DEGREE PROJECT

Investigating the Impact of User Behavior in the Security of Smart Home IoT Devices

Maha Ghunaim

Information Security, master's level (120 credits)
2023

Luleå University of Technology
Department of Computer Science, Electrical and Space Engineering

LULEÅ
UNIVERSITY
OF TECHNOLOGY

[This page intentionally left blank]

ACKNOWLEDGEMENT

I would like to pay my sincere gratitude to **Mr. Abdol Rasoul Habibipour** for helping me to complete this thesis. It was not an easy journey and it could not have been possible to complete this thesis without his help. Moreover, I would like to pay special thanks to my mother for continuously praying for me in this difficult time. Furthermore, I would like to thanks my friends, family members and fellows for supporting me in this arduous journey.

Investigating the Impact of User Behavior in the Security of Smart Home IoT Devices

Abstract

As technology is growing at a fast pace, IoT-based smart home services are increasingly adopted by people. IoT-based smart homes offer numerous unimaginable benefits, including efficiency, safety, effectiveness, scalability of services, devices, and data, among many others. However, there is another side to this technology: security threats. As IoT-based technology is distributed in nature, implementing security measures and policies to protect the infrastructure becomes very difficult. The infrastructure faces threats such as information theft, eavesdropping, distortion, and more. Ensuring the security of smart home IoT devices is a critical concern, and user behavior plays a major role in achieving it. Furthermore, Theory of Planned Behavior (TPB) was utilized throughout the study. This study employed a qualitative research methodology and content analysis technique to investigate the impact of user behavior on the security of smart home IoT devices. The findings revealed several themes, such as the significance of comprehending and resolving security issues, the implementation of security measures, and the impact of user education and awareness. The study offered fresh perspectives on IoT device security and will aid in developing security best practices.

Keywords: Smart Homes, Smart Home Devices, Home Automation, User Behavior, Internet of Things (IoT)

Table of Contents

Table of Abbreviations

Keywords	Abbrevation
TPB	Theory of Planned Behavior
IoT	Internet of Things

List of Figures

List of Tables

1. Introduction

The proliferation of smart home Internet of Things (IoT) devices has transformed the way we interact with our living spaces. IoT-based smart homes offer numerous unimaginable benefits, including efficiency, safety, effectiveness, scalability of services, devices, and data, among many others. By integrating information technology and networking with residential services, a wide range of technologies is employed to outfit household appliances for more sophisticated remote control and monitoring, enabling them to communicate seamlessly with one another (Barker & Parsons, 2022). As a result, routine household chores and activities can be automated in a way that is easier, more useful, more efficient, and safer, either without requiring human interaction or under remote supervision (Kadam, Mahamuni, & Parikh, 2015). However, there is another side to this technology: security threats. IoT gadgets for smart homes have quickly gained popularity, but this has also created new security issues as hackers target these gadgets in order to find vulnerabilities and access private data without authorization (Coboi *et al.*, 2021; Alam & Tomai, 2023).

1.1.Background

The expansion of data analytics, computer devices, widespread connection, and cloud computing have all increased awareness of IoT (Patel, Patel, & Scholar, 2016). It has enabled us to remotely manage several aspects of our lives by utilizing billions of gadgets that are connected to the internet and to one another. Some additional benefits of IoT include improved safety, cost savings, enhanced customer experience, and increased efficiency through automation.

Further, Schuster and Habibipour (2022) concentrates on how users perceive privacy and security in relation to IoT technologies, particularly in the residential sector. According to the report, individuals are very concerned about the security of IoT gadgets, potential hacks, and the exploitation of their private information. Furthermore, there is a lack of confidence in businesses, services, and authorities to protect privacy. The mainstream acceptance of IoT technology is significantly hampered by these security and privacy issues.

Moreover, the popularity of smart home devices is on the rise, with an estimated 1.1 billion devices in use worldwide in 2020, projected to reach 1.6 billion by 2023 (Turulski, 2022). While these devices offer many benefits, including energy management, remote control of appliances, and home security, they also carry risks (Gondal, 2021). Further, an individual's mindset towards utilizing smart home devices, cultural standards around their use, and their sense of authority over

their use can all have an influence on their acceptance and utilization of these devices in the context of smart homes (Mamonov & Benbunan-Fich, 2021).

During the year 2000, the advent of low-cost technologies saw the rise of the smart home (Vibesmarthomes, 2018). Though not yet considered "smart," household appliances were a remarkable development at the time. In 1901, the first vacuum cleaner based on engine power was invented, followed by an improved model of an electrical vacuum in 1907. This paved the way for the creation of other home appliances like refrigerators, irons, washing machines, toasters, dryers, and more (Ray & Bagwari, 2018). These foundational innovations allowed for the integration of home appliances into a network infrastructure. Additionally, the successful simulation of an Internet-based lock system was achieved (Sankar & Srinivasan, 2018). This system consists of a lock gadget, a gateway, and a remote client that can operate and manage the lock gadget (Tan, Lim & Goh, 2002), leading to further advancements in home automation (Dhara *et al.*, 2021).

The year 2005 saw the creation of the first smart wearable healthcare system, which demonstrated how technology could ameliorate lifestyle quality at home (De Rossi & Lymberis, 2005). In 2009, cloud services were integrated into smart home systems, enabling more advanced remote control and home gadget tracking (Belimpasakis &and Moloney, 2009). In 2015, speech was introduced as a controller for smart homes, making interactions with gadgets more user-friendly (Mittal *et al.*, 2016). These developments signify a continuation of the century-old trend towards sophisticated, networked automation systems for homes.

While there are many advantages to the growth of smart home IoT devices, it also brings issues regarding the privacy and security of these connected systems (Setayeshfar *et al.*, 2022). Cyber risks, unauthorized access, hacking attempts, and data thefts can affect smart homes (Bugeja, 2021). In addition to compromising confidentiality, hacked devices can be dangerous if accessed by malicious actors. Therefore, maintaining the security of IoT gadgets in smart homes is essential to safeguarding people's privacy, possessions, and general well-being (Hammi *et al.*, 2022).

User behavior is a crucial factor that has an influence on the security of IoT devices for smart homes (Olabode *et al.*, 2023). The choices and actions taken by users have a significant impact on the security level that is established and upheld in their smart homes (Shuhaiber, Alkarbi & Almansoori, 2023). User behavior includes a variety of actions, such as setting up and configuring

devices, managing passwords, updating software, practicing network security, and adhering to best security practices advised by device makers (Shuhaiber, Alkarbi & Almansoori, 2023).

Researchers have used a variety of frameworks to study how user behavior affects the security of IoT devices for smart homes. Theory of Planned Behavior (TPB), which Icek Ajzen created, offers a thorough framework for comprehending and forecasting human behavior in a variety of circumstances, such as the adoption of technology and security-related behaviors (Mondol, Tang, & Hasan, 2023).

According to the TPB, three fundamental elements - attitude, subjective standards, and perceived behavioral control - are the main determinants of human behavior (Ursavaş, 2022). The term "attitude" refers to a person's overall assessment or opinion about a certain behavior, which may include opinions on the results or repercussions of engaging in the behavior as well as the subjective importance placed on those results. Subjective norms refer to how a person feels about peer pressure or outside influences on certain behavior. It comprises opinions on what close friends and family members believe the individual should or shouldn't do, and also the desire to conform to these perceived expectations. The perceived simplicity or struggle of behavior is related to perceived behavioral control (Asare, 2020).

A deeper understanding of the factors influencing user behavior in relation to the security of IoT devices can be obtained by applying the Theory of Planned Behavior (TPB) within the context of smart home IoT security. This approach involves investigating perspectives on security measures, comprehending the influence of subjective norms, and assessing users' perceptions of control over the security of their devices. By employing the TPB framework, it is possible to gain insights into the various elements that shape user behavior in the realm of smart home IoT security.

To ensure the security of smart home devices, it is essential to investigate the impact of user behavior in the security of smart home IoT devices (Parsons, Panaousis, & Loukas, 2021; Zheng *et al.*, 2018). Understanding user behavior can be done with the help of TPB (Iqbal, 2019). This theory contends that an individual's desire to engage in a behavior, which is impacted by their mental state, perceived behavioral control, and subjective norms determines that behavior (Ajzen, 2019). The mindsets and views of users regarding security measures, the impact of cultural standards on their behavior, and their perceived control over the security of their devices must all

be understood in order to ensure the security of smart home devices (Klobas, McGill, & Wang, 2019).

Through the perspective of the TPB, we will analyze in this study how user behavior impacts the security of smart home IoT devices. In order to fully understand the variables influencing or impeding user adoption of security measures, we will analyze the constructs of mindset, perceived behavioral control, and subjective norms within the context of smart home IoT security.

1.2. Research Problem and Importance

As IoT-based home automation architecture becomes more prevalent, concerns about security have grown (Awotunde *et al.*, 2021). The lack of proper security features in smart home appliances makes them vulnerable to cyberattacks, compromising consumer privacy and the integrity of their data (Elkhediri, 2021). While technical aspects such as authentication, encryption, and other technical measures are important for security, user behavior is also an important factor that can expose smart home IoT devices to cyberattacks (Parsons, Panaousis, & Loukas, 2021). According to TPB, subjective standards, attitudes, and perceived behavioral control, all have an impact on behavior (Pham, Brennan, & Richardson, 2017). In order to better understand user behavior with regard to smart home security, it is imperative to comprehend their mindsets or attitudes, subjective standards, and perceived behavioral control (Mahlous, 2023). The existing research on the security of smart home IoT devices has not adequately addressed the impact of user behavior, specifically through the lens of the theory of planned behavior. This gap in the literature calls for further investigation into the relationship between user behavior and the security of these devices. Therefore, there is a requirement for a comprehensive investigation to determine the impact of user behavior and the factors that can potentially lead to cyberattacks. The ultimate goal is to devise and recommend effective practices for reducing the inherent dangers of cyberattacks. This research problem aims to address the literature gap and do research regarding the impact of user behavior in the security of smart home IoT devices.

The security of IoT devices for smart homes is a topic that requires investigation since smart homes are becoming more prevalent in everyday life (Awotunde *et al.*, 2021). Thermostats, smart speakers, and cameras are among the internet-connected appliances found in these houses. These electronic devices make life more convenient, but they can also pose security threats (Ahmed *et al.*, 2020). I can develop strategies to make these electronic devices safer by comprehending how

users act when utilizing them (Pattnaik, Li, & Nurse, 2023). Determining how user behavior affects the security of IoT-enabled smart homes is the goal of this research work in order to make recommendations on how to ensure privacy for individuals and avoid any possible harm.

The significance of this topic lies in the numerous security risks associated with smart home technology due to user behavior, which make smart home devices an attractive target for hackers. Home automation users, security personnel responsible for protecting remote control, and I will work to enhance the security of these systems from understanding the risks originated from user behavior.

1.1. Research Questions

To achieve the research purpose, I designed the following research questions;

- How does user behavior influence security of smart home IoT devices?
- How can security risks posed by user behavior for smart home IoT devices be mitigated through the development and recommendation of best practices?

1.2. Scope

This research aims to investigate the impact of user behavior on the security of smart home IoT devices. Specifically, the study aims to gain a comprehensive understanding of the different types of user behavior that can potentially contribute to security threats and risks within the realm of smart homes. The research will be conducted within a specified time frame of four months, allowing for meticulous data collection, analysis, and interpretation.

In terms of data collection, the primary focus of this study will be on security personnel who are actively engaged in the IoT-based industry and who possess relevant knowledge and experience in the field. This choice is based on the understanding that security personnel play a crucial role in ensuring the safety and integrity of smart home IoT devices as well as perspectives that enhance the general reliability and validity of the study findings. Their expertise and insights can provide valuable perspectives on user behavior, potential vulnerabilities, and effective security practices. The research intends to obtain extensive knowledge and a thorough comprehension of the topic by choosing individuals who have considerable skills and experience in the IoT market. Furthermore, a convenience sampling technique will be employed, resulting in a sample size of five participants.

The selection of security personnel will ensure the inclusion of individuals who both work in the IoT-based sector and utilize smart home IoT devices in their professional lives.

Moreover, the research methodology will involve conducting interviews with the selected participants, followed by the utilization of content analysis techniques for data analysis. This approach will enable the exploration and identification of patterns, themes, and insights pertaining to user behavior and its impact on the security of smart home IoT devices.

1.3. Thesis Structure

The thesis is structured as follows: chapter 2 provides a literature review, chapter 3 outlines the theory and interview questions, chapter 4 presents the methodology, chapter 5 shares the results, chapter 6 discusses the findings, chapter 7 concludes the thesis, chapter 8 includes the references, and chapter 9 contains the appendices.

2. Literature Review

2.1. Literature Review Method

I am following the method recommended by Levy and Ellis (2006) method for conducting literature reviews. The diagram illustrating the sequential steps employed in this study, devised by the author, is provided as an attachment below.

Further explanation regarding Levi's and Ellis's method is given below.

A conventional way for performing a literature search is the Levi and Ellis method described by Levy and Ellis (2006), which includes the following steps:

- **Phase 1 (Define Research Questions):** The first phase is to precisely describe the study issue or subject that will serve as the basis for the literature evaluation.
- **Phase 2 (Create a Search Strategy Plan):** To find pertinent material, the second phase entails creating a search strategy. This might entail looking through journal articles, electronic databases, conference proceedings, and other resources.
- **Phase 3 (Search for and Locate Articles):** The next phase is to carry out the search and locate appropriate articles after the search plan has been devised.
- **Phase 4 (Selection of Relevant Articles):** After collecting the documents, the following step is to assess and choose the ones that are pertinent to the study issue. Reading the abstracts, skimming the complete text, or checking the bibliographies of pertinent publications may all be necessary for this.
- **Phase 5 (Data Extraction and Analysis):** The final phase is data extraction and analysis from the chosen publications. The data may need to be coded, categorized, and analyzed for trends and common themes.
- **Phase 6 (Synthesize Findings):** In the last phase, the results of the existing literature are combined and put forward in a logical and well-structured way.

According to this approach, first of all, I defined the research question that is mentioned in chapter one. In phase 2, I created a search strategy. My search strategy was to use keywords including "smart home devices", "home automation", "internet of things", "user behavior in smart home security", "user awareness", "cybersecurity in smart homes", "vulnerabilities in smart homes", and "theory of planned behavior in security".

2.1.1. Selection Criteria

In phase 3, I visited libraries including “Google Scholar”, “IEEE Xplore”, “ScienceDirect”, “ACM Digital Library”, and “ResearchGate”. Using these libraries and keywords discussed above, the content was gathered. Furthermore, I searched articles from 2016 and 2023. In addition to this, I searched only English papers.

Moreover, a backward research technique is adopted to search for relevant material. By beginning with a major reference and moving backward through its citations, the backward research approach, often referred to as backward reference searching, is a strategy used in the existing literature to locate relevant material (Andreasen, 1985). It entails locating important sources pertinent to the issue of interest, then looking for relevant information in the references listed in those publications. The backward reference research approach is a helpful tool for doing a thorough and effective literature search. It may assist researchers in discovering important sources and pertinent information that would have escaped their notice through simple electronic databases searchers. I have used many papers as a starting point for backward search and one of them is the work of Ray and Bagwari (2018). Another inclusion criterion was the language of the articles and research papers. Additionally, the forward reference research approach was not utilized in the analysis.

According to phase 4, relevant articles were kept and irrelevant ones were deleted. Furthermore, based on phase 5 data was extracted from the relevant articles, and analysis was made.

