American Journal of Information Science and Technology
2024; Vol. 8, No. 1, pp. 1-14
https://doi.org/10.11648/j.ajist.20240801.11

Research Article

Security and Privacy Concerns in the Adoption of IoT Smart Homes: A User-Centric Analysis

Tinashe Magara[1, *], Yousheng Zhou[1, 2]

[1]College of Computer Science and Technology, Chongqing University of Posts and Telecommunications, Chongqing, China

[2]School of Cyber Security and Information Law, Chongqing University of Posts and Telecommunications, Chongqing, China

Abstract

The advancement of Internet of Things (IoT) technologies has ushered in a new era of smart homes, promising convenience and automation. However, alongside these advancements, concerns regarding the security and privacy of Internet of Things smart homes have garnered significant attention. The study embarked on a user-centric analysis, delving into the intricacies of security and privacy concerns in the adoption of Internet of Things smart homes. The primary purpose of this research was to investigate the security and privacy concerns that users harbour when adopting Internet of Things smart home technologies. We used SMART-PLS version (4.0.9.6) as the data analysis tool, to examine the concerns and to gain a comprehensive understanding of their impact on adoption. The analysis was, rooted in quantitative research design and based on data gathered through an online questionnaire distributed to the target population of 325 participants. The research response rate was 92%. The hypotheses examined unveiled statistically significant relationships, culminating in results indicating an R^2 of 0.762. This implies that approximately 76.2% of the rationale behind individuals' decisions to either adopt or refrain from using IoT smart home devices, with a focus on security and privacy considerations, can be elucidated by our proposed Structural Equation Model. his model served as a comprehensive lens through which we dissected the intricate interplay of variables shaping user attitudes and behaviors. The study sheds light on the critical concerns of security and privacy within the IoT smart home domain. By leveraging quantitative analysis and a well-crafted Structural Equation Model, we offer valuable insights into the factors influencing user adoption decisions. The research contributes to the broader discourse IoT technology adoption and serves as a foundation for future studies and policy considerations in the ever-evolving landscape of smart homes.

Keywords

Internet of Things, Security and Privacy, Smart Homes

1. Introduction

The emergence of Internet of Things (IoT) technologies has brought about significant shifts in the rapidly growing technological world, notably in the domain of smart homes. These Internet of Things enabled smart home technologies promise enhanced convenience and efficiency, revolutionising the everyday lives by decreasing laborious activities and

*Corresponding author: tinashenosh@gmail.com (Tinashe Magara)

Received: 13 November 2023; **Accepted:** 8 February 2024; **Published:** 19 March 2024

improving the quality of interactions with the living surroundings [1]. However, the technical advance comes with a major user security and privacy concerns. Al-Syouf et al. suggest for a secure smart home design that incorporates aspects such as the cloud, secure fog, and powerful firewall mechanisms [2]. Mrabet et al. provides an in-depth examination of IoT/NB-IoT Layered architecture, emphasising the need of multi-layered security [3]. These significant contributions highlight the critical role that security and privacy play in maintaining the effective functioning of IoT devices while protecting against data breaches and privacy violations. Literature has made significant contributions to the understanding of the dynamic landscape.

However, an atmosphere of uncertainty looms over the hopes and opportunities. Consumers are often in the dark about privacy and security measures while using devices for smart homes. Some manufacturers put the needs of their customers ahead of security, while others hide controls to adhere to data-driven business objectives. When coupled with customers' ignorance of smart home technology, functionality, and privacy and security complexities, this complicated interaction poses significant threats to consumer security and privacy.

The main aim of the research study seeks to thoroughly examine how users perceive the adoption of IoT smart homes. The slow rate of IoT smart home adoption, which has been linked to a variety of issues, has been emphasised in recent research as a significant concern. Users' lack of IoT understanding security and privacy comes out as a major barrier among these reasons. Potential customers who are intimidated by the technological intricacies are sometimes turned off by IoT technology's complexity. Users are also reluctant to use smart home devices because of their strong worries about privacy and security. These concerns are not unfounded, since IoT devices have already been exposed to flaws and data breaches. Thus, our research aims to look deeply into the complex framework of user perceptions, requirements, and concerns in order to better understand the user-centric limitations to IoT smart home adoption. By shedding light on these issues, the study paves way for customised solutions that may bridge the knowledge gap, improve security measures, and eventually promote a more seamless and secure transition into the era of IoT smart homes.

Considering these difficulties, a paradigm change is essential. A user-centred strategy must be adopted by manufacturers and other significant players in the smart home ecosystem. This strategy is based on actual data and considers the views, desires, aspirations, and concerns of end users. It demands the development of comprehensive guidelines, user-friendly interfaces, meaningful and effective privacy and security measures, and user-relevant instructional materials. Determining which tasks users are willing and competent to perform on their own and which should be left to others is equally important. Our research study, which aims to close the gap between IoT technology and the protection of user security and privacy in the fascinating domain of smart homes, relies on a user-centric method. Figure 1 summarizes the research contributions and procedures.

The main contributions of this paper are summarized as follows:

1) The research study shows gaps in existing smart home security and recommends solutions to make data and privacy secure in smart homes.
2) The research provides valuable insights into the specific security and privacy concerns of smart home users, offering a deep understanding of their perspectives and anxiety.
3) The research provides smart home developers with realistic design principles for creating user-friendly interfaces and transparent data handling processes that fit with user preferences.
4) The research adds to legislative and regulatory discussions by providing insights into user concerns, potentially leading to the adoption of stronger industry standards for smart home security and privacy.
5) It enhances consumer awareness, ensuring they are well-informed about potential risks and advantages of smart home devices, allowing them to make better informed decisions.

The research study encourages collaboration among technologists, psychologists, sociologists, and legal professionals, bridging the gap between technological and human-centric issues in the smart home domain.

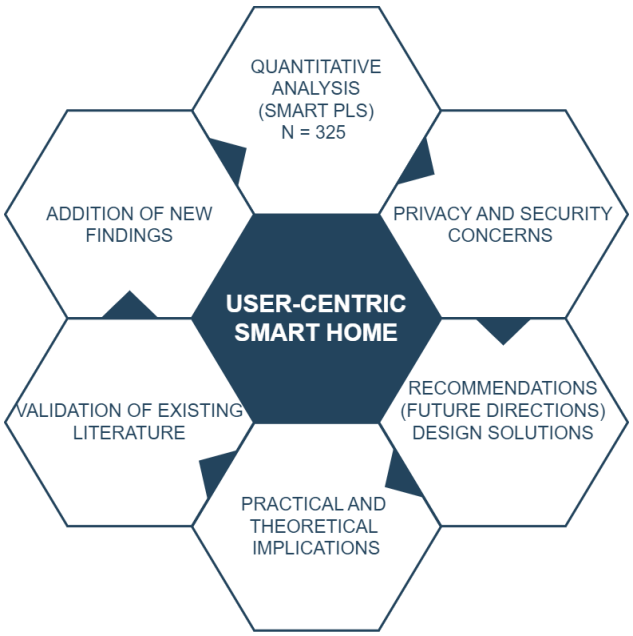

Figure 1. *Research Contribution and Procedure.*

The remainder of the research study has been structured as follows: In Section 2, we provide an overview of the related work in the field of smart IoT. Section 3 outlines the research

method, clarifying the approach employed to conduct the research study. Section 4 presents the research findings and analysing the collected data. Section 5 discusses the research findings and offers recommendations. Finally, in Section 6, we draw conclusions and highlight the significant practical and theoretical implications of the research study.

