JCBI
Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606
Volume 08 Issue 01
2024

Research Article
https://doi.org/10.56979/801/2024

AI-Powered Phishing Detection and Mitigation for IoT-Based Smart Home Security

Noor Fatima[1], Mohsin Ashraf[1], Rabia Tehseen[1*], Uzma Omer[2], Nosheen Sabahat[3], Rubab Javaid[1], Madiha Yousaf[1], Maham Mehr[1], and Ayesha Zaheer[1]

[1]Faculty of Information Technology and Computer Science, University of Central Punjab, Lahore, 57400, Pakistan.
[2]Division of Information Technology, University of Education, Lahore, 57400, Pakistan.
[3]Forman Christian College University, Lahore, 57400, Pakistan.
[*]Corresponding Author: Rabia Tehseen. Email: rabia.tehseen@ucp.edu.pk

Received: April 21, 2024 **Accepted:** September 28, 2024

Abstract: Many people with no technical expertise are implementing smart home technology as it becomes more widely available without fully comprehending the privacy and safety risks involved. We interviewed with 40 smart home users with the goal to learn about their concerns and methods for reducing risks in order to fill this knowledge gap and offer knowledgeable advice. According to our research, users have a variety of concerns which are frequently measured against the benefits they observe in smart home technologies. Although some users expressed their concerns, others demonstrated that they were willing to take some risks. But we observed that these concerns weren't usually followed by robust mitigating strategies, mostly because users had restricted technological knowledge or few possibilities. Our study's distinctive emphasis on user experience reveals significant differences between knowledge and application of security and privacy protocols. This research offers useful recommendations for improving user regulate and create IoT-based technologies to Improved security for intelligent houses. Upcoming efforts to enhance the privacy and security of smart home devices can profit from these insights.

Keywords: Internet of Things; Privacy; Smart Home; Security.

1. Introduction

The rapid growth of Internet of Things (IoT) technology has contributed to an increase in the utilization of smart home devices, particularly among non-technical users who may not fully understand the underlying technology and consequences, such as privacy and security concerns [1]. These devices are becoming more and more popular, but they've also made it easy for security breaches to occur, seriously compromising user privacy, data, and overall safety [2, 3]. Concerns about maintaining privacy and protecting possibly sensitive user's data are also becoming more frequent [4, 5]. Because there is now more risk involved with smart home devices, authorities like the Federal Bureau of Investigation (FBI) in the United States have stepped in. Smart TVs and other Internet of Thing's devices are the focus of security and privacy alerts issued by the FBI [6, 7]. Sadly, no matter how spectacular the technology may be, such education is lacking and that is why consumers usually fail to master the operation of the selected system. Or rather, a smart home has to manage the appropriate defense without denying itself from enjoying the perks that these gadgets afford. To counter the negative effects of the excessive use of smart house technology, more emphasis should be placed on the education of users, user-friendly security design, and regulatory best practices. A plausible concern exists, however, that smart home devices vendors are unlikely to focus sufficiently on the effective establishment of the user interface controls for ease of use or the reasonable privacy disposal measures. Despite the fact that these alternative options have been extensively studied, it is possible that the consumers in this case will be in doubt as to what these alternatives are. Once more, smart home users might not have knowledge on the best preventive measures

or they may opt for very basic measures which are hardly any good. The recent news of mothers and children being stalked with computer devices because of weak security credentials supplied by the users has caused alarm over these devices because of the people targeted.

2. Related Word

Research finds that the common home adoption of smart technology is impeded when people are fretful for the safety and privacy. [8] says that folks who haven't caught up with smart home devices often have a higher awareness of privacy issues and display more suspicion of the companies producing the devices and the safety and privacy solutions they adopt. On the other hand, it is observed that the individuals who resist forming unconventional smart home networks may not like to risk their own privacy if the devices are hacked. From the result of several pieces of research among which were carried out the Parks Associates [5], Emami Naeini et al. [7], Fruchter and Liccardy [4], and Worthy et al. [9], it is seen that all these studies are in support of the same fact: sellers not being able to secure the user data is one of the most pervasive hurdles for the smart home technology industry. The concern for personal safety when personal information is kept in someone's hands is over and above device-related problems. Wifi technologies development have made it that one IoT service has an always-on and another specific feature. Williams et al. [12] found it is appreciated IoT users of their privacy more than non-IoT users.

Detailed analysis of these concerns and attitudes can yield valuable insights into the specific factors eroding confidence and preventing adoption. Understanding the nuanced causes of perceived privacy and security measure deficiencies can help to systematically address these issues [13]. Users will find it easier to embrace and incorporate smart home technology into their lives in this atmosphere.

People who have adopted smart home technology have been found to have similar worries, most notably feeling as though they have no control over their data. Despite these concerns, adopters frequently consciously choose to accept the trade-off between privacy and the convenience and utility that smart home devices offer, and they also tend to show higher tolerance for privacy violations [11]. Their faith in reputable manufacturers may account for this willingness to jeopardize privacy, as some adopters have expressed that they have "nothing to hide" [14].

On the other hand, adopters display sophisticated but unfinished threat models. There is a noticeable lack of knowledge about threats like botnets and the sale of inferred data, even though they generally accept the possibility of being monitored by manufacturers or government agencies and being the target of hackers [1, 3, 15]. The underabundance of knowledge regarding potential risks could be attributed to various factors, such as inadequate education on cybersecurity issues and the dynamic nature of emerging threats in the smart home domain. One of the most frequent security worries among adopters is the possibility of a breach in the cloud infrastructure that could expose user data [14]. This issue arises because many smart home equipment analyzes and store data using cloud-based services. Because of this perceived vulnerability of cloud-based systems [28], questions about the security mechanisms put in place to safeguard user data are raised, and the importance of robust security measures in the cloud architecture of smart home ecosystems is emphasized. Analyzing adopters' attitudes and concerns in-depth might reveal crucial information about the factors influencing their choices. Understanding how trust, privacy concerns, and security perceptions interact can help develop strategies to increase user confidence and address specific problems during the smart home adoption process [16].

Security and privacy matters of smart home devices can be addressed by a myriad of means be it technological or non-technological, as referenced in [17, 13]. Entering strong passwords, establishing secure home networks, and rectifying the user's behaviour when using these devices are some ways to secure them. Through the implementation of these steps, the overall safety and security of smart homes can be greatly increased [18].

Furthermore, the study demonstrated that even though these Internet of Things mitigations are there and consumers can use them to avoid potential risks, often they do not do anything about it; they fail to take actions [19]. Not recognizing the presence and the effectiveness of these security measures is another one of the many roots of this inaction. Hence, it is likely that consumers have no idea about the actions that they have to undertake to improve the overall security of their smart home equipment. Thus, it is no surprise that consumers are unaware of the exact steps they need to follow in order to harden the security of their smart home equipment. Besides, some of the technical mitigations are quite demanding such as

secure home network setup, users with low-level technical skills may find it complicated to deploy them [20]. A significant contributing factor hindering the execution of security measures is the phenomenon referred to as "privacy resignation." Users may feel resigned or accepted about the potential privacy dangers associated with smart home gadgets, which would reduce their propensity to actively implement security measures [11, 14, 21]. This attitude may stem from a feeling that privacy has already been violated in the digital age, that data collection and usage by device manufacturers and other entities is inevitable, or from a feeling that data control is lacking. Moreover, users have a propensity to delegate security responsibilities to parties other than themselves. There may be a perception of a lack of personal accountability among users if they feel that manufacturers, service providers, or government agencies should be in charge of guaranteeing the security of smart home devices [22].

To properly do this and thus enable people to become more cognitive, to bring about prompt action such as installation of some security layers as well as eliminating social barriers that make consumers discount the manufacturers and the privacy of their products, it is necessary to find out the reasons for the lack of user action [9]. If users are made aware of threats and various forms of protection they can use, and if they are helped to understand that it is their duty to contain the threats pose, and be convinced that they should be active participants in the defense [23], it is believable that users will embark on security measures. As per the recent study, one of the impediments to the broader adoption of Internet of Things (IoT) technology especially in smart homes where it is sought most is the issue of privacy security. Mistrust among users that the providers who are supposed to protect their private data will carry out this task is still a nagging concern, Magara and Zhou argue [43]. This kind of mistrust of some devices goes to the whole infrastructure of IoTs, which often comes across as more intrusive than older technologies. Even though such potential advantages do exist, these worries are what will keep IoT from going fully into the smart home framework. Users need allaying such fears if they are to be encouraged to use the IoT devices, hence allaying the fear of privacy by putting in place effective privacy laws and security measures.

