AJSP
المجلة العربية للنشر العلمي
العدد واحد وأربعون
تاريخ الإصدار: 2 – آذار – 2022 م
www.ajsp.net
ISSN: 2663-5798

"Assessment of Consumers' Awareness of Cybersecurity threats in Smart Homes"

By Researchers:

Sumaya M. Alshahrani, Rasha J. Hilal

العدد واحد وأربعون
تاريخ الإصدار: 2 – آذار – 2022 م
www.ajsp.net
ISSN: 2663-5798

Abstract:

The widespread use the Internet of Things (IoT) in home environments has provide a lot of comfort and efficiency for smart home residents. Smart home devices and technologies from various manufacturers, which are rapidly proliferating, can lead to many cyber risks. That affect consumer privacy and safety. These risks make smart homes vulnerable to different types of security attacks. Thus, this study aims to assess the user's awareness of the threats to smart homes and how to deal with them. By applying the quantitative approach to measure security awareness for Saudi Arabia's smart home technologies consumers, And the extent to which consumer awareness affects the reduction of cyber threats. This study identified the level of consumer awareness about smart home technologies. In addition, Results showed the extent to which consumer concerns affect the spread of this technology. As well the research results represent a further step towards developing smart home environments with safe technologies.

Index Terms—Awareness, Cyber security, Internet of Things, Saudi Arabia, Smart **home.**

INTRODUCTION[1]

The Internet of Things (IoT) is a network of systems, machines, equipment and devices that interact with each other over the Internet, and they can be remotely monitored and controlled, usually through a smartphone. IoT is involved in many applications and services, for example in smart cities, smart cars and smart homes, to make the lives more productive and less stressful. The IoT is a model of broad developments in information and communication technology (ICT)[1]. Intelligent IoT-enabled applications such as smart grids and smart cities handle a substantial amount of personal and sensitive information, which is increasingly vulnerable to security threats [2]. According to a study from China, they developed an IoT acceptance model based on several factors. The results of the study supported the impact of perceived usefulness, ease of use, enjoyment, behavior control, and social influence in particular. In addition, the findings of another study concluded that IoT acceptance would be influenced by various contradictory factors, such as perceived privacy risks and individual preferences. Furthermore, regulations, security and disclosure of information were assumed to have a significant impact on adaptation [3]. There are usually a great number of objects involved in IoT networks. Thus, security and privacy protection mechanisms should have the ability to scale [2]. Smart home has been described as application of the concept IoT. New Smart Home services and devices spread at a fast pace, from various manufacturers which may have a limited experience of cyber security. Yet, it is often necessary to integrate these devices in the home Network in order to provide connectivity for data exchange and to perform their operations. Due to these interdependencies, many cyber threats appear with potential consequences for the lives of smart home users. Hence, it becomes important for end users to understand how to secure devices and services to counter these threats [4].

Sumaya M. Author is with the Dept. of IS, College of Computing and Information Technology, University of Bisha, Bisha, KSA (e-mail: 440804862@ub.edu.sa).
Rasha J. Author is with the Dept. of IS, College of Computing and Information Technology, University of Bisha, Bisha, KSA (e-mail: rashahilal@ub.edu.sa).

IoT nascent and the sensitive nature of smart home data call for effective yet scalable methodologies to discover and understand people's privacy norms concerning these devices [5].

Smart Home Architecture

Smart homes, as defined by Korea Association Smart Home (KASH), are living spaces where information technology is used for convenience, welfare, and safety of people in the residential environment [6]. The success of Smart Grid is heavily dependent on communication, V arious entities within this complex, heterogeneous network must be able to communicate efficiently and securely at all times with each other within the Smart Home [7]. There are many smart devices and sensors in the smart home, a remote device that accesses the smart home, and an access point (AP) that connects the smart home devices and the remote device as shown in Figure 1 [6]. There are different specifications for communication and power for smart home devices. Communication between smart home devices and their access points can occur directly, while devices unable to communicate by themselves communicate through another smart home device. As shown in Figure 1, smart home devices generally follow a hierarchical structure. An application layer is responsible for establishing communications in the smart home environment using messaging protocol suitable. Management of communication session is provided by the transport layer. Smart home environment rely on the network layer to provide proper communication between data. The link layer establishes the standards that allow physical communication between devices. The smart home appliance connected to the AP may be communicated with through the dedicated application installed on the remote device. However, smart devices use different standards based on the platform, and the user must install a separate app for each smart device when they add a new one [6]. As this communication relies heavily on information technology, concerns over privacy and security arise inevitably. Inherent vulnerabilities in communication and networking systems significantly affect Smart Grid security, with consequences often far worse than we are used to facing in traditional information systems [7]. Moreover, recent events demonstrate an increase in security threats, such as hackers gaining access to smart home devices or leaking information about their users [6]. A secure smart home environment needs to define security requirements. The research into security issues concerning smart homes and smart grids is still in its early stages [7].