2. Related Works

2.1. Privacy and Security: Technology Acceptance Model

Adoption of IoT smart home devices is inextricably tied to consumers' views of security and privacy, and these factors are critical in the acceptance of the disruptive technology. To understand the delicate interactions between security, privacy, and user adoption in the context of the IoT smart home, current studies must be examined through the lens of the Technology Acceptance Model. Nanda Kumar et al. explore the paradox where users lock the doors to their physical homes but leave their computers vulnerable [4]. The study provides early insights into factors inhibiting home users' adoption of software firewalls, indicating the complex interplay between security practices and user behaviour. Sharma et al. delve into the adoption of IoT smart home services using a Value-Based Adoption Model, emphasising the importance of perceived value on Intention to use smart homes [5].

Heetae Yang et al. extend the theory of planned behaviour to investigate user acceptance of smart home services [6]. Their findings underscore the significance of perceived ease of use and perceived usefulness, which are intimately linked to security and privacy features. Furthermore, Islam analyse the adoption and diffusion of smart homes, shedding light on factors that influence users' decisions [7]. The study emphasises the role of perceived risk, aligning it with privacy concerns as a central determinant of adoption. Pascal Kowalczuk explores consumer acceptance of smart speakers, a component often integrated into IoT smart homes [8]. The study underscores the importance of user experience and usability, factors that closely intersect with the security and privacy features of these devices. Additionally, Kumar et al. present a provably secure and lightweight anonymous user-authenticated session key exchange scheme for IoT, addressing critical security concerns within the IoT ecosystem [9]. Furthermore, Pal et al. investigate prohibitive factors to the acceptance of IoT technology, particularly within a smart home context [10]. The study highlights the role of resistance to technology adoption and the need to address privacy and security-related concerns. It's evident that security and privacy concerns are intricately woven into users' acceptance of IoT smart home technologies. Perceived risks, usability, perceived value, and resistance to technology adoption all hinge on the security and privacy features embedded within smart home systems. Understanding and addressing these concerns will be pivotal in fostering greater user acceptance and facilitating the widespread adoption of IoT smart homes, therefore shaping the future of our living spaces.

2.2. Privacy and Security: Theory of Planned Behaviour

In the landscape of IoT smart homes, understanding the dynamics of user attitudes and behaviours regarding security and privacy concerns is essential. To address the research goals, the study examines current literature through the lens of the theory of planned behaviour (TPB), revealing insight on how users' beliefs, attitudes, and intentions shape their security and privacy decisions in IoT smart home contexts. Anupam Bairagi et al. set the stage by introducing an efficient steganographic approach for protecting communication in IoT critical infrastructures [11]. While not explicitly employing TPB, the study highlights the overarching need for covert communication and data protection, indirectly emphasizing the importance of user attitudes towards secure communication.

Heetae Yang et al. offer a pivotal contribution, extending TPB to investigate user acceptance of smart home services [6]. The study uncovers the role of user attitudes, perceived behavioural control, and subjective norms in shaping intentions to adopt smart home services. It underscores the significance of perceived usefulness and perceived ease of use, which are intrinsically linked to users' security and privacy considerations. Additionally, Yonghee Kim et al. explore the adoption of IoT smart home services using a Value-Based Adoption Model [12]. While not directly employing TPB, the study highlights the importance of user attitudes towards the perceived value of IoT services, closely intertwined with security and privacy aspects.

Piasecki et al. critically analyse the assumptions underpinning smart home cybersecurity standards, offering an intriguing perspective on how regulatory norms can influence user attitudes and behaviors regarding IoT security [13]. Their study indirectly touches upon TPB constructs by examining the impact of norms on user decision-making. Moreover, Robert Henry Thorburn et al. contextualize regulatory requirements with industry best practices to create an integrated privacy protection framework for IoT [14]. While not explicitly employing TPB, their study underscores the significance of norms and industry standards in shaping user attitudes towards privacy and security.

Brittany D. Davis et al. conduct vulnerability studies of IoT devices within smart homes, an area related to user security concerns [15]. Their work indirectly aligns with TPB by highlighting how user attitudes towards device vulnerabilities can influence their security behaviours. Lastly, Zeng et al. explore security aspects and architecture in IoT-based smart homes, emphasizing the importance of user attitudes towards device security [16]. Their study aligns with the

TPB framework by underscoring the significance of perceived control and security in shaping user intentions. The theory of planned behaviour serves as a valuable lens for understanding user attitudes and behaviours in the context of security and privacy concerns within IoT smart homes. These studies collectively emphasize the critical role of user beliefs, attitudes, and intentions, offering valuable insights into how user-centric approaches can enhance security and privacy in IoT smart homes.

2.3. Privacy and Security: Social Cognitive Theory

In the ever-evolving landscape of IoT smart homes, understanding user behaviours and decision-making processes regarding security and privacy concerns is paramount. The research study will examine existing literature through the lens of Bandura's social cognitive theory (SCT) [17], shedding light on how users' cognitive processes, observational learning, and self-regulation shape their security and privacy attitudes and actions in IoT smart home environments. Babu et al. provide insights into machine learning in IoT security, particularly the analysis of outage probability in cognitive networks [18]. While not explicitly employing SCT, the study touches upon user perceptions and decision-making in the context of IoT network reliability, aligning with SCT's emphasis on cognitive processes.

Celik et al. conducted program analysis of commodity IoT applications for security and privacy, offering a deep dive into the security aspects of IoT [19]. Their work indirectly aligns with SCT by addressing user perceptions and the role of observational learning in securing IoT applications. Ashok Kumar Yadav and Karan Singh undertake a comparative analysis of consensus algorithms and the integration of blockchain with IoT [20]. While not directly using SCT, their research indirectly contributes to understanding user perceptions and the cognitive processes involved in securing IoT through blockchain technology.

Hyunae Park et al. explore smart city risk factors and resistance, touching upon user resistance to smart city technologies [21]. Their study was tangentially related to SCT since it considers how people's cognitive processes and perceptions impact their resistance to smart city advances. Moreno Ambrosin et al. introduce a special issue on security and privacy for connected cyber-physical systems, addressing critical aspects of user perceptions and decision-making regarding security and privacy in IoT [22]. Their work aligns with SCT's focus on cognitive processes and self-regulation. Hassan et al. extend the UTAUT2 model with a privacy calculus model to enhance the adoption of health information applications, emphasizing the role of privacy perceptions in user decision-making [23]. The study directly aligns with SCT's emphasis on cognitive processes and self-regulation in the context of privacy concerns.

Aldren Gonzales et al. explore end users' perspectives on the quality and design of mHealth technologies during the COVID-19 pandemic [24]. While not explicitly employing SCT, the qualitative study provides insights into user perceptions and observational learning regarding mHealth technologies, particularly in times of crisis. Social Cognitive Theory offers a valuable framework for understanding user cognitive processes, observational learning, and self-regulation in the context of security and privacy concerns within IoT smart homes. These studies collectively emphasize the role of user beliefs, attitudes, and learning in shaping security and privacy behaviours, providing valuable insights into how user-centric approaches can enhance security and privacy in IoT smart homes.