Ruffner [44], in the article on the Internet of Things, addresses some growing concerns in the areas of security and privacy, especially in the context of mobile phones and smart homes. The University of Albany carried out his research which highlights the dismal state of gonadal awareness among the users of isohel and the security measures that they adhere to. Even with a very low level of anxiety, but especially with moderate to high level of anxiety, consumers of information do not seem to know what data is accumulated by their IoT devices, or even if it is known, adequate measures are rarely taken to ensure security. This stands with the general trend that is confirming people embracing IoT technology despite their worries about the negative impacts. This draws attention to the importance of better user training and improving the use of data in order to eliminate these gaps that have remained in the smart home environment.

A survey-based study by Schuster and Habibipour [45] investigated the issues raised by individuals regarding the security and privacy risks associated with the use of IoT devices at home. Their findings indicated that quite a good number of users expressed concern about their personal information security and the risk of possible infringement and abuse. Fewer than a third of the users said that they would place their faith in the manufacturers and service providers and the government to shield their privacy, which means that these people clearly do not trust these people’s institutions. This mistrust is a fundamental barrier to the wider use of IoT technology, emphasizing the need for more robust security protocols and open privacy guidelines to win over users' trust and enable the seamless integration of IoT into daily life.

A worldwide smart home system oriented towards the Internet of Things (IoT) technologies is not without security and privacy issues, with Geneiatakis et al. [46] doing an in-depth analysis of the scenario and suggesting solutions. Their research reveals that there are some specific threats and considering these Internet of Things devices offer multiple advantages and services however due to their processing capabilities they are prone to grave security and privacy threats. By analyzing a typical smart home environment, the authors illustrate the need for improved threat reduction strategies by pointing out instances where security and privacy breakdown arises. Their findings are corroborated by wider studies which have revealed that the reliance on the interactivity of different IoT devices carries a risk in terms of security and privacy enhancement which only encourages additional countermeasures against security problems. Kuyucu, Bahtiyar and Ince, in their [47] note downward attacks toward the security and privacy of smart IoT systems in smart homes deploying IoT devices. Their research shows how the diversity and large number of smart devices creates barriers to enabling the security and privacy protection desirable.

The authors define some concerns and present a brief description of several approaches designed to address these problems by analyzing the material that has already been written. Their findings highlight the need for all-encompassing solutions that tackle the complex issues of privacy and security in smart homes, highlighting the continuous need for research and development to improve defenses in this quickly developing field.

While looking into the integration between Internet of Things (IoT) devices and cloud computing systems, most researchers such as Singh, Buyya and Kim [48] therefore, focus on cloud models that represent risks for example infrastructure as a service (IAAS) and platform as a service (PAAS). In order to ensure the protection of confidential information regarding users and maintain the correctness of the data, their article points out the importance of effective security policies. It also addresses the concerns which emerge when conventional IoT systems merge with cloud infrastructures. They stress the importance of building sound security architectures within the expanding environment of IoT and provide options for the containment of these exposures and preemptive solutions to potential challenges. Further, Dhanraj et al. [49] investigate a multi-layer approach to enhancing privacy in smart IoT based houses. Measures have to be taken at the device level, network level and user level education on privacy and security matters needs to be incorporated to address the privacy and security issues effectively. Their review outlines research gaps and advocates for scalable and user-friendly policies, and at the same time legal and ethical issues are taken into account. By concentrating on misuse and illegal access to smart home gadgets, Solangi et al. (2024) address security issues in IoT-based home automation systems. For efficient home appliance monitoring and control, they provide a workable solution that combines an Ethernet shield unit and an Arduino microcontroller. By preventing unauthorized usage, their solution improves the security of smart home systems by incorporating an authentication mechanism. Aiming to reduce security risks and enhance the overall safety of IoT-enabled home automation systems, this workable solution is in line with continuing efforts to fix vulnerabilities in smart home technologies [50]. An extensive analysis of security and privacy concerns with IoT smart home access control devices is given by Uppuluri and Lakshmeeswari (2024). Their study discusses the serious problems associated with unauthorized access, such as the risks posed by replay and jamming assaults, which have the potential to undermine smart home systems. They go over several security strategies that fall within the taxonomy of smart home systems, including blockchain, access control, authentication, and cryptography-based solutions. By contrasting these methods, the authors evaluate various attacks on IoT systems for smart homes and draw attention to their individual benefits and drawbacks. Their evaluation includes risk factors like attack methodologies, frequency, severity, and probability. The paper concludes by discussing the current challenges, applications, and future directions for improving security and privacy in smart home IoT devices, providing valuable insights into the ongoing efforts to enhance protection mechanisms in this rapidly evolving field [51].

Our research corroborates several findings from prior studies and introduces supplementary mitigation approaches, including routine updates, careful device selection, and access control. Distinguishing itself from existing research, our analysis surpasses conventional expectations by assembling a comprehensive Wishlist of mitigations. This compilation serves as a valuable resource, capturing user preferences and expectations for privacy and security features in smart home devices in a distinctive manner. The Wishlist is poised to guide manufacturers and other pertinent stakeholders in enhancing consumer privacy and security features within the realm of smart home technology.

3. Methodology

This research uses a mixed-methods approach to investigate privacy and security issues in the Internet of Things (IoT) by combining a Systematic Literature Review (SLR) with qualitative interviews. Initially, the SLR was carried out to create a basic knowledge of the IoT environment by combining previous studies that were released between 2015 and 2024. This procedure established the framework for the qualitative component by identifying major themes and gaps in the literature. In order to have firsthand knowledge of 40 smart home customers' experiences and security and privacy issues, we performed qualitative interviews with them after the SLR. Because the qualitative interviews were intended to be inductive, themes and patterns naturally developed from the participants' answers. We were able to triangulate data

and reach more complex conclusions regarding user issues thanks to this approach, which enhanced the results from the SLR.

To guarantee the inclusion of excellent and pertinent studies, a thorough literature search was conducted across reliable academic databases. We used IoT-related terms in the search strategy, and to improve the selection process, we created inclusion and exclusion criteria. To make sure that only research that satisfied our quality standards were taken into account for analysis, this was essential. Important IoT components, such as technical developments, privacy and security issues, and useful applications, were recognized for data extraction. The reliability and rigor of the chosen studies were assessed using a quality assessment system that examined sample sizes, methodology, and the conclusions' clarity. Participants in the qualitative interviews were chosen to reflect a wide range of demographics, including age, level of technical proficiency, and kinds of smart home appliances utilized. Open-ended questions in a semi-structured interview format let participants to freely express their opinions while addressing important subjects including data privacy, security features, and individual experiences with smart home devices. Every interview took between thirty and sixty minutes, was done in person or over video conference, and was secretly filmed with participants' permission.

After the recorded interviews were transcribed and subjected to thematic analysis, recurrent themes and original insights that represented user concerns could be found. The results from the SLR were given a rich context by this inductive method, which also brought attention to the complexity of user experiences with regard to security and privacy in smart home contexts. The SLR's findings highlight significant trends, obstacles, and developments in the IoT space, providing insightful information for both scholarly study and real-world applications. This study adds to a better understanding of the current status of IoT research and identifies areas that need more investigation by using a methodical and open methodology. Research methodology is presented in figure 1.

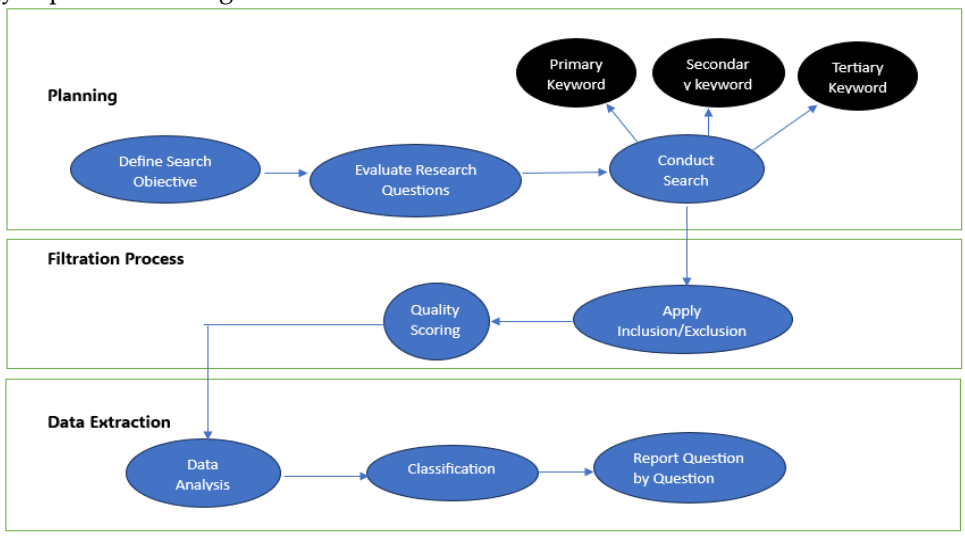

Figure 1. Research Methodology

3.1. Research Objective

In order to improve privacy and security in smart homes and lower potential risks and weaknesses, this study attempts to catalogue IoT-based devices [30, 32]. The study aims to identify significant areas in IoT that can direct future research in smart home security and privacy by performing a Systematic Literature Review (SLR). Among the specific objectives are reading up on the most recent advancements, difficulties, and inventions in IoT devices and smart home security. The study seeks to offer insightful information that will guide further investigation and advancement in this area.