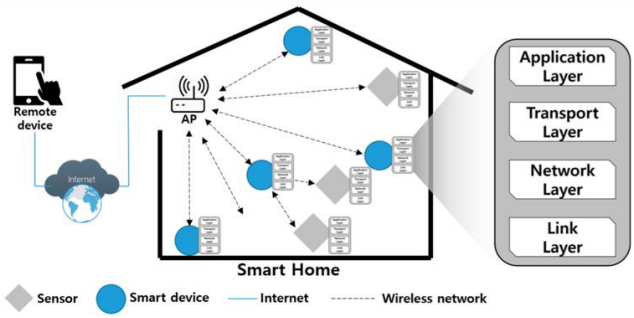

Fig 1. Smart home architecture

ISSN: 2663-5798

Related works

Technology has given insight into a technologically optimistic future where connected objects can utilize the Internet and work intelligently together from anywhere at any time. The IoT represents a network of connected devices with embedded sensors that are linked to a private or a public network as a result of the rapid proliferation of smart devices and high-speed networks. The IoT devices can perform the required functions remotely via the devices' control software. The data is then exchanged among the devices through a network using standard protocol-based communication. There is a wide range of smart connected devices or "things", each with a sensor chip, ranging from simple wearable accessories to large machines [8]. Nevertheless, the IoT is vulnerable to a variety of kinds of vulnerabilities and security threats, as with any communication network. In particular, security is a major challenge for the development of the IoT. Further, there is an enormous amount of data generated by multiple interconnections between objects or between users that is difficult to manage [2]. In today's connected world, home automation and IoT are becoming increasingly common in homes. Because of the saturation of smartphones on the market, smart homes have emerged as a new competitive market for information and communication technology (ICT) companies. There is a rush to develop smart home services/products from major players in the ICT ecosystem. For instance, Amazon's Alexa voice recognition technology provides consumers with access to their home appliances. The global penetration rate of smart homes is 7.5%, despite the launch of competing services/products. A chasm separates the early adopters and the mainstream market for smart homes. Although suppliers are actively offering smart home services, this gap means that smart homes must be analyzed from a consumer perspective. As a result, it is important to determine how to increase smart home demand by analyzing consumers' intentions to adopt smart home services and factors influencing the adoption rate (diffusion) of smart homes. [9]. Electronic sensors, lights, appliances, and locks allow users to control these devices via voice or any other user- defined device. Recent high-profile attacks, such as the Mirai DDoS attacks, also confirm that smart homes and the IoT are vulnerable. Security and privacy concerns have been raised about internet- connected devices in homes. A number of privacy concerns include the risk of leaking sensitive information about residents due to pairing and discovery protocols, insecure communication protocols leaking information to the internet, and vulnerabilities in the devices that could enable an attacker to spy on the residents remotely [10] . Many studies have dealt with the field of the Internet of things, and a few have focused on identifying risks on this area. The following section shed some light on literature about this subject:

- Bugeja et. al. presented some of privacy and security challenges in smart homes. the dynamic, and Internet-connected nature of the home environment adds new risks as private data becomes accessible, often without the householders’ awareness. Technological methods to mitigate security and privacy threats can be divided into device and communication level solutions. The requirement for empirical risk evaluation methods for use within smart connected homes have been identified as a critical security and privacy. requirement. The researchers suggested four major challenges that need to be addressed: identity management, security management methods, information flow control approaches, and risk assessment methods [11].
- Shuhaiber & Mashal proposed in their Study the use of the Technology Acceptance Model (TAM) for predicting and clarifying user behavior toward new technology acceptance and usage. In agreement with TAM postulates, the findings in the research found that trust is an important factor in people's intention to use smart homes. The more the people feel that smart homes are

trustworthy, controllable and eligible, the higher the intention to use them. In addition, sellers of smart homes should pay attention on how to cement consumer trust in smart homes [9].