2.4. Privacy and Security: Unified Theory of Acceptance and Use of Technology

In the dynamic landscape of IoT smart homes, understanding how users perceive and adopt technology, especially concerning security and privacy, is of paramount importance. This section explores the existing literature through the lens of the Unified Theory of Acceptance and Use of Technology (UTAUT), shedding light on how numerous factors influence users' intentions to adopt technology in the context of IoT smart homes, with a focus on security and privacy considerations. Mohamed Merhi et al. conduct a cross-cultural study on the intention to use mobile banking, extending UTAUT2 with security, privacy, and trust factors [25]. The study provides valuable insights into how security and privacy considerations, integral to UTAUT constructs, influence users' technology adoption decisions, bridging cultural differences.

Hanif Adinugroho Widyanto et al. extend UTAUT2 to encourage behavioural intentions to use mobile payment systems, highlighting the importance of trust and perceived security in users' technology adoption decisions, aligning with UTAUT principles [26]. Abul Khayer et al. explore the adoption of cloud computing in small and medium enterprises, shedding light on how factors such as perceived security and privacy influence technology adoption decisions [27]. Their work aligns with UTAUT by emphasizing the role of perceived ease of use and security concerns.

Odai Enaizan et al. examined electronic medical record systems' adoption, emphasizing security and privacy concerns using a multi-perspective analysis. Their research directly aligns with UTAUT constructs, emphasizing the significance of perceived security in healthcare technology adoption [28]. Lakshmi Sujatha Grandhi et al. propose a Security-UTAUT framework to evaluate key security determinants in smart city adoption, aligning with UTAUT principles by emphasizing the role of perceived security in influencing technology adoption within a smart city context [29]. Furthermore, I. Hassan et al. extend UTAUT2 with a privacy calculus model to enhance the adoption of health information applications, emphasizing the role of privacy concerns in users' technology adoption decisions [30]. Their study direct-

ly aligns with UTAUT constructs, emphasizing the importance of perceived privacy and security.

Nuno Nunes et al. model the adoption, security, and privacy of COVID-19 apps using UTAUT, shedding light on how perceived security and privacy influence users' intentions to adopt technology during a public health crisis [31]. Parastoo Amiri et al. conducted a qualitative study on factors influencing ePHR adoption by caregivers and care providers of Alzheimer's patients, extending the UTAUT model. Their research emphasizes the role of perceived security and privacy in healthcare technology adoption, aligning with UTAUT constructs [32]. The Unified Theory of Acceptance and Use of Technology (UTAUT) serves as a comprehensive framework for understanding user perceptions, intentions, and behaviours in the context of technology adoption, with a particular focus on security and privacy considerations. These studies collectively highlight the crucial role of perceived security and privacy in shaping technology adoption decisions within IoT smart homes. The table below summaries the constructs derived from the related work.

Table 1. *Constructs derived from related work.*

#	Theory	Constructs
1	UTAUT	Performance Expectancy, User Perceptions, Intentions, and Behaviours
2	SCT	User Beliefs, Attitudes, and Learning
3	TPB	Subjective Norms, User Beliefs, Attitudes, and Intentions
4	TAM	Perceived Risks, Usability, Perceived Value, and Resistance

The study technique was developed by combining theories obtained from related literature.

3. Research Methodology

In this research study, a quantitative research approach based on the positivist paradigm was used to provide an exploratory perspective into the area of IoT smart homes. An anonymous online questionnaire was used as the major data collecting instrument for the investigation. The questionnaire was distributed to a multinational company found on all continents. For the purpose of research and ethical considerations, the name of the multinational company will be denoted as ABC Multinational Company. The sample was chosen using a random purposive sampling strategy, which involved sending 325 online questionnaires to eligible study participants. The distribution of questionnaires spanned a period of 21 days.

The study engaged IT smart home consumers from around the world. Research participants were provided with clear information regarding the study's objective, which is to investigate security and privacy concerns in the adoption of IoT smart homes. Participation was entirely voluntary. No data was collected that should potentially identify any of the respondents. The anonymity was maintained throughout the research process to ensure the candidness of responses. The initial phase of the study involved an extensive literature review, which served as the fundamental step in identifying and comprehending the security and privacy concerns that are limiting the widespread adoption of IoT smart homes. By integrating existing knowledge and perspectives from the study domain.

The primary objective of the research study was to get an in-depth understanding of privacy and security concerns in the context of IoT smart home adoption. The research study selected upheld ethical norms, protected participant confidentiality, and employed rigorous quantitative analysis techniques to derive meaningful insights from the collected data. A precisely built 7-point Likert scale was developed to collect data and measure respondents' opinions and perceptions to effectively accomplish the study objective. The study model, which includes the key elements under research, is illustrated in the figure below. We used inferential statistical techniques to validate the research model and examine the relationships between each element, allowing the study to objectively verify the hypothesised framework.

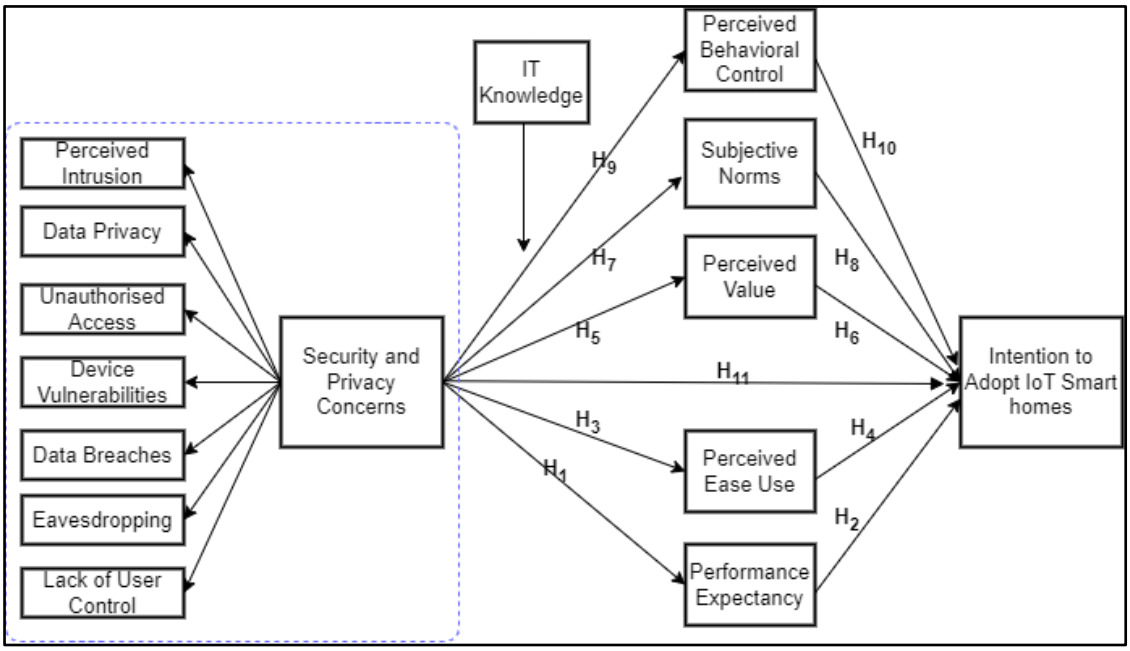

Figure 2. *Conceptual Framework for IoT smart homes adoption.*

Our suggested study model's major objective is to examine the complex interaction between security and privacy concerns and their influence on IoT smart home device adoption and utilisation. A thorough review of the current literature demonstrated an urgent need to employ a variety of technology adoption paradigms. The approach was critical since the adoption of developing Smart IoT Technologies cannot be explained properly by a single theory or model. As a result, the Technology Acceptance Model, the Theory of Planned Behaviour, the Social Cognitive Theory, and the Unified Theory of Acceptance and Use of Technology have all been thoroughly integrated into our suggested model. These frameworks collectively provide a comprehensive and holistic perspective to understand the factors influencing the adoption of IoT smart home technologies.