RO1: To explore the state-of-the-art technologies used in IoT based smart home privacy and security.

RO2: To evaluate how users are implementing security and privacy mitigations and identify the factors that are influencing them in smart home systems.

RO3: Applying IoT based technology to ensure privacy and security of smart homes are adequately protected.

3.2. Research Questions

These lines imply that the research inquiry has explored a particular domain security of smart home ecosystem and looked into its underlying elements and motivations. The term "research question" suggests that the investigation is being driven by a central question. This methodology emphasizes a methodical and comprehensive analysis of the topic, suggesting a deliberate investigation of the fundamental elements within the designated research framework.

RQ1: What are smart home users' privacy and security concerns?

RQ2: What are the factors that impact users in the field of security and privacy mitigations.

RQ3: What features do users want for security and privacy when using IoT technology?

4. Search Scheme

The most important step of conducting an SLR is the preparation of a search plan to collect related research on a particular area. The articles chosen for this literature review are collected from digital repositories such as Springer Link, IEEE Xplore, Wiley and Academics. The keywords used to devise the search string are listed in Table 1 and search strings used to inquire multiple repositories have been listed in Table 2.

Table 1. Keywords used for searching

Primary Keyword	Secondary Keyword	Tertiary Keywords
IoT-based	Smart Home	Privacy
IoT	Home Safety	Usability
Internet of Things	Home security	Security Mitigation

4.1. Inclusion/Exclusion Criteria

In our research, we use a special number called the kappa statistic to check if different people agree on which papers to include or leave out. This helps make sure we're consistent and reliable in choosing papers for our study about privacy and security in smart homes using IoT technology. Cohen's Kappa, another name for the kappa number, indicates how well the reviewers agreed with one another while evaluating the publications. As part of the decision-making process, each article is independently evaluated by a number of reviewers who then classify them as "include" or "exclude" based on specified criteria. The Kappa coefficient can be estimated using the following formula after this initial assessment:

$$K = \frac{P_o - P_e}{1 - P_e}$$

Where:

Po is the observed agreement (the proportion of cases where reviewers agree),

Pe is the expected agreement (the proportion of cases where agreement is expected by chance).

When reviewers agree more, their decisions are more reliable, as indicated by a higher Kappa score. Enforcing uniformity in evaluations requires well-defined guidelines on inclusions and exclusions. Enhancing the frequency and dependability of reviewers' decisions can be achieved by holding practice sessions and regular meetings where they exchange views.

Table 2. Search strings with respect to digital repositories

Repository	Search keywords	Query	No. Of articles
Springer Link	Smart Home and IoT-based Smart Home	("Smart Home") AND ("IoT based") AND ("IoT-based Smart Home") AND ("Privacy Mitigation") AND ("IoT-based Smart Home") AND ("Privacy Mitigation")	8564
IEEE Xplore	Smart Home and IoT-based Smart Home	("Smart Home") AND ("IoT based") AND ("IoT-based Smart Home") AND ("Privacy") AND ("IoT-based Smart Home")	1725
Wiley	Smart Home and IoT-based Smart Home	("Smart Home") OR ("IoT based") AND ("IoT-based Smart Home") AND ("Privacy") AND ("IoT-based Smart Home")	9860

The study is included on the basis of the following criteria.
IC-1: Study targets IoT based technology for smart homes.
IC-2: Study is written on English Language
The study is excluded on the basis of the following criteria.
EC-1: Study is not written in other language.
EC-2: Study is published before 2014.

4.2. Quality Scoring

Evaluating the quality of included studies is a crucial phase in SLR. The selected studies experienced a quality assessment, and their quality was evaluated using the specified criteria.

Table 3. Quality Scoring

Criteria	Description	Rank	Score
	Internal Scoring		
a.	Does the study directly address to the research question or objectives of the SLR?	Yes	1
		Partially	0.5
		No	0
b.	Does the study fall within the specified time frame relevant to the SLR?	Yes	1
		Partially	0.5
		No	0
c.	Does the study report on outcomes or results that are pertinent to the systematic review?	Yes	1
		Partially	0.5
		No	0
	External Scoring		
d.	Is the study focused on a topic unrelated to the systematic literature review's research question or objectives?	Q1	2
		Q2	1.5
		Q3	0.5
		Core A	1
		Core B	1.5
		Core C	0.5

Classification of the literature studied is presented in Table 3 that categorizes studies based on investigation aspects and quality ratings, noting "None" where information is lacking. Abbreviations used to populate Table 3 are listed in figure 2.

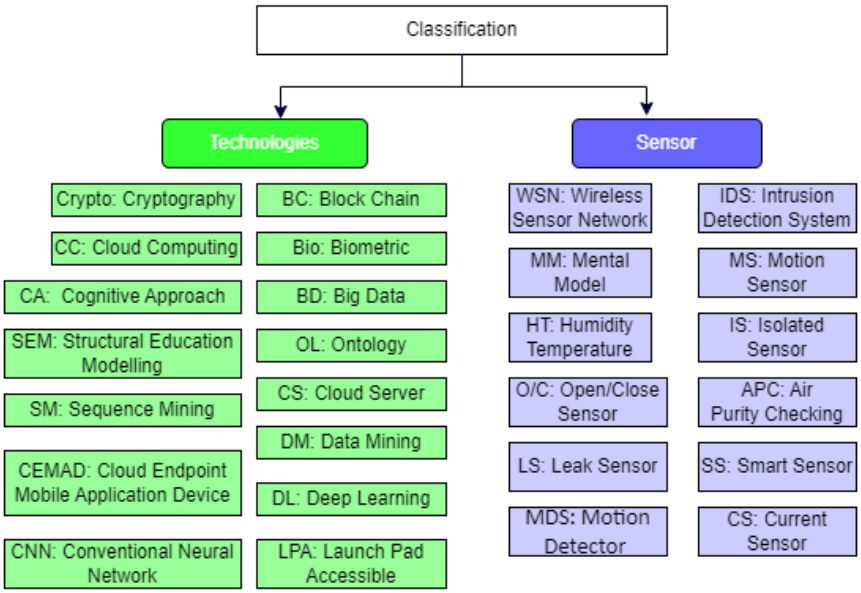

Figure 2. Abbreviation

Table 4. Classification Table

Ref.	Publication		Classification		
	Channel	Year	Technology	Sensors	Dominating Feature
[1]	Journal	2018	Crypto, BC, Bio , OL	WSN	Smart Gov. Smart City,
[2]	Journal	2022	BC	Isolated Sensor	Smart City, smart home
[3]	Journal	2020	DM, SM, Clustering	WSN	smart city, privacy, security
[4]	Journal	2022	BD, CC	None	Smart building
[5]	Conference	2016	ICT	None	None
[6]	Conference	2015	None	WSN	privacy, security, trust
[7]	Journal	2018	CA	WSN	privacy, security, trust
[8]	Journal	2016	ICT, BD	None	Intelligence, interconnection
[9]	Journal	2020	SEM	None	Remotely monitored
[10]	Conference	2019	None	None	None
[11]	Conference	2019	CA	None	privacy, security
[12]	Journal	2018	CS, API	embedded sensors	video doorbells
[13]	Journal	2019	Raspberry pi MM	O/C, MS, LS	home safety
[14]	Journal	2019	CEMAD	None	application-to-device
[15]	Journal	2022	DL, 1D-CNN	None	security
[16]	Journal	2010	DM; SM; Clustering	RFID	activity recognition
[17]	Journal	2020	SDN, SDR, FPGA	WSN	None
[18]	Conference	2017	MM	None	privacy, security, trust
[19]	Conference	2016	DM; SM; Clustering	SS, PIR MS	automation, remote
[20]	Journal	2018	Raspberry pi	None	Speech Recognition
[21]	Journal	2019	Heterogeneous	embedded sensors	Control Remotely
[22]	Journal	2014	Clustering	None	smart grid, security
[23]	Conference	2015	CS, API	O/C, Smart Sense MS	VPN
[24]	Journal	2017	CC, Arduino Yun	AC CC, PIR	automation system
[25]	Journal	2018	Node MCU	IR sensor, APC, HT	smart security