- Mocrii et. al. presented review of major technologies of IoT-based smart homes. Researchers described IoT as moving from function to communication and making data- driven decisions, which means a device can become more useful if it is connected to other devices. The use of these devices which are usually connected to the Internet and, Spreading multitude of sensors around a house, Opens new opportunities for cyber- attacks on the security and privacy of smart home users. Software exploitation is a common threat that could be used by a cybercriminal on a smart home and its inhabitants. This type of attack is mostly due to the neglect of users who do not take necessary security measures ; for example letting the surveillance cameras operating with default credentials or neglecting software update. All stakeholders of smart home devices need to be actively involved, to prevent and mitigate threat issues. According to ENISA, the non-exhaustive list of stakeholders of a smart home ecosystem includes the vendors , the service and solution providers , the electronic communication providers , and the consumers. All of these parties play an critical role in ensuring that the smart home environment is safe and flexible against external attacks [12].
- Shin et. al. suggested analyzing factors affecting adoption and diffusion of smart homes. The technology acceptance model has been used to describe the adoption of smart homes and use of a multivariate probity model to describe the spread of smart homes. The results indicate that compatibility, perceived ease of use and perceived benefit have significant positive effects on the intention to purchase. Usefulness was an important factor affecting of the adoption the smart homes; thus, smart home operators should also take into consideration how smart homes can create a direct utility to consumers [13].
- Ali et.al applied in his study the operationally critical threat, asset, and vulnerability evaluation (OCTAVE) methodology to assess the various security risks of IoT-based smart homes. The risk assessment intended to identify the most severe potential dangers with identify degree of the risk. The highest risk score is relative to cyber or information assets such as user credentials , and user applications , and mobile personal data. Consider reliable user authentication methods such as biometrics and apply them to smart IoT-based homes. Biometrics can be used due to their accuracy and reliability, they provide a strong level of security for electronic and physical access in short processing time. Hardware manufacturers and application programmers should also provide devices with more security capabilities and applications with secure and easy-to-configure user interfaces. Government also has a significant role to play by providing legal support and security standards [14] .
- Manyika et al presented an analysis of more than 150 use cases to get a broader view of the potential benefits and challenges of the IoT and its impact on the global economy. the IoT has a total expected economic impact for 2025 of $3.9 trillion to $11.1 trillion. To achieve this kind of impact, technical and organizational obstacles must be overcome. In particular, companies that offer IoT technology will play a significant role in developing the systems and processes to maximize its value. Customers will capture most of the benefits that IoT applications generate. For example, the remote monitoring could create improving the health of chronic- disease patients. Consumer applications are likely to get the most attention and creating great value, such as fitness monitors and self- driving cars. The IoT can begin to reach its full possibility if

governments embrace the data-driven decision-making process [15].