To provide a clear summary of the research hypotheses, the table below summarises the key propositions and correlations we seek to investigate in our study.

Table 2. *Proposed Research Hypothesis.*

	Proposed Hypothesis
H_1	Security and privacy concerns are negatively associated with performance expectancy of using IoT smart homes
H_2	Performance expectancy is positively associated with intention to adopt to IoT smart homes
H_3	Security and privacy concerns are negatively associated with perceived ease use of using IoT smart homes
H_4	Perceived ease use is positively associated with intention to adopt to IoT smart homes
H_5	Security and privacy concerns are negatively associated with perceived value of using IoT smart homes
H_6	Perceived value is positively associated with intention to adopt to IoT smart homes
H_7	Security and privacy concerns are negatively associated with subjective norms of using IoT smart homes
H_8	Subjective norms are positively associated with intention to adopt to IoT smart homes
H_9	Security and privacy concerns are negatively associated with perceived behavioural control of using IoT smart homes
H_{10}	Perceived behavioural control is positively associated with intention to adopt to IoT smart homes
H_{11}	Security and privacy concerns are negatively associated with intention to adopt to IoT smart homes

Moderating effect of IT knowledge

The significance of IT knowledge in shaping the adoption of IoT-based smart homes is crucial. Numerous scholars have underscored this critical component [33]. For instance, Jo et al. conducted a study focusing on the elderly's perceptions of an IoT-integrated smart home system [34]. Furthermore, Ronville et al. identified the moderating influence of IT skills in their study titled 'Influential Determinants of IoT Adoption in the United States Manufacturing Sector.' Their findings revealed that knowledge of IT had a key impact in influencing the adoption of IoT technology in the US manufacturing industry [35].

Building on previous research, the current study intends to investigate the moderating influence of IT knowledge in the adoption of IoT smart houses. We hypothesized that a large degree of IT knowledge, particularly in administering and monitoring IoT smart home devices, will greatly affect and perhaps accelerate the adoption of these technologies. The research study aims to give empirical data to support the theory and to contribute useful insights to the field of IoT adoption research.

4. Results

This section presents the findings of the research study and offers an in-depth analysis of the raw data obtained. Out of the 325 online questionnaires distributed, we received a total of 300 responses, resulting in 92% response rate. Out of the 325 responses, 25 questionnaires were incomplete and, therefore were discarded from the data analysis. The first section of the online questionnaire was dedicated to collecting demographic information from the respondents, and the ensuing research outcomes are presented in the table provided below. The questionnaire addresses user privacy and security issues in the context of IoT smart home adoption. To investigate empirical data, we used partial least squares structural equation modelling (PLS-SEM). SmartPLS/-Version (4.0.9.6) software was used for measurement validation and model testing.

4.1. Descriptive Statistics

The table 3 below, shows the respondents demographics data. The results show that 68% of the research respondents who participated in the study are male. This implies an unequal response rate between males and females. Therefore, there is a need to encourage more females to participate in IT adoption related research.

Table 3. *Descriptive Statistics.*

Variable	Category	Frequency	Percentage
Gender	Male	204	68
	Female	96	32
Age	<20	6	2
	21-35	99	33
	36-45	66	22
	46-55	111	37
	>56	18	6
Continent	Asia	75	25
	Africa	162	54
	Australia	24	8
	Europe	18	6
	North America	6	2
	South America	15	5
Education	Certificate	27	9
	Diploma	48	16
	Degree	162	54
	Masters	42	14
	PhD	15	5
	None	6	2
IT Experience	<1	15	5
	2-5	27	9
	6-9	108	36
	10-13	129	43
	>13	21	7

The research findings reveal a noteworthy trend among the participating respondents. The majority of the participants hold educational qualifications at the diploma level or higher. Furthermore, most respondents actively engaged in the research exhibit a noteworthy degree of IT expertise, surpassing a minimum threshold of 2 years. Considering these findings, we can assert that the majority of research participants demonstrate a strong understanding of IT knowledge and its associated domains. As a result, we may conclude that the combination of greater educational attainment and considerable IT experience indicates that the research participants have a solid foundation in IT knowledge. The foundation bears direct relevance to the study's central focus on IoT smart home adoption and the pertinent issues of security and privacy concerns.

4.2. Normality Check

The figure below for normality illustrates the results of the normality tests conducted to evaluate the distribution of measurement items before proceeding with the confirmatory analysis (CFA) model. These tests are crucial as the CFA

estimation method assumes data normality.

