from a systems dynamics perspective: the use of causal loop diagrams. *Obesity reviews*, 22(7), e13185.

Widjaja, D., Derrick, Dimas Octaviandra, M. F., Achmad, S., & Sutoyo, R. (2022). Important Security Factors for Implementing Internet of Things in SH Systems. 2022 *International Conference on Informatics Electrical and Electronics* (ICIEE), 1-7. https://doi.org/10.1109/ICIEE55596.2022.10010228

Xia, B., Chen, Q., Walliah, J., Buys, L., Skitmore, M., & Susilawati, C. (2021). Understanding the dynamic behaviour of the Australian retirement village industry: A causal loop diagram. *International Journal of Strategic Property Management*, 25(5), 346-355.

Yamauchi, M., Ohsita, Y., Murata, M., Ueda, K., & Kato, Y. (2020). Anomaly Detection in SH Operation from User Behaviors and Home Conditions. *IEEE Transactions on Consumer Electronics*, 66(2), 183-192. https://doi.org/10.1109/TCE.2020.2981636

Yang, J., & Sun, L. (2022). A Comprehensive Survey of Security Issues of Smart Homes System: “Spear” and “Shields,” *Theory and Practice. IEEE ACCESS*, 10, 124167-124192. https://doi.org/10.1109/ACCESS.2022.3224806

Yang, Z., Lim, Y., & Tan, Y. (2019). An Accident Model with Considering Physical Processes for Indoor Environment Safety. *Applied Sciences*, 9(22), 4732. https://doi.org/10.3390/app9224732

Ye, J., O'Grady, M., & Banos, O. (2020). Sensor technology for Smart Homes. *Sensors*, 20(24), 7046.

Yin, R. K. (2009). *Case Study Research: Design and Methods* (5th ed., Applied Social Research Methods). Thousand Oaks, CA: Sage Publications, Inc.

Zhang, P., Ascencio, R. L., & Poulsom, G. (2021). Exploring Mobile Banking Adoption through Causal-Loop Diagrams.

Zhou, W., Jia, Y., Peng, A., Zhang, Y., & Liu, P. (2018). The effect of iot new features on security and privacy: new threats, existing solutions, and challenges yet to be solved. IEEE Internet of things Journal, 6(2), 1606-1616.

Appendices

Appendix 1 Disconfirmatory interview guide

Appendix 1.1 Interview format

***Phase 1**: Establishing trust*
Express genuine interest in interviewee's professional background and expertise by using the information of the preliminary research to establish trust.

***Phase 2**: Interview introduction*
I'd like to thank you once again for being willing to participate in this validating interview of my study. As I have mentioned to you before, my study seeks to provide insights into the potential cybersecurity risks associated with the interdependencies between different components of a SH ecosystem. The components consist of the following six: house, nodes, users, links, data and policies. I have built the causal loop diagram so far based on literature, which helped me to identify and analyze the interdependencies and interrelationships between the different components of a SH ecosystem which contribute to cybersecurity risks. As I had to make assumptions when interpreting relationships to link variables and determine intermediate variables, I would like to validate the with experts like you. In this interview we're going to walk through the variables and relationships in the model and see if it corresponds with your perception of the 'real' system structure. The feedback loops in the CLD are formed into statements which you may either confirm or falsify. At the end I would like to ask six more questions.

***Phase 3**: Asking for consent for recording and transcription*
Before we proceed with the interview, I would like to kindly request your consent regarding the recording of our conversation. The purpose of recording is to ensure accurate documentation and analysis of the interview. The recording will include both video and audio components. Please let me know if you are comfortable with the video and audio recording by confirming your consent. *If you prefer, we can proceed with audio recording only.* Please remember that your participation in this interview is completely voluntary, and you have the right to withdraw your consent at any time without providing a reason. Additionally, any information you share during the interview will be anonymized and kept confidential and used solely for research purposes. Do you have any questions before we start the interview? [Discuss questions] If any questions arise at any point, you can feel free to ask them at any time. I would be more than happy to answer your questions.

***Phase 4**: Explaining System Dynamics methodology*

Purpose of SD: In the field of system dynamics, the purpose is to gain a comprehensive understanding of how various variables within a system interact and influence one another over time. This approach enables us to identify the feedback loops, interdependencies, and emergent behaviours that occur within complex systems such as the SH ecosystem.