Table 1: Showing Overview of the Literature Review Method Used

Source	**Searched Keyword**	**Inclusion Criteria**	**Exclusion Criteria**	**Backward Research**	**Forward Research**
Google Scholar	-Smart home devices -Home automation -Internet of things -User behavior in smart home security -User awareness	-English language -2016-2023	-other languages. -Older than 2016 -Which discusses	No	No

	-Cybersecurity in smart homes -Vulnerabilities in smart homes -Theory of planned behavior in security		energy related IoT factors		
IEEE Xplore	Same as above cell	Same as above cell	Same as above cell	No	No
ScienceDirect	Same as above cell	Same as above cell	Same as above cell	No	No
ACM Digital Library	Same as above cell	Same as above cell	Same as above cell	No	No
ResearchGate	Same as above cell	Same as above cell	Same as above cell	Yes, backward research from the references (Ray and Bagwari, 2018).	No

2.2. Results of Literature Review

2.2.1. Smart Home and IoT Overview

A house with internet-connected appliances that can be operated from a distance is referred to as a smart home. These devices are connected to a central hub or controller that allows homeowners to remotely manage functions such as temperature, security, and entertainment. According to Li *et al.* (2018), a connected home is a platform that utilizes IoT, information technology, control technology, digital communication mechanism, and visual display technology to satisfy automated demands.

The term "Internet of Things" was first coined by a participant in the Radio Frequency Identification (RFID) design community in 1990. Today, IoT is utilized in various industries including smart buildings, navigation systems, corporate monitoring, environmental protection, smart housing, government work, and senior care. It is used in areas such as intelligent transportation, personal health, and industrial monitoring to create a connected network of devices that can communicate seamlessly and enhance daily lives (Abdullah et al., 2019).

By building a smart, linked network of gadgets that can function and interact with one another, IoT aims to enhance sectors including healthcare, transportation, and agriculture (Abdullah et al., 2019). There are many benefits of IoT such as enhanced safety, comfort, and support for remote payment. The usage of IoT is becoming increasingly important for future development, and it creates an opportunity for individuals to complete tasks from anywhere, even in cooperative organizations.

IoT devices can be found anywhere in today's world including roads, cities, hospitals, homes, air conditioners, controlling doors, and many more. This increase in attack surfaces increases the attackers' starvation to exploit the IoT networks and theft data (Hameed & Alomary, 2019). As technology is growing at the fastest pace. The malicious users are also equipping themselves with the latest technology. They are advancing in malicious technology. The confidentiality and security of IoT devices are being compromised due to technological development. IoT devices collect the personal data of users that is shared with other devices and stored in an online database. The data is always at risk of theft by malicious users (Sharad, 2017). IoT devices are vulnerable to information distortion, disclosure, eavesdropping, and many more. In addition to these threats, IoT applications face problems at the application level. The problems at the application layer are the protection of intellectual property rights, data processing, confidential information protection, and many more (Dash *et al.*, 2019; Bagay, 2020). The IoT components include people and processes, connectivity, and sensors. All the components are vulnerable to security threats in the absence of related standards and measures (Jani & Chaubey, 2020).

For a secure smart home setting, it is essential to comprehend how user behavior affects the security of IoT devices. With an emphasis on TPB as a theoretical framework for comprehending user behavior in connection to smart home IoT security, this literature review intends to analyze the available research on the subject.

2.2.2. Security Objectives of Smart Home

The first step in assuring reliable and persistent functioning is to define the security objectives that the home automation environment is intended to fulfill. The security goals of home automation include availability, confidentiality, integrity, authorization, authenticity, and non-repudiation (Shouran, Ashari, & Kuntoro, 2019). In addition to their sensing and monitoring abilities, sensors cooperate and interact with one another to exchange, disseminate, and analyze sensed data and assist authentic decision-making processes by producing appropriate alerts and reactions. Yet in scenarios involving smart homes, protecting privacy and ensuring adequate security in these essential services offered by wireless sensor networks is a major problem (Islam, Shen, & Wsang, 2012).

Furthermore, in the context of smart homes, understanding users' behavior is essential in comprehending why they may fail to adopt secure behaviors or follow security best practices. TPB can be utilized to understand users' perceptions of security risks and their opinions on the effectiveness of security solutions, which can influence their choices regarding safe behaviors in the realm of smart home security. Secured user behavior is a security objective of smart home IoT security (Sun *et al.*, 2023).

Batalla, Vasilakos and Gajewski (2017) provided a thorough overview of the suggested solutions for security, ranking them according to complexity, use-spreading, compatibility, and efficiency. Further, they reviewed the legitimate and incorrect solutions for the present systems incorporated into the home setting, taking into account all the security objectives where Smart Buildings are at risk, including authenticity, integrity, confidentiality, authorization, nonrepudiation, and availability.

2.2.3. Understanding User Behavior in the Smart Home

Smart homes rely significantly on user behavior for security. Since these devices are frequently linked to the web, hackers may utilize system flaws to enter the network of a user without authorization (Yamauchi *et al.*, 2019). According to research, users' ignorance of security issues and bad security habits, such as using passwords that are weak and not keeping devices up to date, significantly increase the security dangers connected with these electronic devices (Vikas, 2020).

Designing a risk framework for the home requires knowledge of a user's actions and mindset toward IoT devices (Parsons, Panaousis, & Loukas, 2021). Users' intentions to utilize smart home

gadgets are influenced by their impression of security, and they depend on companies to secure their confidentiality (Mahlous, 2023).

Moreover, assessing customers' beliefs, attitudes, and worries regarding the security features and functions of the devices is necessary for comprehending how they see security. This information can assist developers in identifying possible holes or weak points in the current security mechanism and in creating effective ways to close them (Nemec Zlatolas, Feher, & Hölbl, 2022).

Additionally, security choices are crucial in the framework of smart home IoT devices for safeguarding private information, blocking unauthorized access, and maintaining the overall security of the systems and their users. However, if there are significant differences in customers' perceptions of the value of security measures, it may cause them to be unaware of or careless about putting appropriate security practices into place (Goffinet *et al.*, 2021).

In order to combat cyber threats, it is necessary to enhance cyber security culture and place an emphasis on human elements in cybersecurity. The human component has been highlighted as the most vulnerable component in the security of data. By encouraging security behavior and collecting data on all relevant factors, the study suggests a theoretical framework for boosting cyber resilience in IoT users. The framework can serve as the basis for designing policies to increase cyber resilience, particularly in Indonesia (Amraoui *et al.*, 2020).

Further, a paper recommended the use of SPIDAR. The creation of "SPIDAR" to guard against IoT device assaults on residential Wi-Fi networks is the main focus of the paper by (Visoottiviseth *et al.*, 2020). The lack of security knowledge among IoT developers and consumers is discussed in the paper, as is the requirement for an affordable solution to defend networks at home from online threats. The SPIDAR system employs both behavior-based and signature-based preventative techniques to guard against five common attack types. The system consists of a Raspberry Pi, a home Wi-Fi, and a web-based application that shows users' attack information.

Furthermore, the main goal of the paper by Yamauchi *et al.* (2019) is to provide a technique for identifying cyber assaults on IoT gadgets that are challenging to identify since they utilize the identical protocol as authorized user activities. The suggested approach is based on simulating user actions as a series of events, including the use of IoT gadgets and other actions seen by sensors. To identify assaults, the approach compares the order of happenings, including the present

operation, with the learned patterns for each of a predetermined set of circumstances. The authors show the correctness of the suggested strategy while outlining its drawbacks using data gathered by observing the actions of four users.

2.2.4. Role of the Factors of TPB in Smart Home Adoption and Security

The findings of the study by Hadlington (2018) showed a substantial inverse relationship between dangerous cyber security behaviors and cyberspace security beliefs. Research shown that participants who had more unfavorable views towards security exhibited higher levels of unsafe behavior (Nikel & Amaechi, 2022). Additionally, there were noticeable disparities in the incidence of participating in unsafe cyber security behavior and attitudes depending on the scale of the organization and the age category.

Furthermore, the use of smart home security solutions is significantly influenced by how privacy and security are perceived. According to research, people are more likely to do such actions when they believe they are secure and protected (Zimmermann *et al.*, 2020;Wei *et al.*, 2019) . The widespread use of smart home technologies is also significantly impacted by worries about possible security concerns (Cannizzaro *et al.*, 2020). Moreover, the assessment made by parents regarding potential safety risks to their children is significantly impacted by their perception of safety threats specifically related to smart home environments. The level of awareness and concerns they hold regarding the risks associated with smart home technologies play a crucial role in shaping their attitude towards the security threats targeting children in such contexts (Sun *et al.*, 2021).

Additionally, TPB aids in understanding why users could participate in dangerous behaviors that endanger their privacy as well as how treatments based on behavior theory could reduce these risks (Moustafa, Bello, & Maurushat, 2021).

2.2.5. Privacy Threat Analysis

Moreover, by proposing and building a framework for privacy and security threat modeling for a smart devices design using components that are readily available, Geneiatakis *et al.* (2017) created interest in the topic. Authors employ a home automation IoT architecture to do this, allowing consumers to connect with it through a variety of devices that support house automation management, and they assess numerous situations to find any potential privacy and security issues for users. This method gives a realistic impression of privacy and security threat assessments for

a typical connected home design that depends on already-commercially-available IoT platforms and devices.

More dynamically, cyber-connected operating settings are being developed and deployed, including smart cities, smart homes, and smart transport networks. The data security evaluation of these dynamic environments calls for the use of the process of risk assessment methodologies and the modeling of highly dynamic situations. The spread of IoT systems broadens the attack surfaces in the intelligent home setting, which is the focus of Kavallieratos *et al.* (2019). By using a reference design for smart buildings, authors analyze current dynamic threat assessment approaches and discover security threats from a smart home's structural and communicative views while also keeping in mind changing operational factors. In addition, they create a topology generator for smart home networks and a diagram-based attack model to examine how constantly changing conditions are interconnected and how malware spreads.

For modeling and studying the security concerns of smart buildings, Bugeja, Jacobsson, and Davidsson (2021) offer a system called PRASH. It is made up of three parts that work together to determine how much security risk a connected home network is exposed to a threat model, a system model, and a collection of security parameters. Using a formal model to define a smart house, PRASH enables early malware detection, improved preparation for risk management situations, and reduction of probable attacks' effects before they endanger occupants' lives. The suggested formal specifications were used to create an operational version of the smart home configuration, which was then examined to identify potential attack vectors and reduce the effects of those cyberattacks. This was done to show the abilities of PRASH. By doing this, the authors significantly advance our understanding of how to prevent attack agents from invading users' confidentiality at home. In general, people's right to privacy will be protected through the usage of PRASH even when new problems with smart homes arise.

One of the main obstacles to the goal of smart, power-efficient homes and buildings is the implementation of cybersecurity in IoT device settings. Finding the risks associated with using and potentially abusing information about houses, friends, and ultimate consumer is challenging and takes extensive research. It is also necessary to develop strategies for adding security measures into the design. A home automation system that was developed as part of a research project involving significant industrial organizations underwent a risk assessment. Nine of the 32 threats

that were examined were classified as low-impact risks and four as high-impact risks, making the bulk of the dangers fall into the medium-risk category. Both the system's software and human components were seen to provide significant risks. The results demonstrate that both existing and new risks may be diminished to tolerable proportions with the implementation of traditional security measures, but the most significant risks, i.e., those arising from the human element, require extra great consideration provided that they principally challenging to manage. An examination of the consequences of the threat assessment results emphasizes the demand for a more general model of privacy and security to be integrated into the design phase of smart buildings (Jacobsson, Boldt, & Carlsson, 2016).

Technology is anticipated to play a key role in the design of smart buildings by offering residents efficiency and convenience for a greater quality of life. The incorporation of the IoT concept into smart buildings raises questions regarding the validity, privacy, and authenticity of the information sensed, gathered, and communicated by the IoT gadgets. IoT-based home automation is risky as a result of these problems since it is particularly susceptible to many types of security assaults. To provide a thorough image of the security condition of home automation, it is essential to recognize the potential security concerns. Ali and Awad (2018) evaluated the security threats associated with smart homes using the technically critical assets, risks, and vulnerability evaluation method OCTAVE sometimes referred to it as OCTAVE Allegro. The OCTAVE Allegro approach concentrates on data resources and takes into account various information carriers, including databases, actual documents, and people. This study's main objectives are to highlight the numerous security vulnerabilities in IoT-based smart buildings, to describe the hazards to their inhabitants, and to offer solutions for lowering those risks. The study's conclusions might serve as a starting point for enhancing the security specifications for IoT-based smart buildings.

2.2.6. Security Concerns and Risk Associated with Smart Home IoT Devices Due to Human Factors

As technology provides all of the required services, such smart homes may serve as a city in our modern period, but they require ongoing surveillance and maintenance. One of the most significant concerns is related to privacy and surveillance, as smart devices can capture and transmit personal data, leading to potential misuse by hackers or other malicious actors. The main reason behind these concerns is the lack of knowledge and awareness among users. Additionally, maintenance

of smart home devices can be challenging, as software updates and hardware malfunctions can create vulnerabilities and cause devices to malfunction, leading to potential safety risks (Coboi *et al.*, 2021).

2.2.6.1. Privacy Risks

According to OVIC (2021), the possibility of hacking and illegal access to personal information, due to user behavior, is one of the key hazards connected with smart home technology. Personal information, including user preferences and device usage habits, is frequently collected and stored by smart home devices, which might be lucrative to hackers.

2.2.6.2. Physical Risks due to Human Behavior

Physical dangers resulting from human behavior in IoT devices can represent serious concerns to people as well as the environment. When engaging with IoT devices, human actions and behaviors have the potential to directly or indirectly cause personal harm, accidents, and damage to property. Identifying these risks is essential for creating safety measures and reducing possible threats (Cobb, 2021).

2.2.6.3. Human Threats

Human threats are dangers and risks that result from people's purposeful or inadvertent acts that have the goal of harming or disrupting a system. The two categories of these risks are internal threats and external threats. Internal threats arise when users who have been granted access to a network or system abuse their rights to commit hostile acts. On the other side, external threats are people or groups that are not a member of the network but attempt to harm or disrupt operations by taking advantage of security flaws or breaches in the network. These human threats aim to undermine the targeted system's security, potentially causing severe harm or impairing its functionality (Abomhara & Køien, 2015).

2.2.6.4. Malware and Operational Risks

Human interaction with IoT devices can result in a variety of possible risks and vulnerabilities, including malware and operational concerns brought on by these interactions. Human mistakes, ignorance, or malevolent intent are frequently to blame for these dangers. Furthermore, the security of IoT devices is significantly in danger from malware. Malware can unintentionally enter a system through human actions like downloading and installing unverified apps or clicking on unsafe

URLs. Malware can damage a device's operation once it has been infected, steal confidential data, or grant unauthorized access to criminals (Kobis, 2021).

2.2.6.5. Risky Human Factors

Users may be more susceptible to cyberattacks because they are less aware of potential risks and threats connected with IoT devices (Amraoui *et al.*, 2020). Risks resulting from human factors might take many different forms in the context of smart home IoT devices. Users may act irresponsibly by disclosing private information, ignoring the updating of default passwords (Hughes-Lartey *et al.*, 2021), using infected networks, omitting to upgrade software, or participating in risky online behaviors (Kobis, 2021). These acts may leave IoT devices vulnerable to security flaws, allowing unauthorized access, exposing personal information, or engaging in criminal behavior.