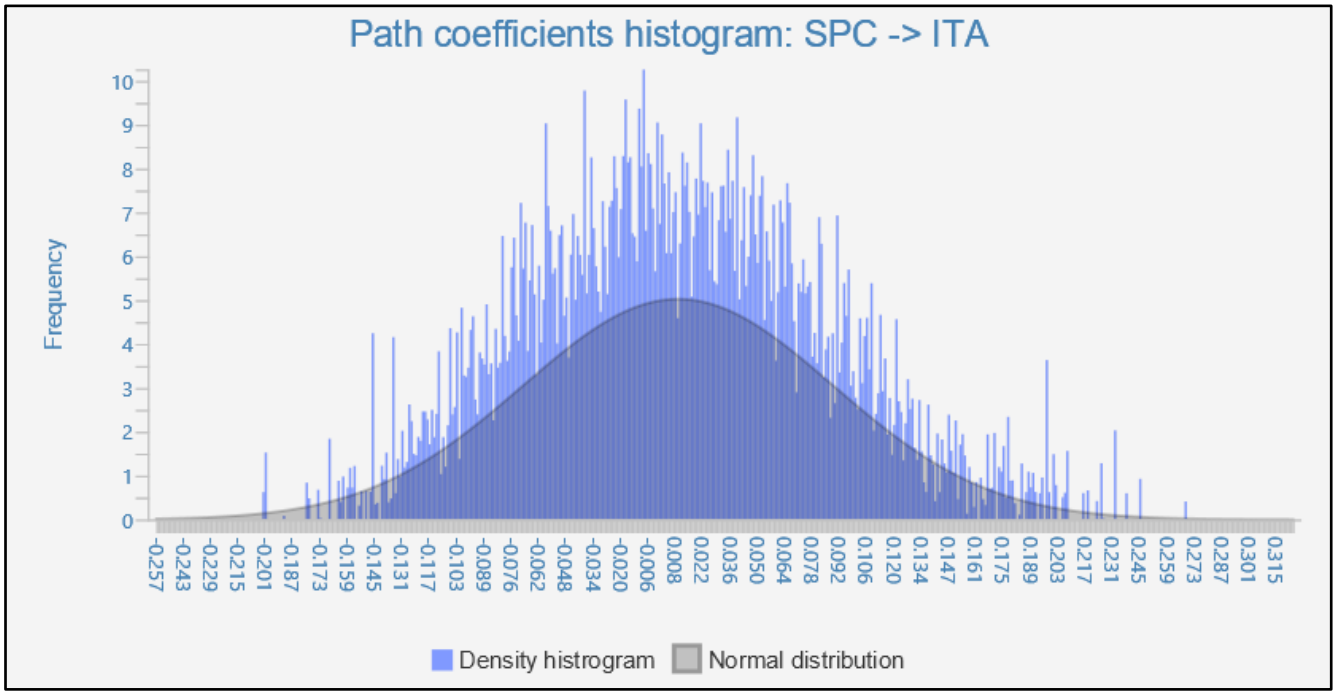

Figure 3. *Normality Test.*

The results of the normality tests demonstrate that both multivariate and univariate normality assumptions have been met. The (p-value ≥ 0.05) for the multivariate normality test fails to reject the null hypothesis of multivariate normality. Similarly, in the Shapiro-Wilk test, all measurement items exhibit p-values greater than or equal to 0.05, indicating that the null hypothesis of univariate normality is not rejected for any of the items.

These findings affirm that the data sufficiently follows a normal distribution, and as a result, you can proceed with the CFA model under the assumption of normality.

Reliability and Validity

An online self-reported questionnaire was used to collect the measurement item data. Every item was evaluated on a 7-likert scale, with 1 denoting strongly disagree and 7 denoting strongly agree. The 7-factor model's exploratory factor analysis was supported by confirmatory factor analysis. The outcomes of the confirmatory factor analysis model's standardised factor loadings demonstrate that the items statistically (p-value 0.001) indicate that they reflect the underlying latent concept. This attests to the measurement model's convergence validity.

Discriminant validity verifies if conceptions that shouldn't be connected to one another are in fact unrelated. Placing the squared correlations of all latent variables in a matrix and contrasting them with their average variance (AVE), as shown in the table 4 below, is one technique to verify this. The following equation is used to determine the AVE:

$AVE = \frac{\sum_{i=1}^{k} SF_i{}^2}{k}$ where SF_i is the standardised factor loadings of the measurement item i and k is the number of items in a factor.

Table 4. *Discriminant Validity Analysis.*

	PI	DP	UA	DV	DB	E	LUC	PBC	SN	PV	PEU	PE	ItA
PI	1.00												
DP	0.322	1.00											
UA	0.342	0.212	1.00										
DV	0.333	0.290	0.121	1.00									
DB	0.293	0.278	0.329	0.216	1.00								

	PI	DP	UA	DV	DB	E	LUC	PBC	SN	PV	PEU	PE	ItA
E	0.311	0.256	0.319	0.338	0.355	1.00							
LUC	0.278	0.276	0.148	0.119	0.307	0.342	1.00						
PBC	0.381	0.323	0.193	0.124	0.401	0.309	0.351	1.00					
SN	0.352	0.347	0.136	0.240	0.102	0.373	0.234	0.387	1.00				
PV	0.301	0.289	0.108	0.336	0.205	0.287	0.218	0.023	0.365	1.00			
PEU	0.111	0.231	0.183	0.247	0.303	0.247	0.260	0.089	0.098	0.345	1.00		
PE	0.290	0.222	0.122	0.179	0.103	0.212	0.311	0.067	0.078	0.067	0.311	1.00	
ItA	0.021	0.019	0.042	0.041	0.091	0.020	0.021	0.088	0.020	0.030	0.090	0.011	1.00
AVE	0.807	0.839	0.808	0.877	0.930	0.960	0.777	0.802	0.783	0.781	0.667	0.919	0.838

The table 5 below shows each factor's composite reliability (CR) and Cronbach's alpha. All factors' Cronbach's Alpha and CR values are higher than the suggested threshold point of 0.70. As a result, we can conclude that the measurement model's reliability has been established. Based on the following equation, CR was determined:

$CR = \frac{(\sum_{i=1}^{k} SF_i)^2}{(\sum_{i=1}^{k} SF_i)^2 + (\sum_{i=1}^{k} ME_i)}$, where ME_i is calculated by $\left(\sum 1 - {SF_i}^2\right)$.

Table 5. *Measurement Assessment and their Reliability.*

Constructs	Factor loadings	t-statistics	AVE (> 0.50)	Cronbach's Alpha (>0.70)	Composite Reliability (>0.70)
Perceived Intrusion (PI)	0.898	47.844	0.807	0.761	0.893
Data Privacy (DP)	0.808	50.067	0.839	0.808	0.912
Unauthorised Access (UA)	0.763	47.707	0.808	0.763	0.894
Device Vulnerabilities (DV)	0.860	63.232	0.877	0.860	0.934
Data Breaches (DB)	0.924	109.131	0.930	0.924	0.964
Eavesdropping (E)	0.958	178.682	0.960	0.958	0.980
Lack of User Control (LUC)	0.713	47.888	0.777	0.713	0.875
Perceived Behavioural Control (PBC)	0.753	41.790	0.802	0.753	0.890
Subjective Norms (SN)	0.722	45.470	0.783	0.722	0.878
Perceived Value (PV)	0.719	34.948	0.781	0.719	0.877
Perceived Ease Use (PEU)	0.747	34.038	0.667	0.747	0.857
Performance Expectancy (PE)	0.912	85.113	0.919	0.912	0.958
Intention to Adopt IoT (ItA)	0.806	54.870	0.838	0.806	0.912

The primary data has been analysed (Table 5) as part of a research study on the drivers of IoT (Internet of Things) adoption in smart homes.

Factor Loadings: Factor loadings have been evaluated as coefficients that measure the linear link between latent constructs and their observable indicators. All constructs in this dataset exhibit significantly high factor loadings, demonstrating a strong and clear relationship between the measured variables and their associated latent constructs.

t-Statistics: The t-statistics, which serve as an indicator of the statistical significance of the observed associations, have been computed. Across all constructs, t-statistics were found to be

extremely high, firmly proving the statistical significance of the identified determinants and their significant influence on the desire to embrace IoT technology in the field of smart homes.

Average Variance Extracted (AVE): AVE, which quantifies the fraction of variance in observable variables explained by underlying constructs relative to the variance attributable to measurement error, has been examined. All constructs in the research have AVE values greater than the suggested threshold of 0.50, indicating their robustness in explaining the observed variation in the empirical data.

Cronbach's Alpha: Cronbach's Alpha has been calculated to measure the internal consistency and dependability of a group of elements inside a construct. Cronbach's Alpha scores for all constructs in the sample above the stated criterion of 0.70, confirming their internal coherence and dependability.

Composite Reliability: Composite reliability has been found as an alternate measure of build dependability. It has been determined that all constructs in the dataset have composite reliability scores more than 0.70, demonstrating their robust dependability.