Polarities: System dynamics recognizes the presence of both positive (+) and negative (-) relationships between variables. A positive relationship implies that as one variable increases, the other variable also increases, and as one variable decreases, the other variable also decreases. This type of relationship indicates a direct correlation between the variables, where they move in the same direction. On the other hand, a negative relationship signifies that as one variable increases, the other variable decreases, and vice versa. In this case, the variables exhibit an inverse relationship, where changes in one variable leads to opposite changes in the other variable.

Feedback loop: One of the fundamental concepts in system dynamics is the feedback loop. A feedback loop represents a recurring pattern of cause-and-effect relationships among variables in a system. It illustrates how changes in one variable can influence other variables, which, in turn, can impact the original variable.

Feedback loops can be either positive (reinforcing) or negative (balancing) in nature. A positive feedback loop occurs when a change in one variable amplifies or reinforces the initial change, creating a self-reinforcing loop. This can lead to exponential growth or decline in the system. Conversely, a negative feedback loop arises when a change in one variable triggers adjustment that counteract the initial change, resulting in a stabilizing effect within the system.

By applying system dynamics, we can delve into the complexities of the SH ecosystem and gain insights into how the variables interact, the presence of feedback loops, and the overall behaviour of the system over time. This knowledge is valuable for understanding the dynamics and potential impacts of various factors within the SH ecosystem.

***Phase 5**: Presenting the CLD*

I will now show you the model I have built. During this, the elements in the model itself will be explained. You may interrupt me any time if you do not agree with a certain part or if you would like further clarification on any aspect.

***Phase 6**: Statements of the feedback loops*

I will now present you the relationships that form the feedback loops in the form of statements. You may either confirm or falsify the statement and then please give an explanation for your reasoning.

Appendix 1.2 Feedback loops transformed into statements

Balancing loops
B1 Awareness loop
Resident security awareness → Human threats to the SH → Resident security awareness

Statement 1: When residents are more aware and educated about security measures, they are likely to reduce the likelihood of human threats. Additionally, experiencing security incidents can raise resident awareness and motivate them to take appropriate security measures

Please confirm or falsify the statement and give an explanation for your reasoning.

B2 Human threat loop 2
Human threats to the SH → resident security awareness → users' speeds of responding to detected threats → human threats to the SH

Statement 2: Human threats in the SH lead to a higher security awareness of residents. When residents are more aware of security, they are likely to respond quicker to detected threats. When residents respond quickly to detected threats, the human threats in the SH will decrease.

Please confirm or falsify the statement and give an explanation for your reasoning.

B3 Human threat loop 1
Human threats to the SH → resident security awareness → susceptibility to engineering → human threats to the SH

Statement 3: Human threats to the SH positively influence the level of resident security awareness, which in turn negatively impacts the occurrence of successful social engineering attacks. These social engineering attacks, in turn, positively contribute to the occurrence of human threats to the SH.

Please confirm or falsify the statement and give an explanation for your reasoning.

B4 Network congestion loop
Network congestion level → packet loss → performance of the SH ecosystem → convenience to users → deployment of SH devices → network congestion level

Statement 4: The level of network congestion can lead to packet loss, which in turn affects the performance of the SH ecosystem. The performance of the ecosystem negatively impacts the convenience experienced by users, which then influences the decision to deploy fewer SH devices. Finally, the deployment of fewer SH devices can contribute to a lower level of network congestion.

Please confirm or falsify the statement and give an explanation for your reasoning.

B5 Deployment loop
Deployment of SH devices → network congestion level → packet loss → data integrity → users' trust in SH devices → deployment of SH devices

Statement 5: The deployment of SH devices contributes to a higher network congestion level, which influences a higher occurrence of packet loss. Packet loss, in turn, negatively affects data integrity within the SH ecosystem, ultimately leading to a lower level of users' trust in SH devices. The level of trust in the devices, in turn, affects the decision for further deployment of SH devices.

B6 Trust loop
Users' trust in SH devices → users' speed of responding to detected threats → Users' trust in SH devices

Statement 6: Users who have a high level of trust in their devices are more likely to respond quickly and effectively to detected threats, increasing their trust in the devices.

Please confirm or falsify the statement and give an explanation for your reasoning.