[26]	Conference	2019	BD, CC	None	smart grid, security
[27]	Journal	2021	TBSA Algo	WSN	None
[28]	Journal	2013	Fuzzy Logic	HSSN	None
[29]	Conference	2021	None	None	WebApp
[30]	Conference	2024	CS, API	SHAS	risk analysis
[31]	Conference	2024	TI CC3200 LPAWifi	Pir MDS	Alarm
[32]	Conference	2024	FLIP	LDR	Webapp
[33]	Journal	2024	Energy Efficient Devices	PIR, ES	Privacy and Security
[34]	Journal	2024	User Perception	General Home IoT Devices	Privacy and Security
[35]	Journal	2024	Multi-layer IoT Security	None	Privacy and Security
[36]	Conference	2024	Arduino, Ethernet Shield	None	Authentication, Security
[37]	Conference	2024	CS, API	O/C, SS MS	Web App

5. Results

The selected articles undergo data extraction and synthesis in accordance with the smart home [29] ecosystem delineated in this investigation. Figure 3 shows the distribution of Internet of Things (IoT)-based smart home devices [35] over the given time period. The summarization of the years in which the chosen studies were published indicates a noteworthy upward trend in publications in this field, especially beginning in 2019. The years 2021 and 2022 are where most of these publications are concentrated.

Out of the 35 papers that make up the review, 21 (or 65%) are journal-published and the remaining 14 (or 35%) are conference presentations. Notably, journal publications are more common in the following years: 2019, 2020, and 2021.

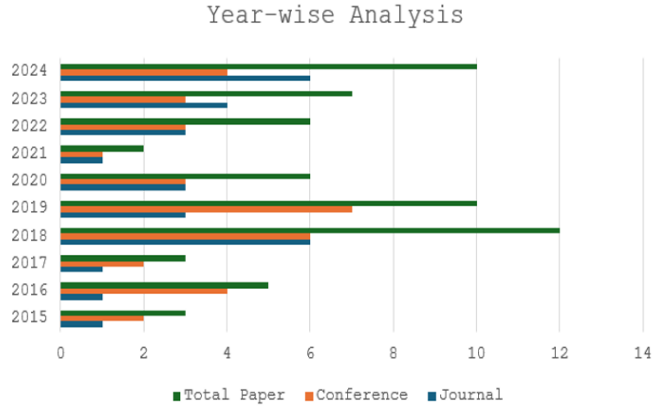

Figure 3. Distribution of selected studies over the years.Figure 4 shows that 59% (19) have undergone validation, while 41% (16) have not. The validation process is typically based on real-time processing of specific devices using machine learning algorithms.

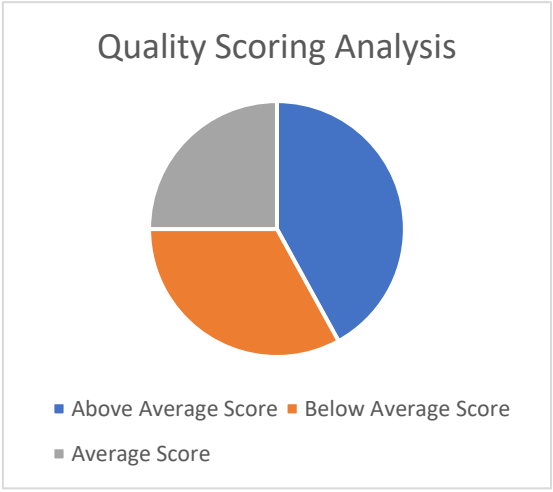

Figure 4. Quality scoring classification analysis.

Table 5. Quality assessment of selected papers

References	Score	Total
[15] [18]	5	2
[4] [12] [20] [22]	4.5	4
[1] [6] [9] [14] [17] [24] [29] [33]	4	8
[2] [10] [23] [30] [34]	3.5	5
[3] [7] [16] [25] [26] [28] [32]	3	7
[19] [21]	2.5	2
[5] [8] [11] [13] [27] [31] [35]	2	7

5.1. Assessment of Question 1- What are smart home users' privacy and security concerns?

Table 5 summarizes participants' privacy and security concerns, noting whether each concern was discussed privately or publicly, how many people raised it, and a sample quote. Key issues include manufacturer data breaches, government access to data, audio and video access via smart devices, and exposure of financial data. Table 4 lists studies by quality scores: 25% below average, 33% average, and 42% above average. Privacy concerns included household habit profiling, data selling, and uncertainty about data use. Security concerns ranged from personal safety and device hacking to apps exposing accounts, default security settings, and disruptive updates [33]. Some participants were indifferent: seven were nonchalant, 24 opposed the information gathered by smart devices [17], and eight denied the risk of hacking [37]. Participants generally accepted these risks to gain benefits. See Figure 5 for more details on privacy and security perceptions.

Table 6. Smart home privacy and security concern presently- number of participants mentioning the concern

Concern	#	Example Participant Quote
Audio/ Video access	34	"I was reading some articles where listens in on some of the conversations we have in our house without it being awake. That kind of freaks me out in the sense that we could be talking about something, and they have that information."
Data breaches	17	"Manufactures can say they can protect things, but in reality, if someone wants something bad enough, I do not know if they really can."

Government access	12	"I would hate to sound like a conspiracy theorist, but I am pretty sure the government and places like that can actually see what you do."
Exposure of financial information	8	"I would not want anybody committing fraud and taking my credit card information to do things they should not be doing."
Household profiling	19	"If someone was in control of this, they might be able to know what my schedule is, when I am usually home, when the house is empty."
Selling data	17	"That's what I am really afraid of, is the packaging my information to get trends and marketing it."
Unknows of data collection	16	"I am concerned because I think we are unaware of the types of information that these smart devices store of us."
Device Hacking	22	"There're just some people who are really smart and they are sitting somewhere, all they are thinking about is how to get into stuff. And if people could hack into the Department of Defense, they can hack into yours."
Safety	17	"It could be life threatening. If you reply on the smart device to keep your locked. If it does misfunction, there could be extreme circumstance."
Gaining Wi-Fi access	6	"Many of these devices, you are giving it your network password, so it has full access of everything on your network."
Linked Accounts	4	"If you use a password commonly access different accounts the same password, if they get hacked. If I log into my Google account might be able to get in because I might use the exact password and username."
Poor default security setting	2	"I would disturb if I saw a device that, for example, had a password you could not change or restricted you to something like a 4-digit key code that's more easily hacked."
Update Issue	2	"I guess one area where I would be worried about would be adding features that may threaten my privacy and security."

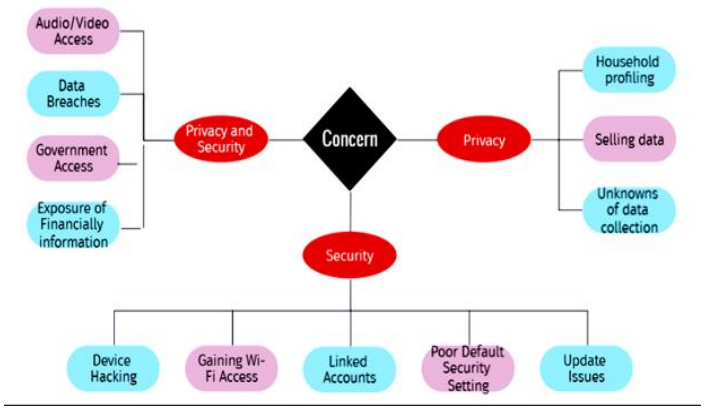

Figure 5. Privacy and Security Concern

5.2. Assessment of Question 2- What are the factors that impact users in the field of security and privacy mitigation?

Our research uncovered a range of mitigation strategies used by participants or other household members to allay worries about security and privacy. Every mitigation was discussed in terms of security and privacy. The percentage of participants who mentioned each mitigation is displayed in Figure 5. We go into greater detail about the mitigations below.

5.2.1. Authentication

When asked how they address their concerns, the participants mentioned using different forms of authentication (e.g., passwords, face recognition, two-factor). But usually, the user was prompted to perform this action during installation rather than being given the option. The majority of the time, authentication was discussed in relation to the device companion apps, which are frequently operated by a smartphone.