4.3. Structural Model and Hypothesis Testing

The proposed structural model was evaluated by examining the R^2 value. The results show that the R^2 value of the model (0.762). This suggests that approximately 76.2% of the reasons why people decide to use or not use IoT smart home devices, considering security and privacy, can be explained by the aforementioned model factors. The table 6 below shows the inferential hypotheses test results.

Table 6. *Hypotheses Test Results.*

#	T-statistics	P-Value	Result
H_1	47.844	0.000	Accepted
H_2	50.067	0.020	Accepted
H_3	47.707	0.000	Accepted
H_4	63.232	0.000	Accepted
H_5	109.131	0.001	Accepted
H_6	178.682	0.000	Accepted
H_7	47.888	0.000	Accepted
H_8	41.790	0.000	Accepted
H_9	45.470	0.000	Accepted
H_{10}	34.948	0.003	Accepted
H_{11}	34.038	0.000	Accepted

The study's findings show that the hypothesised structural model is definitely substantial. This implies that the hypothesised relationships and connections between numerous components are true and are not the result of chance. Security and privacy issues were found to have a negative relationship with performance anticipation, perceived ease of use, perceived value, subjective norms, and perceived behavioural control in the context of adopting IoT smart homes. Performance expectation, perceived ease of use, perceived value, subjective norms, and perceived behavioural control, on the other hand, all showed positive connections with the intention to adopt IoT smart homes. Furthermore, the study revealed that greater security and privacy concerns are associated with a lower overall intention to use IoT smart homes. These findings collectively emphasize the importance of addressing security and privacy issues to encourage the wider acceptance and adoption of IoT smart home technologies.

5. Discussion and Recommendations

The Internet of Things (IoT) has brought a new era of technological ease and connectedness into our lives. Smart homes with IoT capabilities have several advantages, ranging from increased energy efficiency to increased convenience. However, as the IoT ecosystem grows, it brings substantial security and privacy problems to the forefront. These considerations, along with the user-centric viewpoint, serve as the primary topic of this advanced research discussion. We will investigate the complex interplay between user-centricity, IT expertise, and the security and privacy concerns that motivate IoT adoption in smart homes.

IoT devices often do not have effective security measures, rendering them vulnerable to hackers and unauthorised access. The sheer number of linked gadgets expands the attack surface, leaving people susceptible. IoT devices capture massive volumes of data on users' behaviours and preferences. Mishandling of this data can result in major privacy violations and surveillance issues. The lack of consistent security and privacy standards across IoT devices and platforms exacerbates the problem. Users are left to negotiate a complicated network of options and preferences. Patching vulnerabilities requires frequent upgrades. However, many IoT devices do not receive timely upgrades, leaving them vulnerable to known risks.

Understanding the user-centric component is critical for understanding the dynamics of IoT adoption. The acceptance or rejection of IoT technology is heavily influenced by users' perceptions, attitudes, and behaviours. Users frequently express concerns about IoT devices invading their privacy. The study's findings, notably the high factor loading (0.898) for Perceived Intrusion, highlight the importance of this issue. Users' fears of IoT devices tracking their actions, conversations, or even physical areas might stymie adoption. The factor loading of 0.808 for data privacy indicates that people place a high value on the security of their personal information. Users are less likely to adopt IoT devices if they lack faith in its data protection procedures. The Unauthorised Access factor loading of 0.763 increases customers' fears

about unauthorised people having access to their IoT devices. The threat of cyber-attacks resulting in breaches of their home networks can be a significant deterrent. The device vulnerability factor loading of 0.860 emphasises the relevance of device security in consumers' decision-making processes. Advanced IT expertise users may be more aware of possible vulnerabilities, affecting their adoption decisions [36, 37].

Users' knowledge of IT is a critical factor of their perception and awareness of IoT security and privacy threats. Users with a greater degree of knowledge about IT are more likely to be aware of the possible security and privacy issues connected with IoT devices. They may be better qualified to identify the hazards and take preventative steps. IT manufacturers are able customise IoT devices for greater security. They are more likely to upgrade firmware, change default passwords, and use encryption. Understanding the complexities of data encryption and network security, IT customers are more likely to demand strict encryption measures from IoT makers. Users with IT knowledge are more likely to scrutinise privacy rules and terms of service. They may be more skeptical of data-sharing practises and choose gadgets and services that meet their privacy needs [38].

Security and privacy issues are essential in the ever-expanding ecosystem of IoT-enabled smart homes. The user-centric viewpoint, along with IT expertise, is critical in moulding users' attitudes and behaviours towards IoT adoption. This advanced research debate emphasises the importance of these aspects and their interactions, providing useful insights for both scholars and practitioners in the area. Addressing user-centric issues and improving security and privacy protections will be critical in encouraging widespread acceptance and confidence in smart home ecosystems as IoT technology evolves.

Recommendations

When building IoT devices for smart homes, manufacturers should prioritise user-centric design concepts. This includes user interfaces that are easy to use, clear privacy options, and simple security configurations. Initiatives should be launched to educate people about IoT security and privacy threats. Users may make educated judgements with the help of public awareness campaigns, detailed user manuals, and educational programmes. IoT device vendors must commit to offering regular firmware and software upgrades. Regular updates are required to address vulnerabilities and improve security. Privacy issues should be incorporated into the design of IoT devices. Data minimization, user permission, and transparent data management practises are examples of "privacy by design" ideas that should be incorporated into the product development process.

Recognising that not all users have significant IT expertise, producers should provide user-friendly materials as well as readily available customer assistance. This assistance can help less tech-savvy persons efficiently configure security and privacy settings. The industry should endeavour to standardise IoT device security and privacy practises. The implementation of certification programmes can assist consumers in identifying gadgets that fulfil stringent security and privacy criteria. IoT makers should be open about how their customers' data is gathered, saved, and shared. Users should be given with clear and straightforward privacy policies that clarify data usage and sharing practises. IoT devices should utilise strong encryption technologies for data transfer and storage in order to increase customer trust. Users should be confident that their information will be kept private and secure.

Providing users with more control over their IoT devices and data. This provides the possibility to quickly deactivate data collecting or withdraw rights. Manufacturers, politicians, and stakeholders in the sector should work together to develop best practises and rules for IoT security and privacy. A consistent and successful strategy may be achieved by a unified approach. Manufacturers should undertake privacy impact studies before introducing new IoT goods or services to detect possible dangers and adopt mitigation measures. Create a feedback system via which users may report security and privacy problems. Manufacturers should take customer input seriously and respond to concerns as soon as possible. Consider establishing security certification labels, similar to energy efficiency labels, which notify customers about the security level of IoT devices.

Integrating ethical issues into the design and implementation of IoT technologies. Respecting user permission and privacy choices, as well as avoiding invasive surveillance practises, are all part of this. Finally, these guidelines are critical for addressing security and privacy problems in the use of IoT technology in smart homes. The industry can build more confidence and encourage wider use of IoT devices while protecting users' security and privacy rights by concentrating on user-centricity, improving IT expertise, and adopting rigorous security and privacy measures.