- Park et.al explained in his study the security risks of smart homes that can cause information leakage from a hierarchical perspective of cyberspace. In addition, because these smart homes services based on IoT are closely related to human life, considering social damage is a problem. To overcome this, researchers suggested a framework to measure the risk of IoT devices based on security scenarios that can happen in a smart home. Hillary Clinton's e-mail leak, which occurred through the US presidential election in 2016, was also at home, a private space, and a threat to smart homes is at the starting point. This study offered an attack scenario on the assumption that sensor data was leaked during the vulnerability of smart home IoT equipment. FAIR method was used to risk measurement and risk grade classification and clustering method based on the scenario [16].
- Survey conducted by Li et. al have shown that IoT concept is important part of the Internet of the future. The IoT can be defined as access to and control of material things depending on different internet technologies. A critical necessity of an IoT is that the things in the network should be interconnected, for bridges the gap among the virtual and the physical worlds. There are many major challenges facing IoT technology such as technical challenges and challenges to security and privacy. Integrate IoT with the current ICT systems is still a challenge, Because IoT is influenced by all connected things to the ICT environment. The credibility of information and privacy protection of data are one of the main reasons for the social acceptance of IoT technologies and services. Some of the most prominent issues related to the security and privacy of the IoT: the definition of security and privacy from the social, legal and cultural perspectives, security of services and applications, the privacy of communication and user data, the communication security, and the trust mechanism [17].
- A study by Balta et. al. aims to explore social barriers to the dissemination of a smart home from the point of view of experts and consumers, and how these barriers can be addressed. Expert interviews indicated that these barriers relate to: the suitability of current lifestyles, security and privacy, technological complexity, trustworthiness, interoperability and standards. On the other side, consumer concerns have focused on: loss of control, cost, privacy and data security , and trust. Both experts and consumers agreed on some of the most practical social barriers (e.g. reliability and security). These social barriers should not prevent the development and spread of smart homes in society. A clear sense of the benefits of a smart home is one of the most important elements that contribute significantly to building consumer confidence. Therefore, the expected benefits of smart technology and how to achieve and deliver them must be mentioned, as well as explicitly demonstrated. Appropriate security standards and techniques should be developed to address data privacy concerns [18].

A great deal of previous research into The IoT has focused on How to develop smart homes to provide better quality of life. The literature has highlighted many of the benefits and services offered by smart homes. The academic literature has revealed also the emergence of several concerns on smart homes adoption such as difficulty using technology and security and privacy concerns.

methodology

This study was conducted using a quantitative approach. An important component of quantitative research is its structured environment, which often allows researchers to control variables,

environment, and research questions [19]. A quantitative study collects numeric data via standardized questionnaires or experiments, and determines relationships between variables and outcomes through analyses of those data [19]. The data were collected by using Google Forms. The survey asks users how they deal with security and privacy threats that might arise when using the smart home system. In addition to questions about smart devices, the survey asks how users deal with them. In conclusion, data analysis is performed by analyzing the results of the survey using SPSS.

A. Technology Acceptance Model

For the description of an individual's acceptance of information system services, the Technology Acceptance Model (TAM) is the most widely employed and influential theory , developed by Davis [20]. The TAM measures perceived usefulness, perceived ease of use to predict consumer acceptance intentions. The perceived usefulness of a system is the ability of the user to use the system to improve their performance, while perceived ease of use it refers to how easily users can operate the system [13]. According to Legris et al., TAM needs to be adapted for each technology analyzed, as consumers' goals for adopting ICT are different [21]. It is important to note that ease of use and perceived usefulness of an information system positively influence attitudes toward the system, and further positively influence individuals' intentions to use and accept the system. As well, perceived ease of use positively influences perceived usefulness, and both of these are affected by external variables [22].

B. Research model

For this study, awareness and privacy were added as external variables to analyze the users' attitudes towards smart home services. To find out how much awareness people have about security and privacy issues surrounding IoT devices. Learning about how smart devices connect and communicate with each other is certainly an important part of knowledge about smart homes. Also Concerns over security and privacy pose major barriers to implementing smart home technology [9]. In this study, awareness is presumed to be a significant factor in coping with threats to home security. As well, privacy concerns may serve as a deterrent to the adoption of smart home services. as shown in Fig. 2.

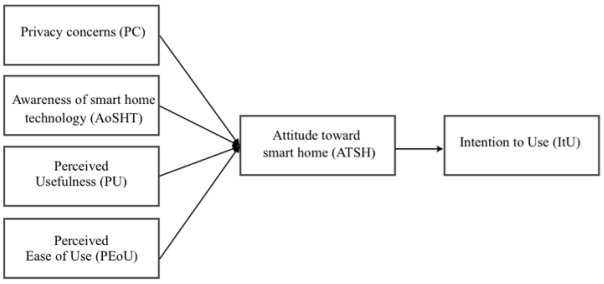

Fig. 2. Research model

ISSN: 2663-5798

C. Collect Data

Based on conceptualizations and developments from literature on smart homes, questionnaire questions were developed in this study according to TAM considering that concerns of privacy and awareness of smart home technology are external factors Measurement items were divided into six sections, each containing 21 paragraphs, as shown in Table 1. In answering questions, a Likert scale of five points was used (where 1 = 'strongly disagree' and 5 = 'strongly agree', and 3 representing ' Neither agree nor disagree'). The survey was created using Google Forms due to the fact that it is free and you are able to generate an unlimited number of questions. The survey included a simplified introduction that outlined the objectives and problem of the research, and assuring respondents that their data would only be used according to the scope of the search. Age and gender have been selected as demographic factors because previous research has shown that these variables affect people's relationship with technology. Gender plays an important role in the adoption of technology by individuals, and older people may have difficulty adopting new technology [23]. In addition to a question about the type of smart devices they own or have previously used.