Reinforcing loops

R1 Vulnerability loop
Number of cyberattacks -> probability of compromising central server -> probability of a system wide breach -> vulnerabilities in SH devices -> data leakage -> Number of cyberattacks

Statement 7: Vulnerabilities in SH devices increase the amount of data leakage, which in turn increases the number of cyberattacks targeting the system. The occurrence of these cyberattacks raises the chance of compromising the central server, which subsequently increases the probability of a system-wide breach. As a result, the system-wide breach exposes additional vulnerabilities in SH devices.

Please confirm or falsify the statement and give an explanation for your reasoning.

R2 Data leakage loop
Data leakage → number of cyberattacks → data leakage

Statement 8: Data leakage contributes to more cyberattacks, since attackers can exploit these to carry out cyberattacks, when a cyberattack is carried out, this potentially results in more data leakage.

Please confirm or falsify the statement and give an explanation for your reasoning.

R3 System breach loop
Vulnerabilities in SH devices → Data leakage → Number of cyberattacks → chance of compromising central server → probability of a system wide breach → vulnerabilities in SH devices

Statement 9: Vulnerabilities in SH devices can lead to data leakage, which in turn increases the number of cyberattacks targeting the system. The occurrence of these cyberattacks raises the chance of compromising the central server, which subsequently increases the probability

of a system-wide breach. As a result, the system-wide breach exposes additional vulnerabilities in SH devices.

Please confirm or falsify the statement and give an explanation for your reasoning.

R4 Convenience loop
Convenience to users → Deployment of SH devices → Degree of interconnectivity → Convenience to users

Statement 10: When users experience increased convenience in their SH ecosystem, they are motivated to deploy more SH devices. The deployment of additional devices leads to a higher degree of interconnectivity within the ecosystem. This increased interconnectivity, in turn, amplifies the convenience experienced by users.

Please confirm or falsify the statement and give an explanation for your reasoning.

Appendix 1.3 Interview questions

1) What are your overall impressions of the CLD?

2) Do the connections make sense to you when evaluated without delving into further analysis or deeper examination? If not, please explain.

3) According to you, do you believe that all the relationships between the variables are correctly represented? If not, please explain.

4) Do you think any additional variables should be added that are significant for the system behaviour and contribute to cybersecurity risks?

5) Do you think any additional intermediate variables are crucial in understanding the causal relationships and dynamics within the system?

6) Do you see any variables that do not offer any additional clarifying explanation about the cybersecurity risks in smart homes and can therefore better be excluded?

Appendix 2 List of papers included in the SSLR

	Author(s)	Title	Year	Discipline
1.	Abbas, S. G., Vaccari, I., Hussain, F., Zahid, S., Fayyaz, U. U., Shah, G. A., Bakhshi, T., & Cambiaso, E.	Identifying and Mitigating Phishing Attack Threats in IoT Use Cases Using a Threat Modelling Approach	2021	Computer Science and Engineering
2.	Shaukat, K., Alam, T. M., Hameed, I. A., Khan, W. A., Abbas, N., & Luo, S.	A review on security challenges in internet of things (IoT)	2021	Computer Science, Decision Science and Mathematics
3.	Allifah, N. M., & Zualkernan, I. A.	Ranking Security of IoT-Based Smart Home Consumer Devices	2022	Computer Science and Engineering
4.	Anthi, E., Williams, L., Slowinska, M., Theodorakopoulos, G., & Burnap, P.	A Supervised Intrusion Detection System for Smart Home IoT Devices	2019	Computer Science
5.	Arif, S., Khan, M. A., Rehman, S. U., Kabir, M. A., & Imran, M.	Investigating Smart Home Security: Is Blockchain the Answer?	2020	Computing and Mathematics
6.	Batalla, J. M., & Gonciarz, F.	Deployment of Smart Home management system at the edge: Mechanisms and protocols.	2019	Computer Science
7.	Cannizzaro, S., Procter, R., Ma, S., & Maple, C.	Trust in the Smart Home: Findings from a nationally representative survey in the UK	2020	Multidisciplinary
8.	Cvitic, I., Perakovic, D., Gupta, B. B., & Choo, K. R.	Boosting-Based DDoS Detection in Internet of Things Systems.	2022	Computer Science
9.	Douha, N. Y.-R., Bhuyan, M., Kashihara, S., Fall, D., Taenaka, Y., & Kadobayashi, Y.	A survey on blockchain, SDN and NFV for the Smart Home security.	2022	Engineering, Management & Accounting and Computer Science
10.	Eze, K. G., Akujuobi, C. M., Hunter, S., Alam, S., Musa, S., & Foreman, J.	A Blockchain-based Security Architecture for the Internet of Things.	2022	Information Science
11.	Flores, M., Heredia, D., Andrade, R., & Ibrahim, M.	Smart Home IoT Network Risk Assessment Using Bayesian Networks.	2022	Computer Science, Engineering,