2.2.6.6. Other concerns

A growing issue is the potential for IoT devices to obtain and collect enormous amounts of data, including data that consumers might not be aware of. Because of their versatility and user-friendliness, smart speakers are becoming more and more common. Recent studies have raised questions regarding the privacy of personal and even national security since it appears that Smart Speakers may still be able to listen in on user conversations even when they are turned off (Jayatilleke, Thelijjagoda, & Pathirana, 2019). By taking into account people's attitudes towards risks associated with subjective norms, privacy for privacy-conscious behavior, and their perceived power over settings for privacy and information security, these issues may be addressed via the TPB's perspective. TPB may help create strategies to encourage responsible user behavior with respect to smart speakers and connected devices. Moreover, all the concerns are displayed in the pictorial form and the picture is attached below.

In summary, security concerns and risks related to IoT devices in smart homes due to human factors include privacy risks related to hacking and unauthorized access to personal information stored by smart devices. Human behavior can also lead to physical risks, such as accidents and property damage, as well as human threats from both internal and external sources. Malware and operational risks can arise from human interactions, including downloading unverified apps and clicking on unsafe URLs. Risky human factors, such as irresponsible behavior and failure to update passwords or software, can leave IoT devices vulnerable to security flaws. Additionally, concerns

related to data collection by IoT devices, particularly smart speakers, raise privacy and security questions. The factors are depicted in the attached pictorial representation.

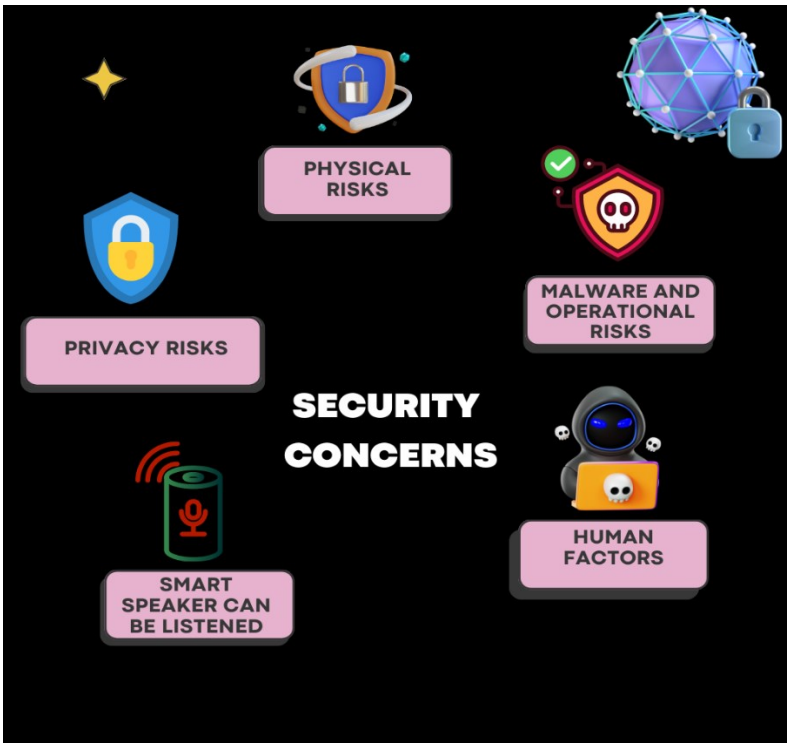

Figure 1: Showing security concerns associated with smart homes

2.2.7. Different Solutions to Smart Home

The study by Amraoui *et al.* (2020) introduces TRICA, a security framework that focuses on securing smart homes from cyber threats. The framework ensures that only authorized users can access and control IoT devices through smartphone apps. To achieve this, TRICA utilizes Anomaly Detection (AD) and User Behavior Analytics (UBA) techniques to gather and analyze user's past cyber and physical activities, as well as the historical states of the smart home system. This data is then used to construct a One Class Support Vector Machines (OCSVM) model, which serves as a benchmark for identifying anomalous commands (i.e., outliers) and legitimate commands (i.e., targets) to be executed. Real-world data has been used to assess the framework and the framework has demonstrated high accuracy in identifying and rejecting anomalous commands while allowing normal commands to be executed. This approach provides a balance between user convenience and security, with low false accept and false reject rates.

Moreover, a system known as "A System for Preventing IoT Device Attacks on Home Wi-Fi Router (SPIDAR)" was created and constructed to defend against attacks on home Wi-Fi networks. The system consists of a SPIDAR Raspberry Pi, a SPIDAR home Wi-Fi router, and a SPIDAR web application that not only protects against attacks but also provides home users with attack statistics. By avoiding the need to buy pricey hardware and intrusion prevention software for installation at home, this solution saves money. The solution uses machine learning and Snort software to analyze the behavior of IoT devices, preventing attacks using both signature-based and behavior-based approaches (Visoottiviseth *et al.*, 2020).

Further, another research introduced a novel user-based method for detecting attacks on IoT devices. The technique put forward describes human behavior as a series of actions, including how IoT devices function as well as any other actions that could be seen by sensors. The method learns occurring sequences for each predetermined set of situations, then compares the present sequence of incidents with the learned patterns to find assaults (Yamauchi *et al.*, 2019).

2.2.8. Summary of Literature Review

The literature review gives a general overview of smart homes and IoT's contribution to the development of automated and linked environments. It emphasizes the advantages of IoT and how widely it is applied across several sectors. However, it also discusses the security issues with IoT devices, such as privacy violations and data theft. The literature analyzes the relevance of the TPB in comprehending user perceptions and decisions, emphasizing the significance of comprehending user behavior in connection with smart home IoT security. It talks about the security goals of smart homes, how user behavior affects security, and the factors influencing user adoption of secure behaviors. Furthermore, different security concerns associated with human factors were also discussed. The review also provides a variety of methods and frameworks for analyzing security and privacy vulnerabilities in IoT devices for smart homes. In order to develop and operate smart homes effectively and securely, it is imperative to take human factors into account.

2.2.9. Research Gap

The summary highlights several studies that propose solutions for improving the security of IoT devices in smart homes by analyzing user behavior. However, there is a gap in the literature regarding the comprehensive investigation of the impact of user behavior on the security of smart

home IoT devices, specifically by utilizing the theory of planned behavior. Although several studies propose solutions that consider user behavior, there is a need for a comprehensive investigation that focuses on the user behavior aspect to develop more effective security practices by utilizing theory of planned behavior.

3. Theory

In the latter part of the 1980s, Icek Ajzen created a behavioral theory known as TPB (Theory of Planned Behavior). It offers a paradigm for comprehending and forecasting behavior in a variety of domains, such as health, the social sciences, and technological adoption. According to the idea, three fundamental elements, subjective standards, attitude, and behavioral control, are the main determinants of human conduct or attitude. First of all, I will talk about attitude. A person's overall assessment or impression of a particular behavior is referred to as their attitude. It includes the individual's perceptions of the results or repercussions of engaging in the behavior as well as the personal significance placed on those results. While a negative mindset may hinder involvement in behavior, a positive mindset is more likely to result in its acceptance (Cannizzaro *et al.*, 2020).

A person's perception of social pressure or external influences on certain behavior is referred to as subjective norms. It contains opinions about what important individuals, such as individuals in social circles, believe the person ought to or ought not to do. Perceived behavioral control is another term for a person's judgment of their ability to engage in the behavior. It covers elements that may influence behavior, including the existence of facilitators or obstacles (Smith, 2003).

TPB holds relevance to the investigation of user behavior's impact on the security of smart home IoT devices due to multiple key reasons. Primarily, it contributes to the comprehension of human behavior within this context (Health Communication Capacity Collaborative, 2021). Additionally, it assists in understanding the variables that affect user behavior (Conner, 2020). Lastly, it provides insights into strategies for modifying and enhancing behavior.

In the context of investigating the impact of user behavior on the security of smart home IoT devices, TPB is a relevant and valuable approach. This theory offers a framework for understanding and predicting human behavior in various domains, including technological adoption and information security. By applying the TPB, I aim to explore the factors that influence user behavior in smart homes enabled by IoT and identify effective strategies for modifying and enhancing user behavior towards information security.

TPB will be utilized to investigate the impact of user behavior on smart home IoT device security. It will help identify common user behaviors that contribute to security risks, examine the influence of demographics on behavior, analyze the evolution of behavior and its implications for security,

and explore the factors that shape user behavior. By employing the TPB, effective strategies and practices can be identified to mitigate security concerns, enhance IoT architecture, and promote user education and awareness. The TPB will serve as a valuable framework for understanding and addressing the relationship between user behavior and smart home IoT device security.

4. Research Methodology

4.1. Research Approach

In this study qualitative research methodology was employed. Qualitative research methodology allows for a comprehensive exploration and understanding of the research topic, particularly when studying complex social problems that are challenging to quantify using numerical data. This approach involves gathering and analyzing non-numerical data, such as interviews, observations, and printed material, to comprehend and explain social trends (MACK *et al.*, n.d.). The qualitative research approach was chosen to gain insights into user behavior and security risks associated with smart home IoT devices.

4.2. Qualitative Research

Qualitative research offers valuable insights into complex societal issues and individual experiences, attitudes, beliefs, and practices. It allows for a comprehensive understanding of subjective aspects of human behavior and social relationships (Maison, 2018). Given the focus of this study on user behavior and security threats in smart home IoT devices, a qualitative approach was selected to thoroughly examine the issue.

The decision to employ a qualitative approach in studying behavioral aspects is driven by multiple reasons. Firstly, qualitative methods are best suited for understanding and investigating behaviors that involve subjective experiences, meanings, and interpretations, requiring in-depth exploration and analysis (Daniel, 2016). Secondly, a qualitative approach aligns with the interpretivist paradigm, which emphasizes comprehending the social and cultural contexts surrounding behavior rather than relying solely on objective measurements. Consequently, a qualitative research approach is considered appropriate for this study, enabling a comprehensive examination of behavior and facilitating a deep understanding of the underlying factors and dynamics influencing it.

Researchers can utilize various qualitative approaches, including observations, interviews, and document analysis, to gather rich and nuanced data that captures the complexity of user behavior (Rahman, 2016). The chosen research methodology plays a pivotal role in effectively addressing the interview questions and ensuring a systematic and structured approach. By adopting this

methodology, the study aims to yield meaningful insights and findings by comprehensively addressing the research questions. The interview questions are outlined in the subsequent section.

4.3. Overview of Interview Questions

My interview questions are based on the literature review findings. The interview questions are written in the **Appendix A**. Their overview is as follows. These questions primarily focus on exploring the relationship between user behavior and the security risks related to smart home IoT devices. They aim to identify common behaviors that may expose these devices to security threats, investigate how user behavior changes based on demographic factors, and examine the impact of evolving user behavior on the security of IoT devices. Additionally, the questions seek to identify the primary factors that influence user behavior in smart homes, identify best practices for lowering security concerns related to user behavior, and suggest ways to improve the architecture of IoT-enabled smart homes to promote safer user behavior. Finally, the questions also aim to understand how user education and awareness can help mitigate security risks for smart home IoT devices.

4.4. Overview of the Interviewees

A total of five individuals, representing various roles within the IoT-based sector, were interviewed as part of this study. These roles included two IoT engineers, one IT manager, and two security analysts. The specific details of each interviewee are provided in the table presented below.

Table 2: Professional overview of Interviewees

Interviewee Number	**Role**	**Experience**
Interviewee 1	IoT Engineer	5 years
Interviewee 2	IT Manager	8 years
Interviewee 3	IoT Engineer	7 years
Interviewee 4	Security Analyst	6 years
Interviewee 5	Security Analyst	7 years

4.5. Data Collection

In this study, data was collected through the primary method interviews. The interviewees, from Sweden, will consist of security personnel from Sweden-based companies that provide security solutions for IoT-based infrastructures. These individuals possess extensive knowledge and

experience in securing IoT systems and can provide valuable insights into the security challenges and solutions in this field.

To gain a thorough grasp of the study issue, numerous data gathering techniques are used in qualitative research. In addition to interviews and surveys, other common methods include document analysis, focus groups, observations, and case studies. However, semi-structured interviews are the best techniques for obtaining data since they allow for in-depth investigation of the research issue and provide the researcher a chance to fully comprehend the participants' experiences, viewpoints, and practices.

4.6. Convenience Sampling

This sampling strategy was a non-probability sampling strategy that involved choosing participants for the study who were easily reachable or readily available. When a researcher has little time, money, or access to the target group, they frequently adopt this strategy. When picking interviewees for convenience sampling, consideration is given to their availability and desire to participate in the study rather than their suitability or representativeness for the research (Bhardwaj, 2019).

4.7. Interviews

In interviews, a researcher communicated with an interviewee in a one-on-one chat to learn more about their views, ideas, and beliefs on a certain topic. In accordance with the amount of flexibility in the questions and the degree to which the researcher has control over the interviews, interviews can take a variety of forms, such as structured interviews, unstructured interviews, or semi-structured interviews. In this work, I utilized interviews for data collection. Interviews were conducted online using Zoom.

4.7.1. Semi-Structured Interviews

In a semi-structured interview, the interviewer has a basic overview or a list of issues to ask the interviewee, but the interview is still open-ended enough just to allow for follow-up queries and more questioning. In-depth and extensive insight into the interviewee's experience, attitudes, and viewpoints may be obtained through this form of the interview since it strikes a balance between flexibility and structure (Adams, 2015). In this research work, semi-structured interviews were conducted. For this, interviews were conducted with 5 participants.

4.8. Data Analysis

With the use of qualitative methods for data analysis like content analysis, the information obtained from interviews were examined. I was able to spot similarities and contrasts in the replies of the participants once the data was processed and arranged into patterns and themes. The data analysis helped the researcher make suggestions for enhancing the security of these systems by revealing the security issues and solutions in IoT-based infrastructures.

In this work, the data analysis was performed using the content analysis technique. Data gathered from various sources was analyzed using content analysis. This approach is used to recognize and examine a text's underlying ideas. (Bell & Bryman, 2007).

The complete research methodology is explained in the attached picture.