6. Conclusion

The research study presented an in-depth examination of the complex interaction between security, privacy, user-centricity, and IT expertise in the context of IoT adoption in smart homes. The findings emphasise the critical relevance of addressing security and privacy concerns from a user-centric approach, while also considering customers' various degrees of IT understanding. The high factor loadings for constructs such as Perceived Intrusion, Data Privacy, Unauthorised Access, and Device Vulnerabilities underscore the importance of rigorous methods to build trust and confidence in users. The implications of these findings are far-reaching. IoT manufacturers should prioritize user-centric design, invest in user education and awareness, and commit to regular updates and transparent data handling practices. To maintain uniformity and efficacy in tackling security and privacy problems, industry collaboration and standardisation activi-

ties are crucial. Additionally, industry practises should be governed by ethical issues related to IoT usage.

It is crucial that the business community and lawmakers take note of the lessons from this research topic as IoT technology develops and becomes more integrated into our daily lives. We can clear the path for the responsible and safe deployment of IoT in smart homes by taking the suggested actions and embracing a user-centric and privacy-centric approach. This not only protects users' right to privacy but also fosters the development and use of this revolutionary technology. In the end, the user-centric analysis provided here acts as an essential benchmark for ongoing study and application in the ever-changing IoT adoption scenario.

6.1. Practical Implications

The study's research findings have significant practical consequences for various stakeholders, including IoT manufacturers, legislators, and consumers. These practical ramifications are critical in resolving the security and privacy problems that have arisen because of IoT adoption in smart homes. In building IoT devices for smart homes, manufacturers should prioritise user-centric design concepts. This includes user interfaces that are easy to use, clear privacy options, and simple security configurations. To ensure that gadgets correspond with users' requirements and preferences, user feedback should be actively solicited and incorporated into product development.

Manufacturers, business organisations, and government agencies should work together to develop educational efforts that enhance consumer knowledge of IoT security and privacy threats. User instructions and documentation should be thorough and easy to read, assisting users in properly securing their devices and protecting their privacy. IoT device manufacturers must commit to offering regular firmware and software upgrades. These upgrades should not only improve functionality but also resolve security issues as soon as possible. Consumers should be informed on the need of device updates and given clear instructions on how to do so. Manufacturers should incorporate privacy concerns into the design of IoT devices. Data reduction and user permission should be normal practise when implementing "privacy by design" concepts. Before introducing new products, privacy impact assessments should be performed to detect and minimise any threats to user data.

Manufacturers should provide accessible support and materials to help consumers, regardless of IT skills, in properly adjusting security and privacy settings. User interfaces should be developed to appeal to both novice and experienced users, while also making security and privacy options available to all. Stakeholders in the industry should collaborate to develop common security and privacy standards for IoT devices. Certification programmes can assist users in identifying items that satisfy these requirements. Policymakers can encourage and enforce compliance with these standards through regulations and incentives. Manufacturers should be transparent about how user data is collected, stored, and shared. Clear and concise privacy policies should be provided to users, explaining data usage and sharing practices in plain language. Communication channels for security incidents and breaches should be established, ensuring that users are promptly informed and advised on necessary actions.

Incorporating these practical consequences into corporate practises and standards might help alleviate security and privacy issues related with smart home IoT deployment. By concentrating on user-centricity, education, transparency, and ethical standards, stakeholders may establish a trusting environment, supporting responsible and safe IoT adoption for consumers.

6.2. Theoretical Implications

The research findings in this study have theoretical implications that contribute to the broader understanding of IoT adoption in smart homes, particularly in the context of security, privacy, user-centricity, and IT knowledge. These theoretical implications can inform future research in the field. The prominence of user-centric constructs, such as Perceived Intrusion, Data Privacy, and Unauthorized Access, underscores the central role of user perceptions and attitudes in IoT adoption. Future research should explore how these user-centric factors interact with technological factors to influence adoption decisions. The research highlights the influence of IT knowledge on users' security and privacy perceptions. Further theoretical exploration can delve into the cognitive processes that underlie this relationship, examining how IT knowledge shapes risk perceptions and decision-making in IoT adoption.

The theoretical framework introduced in this study emphasizes the importance of user empowerment and control in IoT adoption. Future research should investigate the psychological aspects of user control and autonomy, shedding light on how these factors influence users' willingness to adopt IoT technology. The concept of "privacy by design" has appeared as a key theoretical framework. Future research can delve into the practical implementation of these principles and their impact on user trust and adoption. This includes exploring the trade-offs between convenience and privacy in IoT design.

6.3. Limitations and Future Works

One limitation of this study is that the research findings may not be fully generalizable to all user populations and cultural contexts. The data used for this analysis might represent a specific demographic or region, and variations in user perceptions and behaviours should exist in different contexts. The data used in this study are cross-sectional, which limits

the ability to draw causal conclusions. Future research should benefit from longitudinal studies that track changes in user perceptions and behaviours over time. The research relies on self-reported data, which may be subject to response biases and social desirability biases. Future research should incorporate objective measures of IoT adoption behaviour and user knowledge.

IoT technology is rapidly evolving, and the security and privacy landscape is continually changing. This study did not capture the most recent developments and emerging security challenges. Future research should stay current with the evolving IoT ecosystem. The measurement of IT knowledge in this study might not capture the full spectrum of users' technological expertise. Future research should employ more comprehensive assessments of IT knowledge to explore its nuanced impact on IoT adoption.

Future research should employ longitudinal designs to track changes in user perceptions and behaviours over time. This approach can provide insights into the dynamic nature of IoT adoption and how it evolves as technology advances. Comparative studies across diverse cultural contexts can help uncover variations in IoT adoption patterns and the impact of user-centric factors. Understanding cultural influences is crucial for designing global IoT solutions. Investigating the dynamics of entire IoT ecosystems within smart homes can be a promising avenue for future research. This includes examining how interactions among various devices and services influence user perceptions and behaviours. While this study provides useful insights into the interaction between user-centric variables, IT knowledge, and IoT adoption, there is still plenty of potential for future research to expand on these results and meet the increasing problems and possibilities in the IoT ecosystem. Researchers may contribute to a more thorough knowledge of IoT adoption patterns by resolving these constraints and following these pathways for future work.

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] M. G. A. F. M. S. A. Chandradhara, "Design of IoT based Smart Home System," *Journal of University of Shanghai for Science and Technology,* vol. 23, pp. 249-261, 2021.

[2] R. A.-D. B. S. A. Al-Syouf, "Towards a Secure Web-Based Smart Homes," *Conference: 2021 12th International Conference on Information and Communication Systems (ICICS),* pp. 195-200, 2021.

[3] H. &. B. S. &. A. A. &. J. A. Mrabet, "A Survey of IoT Security Based on a Layered Architecture of Sensing and Data Analysis," *Sensors,* vol. 20, p. 3625, 2020.

[4] N. M. K. a. H. R. Kumar, "Locking the door but leaving the computer vulnerable: Factors inhibiting home users' adoption of software firewalls," *Decision support systems,* vol. 46, no 1, pp. 254-264, 2008.

[5] K. S. C. Sharma B. K, "Smart Homes adoption in India–Value-based Adoption Approach," *In 2021 IEEE International Conference on Technology Management, Operations and Decisions (ICTMOD),* no 9-10, pp. 1-6, 2021.