				Mathematics and Physics & Astronomy
12.	Salimitari, M., Chatterjee, M., & Fallah, Y. P.	A survey on consensus methods in blockchain for resource-constrained IoT networks	2020	Computer Science, Engineering and Management & Accounting
13.	Hameed, K., Garg, S., Amin, M. B., Kang, B., & Khan, A.	A context-aware information-based clone node attack detection scheme in Internet of Things.	2022	Computer Science
14.	Haseeb-ur-rehman, R. M. A., Liaqat, M., Aman, A. H. M., Almazroi, A. A., Hasan, M. K., Ali, Z., & Ali, R. L.	A Lightweight and Robust Security Protocol for Smart Home Environments	2022	IT, Computer Science and Physics
15.	Huraj, L., Simon, M., & Horak, T.	Resistance of IoT Sensors against DDoS Attack in Smart Home Environment	2018	Biochemistry, Chemistry, Engineering and Physics & Astronomy
16.	Iqbal, W., Abbas, H., Daneshmand, M., Rauf, B., & Bangash, Y. A.	An In-Depth Analysis of IoT Security Requirements, Challenges, and Their Countermeasures via Software-Defined Security	2020	Computer Science
17.	Kadena, E., & Gupi, M.	Human Factors in Cybersecurity: Risks and Impacts.	2021	Decision Sciences and Psychology
18.	Kavallieratos, G., Chowdhury, N., Katsikas, S., Gkioulos, V., & Wolthusen, S.	Threat Analysis for Smart Homes	2019	Information Security & IT
19.	Kuyucu, M. K., Bahtiyar, S., & Ince, G.	Security and Privacy in the Smart Home: A Survey of Issues and Mitigation Strategies	2019	Computer Science, Decision Science and Engineering
20.	Li, J., Sun, K., Huff, B. S., Bierley, A. M., Kim, Y., Schaub, F., & Fawaz, K.	“It’s up to the Consumer to be Smart”	2023	Psychology and Decision Science
21.	Li, W., Yigitcanlar, T., Erol, I., & Liu, A.	Motivations, barriers and risks of Smart Home adoption: From systematic literature review to conceptual framework.	2021	Social Sciences

22.	Liping, W., & Liding, L.	Research on Data Integrity Detection Method Based on Security Perception Layer of Internet of Things Architecture	2020	Computer Science, Engineering and Mathematics
23.	Liu, Y., Zhao, S., Chen, W., Ge, X., Liu, F., Li, S., & Xiao, N.	NVM Storage in IoT Devices: Opportunities and Challenges.	2021	Computer Science and Engineering
24.	Minoli, D.	Positioning of blockchain mechanisms in IOT-powered Smart Home systems: A gateway-based approach.	2020	Business Management & Accounting, Computer Science and Engineering
25.	Morgan, P. L., Collins, E. I. M., Spiliotopoulos, T., Greeno, D. J., & Jones, D. M.	Reducing risk to security and privacy in the selection of trigger-action rules: Implicit vs. Explicit priming for domestic smart devices	2022	Computer Science, Engineering and Social Sciences
26.	Mulcahy, R., Letheren, K., McAndrew, R., Glavas, C., & Russell-Bennett, R.	Are households ready to engage with Smart Home technology?	2019	Social Sciences and Psychology
27.	Nandy, T., Idris, M. Y. I. B., Md Noor, R., Mat Kiah, M. L., Lun, L. S., Annuar Juma'At, N. B., Ahmedy, I., Abdul Ghani, N., & Bhattacharyya, S.	Review on Security of Internet of Things Authentication Mechanism.	2019	Computer Science and IT
28.	Nassiri Abrishamchi, M. A., Zainal, A., Ghaleb, F. A., Qasem, S. N., & Albarrak, A. M.	Smart Home Privacy Protection Methods against a Passive Wireless Snooping Side-Channel Attack.	2022	Computer Science, Engineering and Physics
29.	Park, M., Oh, H., & Lee, K.	Security risk measurement for information leakage in IoT-based Smart Homes from a situational awareness perspective	2019	Biochemistry, Chemistry, Engineering and Physics & Astronomy
30.	Piasecki, S., Urquhart, L., & McAuley, P. D.	Defence against the dark artefacts: Smart Home cybercrimes and cybersecurity standards.	2021	Business, Management & Accounting, Computer Science and Social Science
31.	Pillai, M. M., & Helberg, A.	Improving Security in Smart Home Networks through user-defined device interaction rules.	2021	Computer Science & Engineering