TABLE I. MEASUREMENT ITEMS

Privacy concerns (PC)	When I use smart home devices, I'm concerned that my personal information may be used for other purposes.
	My concern is that smart home devices could give my personal information to other entities without my permission.
	I am concerned that smart home apps could track my mobile activity.
	The possibility of hackers hacking smart home systems and spying through surveillance cameras makes me less inclined to own them.
	I think smart home devices are at risk of having their security compromised and causing a privacy/data breach
Awareness of smart home technology (AoSHT)	My knowledge of smart home technologies is good.
	I am concerned about using smart home devices because I am not aware of how my data is collected and when.
	If I knew that businesses or organizations could collect data about my household habits and how I used smart home devices, I would not use them or own them
	I find it very important that I know how my personal information will be used.

ISSN: 2663-5798

	I'm more interested in the benefits and services offered by smart home systems than how it works.
	I am likely unaware of the risks associated with smart home devices, which may lead to cyber threats.
	Cyber threats can be reduced in the smart home environment through consumer education and awareness.
Perceived Usefulness (PU)	I am able to get things done more efficiently with the help of smart home devices.
	Using smart home technologies would enable me to accomplish home tasks more easily.
	Using smart home devices would improve the quality of my life.
Perceived Ease of Use (PEoU)	It would be easy for me to learn how to use smart homes devices.
	Controlling the smart home system will be easy for me.
Attitude toward smart home (ATSH)	My attitude toward smart homes is generally positive.
	I believe I would benefit from using smart home technologies.
Intention to Use (ItU)	I intend to continue using smart home devices
	It is likely that I will use smart home devices in the future.

ISSN: 2663-5798

D. Population and Sample

Sample for the study were chosen from consumers of smart devices in Saudi Arabia who are part of the broader study community. Consumers play a crucial role in improving and developing society. By the end of 2018, 71% of Saudi Arabia's Government Services were digitally mature, which is a significant improvement as compared to 58% in 2016 [24]. Creating a digital community that's vibrant, conscious, and engaged is one of the goals of Saudi Arabia's National Vision 2030.Social media platforms were used to distribute the survey questionnaire. Responses totaled 314. The sample consisted of 68 males and 246 females. It is generally accepted that a factor analysis should be conducted on 300 cases, or 50 cases per factor if it is more lenient [25] Based on their sample size guidelines, Comrey and Lee suggest that 50 is considered very poor, 100 poor, 200 fair, 300 good, 500 very good, and 1000 excellent [25].

result and discussions

At this point in the study, a research topic and question has been raised: Assessment of consumers' awareness of cybersecurity threats in smart homes. A questionnaire was designed to determine the extent to which smart home devices are used, and whether there is full awareness of the importance of securing such devices from exposure to cyber-attacks and the extent of fear of the idea of cyber-attacks. Below is a simple presentation of the most important results:

TABLE II. DEMOGRAPHIC CHARACTERISTICS

Demographic characteristics	Frequency	Percentage
Gender		
Male	68	22%
Female	246	78%
Age		
From 18 to 24	124	40%
From 25 to 34	72	23%
From 35 to 44	81	26%
From 45 to 54	29	9%
55 and over	8	3%

AJSP
المجلة العربية للنشر العلمي
العدد واحد وأربعون
تاريخ الإصدار: 2 – آذار – 2022 م
www.ajsp.net
ISSN: 2663-5798

Total	314	100%

As we can see from table (2) above, there is a difference between the percentage of male and female respondents to this questionnaire as the percentage of females (78%) is almost three times higher than the percentage of males (22%). And the largest percentage of respondents to this questionnaire are the youth were aged from 18 years to 24 years (40%), then who aged from 35 and 44 years (26%), and old people who aged more than 55 years have the lowest percentage (3%).