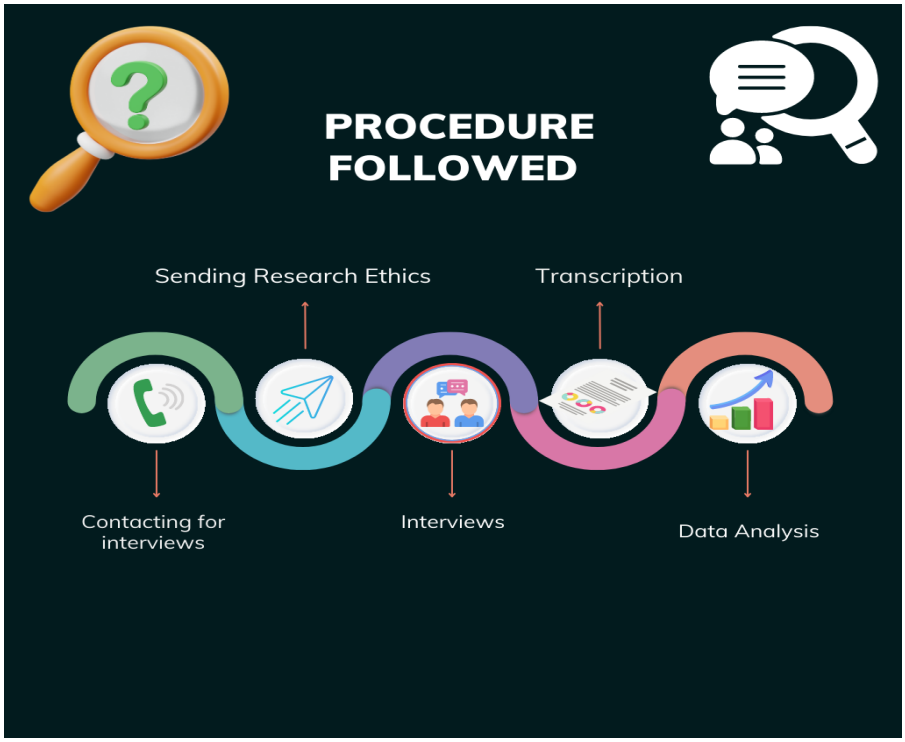

Figure 2: Depiction of research process used

4.9. Research Ethics

Research ethics are a collection of values and guidelines that help researchers do their work in an honest and ethical way. Some research ethics (Parveen & Showkat, 2017) that were utilized in this work include:

- ❖ The goal of the study, the steps involved, and any concerns or advantages that were included were adequately disclosed to the participants. All of the above-discussed aspects were explained with the help of a written document.
- ❖ Researchers took precautions to safeguard the privacy of client data and made sure that no private details were released even without the participant's permission.
- ❖ Participants' privacy was respected, and researchers took care to avoid observing them.

4.10. Validation

A member-checking process, a qualitative research technique used to increase the trustworthiness and reliability of the results, was used to validate the research's findings. The interviewees were informed of the study results during that process, and their input and suggestions were sought. This iterative process made sure that the interviewees had a chance to examine and confirm the results, which gave the findings more credibility.

5. Results

The chosen method for data collection in this study was the interview method. Five professionals in the IoT industry were successfully interviewed via LinkedIn, and their interviews were conducted in video format and subsequently transcribed into written form. The analysis of the responses is available in the form of tables in **Appendix B**.

5.1. Common User Behavior that Exposes IoT Devices to Security Risks

When exploring the question of common user behaviors that may expose smart home IoT devices to security risks, the interviewees unanimously identified a common theme: irresponsible user behavior. The responses highlighted that poor security practices resulting from such behavior significantly undermine the security of smart home IoT devices, posing various security risks. It became evident that irresponsible user behavior constitutes a primary factor leading to security vulnerabilities in the context of smart homes.

The interviewees emphasized several common user behaviors and attitudes that contribute to the aforementioned security risks. Sharing sensitive information emerged as a prevalent concern, as users may unknowingly divulge critical details about their smart home devices, network configurations, or access credentials to unauthorized individuals. Such information sharing can potentially grant malicious actors the means to compromise the security of smart home environment. Another behavior identified was the failure to update default passwords on smart home IoT devices. Exploiting default passwords is a well-known tactic among attackers seeking to gain control over IoT devices and potentially infiltrate the connected network.

Further, using compromised networks was also highlighted as a risky user behavior. This exposes their devices to cyberattacks and unauthorized access by malicious actors present on the same network. In addition to this, neglecting firmware updates was recognized as a detrimental user behavior. Users who fail to regularly update the firmware of their smart home devices miss out on essential security patches and bug fixes provided by manufacturers. This oversight can lead to unaddressed vulnerabilities that attackers can exploit to compromise the device's security.

Furthermore, it was found that the usage of unsecure Wi-Fi networks further exacerbates security risks. Attackers can intercept data transmitted over these networks, gain unauthorized access to devices, or even launch man-in-the-middle attacks, compromising the security of the smart home

system. Moreover, weak password practices were identified as a significant user behavior contributing to security risks. Attackers can employ brute-force or dictionary attacks to exploit weak passwords and gain unauthorized access to the devices and their associated systems.

Additionally, interviewees emphasized the importance of securing the home network as a critical user responsibility. Failure to secure the home network effectively provides a gateway for attackers to compromise smart home IoT devices and potentially gain unauthorized access to sensitive data. Lastly, user behavior related to interacting with suspicious links or downloading unverified apps was highlighted as a significant risk factor. Engaging in the act of downloading unverified applications or interacting with suspicious links can potentially result in disastrous outcomes.

5.2. Demographic Factors and User Behavior

When examining the impact of demographics, such as age, gender, and technical knowledge and experience, on user behavior and its influence on cybersecurity, a consistent theme emerged from the interviews. It became evident that demographic factors play a significant role in shaping user behavior. The interviewees emphasized that age, gender, and technical knowledge and experience have distinct effects on user behavior, particularly regarding device protection, software updating, and self-efficacy in cybersecurity.

One of the interviewees, identified as interviewee 5, answered that older users tend to prioritize software security but may not give equal attention to protecting their devices. This finding suggests that age is a determining factor in the specific cybersecurity behaviors exhibited by users. Moreover, it was observed that self-efficacy, or one's belief in their ability to perform specific actions, mediates the relationship between age and cybersecurity behaviors. This means that the level of self-efficacy influences how age impacts the security practices of individuals. On the other hand, gender was not identified as a significant predictor of security behavior among the interviewees. This finding indicates that gender does not have a substantial influence on user behavior concerning the security of smart homes IoT devices.

To conclude, the analysis of the interviews revealed that user behavior varies based on several demographic factors, including age, gender, technical skills, and cultural differences. Age influences the priority given to software security versus device protection, while self-efficacy plays a mediating role in the connection between age and cybersecurity behaviors. Gender, however, does not emerge as a prominent factor in determining security behavior. These findings highlight

the importance of considering demographic characteristics when designing cybersecurity strategies and educational programs tailored to users' specific needs and behaviors.

5.3. Evolution of User Behavior and Security Implications

When exploring the evolution of user behavior and its implications for the security of smart homes IoT devices, the interviews revealed a mixture of positive and negative impacts. The evolution of user behavior was found to have both advantages and disadvantages in terms of smart home security.

According to interviewee 1, as users become more familiar with smart home IoT devices and their capabilities, they tend to become more comfortable experimenting with different configurations and connecting additional devices to their network. While this experimentation and expansion of device connections can enhance the functionality and convenience of the smart home ecosystem, it also brings forth certain security challenges. The increased number of devices and configurations can expand the attack surface, providing potential attackers with more entry points to exploit. Consequently, securing the entire smart home ecosystem becomes more complex and demanding.

Moreover, the evolution of user behavior may have negative impacts on security as well. Interviewee 4 emphasizes this by stating, *"User behavior can really make a difference when it comes to the IoT devices security. It was found from the research that the more people know about data breaches, personal info leaks, ransomware attacks, and vulnerabilities in devices can affect the more they care about IoT security. But here's the thing: many users don't bother checking their security settings, and they often think they're safe while using IoT devices. So, it's really important to raise awareness about these risks and encourage people to take security seriously".* Simply being aware of security risks does not automatically translate into implementing adequate security measures, and this discrepancy can pose significant vulnerabilities.

5.4. Factors Influencing User Behavior

When asked about the primary factors that influence user behavior when interacting with IoT devices in smart homes and how they affect security risks, a comprehensive analysis of the interviewees' responses revealed a range of influential factors. These factors play an important role in shaping user behavior and attitudes towards IoT devices security.

Based on the analysis, several key factors emerged as influencers of user behavior and the adoption of smart home technology. These factors include convenience, technical knowledge, trust, ease of

use, enjoyment, awareness, perceived risks, demographic factors, technical skills, experience, and security concerns. When it pertains to the security of smart homes IoT devices, each of these variables influences users' decision-making and behavior.

One interviewee, identified as interviewee 1, specifically pointed out that these factors can impact the likelihood of users compromising security in favor of convenience. This highlights the importance of understanding the trade-off between convenience and security and how users prioritize their needs and preferences.

5.5. Best Practices for Lowering Security Concerns

When inquired about the best practices for lowering security concerns associated with user behavior for IoT devices in smart homes, the interviewees shared diverse perspectives and recommendations. After conducting a thorough analysis of their responses, it became evident that implementing a range of security measures is crucial for safeguarding IoT devices, minimizing vulnerabilities, and ensuring data privacy.

One fundamental practice emphasized by the interviewees is changing default credentials. By replacing default usernames and passwords with unique and strong alternatives, the security of IoT devices can be enhanced. This practice acts as an essential first step in fortifying the security of smart home ecosystems. In addition, regularly updating firmware emerged as another crucial practice highlighted by the interviewees. Keeping the firmware of IoT devices up to date ensures that they receive the latest security patches and fixes for known vulnerabilities. By promptly applying firmware updates, users can effectively mitigate potential security.

The interviewees also stressed the significance of downloading applications and software updates exclusively from verified sources. By obtaining software and apps from trusted providers, users can minimize the risk of inadvertently installing malicious software that can compromise the security of their IoT devices. This practice helps ensure the integrity and authenticity of the software being installed.

Enhancing network security emerged as a vital aspect of mitigating security concerns. Interviewees recommended implementing measures such as using secure Wi-Fi networks, enabling encryption protocols, and configuring firewalls to create an additional layer of protection for smart home IoT

devices. By securing the network infrastructure, users can prevent unauthorized access and potential attacks on their devices.

Providing user education and awareness was identified as a critical practice in promoting secure behavior. Interviewees emphasized the importance of educating users about potential security risks, best practices for secure device usage, and the significance of maintaining a security-conscious mindset. By equipping users with knowledge and awareness, they can make informed decisions and actively contribute to the security of their IoT devices.

The interviewees also highlighted the potential of emerging technologies in enhancing security. They recommended leveraging artificial intelligence (AI) and blockchain technology to reinforce the security of smart home IoT devices. AI can help detect and respond to abnormal device behavior or potential threats, while blockchain can provide a decentralized and tamper-resistant platform for secure transactions and data exchange within the smart home ecosystem. As interviewee 1 expressed: *"For me, the best practice is the adoption of latest technology in dealing with security threats related to smart devices and also the awareness among the users. Incorporation of latest technology such as artificial intelligence can prevent cyber-attacks on smart home devices. I believe, raising awareness among users will not only prevent cyber-attacks on smart devices but also helps to develop new ways of tackling cyber threat in smart devices".*

Incorporating these best practices collectively plays a significant role in reducing security risks related to user behavior in IoT devices for smart homes. By implementing measures such as changing default credentials, regularly updating firmware, downloading from verified sources, enhancing network security, providing user education, and leveraging emerging technologies, users can significantly strengthen the security posture of their smart homes and protect their data privacy.

5.6. Enhancing the Architecture of IoT-enabled Smart Homes for Improved Security

During the discussion on how the architecture of IoT-enabled smart homes could be enhanced to promote safer user behavior and reduce security risks, valuable insights were provided by all the interviewees. Their responses revolved around common themes, emphasizing the implementation of various measures to bolster security and protect against potential vulnerabilities.

One prominent aspect highlighted by the interviewees is the use of strong authentication and access control mechanisms. By incorporating robust authentication protocols, such as multifactor authentication or biometric authentication, smart home systems can ensure that only authorized individuals can access and interact with IoT devices. This helps prevent unauthorized access and strengthens the overall security of the smart home ecosystem.

The adoption of cryptographic algorithms emerged as another crucial consideration in improving smart home security. Implementing strong encryption algorithms can safeguard sensitive data transmitted between IoT devices, preventing eavesdropping or unauthorized interception. This ensures the security of data exchanged within the smart home environment.

Subcategories within the interviewees' responses also highlighted the importance of user-friendly interfaces in smart home devices. By designing intuitive and user-friendly interfaces, smart home systems can facilitate seamless user interactions, reducing the likelihood of user errors or unintentional security vulnerabilities.

Furthermore, ensuring accessibility of smart home devices to lower social classes was deemed significant. The interviewees recognized the importance of making IoT-enabled smart homes inclusive and affordable to a wider population, enabling more individuals to benefit from the convenience and security offered by these systems. This inclusivity helps bridge the digital divide and promotes safer user behavior across different socioeconomic groups.

Overall, the interviewees provided valuable insights on improving the architecture of IoT-enabled smart homes to promote safer user behavior and reduce security risks. Common themes such as strong authentication and access control mechanisms, cryptographic algorithms, software updating and device patching, and proactive user training emerged as essential considerations. Additionally, the subcategories of user-friendly interfaces and accessibility to lower social classes were recognized as important factors in enhancing smart home security. By addressing these aspects, smart homes can create a more secure and user-centric environment for their inhabitants.

6. Discussion

The primary objectives of this study were to identify the various user behaviors that can put IoT devices at risk for security threats, to determine the factors that influence user behavior and can expose these devices to security risks, and to develop and recommend best practices for reducing security risks brought on by user behavior for smart home IoT devices. The development of best practices to reduce security risks posed by user behavior for smart home IoT devices, as well as the identification of various types of user behavior and factors that can lead to security threats, were all done in order to achieve these objectives.

The paper by Schuster and Habibipour (2022) presented a comprehensive analysis of privacy and security concerns. This paper indicated that individuals exhibit significant apprehension regarding security and privacy issues. A majority of users express a lack of trust in the security measures implemented by IoT products and the entities involved in their provision. This study examines the specific user behaviors that contribute to security risks in smart home IoT devices, including practices such as information sharing, neglecting password updates, and utilizing compromised networks. It highlights irresponsibility as the primary behavioral factor associated with security risks. Moreover, the study investigates various other factors related to user behavior. Therefore, there is a significant difference between this work and by Schuster and Habibipour (2022) in terms of focus and scope.

From the literature review, it was found that user behavior puts smart home IoT devices at risk. I could not find data that directly addresses how user behaviors change based on demographics such as age, gender, and technical knowledge and experience. However, I found that users' intentions to use IoT devices in smart homes are impacted by their impression of security and that developers can improve devices and increase consumer knowledge of security by knowing how consumers perceive security while using the devices (Nemec Zlatolas, Feher, & Hölbl, 2022). While I agree with this statement, I found some additional factors that should be considered to avoid security risks associated with smart home devices. These factors include age, gender, technical skills and knowledge, and culture. The significance of these factors in the overall security mechanism cannot be overlooked.

After conducting a literature review, it was found that users' lack of security knowledge and user perception of security put smart home IoT devices at risk (Amraoui *et al.*, 2020). However, the

findings from the interviews conducted for this study presented a different perspective. According to the findings of the interviews, users may grow more unsure about IoT security the more informed they are. One interviewee stated that, *"While user awareness of security risks can lead to more care about IoT security, many users do not check their security settings and think they are safe while using IoT devices".*

According to research, users' lack of knowledge about security issues and users' bad security habits, such as using weak passwords and not updating their devices, significantly increase the security risks associated with these electronic devices (Vikas, 2020). However, the results obtained from the interviews were surprising and slightly different. The analysis indicates that the evolution of user behavior has both negative and positive impacts on security. Many users do not check their security settings and believe they are safe when using IoT devices. On the other hand, some users are more aware of security and take care of it as their behavior evolves. The findings of this question show that people should be urged to prioritize security in everyday life and to develop a security-first mentality to enhance security.

The literature suggests possible solutions, such as enhancing cyber security culture, encouraging security behavior, and designing a risk framework for the home that considers users' actions and mindset towards IoT devices. Visoottiviseth *et al.* (2020) discusses the creation of a technology named "SPIDAR" to guard against IoT device assaults on residential Wi-Fi networks. On the other hand the paper by Yamauchi *et al.* (2019) provides a technique for identifying cyber assaults on IoT gadgets that are challenging to identify because they use the identical protocol as authorized user activities. During the interviews, I discovered additional practices for lowering security concerns associated with user behavior, including changing default credentials, regularly updating firmware, downloading from verified sources, enhancing network security, providing user education, and using artificial intelligence and blockchain. Incorporating these practices can significantly reduce security risks.