32.	Guan, Y., & Choi, B. J.	Design, Implementation and verification of topology network architecture of smart home tree.	2021	Computer Science
33.	Plachkinova, M., & Menard, P.	An Examination of Gain- and Loss-Framed Messaging on Smart Home Security Training Programs.	2022	Computer Science & Mathematics
34.	Sharma, O., Rathee, G., Kerrache, C. A., & Herrera-Tapia, J.	Two-Stage Optimal Task Scheduling for SH Environment Using Fog Computing Infrastructures.	2023	Computer Science & Engineering
35.	Shuhaiber, A., & Mashal, I.	Understanding users' acceptance of Smart Homes	2019	Business, Management & Accounting and Social Sciences
36.	Subhita, Divya, & Kavita.	Scalable and Secure Architecture for Smart Home using Blockchain with data analysis for security risk	2023	Computer Science, Decision Sciences and Engineering
37.	Wang, J., & Zhang, Y. C.	A Review on Internet of Things Based Smart Home.	2021	Computer Science, Engineering and Social Sciences
38.	Widjaja, D., Derrick, Dimas Octaviandra, M. F., Achmad, S., & Sutoyo, R.	Important Security Factors for Implementing Internet of Things in Smart Home Systems.	2022	Computer Science, Engineering and Physics
39.	Yamauchi, M., Ohsita, Y., Murata, M., Ueda, K., & Kato, Y.	Anomaly Detection in Smart Home Operation from User Behaviors and Home Conditions	2020	Computer Science and Engineering
40.	Yang, J., & Sun, L.	A Comprehensive Survey of Security Issues of Smart Home System: "Spear" and "Shields," Theory and Practice.	2022	Computer Science, Engineering

Appendix 3 Research ethics

The research abided by the ethical principles outlined in the British Sociological Association's Statement of Ethical Practice (BSA, 2017). As noted by Denscombe (2012), all codes of research ethics consist of three main themes: preventing harm to participants, obtaining voluntary consent, and maintaining scientific integrity. To prevent harm, measures such as maintaining participant confidentiality and securely handling data (including anonymizing it) were implemented. Participants of the interviews were fully informed about the research, had the opportunity to ask questions and raise concerns before deciding to participate, and had the right to withdraw their consent at any time (Myers, 2019).

To maintain scientific integrity, we followed several steps: suitable methods were used, openness and honesty were maintained, bias was avoided, and compliance with laws and technical regulations was ensured (Denscombe, 2012). Suitable methods were carefully selected and justified, and all collected and analysed data were fully reported, acknowledging any limitations or biases and addressing them. To mitigate bias, we conducted interviews with a diverse range of participants. The interviews were transcribed and subjected to a double-checking process. Subsequently, an interview report was created and shared with the participants for member-checking, allowing them to review and validate the accuracy of the information provided. The research also complied with all relevant laws and technical regulations, ensuring its ethical and valid nature. The findings were clearly communicated and made available for review and evaluation by the research community.

Appendix 4 Suggestions by experts that have been omitted

This section further elaborates on the exception to clarify why certain suggestions from experts were omitted.

7.1 Lightweight algorithm cryptography security practices

C1 suggested that instead of heavy traditional security measures, there are other ways of protecting the limited resource devices. These lightweight security measures were not included in the model because they do not directly contribute to CSR. Instead, they serve as mitigating factors that enhance security measures. The focus of the model is to identify and analyse the risks associated with SH devices, rather than specific security practices.