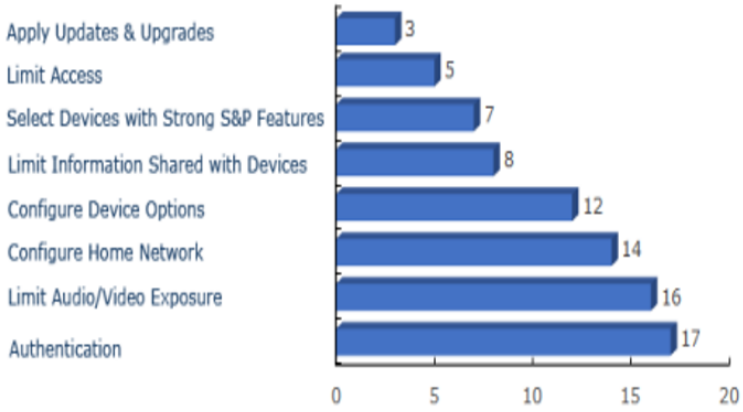

Figure 6. Security and Privacy mitigation mentioned by participants.

The most popular authentication method provided by device companion apps was passwords, which was also used frequently as the only mitigation mentioned in Figure 6. Even though it's not always easy, one participant said they password-protect their devices to avoid unauthorized access[6]. A lot of people discussed creating secure passwords, including choosing odd combinations that aren't in dictionaries. Although two-factor authentication was brought up by one person as an extra security precaution, the idea was not extensively explored in the group.

5.2.2. Limiting Exposure to Audio and Video

There are threats of illegitimate access to participants' audio and video data, participants observed while putting the cameras in less private zones and switching off the devices during intimate scenes. New methods of combating network threats such as VPN[37] were noted, however, password protected WPA/WPA2 and constantly changing passwords were more popular.

5.2.3.Option Configuration

Twelve people changed privacy and security settings in total. For the most part, this meant turning off default functionality. To prevent unintentional purchases, one participant, for instance, turned off their virtual assistant's capacity to place online orders. Eliminating the microphone on his smart TV gave a tech-savvy participant a sense of security. He also mentioned removing some settings that could disclose more information or allow excessive access to the device.

5.2.4. Limiting Shared Information

Only the information required by the device manufacturers, generally for establishing related apps, was mentioned by eight participants. One participant shared that they use two email addresses: one to register for accounts they never check and another to sign up for events they actually want to go to. Another participant said that they don't keep sensitive information or any specific data on their virtual assistant. Furthermore, some people save their real address or credit card details for instant purchases.

6.2.5. Device Selection

Some individuals prioritize security and privacy when purchasing devices. One person emphasized awareness of data usage, illegal access risks, and gadget safety [22]. Another stressed the importance of

investing in secure equipment, even at a higher cost. Participants also favored products from reputable manufacturers using well-known cloud services for added security assurance.

5.2.6. Limiting Access

The five participants explored various methods to limit access to smart home devices and associated apps. Three discussed implementing steps like restricting visitors and service providers from bringing devices into the house. Someone acknowledged using their VPN-equipped machine for private work. Another recommended keeping their phone safe and avoiding free Wi-Fi when using the apps to safeguard access to their phone, which contains apps for gadget companions.

5.2.7. Lack of Mitigation

Researchers found out why individuals decided not to implement mitigating strategies. Some claimed that there weren't enough privacy/security alternatives or that they weren't aware of the options. The explanation of controls was frequently ambiguous, which caused ambiguity regarding privacy settings, they mentioned. A number of people reported an overwhelming feeling of despair and termination, claiming that there was no way to manage the gathering of data. Some stated that they were not knowledgeable about cybersecurity and that they were not willing to learn more about it.

5.2.8.Mitigation Wish List

Users prioritize privacy and security despite accepting associated risks. Many express a desire for more control and confidentiality but lack the knowledge or capability to implement safeguards [31]. Manufacturers should provide educational resources and tools to empower users to adopt effective security measures.

5.2.9.Security and Privacy Controls

Survey participants wanted more control over device and data sharing, including setting security parameters and implementing two-factor authentication [36]. Users with technical backgrounds sought APIs for device functionality and preferred local data storage, limiting active interfaces and voice control to specific devices.

5.2.10. Security Features Concern

Four people responded that they wanted to know how devices are secured. Someone brought up the point that while security features aren't always obvious, it's important to understand them. In addition, participants requested the ability to choose between higher security levels and inquired as to whether they should fortify the security of their home network in order to address possible flaws in smart home security.

5.2.11. Assistance for Users

Four participants acknowledged they wanted recommendations and instructions to increase their devices' security. A participant expressed how important it was to receive advice on security best practices because they were knowledgeable of them. Another idea was to allow users to receive alerts from apps encouraging them to take security precautions. A regular user of smart home devices was looking for clear instructions on how to identify and fix security flaws in his devices and was concerned about the best ways to secure them.

5.3. Assessment of Question 3- What feature do users want for security and privacy when using IoT technology?

Participants' current security and privacy measures, along with their wish lists, can guide manufacturers in creating new products and reducing user burden by defaulting to robust security and privacy. Our interview study, which covered more than just privacy and security, revealed that participants rarely changed settings after the initial setup. Therefore, further investigation is needed to determine if installation is the best time to ask users about their security and privacy options.

5.3.1. Safe and confidential by default

People frequently exhibit reluctance to modify default security settings, as demonstrated by earlier usable security studies [25, 19]. Therefore, manufacturers may be able to set some settings to be the most private and secure by default, relieving users of an unnecessary burden. To understand how setting defaults to the most private/secure options may improve or worsen usability, more research is necessary.

5.3.2. Opt-in/opt-out

At the moment, it could not be feasible or difficult to refuse data gathering and its different applications. For instance, one manufacturer demanded that a letter asking for a restriction on data sharing

be mailed. Given that participants want more choice over how their data is used, further investigation is required into how manufacturers can provide an easy-to-configure opt-in/opt-out option.

5.3.3.Transparency in data usage

Users are often unaware of data collection practices due to the difficulty and rarity of reading device privacy rules and user agreements. Manufacturers should be more open about what information is gathered, where it travels, how long it's kept, and with whom it's shared.

5.3.4.Data localization

A common concern expressed by our participants was the manufacturer's profiling of their households, the sale of their personal information, and potential breaches of manufacturer data storage. Instead of sending everything to the manufacturer's cloud, manufacturers could offer options to localize whatever data processing is localizable, in order to allay these worries.

5.3.5.Securability

"Securability" is the ability and knowledge to enable and configure appropriate security features, essential in user-context scenarios [13]. Manufacturers can enhance product security by providing real-time support, such as configuration wizards, to help users set the right security levels for their needs.

5.3.6.Fine-grained options for experienced users

Experienced users emphasized the importance of enhanced security controls. Manufacturers should provide detailed options for technical users and user-friendly wizards for others. Balancing these needs requires further research into effective interface solutions.

5.3.7. Update transparency

Since updates may be the only defense against some types of vulnerabilities in smart home devices (like those in the code), they are particularly crucial. Manufacturers should either offer an option for automatic updates or push notifications to users with clear installation instructions and descriptions of the importance of applying the update. This is in line with the NIST Interagency Report 8267 (Draught) Security Review of Consumer Home Internet of Things (IoT) Products [5] recommendation that users receive update notifications in a timely manner.

5.3.8. Advice on network security

In order to safeguard smart home appliances, home networks must be secured. But frequently, people lack the information and drive to act. For instance, despite the fact that few study participants possessed the necessary technical skills, the FBI advises users to segment their networks [26]. In addition to the security features offered by the devices themselves, a number of study participants stated that they would like manufacturers to offer detailed instructions on home network security (such as configuring secure Wi-Fi and password-protecting every device on the network).

5.4. Proposed Taxonomy

Figure 7 illustrates the design of an IoT-based women's safety taxonomy that summarizes the research findings. Table 6 presents the articles retrieved in this study as per taxonomy level.

5.4.1. Smart Security

The foundation of this taxonomy is the idea of smart security, which entails putting strong safeguards in place like access control and user authentication. This involves using cutting-edge methods like multi-factor authentication and biometrics to guarantee that only authorized users can access systems and gadgets in smart homes. Additionally, using secure communication channels and encryption protocols for data breaches and unauthorized access creates a stronger defense.

5.4.2. Home Environment Protection

The protection of the home network goes beyond the internet. Frequent firmware and software updates for devices act as a vital mitigation technique, improving security features and patching vulnerabilities. In order to ensure a strong defense against external threats, network security measures, such as firewalls and intrusion detection systems, are essential for strengthening the home environment's overall security posture.