By encouraging security behavior and collecting data on all relevant factors, the study suggests a theoretical framework for boosting cyber resilience in IoT users. This framework can serve as the basis for designing policies to increase cyber resilience, particularly in Indonesia (Amraoui *et al.*, 2020). While the results I obtained from the analysis of interviews are comprehensive and focuses on basic security which most of the times is ignored. The results I obtained include the use of

strong authentication and access control mechanisms, cryptographic algorithms, software updating and device patching, and proactive user training. Furthermore, subcategories highlighted the importance of user-friendly interfaces, accessibility of devices to lower social classes, and encouragement of user awareness and education to detect and address security flaws.

Moreover, during this research, I found several instances emphasized the importance of user education and awareness for smart home IoT device security. In one such instance, a study suggests a theoretical framework for boosting cyber resilience in IoT users by encouraging security behavior and collecting data on all relevant factors (Amraoui *et al.*, 2020). My findings are consistent with this statement. The results of the interviews indicate that user education and awareness are crucial for ensuring the security of IoT devices in smart homes.

6.1. Reflection on the Theory (TPB)

Reflecting on TPB based on the results obtained in the study provides interesting insights into the factors influencing user behavior and their implications for the security of IoT devices in smart homes. The TPB framework can help in understanding and predicting user behavior to promote secure practices and mitigate security risks.

The theory focuses on perceived behavioral control, subjective norms, and attitude (Ajzen, 2019). The findings highlight some additional factors too. The findings highlight the significance of user education and awareness, demographic factors, evolving user behavior, and influential factors in shaping security practices. The practical recommendations derived from these insights can guide stakeholders in developing strategies to promote secure user behavior and mitigate security risks for smart home IoT devices.

Attitude

The results of the study shed light on the attitudes of users towards the security of IoT devices in smart homes. Attitude refers to individuals' positive or negative evaluation of a behavior (Sommestad & Swedish, 2013). In the context of smart home IoT devices, users' positive attitudes towards security practices, such as regularly updating devices, using strong passwords, not downloading irrelevant applications and files, not sharing confidential information, not connecting with unsecure networks, and securing the home network, can greatly influence their behavior (Sommestad & Swedish, 2013). These positive attitudes should be adopted by emphasizing the

benefits and highlighting the potential risks of neglecting security measures, and providing user-friendly interfaces and accessible devices. These findings align with the TPB model as they relate to the constructs of attitudes. Understanding these behaviors can inform interventions aimed at promoting responsible user behavior and reducing security vulnerabilities (Sommestad & Swedish, 2013).

Further, Interviewee 4 pointed out that while users' awareness of security risks can potentially lead to a greater emphasis on IoT security, many users fail to check their security settings and mistakenly believe they are safe while using IoT devices. This observation underscores the importance of bridging the gap between user awareness and actual security practices. This observation emphasizes the need to address this gap and promote a consistent alignment between users' attitudes and their behavior in relation to IoT security.

Perceived Behavioral Control

It refers to individuals' perception of their ability to perform the desired behavior. Perceived behavioral control has been demonstrated to have a favorable impact on both direct and indirect variables that influence privacy-protection behaviors (Chen, Wang, & Zhang, 2023). The findings of this study underscored the presence of similar aspects. The study highlighted various factors that influence user behavior and the adoption of smart home technology, such as convenience, technical knowledge, trust, and perceived risks (Chen, Wang, & Zhang, 2023). These factors contribute to users' perceived behavioral control, i.e., their belief in their ability to perform specific actions to ensure security. Understanding users' perceived control over their actions can inform interventions aimed at empowering users and equipping them with the necessary knowledge and tools to mitigate security risks effectively (Chen, Wang, & Zhang, 2023). By enhancing users' perceived control, interventions can promote secure behavior and reduce vulnerabilities. These findings expand the scope of the TPB model by incorporating additional factors that influence user behavior and can inform the design of interventions targeting specific influences to promote secure behavior.

Subjective Norms

Subjective norms encompass the social influence and norms that individuals perceive regarding a particular behavior (Lin *et al.*, 2021). From the research it was found that a negative relationship

exists between security risk and attitudes towards adopting smart home services (Yang, Lee, & Zo, 2017). But this study examined the influence of demographic factors, such as age and gender, on user behavior and its implications for cybersecurity. The findings indicated that age influences the specific cybersecurity behaviors exhibited by users, while gender does not emerge as a significant predictor of security behavior. These results provide insights into the subjective norms that shape user behavior. By considering social norms and cultural influences, interventions can be designed to promote secure behavior by emphasizing the importance of cybersecurity among different demographic groups. Furthermore, the analysis suggests that culture, and social class have an impact on users' security practices.

To conclude, the analysis revealed several important themes that provide insights into various user behaviors that may lead to security issues for smart home IoT devices. It also identified the factors that influence user behavior and recommended practices for minimizing security risks. While some of the findings are in line with existing research, others are contradictory. Further research can build upon these results to create more effective IoT smart home security measures and improve user education and awareness.

7. Conclusion

In summary, this study aimed to identify the various user behavior patterns that could result in security threats for IoT devices, identify the factors influencing user behavior that could expose those devices to security risks, and develop and recommend best practices for reducing security risks brought on by user behavior for those devices.

7.1. Reflection

The findings of the study and insights from the interviews provide valuable reflections on the crucial factors influencing users' behavior in relation to IoT security. Positive attitudes towards security practices, subjective norms, and perceived behavioral control emerged as key determinants of responsible user behavior (Ajzen, 2019). The study highlights the need to foster positive attitudes, create normative environments, and bridge the gap between awareness and actual security practices. Furthermore, the potential of emerging technologies, such as AI and blockchain, in enhancing IoT security was emphasized (Zheng *et al.*, 2018). These reflections underscore the importance of comprehensive education, awareness campaigns, and the adoption of advanced technologies to promote responsible user behavior and mitigate security vulnerabilities in the ever-expanding IoT landscape.

7.2. Research Questions

The research questions center around user behavior and security risks related to smart home IoT devices. The first question delves into the various types of user behavior that can potentially give rise to security threats. The response highlights several common behaviors including the neglect of device updates, utilization of weak or easily guessable passwords, downloading of unknown or suspicious applications and files, sharing of confidential information, connecting to unsecure or public networks, and overlooking home network security measures. Additionally, user behavior can be influenced by demographic factors.

The second research question investigates strategies to mitigate security risks. In response, the study suggests implementing best practices such as changing default passwords, refraining from downloading irrelevant applications and files, enhancing network security, harnessing emerging technologies, regularly updating firmware, and providing user education. Employing these measures can substantially diminish security concerns associated with IoT devices. It is recommended that IoT device manufacturers prioritize the creation of user-friendly interfaces and

detailed instructions for device setup, update and maintenance, and data protection based on these themes. Additionally, it is recommended that users be urged to adopt strong authentication and access control methods, employ cryptographic algorithms, and take preventative measures to safeguard their devices and networks. User awareness and education programs should be developed to make sure users are apprised of the potential security hazards connected to their gadgets and how to minimize them.

7.3. Contribution

When it comes to the contributions, this work has made contributions to the security of smart home IoT devices. First, it has identified and analyzed the various user behaviors and demographic factors that can lead to security threats for smart home IoT devices. The factors were not discussed in the research explicitly. Second, it has proposed a comprehensive set of best practices, based on the results of interviews, that can be implemented to mitigate these security risks. Finally, it has highlighted the importance of user education and awareness in improving the security of smart home IoT devices.

Regarding the contribution of findings to the theory, the research has explored user behavior and identified potential security concerns associated with IoT devices for smart homes. Preliminary evidence suggests a possible connection between irresponsible user behavior and the vulnerability of these devices to security threats. However, it is important to note that further research is required to establish a definitive causal relationship. The study offers initial indications rather than absolute clarity on user behavior and its impact on device security. Furthermore, age, gender, technical proficiency, and experience were found to be important determinants of user behavior. The evolution of user behavior, best practices for security issues, architectural advancements, and the significance of user education and awareness were also examined. By expanding our knowledge of attitude, arbitrary standards, and perceived behavior control in the context of IoT device security for smart homes, these findings provide additional insights that contribute to the knowledge base of TPB and its applicability to the field of IoT device security.

The results of this study offer valuable insights into the development of strategies aimed at promoting responsible user behavior and mitigating security concerns. While the study does not specifically involve the creation and implementation of such strategies, it provides a foundation for understanding the factors that influence user behavior and the potential implications for

security. By identifying key behaviors and attitudes that contribute to security risks, the study highlights areas of focus for designing effective strategies. The findings inform the development of targeted interventions, educational programs, or awareness campaigns that address the identified user behaviors and promote security-conscious practices.

7.4. Limitations and Future Work

The limitation of this work is that interviews were conducted online and considered only a limited set of professional. Therefore, future research can be extended to cover more diverse populations and demographics to gain a better understanding of the impact of user behavior on cybersecurity in smart homes. Furthermore, it is recommended to further enhance the methodological robustness by incorporating data source triangulation. This approach would provide a more comprehensive and holistic understanding of the research topic by drawing on multiple data sources. By utilizing a combination of interviews, surveys, observations, and existing datasets, researcher would obtain a richer dataset that captures different perspectives and reduces potential biases.

8. References

Abdullah, A. *et al.* (2019) 'CyberSecurity: A Review of Internet of Things (IoT) Security Issues, Challenges and Techniques', *2nd International Conference on Computer Applications and Information Security, ICCAIS 2019*, pp. 1–6. doi:10.1109/CAIS.2019.8769560.

Abomhara, M. and Køien, G.M. (2015) 'Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks', *Journal of Cyber Security and Mobility*, 4(1), pp. 65–88. doi:10.13052/jcsm2245-1439.414.

Adams, W.C. (2015) 'Conducting Semi-Structured Interviews', *Handbook of Practical Program Evaluation: Fourth Edition*, (August 2015), pp. 492–505. doi:10.1002/9781119171386.ch19.

Ahmed, E. *et al.* (2020) 'Internet of Things (IoT): Vulnerabilities, Security Concerns and Things to Consider', *2020 11th International Conference on Computing, Communication and Networking Technologies, ICCCNT 2020* [Preprint], (July). doi:10.1109/ICCCNT49239.2020.9225283.

Ajzen, I. (2019) 'The theory of planned behavior', *Organizational Behavior and Human Decision Processes*, 50(2), pp. 179–211. doi:10.1016/0749-5978(91)90020-T.

Alam, H. and Tomai, E. (2023) 'Security Attacks and Countermeasures in Smart Homes', *International Journal on Cybernetics & Informatics*, pp. 109–119. doi:10.5121/ijci.2023.120209.

Ali, B. and Awad, A.I. (2018) 'Cyber and physical security vulnerability assessment for IoT-based smart homes', *Sensors (Switzerland)*, 18(3), pp. 1–17. doi:10.3390/s18030817.

Amraoui, N. *et al.* (2020) 'Securing Smart Homes using a Behavior Analysis based Authentication Approach', *2020 8th International Conference on Communications and Networking, ComNet2020 - Proceedings*, pp. 1–5. doi:10.1109/ComNet47917.2020.9306081.

Andreasen, A.R. (1985) '"Backward" Market Research', (June).

Asare, M. (2020) 'Using the Theory of Planned Behavior to Determine the Condom Use Behavior Among College Students', *American Journal of Health Studies*. doi:10.47779/ajhs.2015.168.

Awotunde, J.B. *et al.* (2021) 'Privacy and Security Concerns in IoT-Based Healthcare Systems',

Internet of Things, pp. 105–134. doi:10.1007/978-3-030-75220-0_6.

Bagay, D. (2020) 'Information security of Internet things', *Procedia Computer Science*, 169(2019), pp. 179–182. doi:10.1016/j.procs.2020.02.132.

Barker, S. and Parsons, D. (2022) 'Smart Homes or Real Homes: Building a Smarter Grid With "Dumb" Houses', *IEEE Pervasive Computing*, pp. 100–104. doi:10.1109/MPRV.2022.3160752.

Batalla, J.M., Vasilakos, A. and Gajewski, M. (2017) 'Secure Smart Homes: Opportunities and challenges', *ACM Computing Surveys*, 50(5). doi:10.1145/3122816.

Belimpasakis, P. and Moloney, S. (2009) 'A platform for proving family oriented RESTful services hosted at home', *IEEE Transactions on Consumer Electronics*, 55(2), pp. 690–698. doi:10.1109/TCE.2009.5174441.

Bell, E. and Bryman, A. (2007) 'The ethics of management research: An exploratory content analysis', *British Journal of Management*, 18(1), pp. 63–77. doi:10.1111/j.1467-8551.2006.00487.x.

Bhardwaj, P. (2019) 'Types of Sampling in Research'. doi:10.4103/jpcs.jpcs.

Bugeja, J. (2021) *ON PRIVACY AND SECURITY*.

Bugeja, J., Jacobsson, A. and Davidsson, P. (2021) 'PRASH: A framework for privacy risk analysis of smart homes', *Sensors*, 21(19). doi:10.3390/s21196399.

Cannizzaro, S. *et al.* (2020) 'Trust in the smart home: Findings from a nationally representative survey in the UK', *PLoS ONE*, 15(5), pp. 1–30. doi:10.1371/journal.pone.0231615.

Chen, M., Wang, H. and Zhang, R. (2023) 'Using the Extended Theory of Planned Behavior to Predict Privacy-Protection Behavioral Intentions in the Big Data Era: The Role of Privacy Concern', *SHS Web of Conferences*, 155, p. 03011. doi:10.1051/shsconf/202315503011.

Cobb, M. (2021) 'What is physical security?', *TechTarget* [Preprint]. Available at: https://www.techtarget.com/searchsecurity/definition/physical-security.

Coboi, A. *et al.* (2021) 'Security Problems in Smart Homes', *ICSES Transactions on …* [Preprint], (September). Available at: https://www.researchgate.net/profile/Alberto-Coboi/publication/354859434_Security_Problems_in_Smart_Homes/links/61518babf8c9c51a8af

6c2a3/Security-Problems-in-Smart-Homes.pdf.

Conner, M. (2020) 'Theory of Planned Behavior', *Handbook of Sport Psychology*, pp. 1–18. doi:10.1002/9781119568124.ch1.

Daniel, E. (2016) 'The Usefulness of Qualitative and Quantitative Approaches and Methods in Researching Problem-Solving Ability in Science Education Curriculum', *Journal of Education and Practice*, 7(15), pp. 91–100. doi:2222-288X.

Dash, S. *et al.* (2019) 'Big data in healthcare: management, analysis and future prospects', *Journal of Big Data*, 6(1). doi:10.1186/s40537-019-0217-0.

Dhara, S.K. *et al.* (2021) 'Iot Based Digital Door Lock', *International Research Journal of Engineering and Technology*, (October), pp. 53–60. Available at: www.irjet.net.

Elkhediri, F.A.S. (2021) 'Efficient Security Solutions for IoT Devices', *International Journal of Advanced Computer Science and Applications*, 12(4), pp. 698–707. doi:10.14569/IJACSA.2021.0120486.