7.2 GDPR privacy policies

Although important for data protection, GDPR privacy policies were not incorporated into the model as they lie outside of its boundary. The model primarily focuses on analysing the internal factors related to SH CSR, rather than external policies and regulations. However, it is acknowledged that adherence to GDPR can potentially reduce data leakage risks by ensuring better privacy practices, as mentioned by C1.

7.3 Risk of modification data subject and system failure

The risks of data modification and system failure have been included in the model under the variable of the number of cyberattacks. These risks are considered as potential outcomes of cyberattacks, where unauthorized access or control over the SH system can lead to data modification and system failures. Therefore, they are addressed within the context of cyberattacks rather than as separate variables.

7.4 Environmental factors

The impact of environmental factors, such as packet loss caused by disruptions in magnetic fields, as mentioned by C1, was not included in the model as it falls outside of its boundary. The model primarily focuses on internal factors related to SH devices and their CSR, rather than external environmental factors. While such incidents can affect data transmission, they are not within the scope of the model's analysis.

7.5 Economic factors

Economic considerations, although significant in real-world scenarios, were not within the scope of the model's analysis. C1 and IT1 highlighted an important point regarding the influence of economic factors, such as the cost price of SH devices, on users' decision-making process for deploying these devices. While this aspect is undoubtedly relevant, it was not included in the model as it falls outside the defined boundary. Furthermore, IT1 highlighted the correlation between economic factors and the security of the smart home ecosystem. IT1 pointed out that higher-priced devices often come with added complexity during setup, requiring more knowledge, offering better protection against certain threats. Conversely, opting for cheaper devices may introduce potential risks as these manufacturers do not prioritize security.

Appendix 5 Assumptions and implicit structures in the model

In our SSLR, we examined the association between CSRs and the components of the SHES, which revealed that various device characteristics contributed to vulnerabilities. However, our analysis resulted in a pattern indicating minimal interconnections between factors leading to vulnerabilities, known as a "dead buffalo" in SD terms (Waterlander et al., 2021).

To overcome this, we introduced two intermediate variables to facilitate a better understanding of relevant system dynamics (Waterlander et al., 2021). The first variable we introduced is the *complexity of the SHES*, which mediates the effects of *device heterogeneity*, *device interconnectivity*, and *limited resource capacity*. We identified these factors in the literature as contributing to the complexity of managing the SHES. The second variable we introduced is *device reliability*, which mediates the effects of the *number of firmware updates* and *configuration errors*. A lack of firmware updates can lead to tampering and repudiation, indicating a less reliable device (Abbas, 2021), while configuration errors can result in vulnerabilities such as data loss, which are associated with device reliability (Batalla & Gonciarz, 2019). Both introduced intermediate variables contribute to vulnerabilities in SH devices, and can be found in the vulnerabilities part of the theoretical model in figure 4.

Second, the relationship from *resident security awareness* leading to an *increase of user response time to detected threats*. This assumption is grounded in the belief that residents with a high level of security awareness are motivated to take pro-active security measures as mentioned by Plachkinova & Menard (2022). By being proactive and knowledgeable about security risks, residents are expected to take quick and appropriate actions when threats are detected, ensuring the protection of their SHES. The relationship can be found in both the human behaviour part in the theoretical model in figure 3.

Furthermore, when tasks cannot be executed effectively, it is assumed that therefore the convenience to users is influenced negatively. This relationship can be found in the deployment part of the theoretical model in figure 6. It is absent in the final model as C1 and IT1 suggested to omit the linked variable *performance of the smart-home ecosystem*, because it does not contribute to CSRs.

Appendix 6 Loop identification

6.1 Balancing feedback loops

This section will describe the balancing feedback loops.

6.1.1 B1 Awareness loop

When residents are more aware of the security risks in their SH, they are more likely to implement mitigation strategies, eventually decreasing the human vulnerabilities to the SH. Conversely, when residents personally encounter human vulnerabilities, it triggers a heightened sense of awareness regarding the importance of security measures and practices within their SHs. The loop emphasizes the importance of security awareness.

It is important to note that one significant risk lies in the fact that users often lack awareness of the potential vulnerabilities they may face in their SHs. This exposes them to higher risks, as the likelihood of cyberattacks increases without implementing adequate mitigation strategies.