5.4.3.Virtual Assistants and Behavioral Analysis

Virtual assistant integration adds a dynamic dimension to security considerations. Differentiating between potential security threats and regular patterns of interaction requires the application of behavioral analysis and anomaly detection. Algorithms that employ machine learning techniques can examine user

behavior and spot variations that could point to malevolent or illegal activity. This proactive strategy fits in with the rapidly changing field of smart home technologies [27] by adding an intelligent layer to security protocols. Taxonomy of approaches is presented in Figure 7.

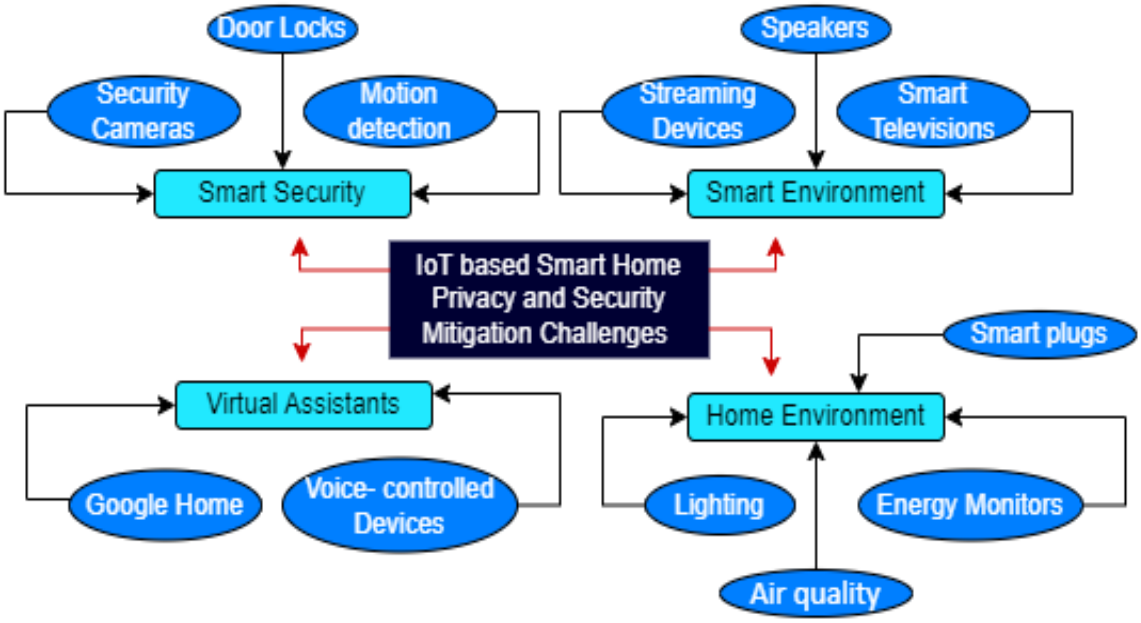

Figure 7. Taxonomy of IoT based Smart Home

5.4.4.Smart Environment

Third-party security audits and certifications are required in order to take the smart environment into consideration. Obtaining independent assessments from reliable sources guarantees a fair appraisal of the security measures' efficacy. In addition to boosting user confidence, adhering to industry standards and certification schemes gives manufacturers a benchmark against which to measure their progress and adjust to new security threats.

We have compared our methodology with the existing research in Table 7. In the existing literature, various studies have explored aspects of privacy and security in smart home environments. For instance, the paper titled "Factors At Play: Investigating The Dimensions Of Privacy And Security In Smart Home Environments" [39] primarily identifies theoretical dimensions of privacy and security concerns but does not delve into user experiences or provide actionable solutions. Similarly, "IoT Based Home Automation System: Security Challenges and Solutions" [40] outlines specific security challenges within IoT systems and proposes general solutions; however, it lacks an in-depth exploration of user perceptions and behaviors regarding these security measures.

Another relevant work, "A Review on Mitigating Privacy Risks in IoT-Enabled Smart Homes" [41], highlights privacy risks and offers broad mitigation strategies, yet its review format limits the inclusion of original qualitative insights from users, which is crucial for understanding real-world applications. Additionally, the survey titled "Security in Smart Home Environment: Issues, Challenges, and Countermeasures" [42] focuses on security issues and countermeasures but fails to provide qualitative data that reflect user experiences or their willingness to adopt recommended security practices.

In contrast, our study uniquely combines qualitative interviews with 40 smart home users to explore the multifaceted impact of smart home technology and IoT integration. We analyze user concerns regarding safety, convenience, energy efficiency, and security vulnerabilities, revealing a significant gap between awareness and action in risk mitigation. By focusing on lived experiences, we offer actionable recommendations that address both user knowledge gaps and practical design improvements. This user-centric approach not only highlights specific barriers to effective security practices but also sets our work apart from existing literature, emphasizing the importance of understanding user behavior in the development of safer and more secure smart home technologies.

Table 7. IOT BASED SMART HOME AND SECURITY MITIGATION CHALLENGES.

Domain	Sub Domain	Ref.
Smart Security	Security Cameras	[5], [22]
	Motion Detection	[9]
	Door Locks	[11], [23]
Home Environment Protection	Smart plugs	[27]
	Energy Monitors	[32],[17],[10]
	Thermostat	[8], [15]
	Home and air quality	[17]
	Lighting	
Virtual Analysis and Behavior	Google Home	[33], [28],[29]
Analysis	Voice-controlled devices	[14]
Smart Environment	Smart Television	[7], [18]
	Streaming Devices	[6]
	Speakers	[16], [22]
	Other connected media systems	[25], [31]

Table 8. Comparison with existing solutions

Ref.	Methodology and Contribution
[39]	Factors At Play: Investigating The Dimensions Of Privacy And Security In Smart Home Environments
[40]	Identification of security challenges and proposal of solutions in IoT-based home automation.
[41]	Review of privacy risks and mitigation strategies in IoT-enabled smart home environments.
[42]	Survey-based study focusing on security issues and countermeasures in smart home environments.
Proposed Work	Survey and qualitative analysis exploring the impact of smart home technology and IoT integration on safety, convenience, energy efficiency, and security vulnerabilities.

5.4.5. User Awareness and interface Design

Educating users about threats and precautions is essential for smart home security. User-friendly interfaces that simplify privacy settings empower users. This taxonomy aids developers, manufacturers, and users in navigating IoT-based smart home privacy and security, promoting a secure ecosystem.

5.4.6. Implications

People used different methods to handle the risks of smart home devices. Some were careful about privacy and security, while others didn't fully understand the issues. Methods included setting up passwords and moving devices to different locations. Many people wanted to control their data but found it hard to choose the right options. Protecting home internet connections was difficult for a lot of people. In general, people were worried about privacy and security but felt they couldn't do much about it. Companies could make easier-to-use tools to help people make better security choices, and more research and practical tests could lead to better solutions.

5.4.7.Snowball Approaches

On the issue of privacy and security in IoT-based Smart Home, measures can be taken in a way that is like compounding. Responding to one problem, for instance, user authentication, sheds the light on other issues like data encryption. Improvements through firmware updates and networks cause a greater need for third-party audit and apex behavioral analysis for virtual assistants, showing that a holistic view is necessary.

5.4.8. Recommendation to the Researchers

Researchers play a crucial role in mitigating privacy and security issues in IoT-based Smart Homes [34]. They must conduct comprehensive risk assessments, develop user-centric design principles, and

innovate in behavioral analysis [38]. By leveraging advanced machine learning and anomaly detection techniques, researchers can enhance security and privacy measures within user interactions [36], leading to robust, user-friendly, and adaptable solutions.

5.5. Limitations

The study that used interviews has some problems. People might not remember things correctly, they might tell us what they think we want to hear, and they might not want to look bad by telling the truth. Also, the people in the study are well-educated and rich, so the results might not apply to everyone. Different countries have different ideas about privacy because of their culture and government. The study didn't look at people who don't use or only use a little bit of smart home technology. Even with these issues, the study gives us a new way to understand what people who use smart homes think and do, which can help us do bigger and better studies in the future.

7. Discussion

Using the mixed-methods approach, we were able to take advantage of the strengths of each of the qualitative interviews and SLR reviews, for instance, how the so-called SLR portraits the IoT environment and the qualitative interviews where opinions about user's experiences are vivid and in-depth. This is related to the complexity of integrating privacy and security within the smart home technology that contributes to the credibility of the research findings. Key concerns that revolved around security and privacy were highlighted by the 40 users that were interviewed. Normal concerns that were raised by the participants included the effectiveness of security measures introduced by the manufacturers of the devices as well as how they control their devices and the actual process of collecting and using of data obtained. There are, however, certain phenomena that have challenged this assertion, and our findings offer such evidence.