Geneiatakis, D. *et al.* (2017) 'Security and privacy issues for an IoT based smart home', *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2017 - Proceedings*, pp. 1292–1297. doi:10.23919/MIPRO.2017.7973622.

Goffinet, S. *et al.* (2021) 'Controlling Security Rules Using Natural Dialogue: An Application to Smart Home Care', *UbiComp/ISWC 2021 - Adjunct Proceedings of the 2021 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2021 ACM International Symposium on Wearable Computers*, pp. 194–197. doi:10.1145/3460418.3479331.

Gondal, F.K. (2021) 'Security and Privacy Challenges for theIOT-based Smart Homes with Limited Resources and Adoption Immaturity', *Innovative Computing Review*, 1(1). doi:10.32350/icr.0101.04.

Hadlington, L. (2018) 'Employees attitude towards cyber security and risky online behaviours: An empirical assessment in the United Kingdom', *International Journal of Cyber Criminology*, 12(1), pp. 269–281. doi:10.5281/zenodo.1467909.

Hameed, A. and Alomary, A. (2019) 'Security issues in IoT: A survey', *2019 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies, 3ICT 2019*, pp. 1–5. doi:10.1109/3ICT.2019.8910320.

Hammi, B. *et al.* (2022) 'Survey on smart homes: Vulnerabilities, risks, and countermeasures', *Computers and Security*, 117(March). doi:10.1016/j.cose.2022.102677.

Health Communication Capacity Collaborative (2021) 'What is Theory of Planned Behavior?', *HC3 Research Primer*, pp. 1–2. Available at: https://www.healthcommcapacity.org/wp-content/uploads/2014/03/theory_of_planned_behavior.pdf.

Hughes-Lartey, K. *et al.* (2021) 'Human factor, a critical weak point in the information security of an organization's Internet of things', *Heliyon*, 7(3), p. e06522. doi:10.1016/j.heliyon.2021.e06522.

Iqbal, M.M. (2019) 'Attitude Towards the Behavior , Subjective Norm , Perceived Behavioral Control and Intention To Be a Disaster Volunteer', (May). doi:10.13140/RG.2.2.31270.37445.

Islam, K., Shen, W. and Wang, X. (2012) 'Security and privacy considerations for Wireless Sensor Networks in smart home environments', *Proceedings of the 2012 IEEE 16th International Conference on Computer Supported Cooperative Work in Design, CSCWD 2012*, pp. 626–633. doi:10.1109/CSCWD.2012.6221884.

Jacobsson, A., Boldt, M. and Carlsson, B. (2016) 'A risk analysis of a smart home automation system', *Future Generation Computer Systems*, 56, pp. 719–733. doi:10.1016/j.future.2015.09.003.

Jani, K.A. and Chaubey, N. (2020) *IoT and Cyber Security*. doi:10.4018/978-1-7998-2253-0.ch010.

Jayatilleke, A., Thelijjagoda, S. and Pathirana, P. (2019) 'Security Awareness among Smart Speaker Users', *2019 National Information Technology Conference, NITC 2019*, pp. 8–10. doi:10.1109/NITC48475.2019.9114497.

Kadam, R., Mahamuni, P. and Parikh, Y. (2015) 'Smart Home System', 2(1), pp. 81–86. Available at: https://www.researchgate.net/publication/335169004_Smart_Home_System.

Kavallieratos, G. *et al.* (2019) ‘Threat Analysis for Smart Homes’, *Future Internet*, 11(10), p. 207. doi:10.3390/fi11100207.

Klobas, J.E., McGill, T.J. and Wang, X. (2019) ‘How perceived security risk affects intention to use smart home devices_ A reasoned action explanation’.

Kobis, P. (2021) ‘Human factor aspects in information security management in the traditional IT and cloud computing models’, *Operations Research and Decisions*, 31(1), pp. 61–76. doi:10.37190/ord210104.

Levy, Y. and Ellis, T.J. (2006) ‘A systems approach to conduct an effective literature review in support of information systems research’, *Informing Science*, 9(January), pp. 181–211. doi:10.28945/479.

Li, M. *et al.* (2018) ‘Smart home ： architecture, technologies and systems’, *Procedia Computer Science*, 131, pp. 393–400. doi:10.1016/j.procs.2018.04.219.

Lin, C.W. *et al.* (2021) ‘Applying the Decomposed Theory of Planned Behavior to Explore the Influencing Factors of NTC App Usage Intention’, *Journal of Function Spaces*, 2021. doi:10.1155/2021/7045242.

MACK, N. *et al.* (no date) *Qualitative Research Methods*.

Mahlous, A.R. (2023) ‘Threat Model and Risk Management for a Smart Home IoT System’, 47, pp. 51–64.

Maison, D. (2018) ‘Qualitative Marketing Research’, *Qualitative Marketing Research* [Preprint], (September 2018). doi:10.4324/9780429467028.

Mamonov, S. and Benbunan-Fich, R. (2021) ‘Unlocking the smart home: exploring key factors affecting the smart lock adoption intention’, *Information Technology and People*, 34(2), pp. 835–861. doi:10.1108/ITP-07-2019-0357.

Mittal, Y. *et al.* (2016) ‘A voice-controlled multi-functional Smart Home Automation System’, *12th IEEE International Conference Electronics, Energy, Environment, Communication, Computer, Control: (E3-C3), INDICON 2015*, pp. 1–6. doi:10.1109/INDICON.2015.7443538.

Mondol, S.K., Tang, W. and Hasan, S. Al (2023) ‘A Case Study of IoT Based Biometric Cyber

Security Systems Focused on the Banking Sector A Case Study of IoT Based Biometric Cyber Security Systems Focused on the Banking Sector', (March).

Moustafa, A.A., Bello, A. and Maurushat, A. (2021) 'The Role of User Behaviour in Improving Cyber Security Management'.

Nemec Zlatolas, L., Feher, N. and Hölbl, M. (2022) 'Security Perception of IoT Devices in Smart Homes', *Journal of Cybersecurity and Privacy*, 2(1), pp. 65–74. doi:10.3390/jcp2010005.

Nikel, F.H. and Amaechi, A.O. (2022) 'An Assessment of Employee Knowledge, Awareness, Attitude towards Organizational Cybersecurity in Cameroon', *Network and Communication Technologies*, 7(1), p. 1. doi:10.5539/nct.v7n1p1.

Olabode, S. *et al.* (2023) 'Complex Online Harms and the Smart Home: A Scoping Review', *SSRN Electronic Journal*, (March), pp. 2021–2023. doi:10.2139/ssrn.4377201.

OVIC (2021) 'Internet-of-Things-and-Privacy-Issues-and-Challenges'. Available at: https://ovic.vic.gov.au/privacy/resources-for-organisations/internet-of-things-and-privacy-issues-and-challenges/#:~:text=The passive nature of many,not want their information collected.

Parsons, E.K., Panaousis, E. and Loukas, G. (2021) 'How Secure is Home:Assessing Human Susceptibility to IoT Threats'.

Parveen, H. and Showkat, N. (2017) 'Research Ethics', (July).

Patel, K.K., Patel, S.M. and Scholar, P.G. (2016) 'Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges', *International Journal of Engineering Science and Computing*, 6(5), pp. 1–10. doi:10.4010/2016.1482.

Pattnaik, N., Li, S. and Nurse, J.R.C. (2023) 'A Survey of User Perspectives on Security and Privacy in a Home Networking Environment', *ACM Computing Surveys*, 55(9). doi:10.1145/3558095.

Pham, H., Brennan, L. and Richardson, J. (2017) 'Review of Behavioural Theories in Security Compliance and Research Challenge', *Proceedings of the 2017 InSITE Conference*, (October), pp. 065–076. doi:10.28945/3722.

Rahman, M.S. (2016) 'The Advantages and Disadvantages of Using Qualitative and Quantitative Approaches and Methods in Language "Testing and Assessment" Research: A Literature Review', *Journal of Education and Learning*, 6(1), p. 102. doi:10.5539/jel.v6n1p102.

Ray, A.K. and Bagwari, A. (2018) 'Study of smart home communication protocol's and security & privacy aspects', *Proceedings - 7th International Conference on Communication Systems and Network Technologies, CSNT 2017*, pp. 240–245. doi:10.1109/CSNT.2017.8418545.

De Rossi, D. and Lymberis, A. (2005) 'Guest Editorial: New generation of smart wearable health systems and applications', *IEEE Transactions on Information Technology in Biomedicine*, 9(3), pp. 293–294. doi:10.1109/TITB.2005.854504.

Sankar, S. and Srinivasan, P. (2018) 'Internet of things based digital lock system', *Journal of Computational and Theoretical Nanoscience*, 15(September), pp. 2758–2763. doi:10.1166/jctn.2018.7535.

Schuster, F. and Habibipour, A. (2022) 'Users' Privacy and Security Concerns that Affect IoT Adoption in the Home Domain', *International Journal of Human-Computer Interaction*, 0(0), pp. 1–12. doi:10.1080/10447318.2022.2147302.

Setayeshfar, O. *et al.* (2022) 'Privacy invasion via smart-home hub in personal area networks', *Pervasive and Mobile Computing*. doi:10.1016/j.pmcj.2022.101675.

Sharad, A. (2017) 'Internet of Things (IoT) Security', (August).

Shouran, Z., Ashari, A. and Kuntoro, T. (2019) 'Internet of Things (IoT) of Smart Home: Privacy and Security', *International Journal of Computer Applications*, 182(39), pp. 3–8. doi:10.5120/ijca2019918450.

Shuhaiber, A., Alkarbi, W. and Almansoori, S. (2023) 'Trust in Smart Homes: The Power of Social Influences and Perceived Risks', *Lecture Notes in Networks and Systems*, 578(January), pp. 305–315. doi:10.1007/978-981-19-7660-5_27.

Smith, J. (2003) 'Theory of planned Behaviour', (2001), pp. 2–6. Available at: http://www.stopaidsnow.org/node/237.

Sommestad, T. and Swedish, J.H. (2013) 'Security and Privacy Protection in Information

Processing Systems: 28th IFIP TC 11 International Conference, SEC 2013 Auckland, New Zealand, July 8-10, 2013 Proceedings', *IFIP Advances in Information and Communication Technology*, 405(July). doi:10.1007/978-3-642-39218-4.

Sun, J. *et al.* (2023) 'Internet of Behaviors: A Survey', *IEEE Internet of Things Journal*, pp. 1–17. doi:10.1109/JIOT.2023.3247594.

Sun, K. *et al.* (2021) 'Child Safety in the Smart Home: Parents' Perceptions, Needs, and Mitigation Strategies', *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW2). doi:10.1145/3479858.

Tan, K.K., Lim, Y.L. and Goh, H.L. (2002) 'REMOTE ADAPTIVE CONTROL AND MONITORING', pp. 892–896.

Turulski, A. (2022) 'Statistiken zur Nutzung sozialer Medien in der Schweiz | Statista', *24.Januar.2022* [Preprint]. Available at: https://de.statista.com/themen/2782/social-media-in-der-schweiz/#dossierKeyfigures.

Ursavaş, Ö.F. (2022) 'Theory of Planned Behavior'.

Vibesmarthomes (2018) 'The Evolution of Smart Home Technology', *Information Technology* [Preprint]. Available at: https://www.vibesmarthomes.com/the-evolution-of-smart-home-technology/.

Vikas, K. (2020) 'IoT Security-Challenges & Best Practices'. Available at: https://www.happiestminds.com/wp-content/uploads/2020/12/IoT-Security-Challenges-and-Best-Practices.pdf.

Visoottiviseth, V. *et al.* (2020) 'Signature-based and behavior-based attack detection with machine learning for home IoT devices', *IEEE Region 10 Annual International Conference, Proceedings/TENCON*, 2020-Novem, pp. 829–834. doi:10.1109/TENCON50793.2020.9293811.

Wei, N.T. *et al.* (2019) 'Factors Affecting User's Intention to Adopt Smart Home in Malaysia'.

Yamauchi, M. *et al.* (2019) 'Anomaly Detection for Smart Home Based on User Behavior', *2019 IEEE International Conference on Consumer Electronics, ICCE 2019*, (1), pp. 1–6. doi:10.1109/ICCE.2019.8661976.

Yang, H., Lee, H. and Zo, H. (2017) 'User acceptance of smart home services: An extension of the theory of planned behavior', *Industrial Management and Data Systems*, 117(1), pp. 68–89. doi:10.1108/IMDS-01-2016-0017.

Zheng, S. *et al.* (2018) 'User Perceptions of Smart Home IoT Privacy'.

Zimmermann, V. *et al.* (2020) 'Assessing users' privacy and security concerns of smart home technologies', *I-Com*, pp. 197–216. doi:10.1515/icom-2019-0015.

9. Appendices

9.1. Appendix A: Interview Questions

1. What are the common behaviors that users engage that might expose smart home IoT devices to security risks?
2. How do user behaviors change based on various demographics like age, gender, and technical knowledge and experience?
3. What effects does the evolution of user behavior have on the security of IoT devices used in smart homes?
4. What are the primary factors that influence user behavior when interacting with IoT devices in smart homes, and how do these factors affect security risks?
5. What are the best practices for lowering security concerns provided by user behavior for IoT devices in smart homes, and how effective are these practices at doing so?
6. How may the architecture of IoT-enabled smart homes be enhanced to promote safer user behavior and reduce security risks?
7. How do you think user education and awareness can help in mitigating security risks for smart home IoT devices?