6.1.2 B2 Human vulnerability loop 1

When residents are more aware of the security risks in their SH, they will become less susceptible to social engineering techniques, decreasing human vulnerabilities to the SH. The loop emphasizes that resident security awareness is crucial in mitigating the impact of social engineering and subsequent human threats. By promoting security awareness among residents through education, training, and effective communication, it is possible to enhance their ability to recognize and respond to social engineering attempts. This, in turn, contributes to a more secure SH environment by reducing the likelihood and impact of human threats.

The same applies here; the risk lies in the fact that users are often unaware of the security risks in their homes.

6.1.3 B3 Human vulnerability loop 2

When residents are more aware of the security risks in their SH, they are more likely to seek ways to mitigate them and apply appropriate strategies, making them more capable of acting. When they are more capable of acting, they are likely to respond quickly to detected threats, reducing human vulnerabilities to the SH. However, this depends on many external factors that

influence their behaviour, such as motivation to act, availability of resources and priority of threat response. Likewise, in this feedback loop, security unawareness creates a significant risk.

6.1.4 B4 Deployment loop

When SH devices are increasingly deployed, it increases the network congestion level. This congestion leads to packet loss. The packet loss compromises the data integrity of the SH, undermining the trust users have in the devices. The decrease in data integrity negatively impacts the perceived trustworthiness of the SH devices among users. As a result, users may be hesitant to deploy additional devices in their SH setup due to concerns about compromised data integrity and trust issues.

The risk within this loop is rooted in the erosion of trust in SH devices caused by compromised data integrity. This loss of trust has significant implications, including the perceived effectiveness of security measures and the motivation to respond promptly to detected threats. Consequently, the delayed response time to security threats increases the potential for adversaries to exploit the compromised SH environment with greater efficiency, as there are no effective barriers to hinder their malicious activities.

6.1.5 B5 Trust loop

Similar to B5, this loop involves the variables deployment of SH devices, network congestion level, packet loss, and users' trust in SH devices. However, instead of compromising data integrity, the packet loss directly impacts users' trust in the SH devices. The risk within this loop is consistent with the risk mentioned in B4.

6.2 Reinforcing feedback loops

This section will describe the reinforcing feedback loops.

6.2.1 R1 Vulnerability loop 1

This loop shows how vulnerabilities can eventually lead to a system-wide breach in which every device in the network gets compromised. Vulnerabilities in SH devices serve as potential entry points for cyberattacks. As cyberattacks increase, so does the probability of compromising the central server. This raises the likelihood of a system-wide breach, where unauthorized access and control over the entire smart-home network is achieved. This potentially exposes sensitive data and compromises the security and privacy of the whole SHES.

6.2.2 R2 Data leakage loop

As the number of cyberattacks increases, the risk of data leakage also rises, creating a cycle where each instance of data leakage fuels more cyberattacks. This reinforcing loop underscores the critical importance of effectively addressing data leakage to break this cycle and eventually enhance the security and resilience of the system.

6.2.3 R3 System breach loop

This loop is similar to R1; however, in this loop, the focus shifts from the exploitation of vulnerabilities to the adversary's utilization of leaked data resulting from vulnerabilities in the devices to execute cyberattacks. The same consequences as R1 apply here.

6.2.4 R4 Usefulness loop

As more SH devices are deployed, the level of interconnectivity among these devices increases. This increased interconnectivity enhances users' perceived usefulness and functionality in their SHs, making their daily lives more efficient and seamless. In turn, the perceived usefulness and benefits derived from the interconnected devices further encourage the deployment of additional SH devices.

The risk within this loop stems from the rapid and widespread deployment of SH devices, which can give rise to CSR. As more and more devices are added to the network, the attack surface increases, creating more potential vulnerabilities. This expansion provides adversaries with increased entry points to exploit within the SHES.