The induced complexities regarding the costs of opting out and the procedures for opting in to share data have been described as the bane of all democratic decision making. A majority of the participants stated that they were not aware of how these mechanisms function, producing an impression that a majority were willing to accept the default configurations without further deliberation. Producers of such components should deal with this by providing efficient, user-friendly systems that optimize these activities.

Using a tiered consent model would protect provide consumers clear-cut options about data sharing at the time of initial setup, making it simple for them to change their minds later. Including visual cues like progress bars or icons could also make it easier for users to quickly understand their data-sharing options. Technical issues form another major barrier, which our survey performed in this area found consumers encountering when trying to set up their smart appliances. There is little knowledge among many consumers who are not tech-savvy of how to navigate through complex security features and agreements. This might be alleviated by manufacturers providing comprehensive onboarding experiences that guide users through the process of setting up security in an incremental manner. Using things like interactive tour guides or videos could greatly enhance the user's comprehension. Similarly, allowing users to access help related to the tasks at hand, like tooltips or FAQs or even contextual help, can be more useful in ensuring educated but not too knowledgeable users are not bored. What users usually consider ease of use as the most important feature, above which, according to our findings, poses a lot of risks in smart houses. This implies that the manufacturers will have to come up with strategies which will make the consumers enjoy the process of enhancing security. The behavior of the users toward a more security-conscious mind can also be controlled by offering rewards to the users who are involved in the protection of their devices. Such reward can be monetary but work based, for example completing assigned tasks such as frequent password changes, consistent updating of security software checks.

Additionally, there is a pivotal aspect of education. Licensing is not an easy task since there seems to be a very big lack of understanding, showing that quite a number of consumers still need to familiarize themselves with some basic ways of protecting their devices. Therefore, it is suggested that there should be a shift in the approach of the manufacturing companies towards preparing simple and easy infographics, webinars and community forums. This will assist to elevate the levels of user awareness concerning security and offer useful tips. Collaborating with cybersecurity experts in producing credible materials can further spike the interest and confidence more.

Overall, the findings of our research confirm that a complete approach, which contains both motivation and extensive training combined with simplicity of design, increases the ability of users to understand and manage security and privacy issues on smart home technologies. These issues must be addressed if it were to create a better and secure on the IoT environment.

8. Conclusion

Our research ends up with a conclusion that explains the importance of addressing the privacy and security challenges regarding the smart home technology. As much as clients express genuine worries, most of these concerns remain unaddressed due to convoluted contracts and difficult technology which thwart any attempts to implement such security measures. This inconsistency necessitates new measures and mechanisms involving the manufacturers, the state bodies, and the end-users, in order to enhance transparency, enforce sufficient and efficient security measures and allow individuals to have control over their information. What is more, the development of the proper user experiences and the defined risks of their insufficient management comprise the primary novel contributions of our research. Such technology is extending the practical limits of what can be done to nurture user creativity and design capabilities, encouraging manufacturers to make their products trustable and user-friendly.

These dilemmas are not only limitations in the interaction design of users as well as technologies, but also need to address user privacy concerns to create trust in the possibilities of IoT solutions. Through working together, the contributions of all the stakeholders to the development of smart home technologies can ensure that such systems progress in a constructive manner, meeting user expectations even as security and privacy issues are emphasized. Finally, facing non-corporate users our drape concludes the story with a market approach. All users will be empowered without any heresy and distrust of users and making their prime focus on developing and deploying new smart home technologies.

Funding: This research received no external funding
Data Availability Statement: Data will be made available on request.
Acknowledgments: We are thankful to Mr. M . Inayat Ali for his help , guidance and support throughout research.
Conflicts of Interest: The authors declare no conflict of interest.

References

1. Cui, L., Xie, G., Qu, Y., Gao, L., & Yang, Y. (2018). Security and privacy in smart cities: Challenges and opportunities. IEEE access, 6, 46134-46145. Doi:10.1109/ACCESS.2018.2853985
2. Haque, A. B., Bhushan, B., & Dhiman, G. (2022). Conceptualizing smart city applications: Requirements, architecture, security issues, and emerging trends. Expert Systems, 39(5), e12753. Doi:10.1111/exsy.12753
3. Ismagilova, E., Hughes, L., Rana, N. P., & Dwivedi, Y. K. (2020). Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework. Information Systems Frontiers, 1-22. Doi:10.1007/s10796-020-10044-1
4. Singh, T., Solanki, A., Sharma, S. K., Nayyar, A., & Paul, A. (2022). A Decade Review on Smart Cities: Paradigms, Challenges and Opportunities. IEEE access. Doi:10.1109/ACCESS.2022.3184710
5. Joshi, S., Saxena, S., & Godbole, T. (2016). Developing smart cities: An integrated framework. Procedia Computer Science, 93, 902-909. Doi:10.1016/j.procs.2016.07.258
6. Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. Computer networks, 76, 146-164. Doi:10.1016/j.comnet.2014.11.008
7. Sfar, A. R., Natalizio, E., Challal, Y., & Chtourou, Z. (2018). A roadmap for security challenges in the Internet of Things. Digital Communications and Networks, 4(2), 118-137. Doi:10.1016/j.dcan.2017.04.003
8. Mohanty, S. P., Choppali, U., & Kougianos, E. (2016). Everything you wanted to know about smart cities: The Internet of things is the backbone. IEEE Consumer Electronics Magazine, 5(3), 60-70. Doi:10.1109/MCE.2016.2556879
9. Guhr, N., Werth, O., Blacha, P. P. H., & Breitner, M. H. (2020). Privacy concerns in the smart home context. SN Applied Sciences, 2, 1-12. Doi:10.1007/s42452-020-2025-8
10. Yao, Y., Basdeo, J. R., Mcdonough, O. R., & Wang, Y. (2019). Privacy perceptions and designs of bystanders in smart homes. Proceedings of the ACM on Human-Computer Interaction, 3(CSCW), 1-24. Doi:10.1145/3359161
11. Yao, Y., Basdeo, J. R., Kaushik, S., & Wang, Y. (2019). Defending my castle: A co-design study of privacy mechanisms for smart homes. Proceedings of the 2019 chi conference on human factors in computing systems, Doi:10.1145/3290605.3300428
12. Wilson, C., Hargreaves, T., & Hauxwell-Baldwin, R. (2015). Smart homes and their users: a systematic analysis and key challenges. Personal and Ubiquitous Computing, 19, 463-476. Doi:10.1007/s00779-014-0813-0
13. Yoshigoe, K., Dai, W., Abramson, M., & Jacobs, A. (2015). Overcoming invasion of privacy in smart home environment with synthetic packet injection. 2015 TRON Symposium (TROnShOW), Doi:10.1109/TRONSHOW.2014.7396875
14. Kodali, R. K., Jain, V., Bose, S., & Boppana, L. (2016). IoT based smart security and home automation system. 2016 international conference on computing, communication and automation (ICCCA), Doi:10.1109/CCAA.2016.7813916
15. Zheng, S., Apthorpe, N., Chetty, M., & Feamster, N. (2018). User perceptions of smart home IoT privacy. Proceedings of the ACM on Human-Computer Interaction, 2(CSCW), 1-20. Doi:10.1145/3274469
16. Murdan, A. P., & Gunness, L. (2017). An Internet of Things based system for home automation using Web Services and Cloud Computing. Journal of Electrical Engineering, Electronics, Control and Computer Science, 3(1), 29-36. Doi:10.2139/ssrn.3645458
17. Almusaylim, Z. A., & Zaman, N. (2019). A review on smart home present state and challenges: linked to context-awareness internet of things (IoT). Wireless networks, 25, 3193-3204. Doi:10.1007/s11276-018-1712-5
18. Malche, T., & Maheshwary, P. (2017). Internet of Things (IoT) for building smart home system. 2017 International conference on I-SMAC (IoT in social, mobile, analytics and cloud)(I-SMAC) Doi:10.1109/I-SMAC.2017.8058258
19. Mahadik, S., Pawar, P. M., & Muthalagu, R. (2022). Efficient Intelligent Intrusion Detection System for Heterogeneous Internet of Things (HetIoT). Journal of Network and Systems Management, 31(1), 2. Doi:10.1007/s10922-022-09697-x
20. Elrawy, M. F., Awad, A. I., & Hamed, H. F. A. (2018). Intrusion detection systems for IoT-based smart environments: a survey. Journal of Cloud Computing, 7(1), 21. Doi:10.1186/s13677-018-0123-6
21. Tabassum, M., Kosinski, T., & Lipford, H. R. (2019). " I don't own the data": End User Perceptions of Smart Home Device Data Practices and Risks. Fifteenth symposium on usable privacy and security (SOUPS 2019), Doi:10.1007/978-3-031-62918-1_7
22. Komninos, N., Philippou, E., & Pitsillides, A. (2014). Survey in smart grid and smart home security: Issues, challenges and countermeasures. IEEE Communications Surveys & Tutorials, 16(4), 1933-1954. Doi:10.1109/COMST.2014.2320093
23. Rashidi, P., Cook, D. J., Holder, L. B., & Schmitter-Edgecombe, M. (2010). Discovering activities to recognize and track in a smart environment. IEEE transactions on knowledge and data engineering, 23(4), 527-539. Doi:10.1109%2FTKDE.2010.148
24. Mohamed Ben Ahmed, Anouar Abdelhakim Boudhir, Rani El Meouche, İsmail Rakıp Karaş (2023). Innovations in Smart Cities Applications Volume 7 The Proceedings of the 8th International Conference on Smart City Applications, Volume 1 Doi:10.1007/978-3-031-53824-7
25. Alrawi, O., Lever, C., Antonakakis, M., & Monrose, F. (2019). Sok: Security evaluation of home-based iot deployments. 2019 IEEE symposium on security and privacy (sp), Doi:10.1109/SP.2019.00013
26. Kousalya, S., Priya, G. R., Vasanthi, R., & Venkatesh, B. (2018). IOT based smart security and smart home automation. International Journal of Engineering Research & Technology (IJERT), 7(04), 43-46. 10.17577/IJERTV7IS040026