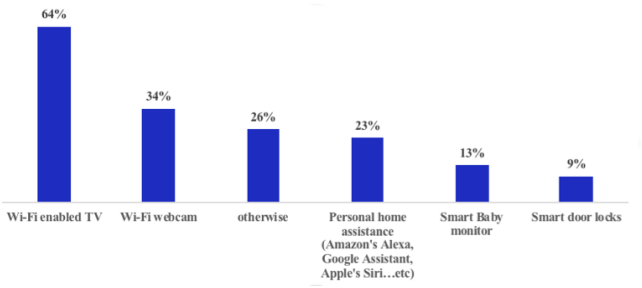

Fig. 3. mart devices owned or used by respondents

Figure (3) above shows the most used smart home devices by respondents, and as we can see that “Wi-Fi enabled TV” is the most used device, as there is about (64%) of respondents own or use this device. Then “Wi-Fi webcam” it is used or owned by almost (34%) of respondents. And “Smart door locks” is used by just (9%) of respondents. And there is about (23%) uses or owned other devices than these devices. With regard to privacy concerns we can see that the majority of respondents (58%) are agree that “When they use smart home devices, they are concerned that their personal information may be used for other purposes”, (59%) are agree that “smart home devices could give their personal information to other entities without their permission”, and about (63%) are agree that “smart home devices are at risk of having their security compromised and causing a privacy/data breach". From above results, we can easily say that in general, almost all respondents are agreeing that they have privacy concerns towards smart devices. About (70%) “see that their knowledge of smart home technologies is good”, (50%) “are aware of using smart home devices but have concerns because they are not aware of how they data is collected and when”, (91%) “find it is very important that they know how their personal information will be used”, and about (90%) see that “Cyber threats can be reduced in the smart home environment through consumer education and awareness". In general, we can say that most of respondents see that they should be aware of smart devices technology and how their data is collected and used and they also should know the risks associated with smart home devices to avoid any cyber threats. that almost all respondents are agree that using smart devices is very useful, as (80%) are agree that “they are able to get things done more efficiently with the help of smart home devices”, “Using smart home technologies would enable them to accomplish home tasks more easily”, and about (76%) see that “Using smart home devices would improve the quality of their life”. Majority of respondents are agreed that using smart devices is easy to learn, as (88%) are agree that “it is easy

for them to learn how to use smart homes devices", and about (80%) see that "Controlling the smart home system are easy for them". The majority of respondents (78%) are agreed that "they would benefit from using smart home technologies", and about (76%) are "feeling positive towards smart home". (77%) agree that "they intend to continue using smart home devices", and about (90%) see that "they will use smart home devices in the future".

Conclusion

Through this study we conclude that, there are statistically significant differences in respondents' opinion towards (privacy concerns – perceived usefulness – perceived ease of use – attitude toward smart home – intention to use) between males and females, as females have more privacy concerns, see that smart devices are very useful and easy to use, are more positive towards smart home technologies, and intend to use smart home devices in future than males. But there is no statistically significant difference between males and females in the awareness of smart home technologies, the level of awareness for both is almost the same. We can say there is no significant difference in any dimension between who aged more less than 45 years and more than 45 years, as respondents who aged between 18 to 44 years almost have the same privacy concerns, the same level of awareness of smart home technologies, see that smart devices are very useful and easy to use, are positive towards smart home technologies, and intend to use smart home as who aged 45 and over. In this study, we explored the level of consumer awareness of smart home technologies in Saudi Arabia. Also highlighted was the impact of privacy concerns on the adoption of smart home technology. According to the study, concerns about cyber threats in the smart home environment appear to affect consumer attitudes. The study also revealed that consumers want to gain a deeper understanding of smart home technologies. In light of these findings, it is advisable that smart home services providers take into account protecting personal information as well as different levels of awareness among various groups in society when publishing their services. Ensuring appropriate systems, services and support for customers should be a priority for smart home services providers. In order to make sure that vulnerabilities are fixed, It is imperative that vendors give their customers an easy and secure way to update their devices. Organizations such as the Saudi Federation for Cybersecurity, Programming & Drones (SAFCSP) and the Communications & Information Technology Commission (CITC) could increase consumer awareness by guiding and advising them about proper and safe practices in smart home environments. The findings from these studies suggest that consumer privacy protection can have an effect on adopt smart home technologies. The manufacturers of smart home devices and Internet service providers must protect consumers' private data in order to gain their trust. If they do, smart home technologies will be widely adopted. The issue of trust in the smart home system is an intriguing one which could be usefully explored in further research. Through understanding the extent to which confidence impacts the adoption of smart homes in the Kingdom of Saudi Arabia by adding confidence as an external variable in TAM. To conclude, I suggest repeating this study with a broader sample frame and using different research tools. This will enable us to determine the reasons that may hinder the adoption of smart home technologies.