Appendix 7 SSLR relationships table

Cause	Effect	Effect 2	Polarity	Source
Ability to use traditional advanced security measures	Data integrity		-	(Salimitari et al., 2020)
Configuration errors	Data security		-	(Eze et al., 2022)
Data security	Data leakage			
User proficiency in managing SHs	Human threats to the SH		-	(Park et al., 2019)
Deployment of smart-home	Vulnerabilities of SH devices		+	(Anthi et al., 2019)
Deployment of smart-home	Network congestion level	Packet loss	+, +	(Plachkinova & Menard, 2022)
Deployment of smart-home	Attack surface		+	(Widjaja et al., 2022)
Deployment of smart-home devices	Interconnectivity	Vulnerabilities of smart-home devices	+, +	(Kavallieratos et al., 2019)
Deployment of smart-home devices	Network congestion	Packet loss	+, +	(Liping & Liding, 2020)
Heterogeneity of devices	Ability to use traditional advanced security measures		-	(Anthi et al., 2019; Batalla & Gonciarz, 2019)
Heterogeneity of devices	Vulnerabiilities of SH devices		+	(Huraj et al., 2020)
Heterogeneity of devices	Susceptibility to social enginering		+	(Yang & Sun, 2022)
Human threats to the SH	Resident security awareness		+	(Li et al., 2023)
Interconnectivity	Convenience to users		+	(Flores et al., 2022; Nassiri et al., 2022)

Likelihood of compromising central server	System wide breach		+	(Arif et al., 2020)
Limited resource capacity	Ability to use traditional advanced security measures		-	(Abbas et al., 2021; Arif et al., 2020; (Batalla & Gonciarz, 2019; Cvitic et al., 2022; Mulcahy et al., 2019; Nandy et al., 2019)
Limited resource capacity	Configuration errors		+	(Shaukat et al., 2021)
Limited resource capacity	Vulnerabilities of SH devices		+	(Allifah & Zualkerman, 2022; Arif et al., 2020; Huraj et al., 2020)
Limited resource capacity	Simultaneous attacks		+	(Huraj et al., 2020)
Number of cyberattacks	Potential harm to users		+	(Cannizzaro, 2020; Huraj et al., 2020; Park et al., 2019)
Number of cyberattacks	Data leakage		+	(Hameed et al., 2022)
Number of cyberattacks	Likelihood of compromising central server		+	(Morgan et al., 2022)
Number of firmware updates	Vulnerabilities of smart-home devices		+	(Abbas et al., 2021; Huraj et al., 2020)
Packet loss	Data integrity		-	(Minoli, 2020)
Packet loss	Performance of the smart-home		-	(Guan & Choi, 2021)
Perceived risk	Trust in smart-home devices	Deployment of SH devices	-, +	(Li et al., 2021)
Perceived risk	Users' trust in smart-home devices		-	(Shuhaiber & Mashal, 2019; Li et al., 2021)
Power outages	Data leakage		+	(Liu et al., 2021)
Power outages	Convenience		+. +	(Subhita et al., 2023)
Resident security awareness	Susceptibility to social engineering		-	(Iqbal et al., 2020; Pillai & Helberg, 2021)

Resident security awareness	Human threats to the SH		-	(Kadena & Gupi, 2021; Kuyucu et al., 2019)
Resident security awareness	Configuration errors		-	(Wang & Zhang, 2021)
Smart-home user proficiency	Configuration errors	Data leakage	-, +	(Batalla & Gonciarz, 2019)
Smart-home user proficiency	Configuration errors	Number of cyberattacks	-, +	(Batalla & Gonciarz, 2019)
Smart-home user proficiency	Configuration errors		-	(Douha et al., 2022; Piasecki et al., 2021; Batalla & Gonciarz, 2019)
Simultaneous attacks	Power outages	Vulnerabilities of smart-home devices	+. +	(Huraj et al., 2020)
Simultaneous attacks	Energy demands	Power outages	+, +	(Yamauchi et al., 2020)
Susceptibility to social engineering	Risk of privacy data access by hackers		+	(Haseeb-ur-rehman et al., 2022)
Susceptibility to social engineering	Human threats to the SH		+	(Haseeb-ur-rehman et al., 2022)
Susceptibility to social engineering	Risk of privacy data access by hackers		+	(Park et al., 2019)
Third-party integrations	Interconnectivity	Vulnerabilities of SH devices	+, +	(Batalla & Gonciarz, 2019)
Users' response time to detected threats	Human threats to the SH		-	(Batalla & Gonciarz, 2019)
Users’ trust in smart-home devices	Deployment of SH devices		+	(Sharma et al., 2023)
Users’ trust in smart-home devices	Convenience to users		+	(Shuhaiber & Mashal, 2019)
Vulnerabilities in SH devices	Data leakage	Risk of privacy data acces by hackers	+, +	(Park et al., 2019)