[6] L. H. Z. H. Yang H, "User acceptance of smart home services: an extension of the theory of planned behavior," *Industrial Management & Data Systems,* vol. 117, no 1, pp. 68-89, 2017.

[7] M. Islam, "An Assessment on the Smart Home Technology Adoption: Users' Perspective," 2018.

[8] P. Kowalczuk, "Consumer acceptance of smart speakers: a mixed methods approach," *Journal of Research in Interactive Marketing,* vol. 12, no 4, pp. 418-431, 2018.

[9] J. S. K. A. P. P. S. Kumar D, "An improved lightweight anonymous user authenticated session key exchange scheme for Internet of Things," *Journal of Ambient Intelligence and Humanized Computing,* pp. 1-17, 2020.

[10] Z. X. S. S. Pal D, "Prohibitive factors to the acceptance of Internet of Things (IoT) technology in society: A smart-home context using a resistive modelling approach," *Technology in Society,* vol. 66, p. 101683, 2021.

[11] K. R. I. R. Bairagi A K, "An efficient steganographic approach for protecting communication in the Internet of Things (IoT) critical infrastructures," *Information Security Journal: A Global Perspective,* vol. 25, no 4-6, pp. 197-212, 2016.

[12] P. Y. C. J. Kim Y, "A study on the adoption of IoT smart home service: using Value-based Adoption Model," *Total Quality Management & Business Excellence,* vol. 28, no 9-10, pp. 1149-1165, 2017.

[13] U. L. M. D. Piasecki S, "Defence against the dark artefacts: Smart home cybercrimes and cybersecurity standards," *Computer Law & Security Review,* vol. 42, p. 105542, 2021.

[14] A. M. F. P. Thorburn Robert, "Towards an integrated privacy protection framework for IoT: contextualising regulatory requirements with industry best practices," pp. 45-6, 2019.

[15] M. J. C. A. M. Davis B D, "Vulnerability studies and security postures of IoT devices: A smart home case study," *IEEE Internet of Things Journal,* vol. 7, no 10, pp. 10102-10110, 2020.

[16] M. S. R. F. Zeng E, "End user security and privacy concerns with smart homes," *In thirteenth symposium on usable privacy and security,* vol. SOUPS 2017, pp. 65-80, 2017.

[17] K. B. D. M. Devi B, "Application of Bandura's social cognitive theory in the technology enhanced, blended learning environment," *International Journal of Applied Research,* vol. 3, no 1, pp. 721-724, 2017.

[18] N. A. S. A. Babu R G, "Machine learning in IoT security performance analysis of outage probability of link selection for cognitive networks," *In 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC),* pp. 15-19, 2019.

[19] F. E. P. E. T. G. M. P. Celik Z B, "Program analysis of commodity IoT applications for security and privacy: Challenges and opportunities," *ACM Computing Surveys (CSUR),* vol. 52, no 4, pp. 1-30, 2019.

[20] S. K. Yadav A K, "Comparative analysis of consensus algorithms and issues in integration of blockchain with IoT," *In Smart Innovations in Communication and Computational Sciences: Proceedings of ICSICCS 2020,* pp. 25-46, 2021.

[21] Y. Y. L. H. Park H, "A Study on Smart City Risk Factors and Resistance," *Convergence Security Journal,* vol. 20, no 2, pp. 15-28, 2020.

[22] C. M. L. R. Y. C. M. Ambrosin M, "Introduction to the special issue on security and privacy for connected cyber-physical systems," *ACM Transactions on Cyber-Physical Systems,* vol. 5, no 1, pp. 1-2, 2020.

[23] I. M. M. E.-S. I. a. L. J. Bile Hassan, "Extending the UTAUT2 model with a privacy calculus model to enhance the adoption of a health information application in Malaysia," *In Informatics,* vol. 9, no 2, p. 31, 2022.

[24] C. R. L. M. C. L. M. A. Gonzales A, "End Users' Perspectives on the Quality and Design of mHealth Technologies During the COVID-19 Pandemic in the Philippines: Qualitative Study," *JMIR Formative Research,* vol. 7, no 1, p. e41838, 2023.

[25] H. K. T. A. Merhi M, "A cross-cultural study of the intention to use mobile banking between Lebanese and British consumers: Extending UTAUT2 with security, privacy and trust," *Technology in Society,* vol. 59, p. 101151, 2019.

[26] K. K. A. S. A. Widyanto H A, "Encouraging behavioral intention to use mobile payment: an extension of Utaut2," *Journal Muara Ilmu Ekonomi Dan Bisnis,* vol. 4, no 1, pp. 87-97, 2020.

[27] T. M. S. B. Y. H. M. N. Khayer A, "Cloud computing adoption and its impact on SMEs' performance for cloud supported operations: A dual-stage analytical approach," *Technology in Society,* vol. 60, p. 101225, 2020.

[28] E. B. A. M. A.-R. A. S. A. Enaizan O, "Effects of privacy and security on the acceptance and usage of EMR: the mediating role of trust on the basis of multiple perspectives," *Informatics in Medicine Unlocked,* vol. 21, p. 100450, 2020.

[29] G. S. W. S. Grandhi L. S, "A security-UTAUT framework for evaluating key security determinants in smart city adoption by the Australian city councils," *In 2021 21st ACIS International Winter Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD-Winter),* pp. 17-22, 2021.

[30] M. M. E.-S. I. L. J. Bile Hassan I, "Extending the UTAUT2 model with a privacy calculus model to enhance the adoption of a health information application in Malaysia," *In Informatics,* vol. 9, no 2, p. 31, 2022.

[31] A. G. R. M. R. G. B. R. G. E. T. P. N. V. Nunes N, "Modeling adoption, security, and privacy of COVID-19 apps: findings and recommendations from an empirical study using the unified theory of acceptance and use of technology," *MIR Human Factors,* vol. 9, no 3, p. e35434, 2022.

[32] P. H. B. K. B. M. K. P. N. Z. Amiri P, "A qualitative study of factors influencing ePHR adoption by caregivers and care providers of Alzheimer's patients: An extension of the unified theory of acceptance and use of technology model," *Health Science Reports,* vol. 6, no 7, p. e1394, 2023.

[33] N. S, "Factors driving the adoption of smart home technology: An empirical assessment," *Telematics and Informatics,* vol. 45, p. 101283, 2019.

[34] M. J. C. S. Jo T. H, "Elderly perception on the internet of things-based integrated smart-home system," *Sensors,* vol. 21, no 4, p. 1284, 2021.

[35] J. M. B. Ronville Savoury, "Exploring the Influential Determinants of IoT Adoption in the US Manufacturing Sector," *International Journal of Applied Management and Technology,* vol. 20, no 1, p. 11, 2021.

[36] S. N. M. M. Kayali M, "The Effect of Individual Factors Mediated by Trust and Moderated by IT Knowledge on Students' Adoption of Cloud Based E-Learning," *Int. J. Innov. Technol. Explor. Eng,* vol. 9, no 3, 2019.

[37] Statista, "Internet of things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions).," 2023. [Online]. Available: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/. [Använd September 2023].

[38] W. Y. T. E. I. a. L. A. Li, "Motivations, barriers and risks of smart home adoption: From systematic literature review to conceptual framework," *Energy Research & Social Science,* vol. 80, p. 102211, 2021.