9.2. Appendix B: Analysis Tables

9.2.1. Questions 1 Result

Question 1: What are the common behaviors that users engage that might expose smart home IoT devices to security risks?
Interviewee 1 Response: According to me, there are several common behaviors that users tend to engage in, which can pose a risk to the security of smart home IoT devices. These behaviors include not changing default passwords, sharing personal information, not updating firmware,

using unsecured Wi-Fi networks, using weak passwords, failing to secure the home network, and clicking on suspicious links or downloading unverified apps.				
Interviewee#	**Condense Meaning Unit**	**Sub Categories**	**Categories**	**Common Theme**
Interviewee 1	Behaviors that expose IoT devices to security risks include not changing default passwords, sharing personal information, not updating firmware, using unsecured Wi-Fi networks, using weak passwords, failing to secure the home network, and clicking on suspicious links or downloading unverified apps	• Not changing default passwords • Sharing personal information • Not updating firmware • Using unsecured Wi-Fi networks • Using weak passwords • Failing to secure the home network • Clicking on suspicious links or downloading unverified apps.	Common user behaviors that pose security risks to smart home IoT devices	The impact of poor security practices due to irresponsible user behavior on the security of smart home IoT devices pose security risks. The common user behavior includes sharing information, not updating default password, use of compromised network, etc.
Interviewee 2 Response: There are many common behaviors that we have exposed in the recent times when it comes to using smart home IoT devices. Users don't care about security practices. For me the most common user behaviors include failure to update the password on regular basis, use of an insecure Wi-Fi connection particularly when operating smart home IoT devices, unable to perform patching at the appropriate time, and failure to monitor the				

<table>
<tr><td colspan="4">device activity. These behaviors are motivated by lack of expertise or seriousness shown by users while configuring and operating IoT devices. These behaviors can be changed when we apply proper security policies and procedures to operate and manage IoT devices.</td><td></td></tr>
<tr><td>Interviewee 2</td><td>Behaviors include failure to update passwords regularly, using an insecure Wi-Fi connection, failing to patch vulnerabilities, and failure to monitor device activity</td><td>• Failure to update passwords regularly
• Using an insecure Wi-Fi connection
• Failing to patch vulnerabilities
• Failure to monitor device activity</td><td>The impact of lack of security policies and procedures on user behavior</td><td></td></tr>
<tr><td colspan="4">Interviewee 3 Response: Well, there are a lot of common behaviors of users due to which smart home IoT devices are exposed to security risks and these are including incorrect access control of the devices using default passwords, not implementing any security measures and controls from the security of cyber criminals, relying on the outdated versions of the software, having intrusion ignorance, incorporate insufficient privacy protection while interacting with vendors, applying insufficient physical security while monitoring the IoT devices, do not switching off the Wi-Fi connectivity after using it, having lack of awareness of using IoT devices, and not patching of the IoT devices. The security of IoT devices is mandatory for everyone. That's why it is the responsibility of every user to alter their insecure and inappropriate behavior in order to maintain the security of IoT devices from any security risks.</td><td></td></tr>
</table>

Interviewee 3	Behaviors include using default passwords, not implementing security measures, relying on outdated software, having intrusion ignorance, incorporating insufficient privacy protection, applying insufficient physical security, not turning off Wi-Fi connectivity after use, having a lack of awareness of IoT devices, and failing to patch IoT devices	• Using default passwords • Not implementing security measures • Relying on outdated software • Having intrusion ignorance • Incorporating insufficient privacy protection • Applying insufficient physical security • Not turning off Wi-Fi connectivity after use • Having a lack of awareness of IoT devices • Failing to patch IoT devices	Common user behaviors that expose IoT devices to security risks	
Interviewee 4 Response: Well, you see, when it comes to securing smart home IoT devices, the way users behave can play a big role. There are some common actions that people take, like using default passwords, not properly configuring their devices, and not patching known vulnerabilities. These behaviors can create security risks and make it easier for hackers to get into a smart home				

system. And once one device is compromised, well, that's when things can really start to go downhill. Hackers can use that one entry point to launch more attacks and do all kinds of malicious things, depending on what the compromised device can do.				
Interviewee 4	Common behaviors include using default passwords, not configuring devices properly, and not patching known vulnerabilities	• Using default passwords • Not configuring devices properly • Not patching known vulnerabilities	Poor security practices due to irresponsible user behavior	
Interviewee 5 Response: Several typical user behaviors might expose smart home IoT devices to security vulnerabilities. Using default passwords that are simple for hackers to guess is one example of this behavior. Many users leave their device default passwords unchanged, making them accessible to unauthorized users. Poor network security is another practice, where people leave their home networks unprotected by encryption and strong passwords. This leaves IoT devices vulnerable to attacks from hackers who have gained access to the network. Another popular practice that might put IoT devices in smart homes at danger is sharing personal information on social media, such as house addresses and calendars.				
Interviewee 5	Common behaviors include using default passwords, poor network security, and sharing	• Using default passwords • Poor network security • Sharing personal information on social media	Security risks due to irresponsible user behavior	

	personal information on social media			

9.2.2. Questions 2 Result

Question 2: How do user behaviors change based on various demographics like age, gender, and technical knowledge and experience?				
Interviewee 1 Response: User behaviors related to smart home IoT devices depends on various demographics such as age, gender, and technical knowledge and experience. Some examples are listed below: **Age:** Older users may be less tech-savvy and may struggle with setting up and securing smart home IoT devices as compared to younger users. **Gender:** There may be some gender differences in how users approach smart home IoT devices. For example, research has shown that women may be more concerned about the privacy and security implications of using these devices, while men may be more interested in the convenience and novelty aspects. **Technical knowledge and experience:** Users with more technical knowledge and experience may be more likely to understand the security risks associated with smart home IoT devices and take steps to secure their devices, such as changing default passwords and updating firmware. On the other hand, less technically knowledgeable users may be more likely to use weak passwords and fail to update firmware, leaving their devices vulnerable to attacks.				
Interviewee#	**Condensed Meaning Unit**	**Sub Categories**	**Categories**	**Common Theme**
Interviewee 1	User behaviors related to smart home IoT devices depend on demographics such as age, gender, and technical	• Age • Gender • Technical knowledge and experience	User behavior and demographics	How user behavior changes in relation to smart home IoT devices based on various

	knowledge. Older users may struggle with setup and security, women may prioritize privacy, and technically knowledgeable users may be more likely to secure devices.			demographics, such as age, gender, technical knowledge, and experience.
Interviewee 2 Response: Well, this is tough question because demographics can produce different results. For instance, in Asia, we can say people don't have much awareness about threats posed by attackers to smart devices. In this I don't think so gender or age play any role. However, technical expertise does play role and this has greatly improved the user behavior when it comes to dealing with IoT devices. There is another reason for this because some parts of Asia are not much developed and the smart devices are not accessible to all the population. On the other hand, in Europe or other western nations, people have much more awareness about smart devices, technology is advanced and people can have easy access to smart devices because they are using them in their daily life routine and this has greatly reduced the chances of being attacked irrespective of gender, age or technical experience.				
Interviewee 2	In Asia, lack of awareness about security threats is an issue for all demographics. In developed regions like	• Cultural differences • Technical expertise • Accessibility to smart devices	Regional differences in user behavior	

	Europe, awareness is higher, and access to smart devices is easier, reducing the risk of attacks regardless of demographics.			
Interviewee 3 Response: While using smart home IoT devices there is a significant change which a user behavior plays on the basis of various demographics like age, gender, and technical knowledge and experience. It is considered that the elderly age users show a more positive response while using smart home IoT devices than the young because they do not experience much while using these devices. Furthermore, it is acknowledged that the automated technology of smart homes gives numerous advantages to elderly age groups in terms of monitoring their health conditions. it is acknowledged in research that the ratio of females while using smart home devices is larger than the males because smart home services are used more than the males without knowing the cyberattacks which are imposed by the cyber criminals. If a smart home IoT device is used without any proper awareness it will give space to cyber criminals. The experience also influenced the behavior change of a user because the technology aware user acts wisely while using the smart home IoT devices and always adopts security measures and controls more than the inexperienced one because he knows about the security risks which are imposed by the cyber criminals if security controls are not implemented. Similarly technical knowledge changes the user behavior while dealing with any technicalities of using smart home IoT devices because an aware user changes differently than the unaware one. It means that the user behavior				

changes on the basis of various demographics including age, gender, experience, and technical knowledge.				
Interviewee 3	User behavior changes with smart home IoT devices based on age, gender, technical knowledge, and experience. Elderly users are positive about smart home devices. While females use them more but may be less aware of cybersecurity risks. Experienced and technically knowledgeable users adopt security measures and controls.	• Elderly age group • Gender • Experience • Technical knowledge	Role of user behavior and demographics in smart homes	
Interviewee 4 Response: Age, gender, technical expertise, and experience are just a few of the variables that might have an impact on user behaviors for IoT security. For instance, younger people could be more willing to accept the newest technology but also more prone to use IoT devices riskily. However,				

despite having less technological training and expertise, older people may be more careful when it comes to IoT security. Gender may be a factor in technology use, with males being confident and prepared to take risks.				
Interviewee 4	User behaviors for IoT security can be influenced by factors including age, gender, technical skill, and experience. Older users may be more cautious, whereas younger users may be more open to new technology yet also utilize it riskily. Technology use may be influenced by gender.	• Age • Gender • Technical expertise • Risk-taking behavior	User behavior and demographics in smart homes security	
Interviewee 5 Response: Let's talk about users' cybersecurity behavior and how it can be affected by various factors such as age, gender, and technical knowledge. There are age differences in cybersecurity behavior, particularly in device protection, password creation, proactive checking, and software updating. Interestingly, older users are more likely to create secure passwords and show awareness of potential risks by regularly updating their software, but less likely to protect their devices compared to younger users. Gender, on the				

other hand, is not a substantial predictor of security behavior. However, self-efficacy is a mediator between age and three cybersecurity behaviors: proactive checking, password creation, and updating.				
Interviewee 5	Age affects cybersecurity behavior in areas such as device protection and software updating, with older users more likely to prioritize software security but less likely to protect devices. Gender is not a significant predictor of security behavior. Self-efficacy mediates age and cybersecurity behaviors.	• Age • Gender • Password creation • Software updating • Device protection • Self-efficacy	User behavior and demographics in smart homes security	

9.2.3. Questions 3 Result

Question 3: What effects does the evolution of user behavior have on the security of IoT devices used in smart homes?
Interviewee 1 Response: The evolution of user behavior can have significant effects on the security of IoT devices used in smart homes. As users become more familiar with smart home IoT devices and their capabilities, they may become more comfortable experimenting with

different configurations and connecting more devices to their network. This can increase the attack surface for potential attackers and make it more difficult to secure the entire smart home ecosystem.				
Interviewee#	**Condensed Meaning Unit**	**Sub Categories**	**Categories**	**Common Theme**
Interviewee 1	As users become more comfortable with smart home IoT devices, they may experiment with different configurations and connect more devices to their network, increasing the attack surface for potential attackers and making it more difficult to secure the smart home ecosystem.	• Increased attack surface • Difficulty securing entire smart home ecosystem	Effects of user behavior on IoT security in smart homes	The significance of comprehending and resolving security issues related to the usage of IoT devices, including both user behavior and manufacturer design considerations, is a common theme among these interviewees.
Interviewee 2 Response: There are negative as well as positive effects of using smart home IoT devices as the user is more familiar with the smart devices. On the positive side, users will try to limit the likelihood of cyber-attacks on smart home devices. They will engage in positive mind set. They might consider setting strong passwords, use secure internet connection, perform patching, and implement strong authentication controls and so on. On				

the negative side, as users become more reliant on smart home technology and engage in more complex behavior, they may inadvertently introduce new security risks. For example, they may use third-party services or applications that interact with smart home IoT devices but are not properly secured. Additionally, as users become more comfortable with their devices, they may become complacent and fail to take necessary security precautions, such as regularly updating firmware or using strong passwords.				
Interviewee 2	Users' familiarity with smart home technology can have both positive and negative effects on security. Positive effects include implementing stronger security measures, while negative effects include introducing new security risks or becoming complacent and failing to take necessary security precautions.	• Positive effects of user behavior (For example, setting strong passwords, using secure internet connections) • Negative effects of user behavior (For example, using third-party services or applications, becoming complacent)	Positive and negative user behaviors affect IoT security	

Interviewee 3 Response: The security of IoT devices used in smart homes has been dramatically influenced by changes in user behavior. There is a higher chance of being exposed to cyber-attacks as more individuals use IoT devices and incorporate them into their everyday lives. However, by following recommended practices like using strong passwords, upgrading software often, and being cautious when disclosing personal information, human behavior may also play a significant part in boosting security. Manufacturers of IoT devices must prioritize security in their designs and regularly provide fixes and upgrades to fix vulnerabilities.				
Interviewee 3	User behavior has a significant impact on the security of IoT devices used in smart homes. By following recommended security practices, such as using strong passwords and upgrading software, users can boost security. However, manufacturers also need to prioritize security in their	• Higher chance of exposure to cyber attacks • Need for manufacturers to prioritize security in designs	Impact of user behavior and manufacturer priorities on IoT security	

	designs and regularly provide fixes and upgrades to fix vulnerabilities.			
Interviewee 4 Response: User behavior can really make a difference when it comes to the IoT devices security. It was found from the research that the more people know about data breaches, personal info leaks, ransomware attacks, and vulnerabilities in devices can affect the more they care about IoT security. But here's the thing: many users don't bother checking their security settings, and they often think they're safe while using IoT devices. So, it's really important to raise awareness about these risks and encourage people to take security seriously.				
Interviewee 4	While user awareness of security risks can lead to more care about IoT security, many users do not check their security settings and think they are safe while using IoT devices. Therefore, raising awareness about risks and	• Awareness of security risks can affect user behavior • Many users don't check security settings and think they're safe • Importance of raising awareness and encouraging users to take security seriously	Importance of security awareness and education	

	encouraging people to take security seriously is crucial.			
Interviewee 5 Response: When it comes to the security of IoT devices, user behavior plays a significant role. If users are aware of the potential security risks associated with these devices, they may take proactive steps to reduce those risks. This may include updating firmware and changing default credentials. However, if users do not adjust their behavior to address security risks, their devices can be vulnerable to attacks. For example, using weak or default passwords, failing to update firmware, and neglecting to secure home networks are some of the behaviors that could expose users to risks.				
Interviewee 5	User behavior plays a significant role in IoT device security. If users adjust their behavior to address security risks by updating firmware, changing default credentials, and securing home networks, they can reduce risks. However, neglecting to do so can expose	• User behavior plays significant role in IoT device security • Proactive steps to reduce risks (For example, updating firmware, changing default credentials) • Behaviors that could expose users to risks	IoT security and user behavior	

	devices to attacks.	(For example, using weak passwords, neglecting to secure home networks)		

9.2.4. Questions 4 Result

Question 4: What are the primary factors that influence user behavior when interacting with IoT devices in smart homes, and how do these factors affect security risks?				
Interviewee 1 Response: There are several primary factors that influence user behavior when interacting with IoT devices in smart homes, and these factors can affect security risks. For example, 1. Convenience: when it comes with IOT devices then security compromises. 2. Technical Knowledge: Users equipped with more knowledge are passionate about the security, and take steps to enhance the security of their IOT devices. 3. Trust on Manufacturers of IOT devices also have an influence on security of IOT devices. If manufacturer is trusty then user use the devices without taking additional security, while those users who are not make trust on manufacturer take precautionary step to keep the security of their devices and network.				
Interviewee#	**Condensed Meaning Unit**	**Sub Categories**	**Categories**	**Common Theme**
Interviewee 1	Convenience, technical proficiency, and manufacturer trust are factors that affect user behavior with IoT devices. These elements	• Convenience as a primary factor • Technical knowledge as a primary factor	Primary factors influencing user behavior when interacting with IoT devices in smart homes	The factors that influence the adoption of smart home technology, including convenience, technical knowledge,

	may influence the likelihood that users might compromise security in favor of convenience.	• Trust in manufacturers as a primary factor		trust, ease of use, enjoyment, awareness, perceived risks, user behavior, demographic factors, technical skill, experience, and security concerns.
Interviewee 2 Response: As per my experience there are multiple factors that influence the user behavior while interacting smart devices. Users want ease of use while working with smart devices and by doing so they risk their devices such as a user can set a weak password by saying that I cannot remember strong and long password. In the same way trust and usability are other two important primary factors that play their part in exposing smart devices to attacks. A smart device with a complex interface may provide more attack surfaces than the easy one. Likewise, trust is subjective. Users trust companies which can have strong security history like their devices are safe from attacks. When we talk about user behavior in the context of security societal norms do play their part. For instance, if an employee is not taking security seriously others might follow him. So there are many other factors but the above-mentioned, I think, are the primary ones which cannot be neglected.				
Interviewee 2	Ease of use, confidence in manufacturers, and cultural standards are all factors that affect user behavior with IoT devices. Security threats, such as people creating weak passwords or not	• Ease of use as a primary factor • Trust in companies as a primary factor • User behavior influenced by societal norms	Factors influencing user behavior and perception	

	taking security seriously, can be impacted by these variables.			
Interviewee 3 Response: The primary factors that influence user behavior when interacting with the IoT devices in smart homes are trust, enjoyment, perceived ease of use smart home devices, awareness, perceived risks, and perceived usefulness. While interacting with the IoT devices a user requires ease of use and not think about precautionary measures which affect the security risks of cyber-attacks. Such as not setting up a strong password while using smart home devices because that particular password is used several times while working automatically. As it is acknowledged that the attack surface of using smart home IoT devices is large due to which these devices are more vulnerable to cyberattacks if proper security measures are not implemented. The trust factor also influences the user behavior while interacting with the IoT devices in smart homes as a subjective norm. These factors affect the security risks in terms of not implementing security controls and policies. For example if a strong password policy is not implemented while interacting with the IoT devices in smart homes it gives space to cyber criminals to a user's network and system.				
Interviewee 3	Trust, pleasure, perceived usability, awareness, perceived risks, and perceived benefit are factors that affect user behavior with IoT devices.	• Trust • Enjoyment and perceived ease of use • Awareness and perceived risks	Factors influencing user adoption and trust in technology	