27. Zimmermann, V., Gerber, P., Marky, K., Böck, L., & Kirchbuchner, F. (2019). Assessing users' privacy and security concerns of smart home technologies. i-com, 18(3), 197-216. Doi:10.1515/icom-2019-0015
28. Stolojescu-Crisan, C., Crisan, C., & Butunoi, B.-P. (2021). An IoT-based smart home automation system. Sensors, 21(11), 3784. Doi:10.3390/s21113784
29. Sang-Hyun, L., Lee, J.-G., & Kyung-Il, M. (2013). Smart home security system using multiple ANFIS. International Journal of Smart Home, 7(3), 121-132. DOI: 10.1007/s10916-016-0549-7
30. Jacobsson, A., Boldt, M., & Carlsson, B. (2016). A risk analysis of a smart home automation system. Future Generation Computer Systems, 56, 719-733. Doi:10.1016/j.future.2015.09.003
31. Pătru, I.-I., Carabaş, M., Bărbulescu, M., & Gheorghe, L. (2016). Smart home IoT system. 2016 15th RoEduNet Conference: Networking in Education and Research Doi:10.1109/RoEduNet.2016.7753232
32. Yadav, C. (2018). Iot based surveillance system and home automation. Int Res J Eng Technol, 5(5), 2031-2036. Doi:10.1007/978-981-16-8721-1_48
33. Bauwens, J., Ruckebusch, P., Giannoulis, S., Moerman, I., & De Poorter, E. (2020). Over-the-air software updates in the internet of things: An overview of key principles. IEEE Communications Magazine, 58(2), 35-41. Doi:10.1109/MCOM.001.1900125
34. Zeng, E., Mare, S., & Roesner, F. (2017). End user security and privacy concerns with smart homes. thirteenth symposium on usable privacy and security (SOUPS 2017) , 978-1-931971-39-3
35. Alam, A., Molyneaux, H., & Stobert, E. (2021, 2021//). Authentication Management of Home IoT Devices. HCI for Cybersecurity, Privacy and Trust, Cham. Doi:10.1007/978-3-030-77392-2_1
36. Costa, L., Barros, J. P., & Tavares, M. (2019). Vulnerabilities in IoT devices for smart home environment. Proceedings of the 5th International Conference on Information Systems Security e Privacy, ICISSP 2019. Doi:10.3390/fi14100276
37. Ahmed A. Abd El-Latif, Lo'ai Tawalbeh, Yassine Maleh, Brij B. Gupta (2023) Secure Edge and Fog Computing Enabled AI for IoT and Smart Cities. International Conference on Advanced Computing & Next-Generation Communication (ICACNGC 2022) 978-3031510960
38. Asim, M., Junhong, C., Wenyin, L., Abd El-Latif, A.A. (2024). Artificial Intelligence-Based Secure Edge Computing Systems for IoTDs and Smart Cities: A Survey. In: Abd El-Latif, A.A., Tawalbeh, L., Maleh, Y., Gupta, B.B. (eds) Secure Edge and Fog Computing Enabled AI for IoT and Smart Cities . EAI/Springer Innovations in Communication and Computing. Springer, Cham. Doi:10.1007/978-3-031-51097-7_13
39. S. Nagarkar, P. Mishra, V. Gaikwad, "Factors At Play: Investigating The Dimensions Of Privacy And Security In Smart Home Environments," Educational Administration: Theory and Practice, vol. 30, no. 5, 2024, pp. 3197-3203. Doi:10.53555/kuey.v30i5.3414
40. [40] N. Solangi, A. Khan, M. F. Qureshi, N. Zaki, U. M. Qureshi, Z. Umair, "IoT Based Home Automation System: Security Challenges and Solutions," 2024 5th International Conference on Advancements in Computational Sciences (ICACS), Lahore, Pakistan, pp. 1-6, doi: 10.1109/ICACS60934.2024.10473277.
41. T. Dhanraj, M. Kumar, S. Singh, R. Kumar, P. Jaiswal, H. Mohapatra, "A Review on Mitigating Privacy Risks in IoT-Enabled Smart Homes," Computer Networks and Communications, 2024, pp. 132-147. Doi:10.37256/cnc.2120244736
42. R.M. Saad, K.A.A. Soufy, S.I. Shaheen, "Security in smart home environment: issues, challenges, and countermeasures-a survey," International Journal of Security and Networks, vol. 18, no. 1, 2023, pp. 1-9. Doi:10.1504/IJSN.2023.129887
43. Magara, Tinashe, and Yousheng Zhou. "Internet of Things (IoT) of Smart Homes: Privacy and Security." Journal of Electrical and Computer Engineering 2024, no. 1 (2024): 7716956. Doi: 10.1155/2024/7716956
44. Ruffner, Jack. "Investigating User Awareness of Privacy and Security Concerns in the IoT Era." (2024). Doi: 10.1007/978-3-031-18458-1_13
45. Schuster, Frederik, and Abdolrasoul Habibipour. "Users' privacy and security concerns that affect IoT adoption in the home domain." International Journal of Human–Computer Interaction 40, no. 7 (2024): 1632-1643. Doi: 10.1080/10447318.2022.2147302
46. Geneiatakis, Dimitris, Ioannis Kounelis, Ricardo Neisse, Igor Nai-Fovino, Gary Steri, and Gianmarco Baldini. "Security and privacy issues for an IoT based smart home." In 2017 40th international convention on information and communication technology, electronics and microelectronics (MIPRO), pp. 1292-1297. IEEE, 2017. Doi: 10.23919/MIPRO.2017.7973622
47. Kuyucu, Meral Korkmaz, Şerif Bahtiyar, and Gökhan İnce. "Security and privacy in the smart home: A survey of issues and mitigation strategies." In 2019 4th International Conference on Computer Science and Engineering (UBMK), pp. 113-118. IEEE, 2019. Doi: 10.1145/3558095
48. Singh, Nivedita, Rajkumar Buyya, and Hyoungshich Kim. "Securing Cloud-Based Internet of Things: Challenges and Mitigations." arXiv preprint arXiv:2402.00356 (2024). Doi: 10.3390/app10124102
49. Dhanraj, Tushar, Manash Kumar, Suhani Singh, Rounit Kumar, Priyanshu Jaiswal, and Hitesh Mohapatra. "A Review on Mitigating Privacy Risks in IoT-Enabled Smart Homes." Computer Networks and Communications (2024): 132-147. Doi: 10.37256/cnc.2120244736

50. Solangi, Nighat, Aiman Khan, Mehak Fatima Qureshi, Nafeesa Zaki, Umair Mujtaba Qureshi, and Zuneera Umair. "IoT Based Home Automation System: Security Challenges and Solutions." In 2024 5th International Conference on Advancements in Computational Sciences (ICACS), pp. 1-6. IEEE, 2024. Doi: 10.1109/icacs60934.2024.10473277
51. Uppuluri, Sirisha, and G. Lakshmeeswari. "Review of Security and Privacy-Based IoT Smart Home Access Control Devices." Wireless Personal Communications (2024): 1-40.Doi: 10.14569/IJACSA.2020.0110234