	These factors may influence security risks, such as those brought on by improper use of security controls or policies.			
Interviewee 4 Response: Well, when it comes to using IoT devices in smart homes, there are a few factors that can really impact how people behave. One big one is age - younger folks might be more comfortable with all the complicated settings and features, while older folks might prefer things to be more straightforward. And there's also gender - studies have shown that men are generally more confident when it comes to using technology. But it's not just about demographics. Technical skill and experience can also play a big role. People who are more experienced with technology might be more cautious and aware of security risks, for example. And all of this can have a big impact on the security risks associated with using IoT devices in smart homes. People who aren't as tech-savvy or who feel overly secure might be more likely to use default passwords or forget to update their software - things that could make them more vulnerable to attack. So it's really important to take all these factors into account when designing and using these devices.				
Interviewee 4	Demographics, technical expertise, and experience are some factors that affect user behavior with IoT devices in	• Demographic factors • Technical skill and experience • Impact on security risks	Factors influencing user behavior and security	

	smart homes. These variables may have an impact on security concerns, such as making users more susceptible to attacks owing to a lack of technical expertise or causing them to overlook software updates.			
Interviewee 5 Response: A user's behavior is largely influenced by their knowledge and familiarity with the technology as well as their ability to manage security and privacy issues. Smart home technology usage is becoming more common, and it's not just technically adept individuals but also non-technical users who may not know how to adequately address security and privacy concerns that are adopting these devices.				
Interviewee 5	Knowledge and comfort with technology, as well as the capacity to handle security and privacy concerns, are factors that affect	• Knowledge and familiarity with technology as an influencer • Non-technical users as adopters of	Factors influencing the adoption of smart home technology by non-technical users	

	user behavior with IoT devices in smart homes. These factors can affect security risks, such as non-technical users not knowing how to adequately address security and privacy concerns.	smart home technology • Importance of addressing security and privacy concerns.		

9.2.5. Questions 5 Result

Question 5: What are the best practices for lowering security concerns provided by user behavior for IoT devices in smart homes, and how effective are these practices at doing so?				
Interviewee 1 Response: To lower security concerns caused by user behavior for IoT devices in smart homes, there are various best practices that can be implemented. Firstly, changing the default login credentials of IoT devices is a necessary step for securing them. Secondly, firmware updates should be regularly performed to ensure that any security vulnerabilities are patched. Thirdly, it is important to secure the home network, for example, by using strong passwords and firewalls. Fourthly, downloading should be done with caution, and only from verified sources. Lastly, it is crucial to provide awareness and education to users about the importance of security practices to avoid security risks.				
Interviewee #	**Condensed Meaning Unit**	**Sub Categories**	**Categories**	**Common Theme**
Interviewee 1	Change default login credentials, update	• Changing default login credentials	Best practices for IoT security	Implementation of different security measures to

	firmware, protect the home network, only download from reputable sources, and educate users are the best practices for reducing security risks with user behavior for IoT devices in smart homes.	• Regular firmware updates • Securing home network with strong passwords and firewalls • Downloading from verified sources only • User education and awareness		safeguard IoT devices from attacks and preserve data privacy comprise changing default credentials, regular updating firmware, downloading from verified source, network security, user education, and use of artificial intelligence.
Interviewee 2 Response: For me, the best practice is the adoption of latest technology in dealing with security threats related to smart devices and also the awareness among the users. Incorporation of latest technology such as artificial intelligence can prevent cyber-attacks on smart home devices. I believe, raising awareness among users will not only prevent cyber-attacks on smart devices but also helps to develop new ways of tackling cyber threat in smart devices.				
Interviewee 2	The best strategies to reduce security issues with user behavior for IoT devices are to use the latest innovations to avoid	• Adoption of latest technology for security • User awareness and education	Best practices for IoT security	

	cyberattacks and to increase user knowledge on how to prevent attacks and find new ways to combat cyber threats.			
Interviewee 3 Response: The best practices for lowering security concerns provided by user behavior for IoT devices in smart homes are to keep up to date with the IoT devices by updating software at specific intervals, changing the name of your router, setting up of strong passwords, using a strong and secure Wi-Fi encryption method, use of multifactor authentication mechanism, disabling the unnecessary and unused features of the devices, and be careful while using public Wi-Fi. From the security of cyber criminals all of these practices ensure cybersecurity. Furthermore, blockchain technology can also be used for the security of IoT devices. All of the best practices which are mentioned are effective because these practices ensure the security of the critical assets of an individual from any cyber related risks.				
Interviewee 3	Best practices for reducing security concerns with user behavior for IoT devices include : regularly updating software, changing the	• Updating software at specific intervals • Changing router name and using strong passwords • Using secure Wi-Fi encryption method and multifactor authentication	Best practices for IoT device security through user behavior	

	name of the router, using strong passwords and secure Wi-Fi encryption, enabling multifactor authentication, turning off unused device features, and being cautious when using public Wi-Fi. Using blockchain technology for security is also possible.	• Disabling unnecessary device features • Being careful when using public Wi-Fi • Blockchain technology for security		
Interviewee 4 Response: Well, there are a number of things you can do to address security concerns stemming from user behavior when it comes to IoT devices in smart homes. Some of the best practices include updating the software on your devices, changing any default passwords or credentials, closely monitoring and managing each IoT device, and making sure all your applications are up-to-date. By taking these steps, you can really help mitigate any security risks that might come up as a result of user behavior.				
Interviewee 4	Best practices for reducing security risks with user	• Updating software on devices	Best practices for securing IoT devices	

	behavior for IoT devices in smart homes include updating the device software, changing default passwords or credentials, regularly monitoring and managing each IoT device, and making sure all applications are current.	• Changing default passwords/credentials • Closely monitoring and managing IoT devices • Ensuring all applications are up-to-date	through software and device management	
Interviewee 5 Response: So, if you want to make sure your IoT devices in your smart home are secure, there are some recommended practices you can follow. First, make sure you protect your data privacy, keep your network secure, and secure every endpoint for each IoT device. You should also keep your device software up-to-date, update encryption protocols, and change your default passwords and credentials. Now, when you're designing an IoT solution, it's important to keep in mind the possible risks and threats and to incorporate security measures throughout the design process. By doing so, you can strengthen and maintain the security of your solution.				
Interviewee 5	Best practices for reducing security	• Protecting data privacy	Best practices for	

	problems with user behavior for IoT devices include protecting data privacy, securing networks and each IoT device endpoint, maintaining device software updates, updating encryption algorithms, and changing default passwords and credentials. To increase and sustain security, include security measures throughout the design phase of an IoT system.	• Keeping network secure • Securing every endpoint for each IoT device • Keeping device software up-to-date • Updating encryption protocols • Changing default passwords/credentials • Incorporating security measures throughout design process.	securing IoT devices	

9.2.6. Questions 6 Result

Question 6: How may the architecture of IoT-enabled smart homes be enhanced to promote safer user behavior and reduce security risks?				
Interviewee 1 Response: Enhancing the architecture of IoT-enabled smart homes can promote safer user behavior and reduce security risks associated with these devices. It is important for manufacturers and developers to prioritize security in the design and development of their devices, and for users to remain vigilant and proactive in securing their devices and networks.				
Interviewee#	**Condensed Meaning Unit**	**Sub Categories**	**Categories**	**Common Theme**
Interviewee 1	It is possible to encourage safer user behavior and lower security risks by improving the architecture of IoT-enabled smart homes, giving security top priority in device design and development, and encouraging users to be aware and proactive in protecting their devices and networks.	• Need for users to remain vigilant and proactive in securing their devices and networks	User responsibility in IoT security	The use of strong authentication and access control mechanisms, the incorporation of cryptographic algorithms, the updating of software and patching of devices, and training users to be careful and proactive in securing their devices and networks

Interviewee 2 Response: Well, the architecture can be improved in many ways like an interactive and easy to use interface, by having strong authentication methods, proper patching of devices, strong access control methods and by raising awareness among the users. I believe, the availability of smart devices at the lower levels of the society will also help to promote awareness and also will help to tackle lower-level cyber-attacks on smart devices.				are among the common themes. The subcategories also place emphasis on the necessity of user-friendly user interfaces, the accessibility of devices at lower social classes, and the encouragement of user awareness and education in order to discover and address security flaws.
Interviewee 2	It is possible to encourage safer user behavior and lower security risks by enhancing the architecture of IoT-enabled smart homes with an interactive and user-friendly interface, strong authentication techniques, appropriate device patching, strong access control techniques, raising user awareness, and accessibility to smart devices at	• Strong authentication methods • Proper patching of devices • Strong access control methods • Raising awareness among users • Availability of smart devices at the lower levels of society	Enhancing the architecture of IoT devices through user-centric design and awareness	

	lower levels of society.			
Interviewee 3 Response: According to me, the architecture of IoT-enabled smart homes be enhanced to promote safer user behavior and reduce security risks by incorporating the cryptographic algorithms within the smart home IoT devices. Furthermore, by implementing best practices which are discussed such as updated software, changing the name of your router, setting up of strong passwords, using a strong and secure Wi-Fi encryption method, patching, and use of multifactor authentication mechanism enhance the security from cyber criminals and reduce the security risks as well.				
Interviewee 3	By incorporating cryptographic algorithms into IoT devices, implementing best practices like updated software, changing the name of the router and setting strong passwords, and using secure Wi-Fi encryption, patching, and multifactor authentication	• Incorporation of cryptographic algorithms within smart home IoT devices • Implementation of best practices such as updated software, strong passwords, and multifactor authentication • Use of secure Wi-Fi	Strategies to enhance the security of IoT devices	

	mechanisms, it is possible to improve the architecture of IoT-enabled smart homes and lower security risks.	encryption methods • Patching to enhance security and reduce risks from cyber criminals		
Interviewee 4 Response: I think a great way to enhance the security and privacy of smart homes that are powered by IoT technology is to implement solutions that prioritize both security and privacy. You can do this by using cryptographic algorithms to prevent security threats. Plus, it's essential to educate users about the best practices for safely interacting with IoT devices in their smart homes.				
Interviewee 4	By implementing security and privacy-focused solutions, utilizing cryptographic algorithms to guard against security threats, and informing users about the best ways to interact with IoT devices, it is possible to improve the	• Use of cryptographic algorithms to prevent security threats • Education of users about best practices for safely interacting with IoT devices	Strategies to enhance the security of IoT devices	

	security and privacy of smart homes powered by IoT technology. This can encourage safer user behavior and lower security risks.			
Interviewee 5 Response: If we want to make IoT-enabled smart homes safer and reduce security risks, we need to make some improvements to the architecture of these systems. First, we should implement strong authentication and access control mechanisms, as well as encryption protocols to ensure data privacy and prevent unauthorized access. Second, we should make it easy for users to identify and fix any security vulnerabilities or issues in their smart home devices. Lastly, we need to promote user education and awareness by providing clear and concise information about security risks and best practices for securing IoT devices. This could include regular security updates, training programs, workshops, or easy-to-understand security guides and manuals.				
Interviewee 5	It is possible to encourage safer user behavior and lower security risks by improving the architecture of IoT devices with robust authentication	• Implementation of strong authentication and access control mechanisms • Encryption protocols to ensure data privacy and	Strategies to enhance the security of IoT devices	

	and access control mechanisms, encryption protocols, making it simple for users to identify and fix any security vulnerabilities, promoting user education and awareness, and providing clear and concise information about security risks and best practices.	prevent unauthorized access • Making it easy for users to identify and fix security vulnerabilities or issues in smart home devices • Promotion of user education and awareness through regular security updates, training programs, workshops, or easy-to-understand security guides and manuals		

9.2.7. Questions 7 Result

Question 7: How do you think user education and awareness can help in mitigating security risks for smart home IoT devices?
Interviewee 1 Response: User education and awareness can play a critical role in mitigating security risks for smart home IoT devices. By educating users on the risks associated with using

<table>
<tr><td colspan="5">these devices and how to secure them, manufacturers and developers can empower users to take proactive steps to protect their devices and networks.</td></tr>
<tr><td>Interviewee#</td><td>Condensed Meaning Unit</td><td>Sub Categories</td><td>Categories</td><td>Common Theme</td></tr>
<tr><td>Interviewee 1</td><td>User education and awareness can mitigate security risks for smart home IoT devices.</td><td>• Enabling users to take preventative measures to safeguard their systems</td><td>Role of users for security</td><td rowspan="4">The common theme is that user education and awareness play a significant role in mitigating security risks associated with IoT devices.</td></tr>
<tr><td colspan="4">Interviewee 2 Response: For me, both of them are necessary. User education will limit security risks my providing first line of defense in the form of experience users and awareness will provide opportunities to deal with cyber threats that are by passed the first line of defense.</td></tr>
<tr><td>Interviewee 2</td><td>User education and awareness are both necessary for mitigating security risks for smart home IoT devices.</td><td>• Limiting security risks through user education
• Dealing with cyber threats through user awareness</td><td>Mitigating security risks through user education and awareness</td></tr>
<tr><td colspan="4">Interviewee 3 Response: There is crucial role of user education and awareness in mitigating the security risks for smart home IoT devices because through education we learn about useful techniques and best practices which are applied for the security of IoT devices from cyber related risks and cyber criminals and awareness of user helps to act against any security risks wisely.</td></tr>
</table>

Interviewee 3	User education and awareness play a crucial role in mitigating security risks for IoT devices.	• Crucial role of user education and awareness • Learning useful techniques and best practices	Importance of user education and awareness for mitigating security risks in IoT devices	
Interviewee 4 Response: Making customers aware of safe practices is one of the most important strategies to mitigate the security concerns connected to IoT devices in smart homes. By being aware of possible security issues, customers will be better equipped to take preventative action. Educating users on how to modify default passwords, update firmware and software, and manage each IoT device can reduce security risks. By increasing user awareness of security threats associated with IoT devices in smart homes, users can become more careful and take the required precautions to secure their smart homes. This can lessen the likelihood of security breaches and guard against the compromise of user data.				
Interviewee 4	User awareness of safe practices can mitigate security concerns associated with IoT devices.	• Preventative action through user awareness • Reducing security risks through user education	Mitigating security risks through user education and awareness	
Interviewee 5 Response: If you're looking to minimize the security risks associated with IoT devices in smart homes, educating users and promoting awareness is essential. By familiarizing themselves with potential security threats and how to effectively mitigate them, users can take preventative measures to secure their devices and safeguard their privacy. This may include				

upgrading software, changing default passwords and login information, and being cautious when granting access to other programs.				
Interviewee 5	User education and awareness are essential for minimizing security risks associated with IoT devices.	• Minimizing security risks with user education and awareness • Familiarizing with potential security threats • Effectively mitigating security threats through user education	Importance of user education and awareness for mitigating security risks in IoT devices	