REFERENCES

[1] Akil, M., Islami, L., Fischer-Hübner, S., Martucci, L. A., & Zuccato, A. (2020). Privacy-Preserving Identifiers for IoT: A Systematic Literature Review.IEEE Access,8, 168470-168485 J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.
[2] Grammatikis, P. I. R., Sarigiannidis, P. G., & Moscholios, I. D. (2019). Securing the Internet of Things: Challenges, threats and solutions. Internet of Things, 5, 41-70.
[3] Zhai, Y., Liu, Y., Yang, M., Long, F., & Virkki, J. (2014). A survey study of the usefulness and concerns about smart home applications from the human perspective. Open Journal of Social Sciences, 2(11), 119.
[4] Chong, I., Xiong, A., & Proctor, R. W. (2019). Human factors in the privacy and security of the internet of things. Ergonomics in Design, 27(3), 5-10.
[5] Apthorpe, N., Shvartzshnaider, Y., Mathur, A., Reisman, D., & Feamster, N. (2018). Discovering smart home internet of things privacy norms using contextual integrity. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 2(2), 1-23.
[6] Hong, N., Kim, M., Jun, M. S., & Kang, J. (2017). A Study on a JWT- Based User Authentication and API Assessment Scheme Using IMEI in a Smart Home Environment. Sustainability, 9(7), 1099.
[7] 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.
[8] Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. Future generation computer systems, 82, 395-411.
[9] Shuhaiber, A., & Mashal, I. (2019). Understanding users' acceptance of smart homes. Technology in Society, 58, 101110.
[10] Zeng, E., Mare, S., & Roesner, F. (2017). End user security and privacy concerns with smart homes. In thirteenth symposium on usable privacy and security ({SOUPS} 2017) (pp. 65-80).
[11] Bugeja, J., Jacobsson, A., & Davidsson, P. (2016, August). On privacy and security challenges in smart connected homes. In 2016 European Intelligence and Security Informatics Conference (EISIC) (pp. 172-175). IEEE.
[12] Mocrii, D., Chen, Y., & Musilek, P. (2018). IoT-based smart homes: A review of system architecture, software, communications, privacy and security. Internet of Things, 1, 81-98.
[13] Shin, J., Park, Y., & Lee, D. (2018). Who will be smart home users? An analysis of adoption and diffusion of smart homes. Technological Forecasting and Social Change, 134, 246-253.
[14] Ali, B., & Awad, A. I. (2018). Cyber and physical security vulnerability assessment for IoT-based smart homes. sensors, 18(3), 817.
[15] Manyika, J., Chui, M., Bisson, P., Woetzel, J., Dobbs, R., Bughin, J., & Aharon, D. (2015). Unlocking the Potential of the Internet of Things. McKinsey Global Institute.
[16] Park, M., Oh, H., & Lee, K. (2019). Security risk measurement for information leakage in IoT-based smart homes from a situational awareness perspective. Sensors, 19(9), 2148.
[17] Li, S., Da Xu, L., & Zhao, S. (2015). The internet of things: a survey. Information Systems Frontiers, 17(2), 243-259.
[18] Balta-Ozkan, N., Davidson, R., Bicket, M., & Whitmarsh, L. (2013). Social barriers to the adoption of smart homes. Energy Policy, 63, 363- 374.

[19] Rutberg, S., & Bouikidis, C. D. (2018). Focusing on the fundamentals: A simplistic differentiation between qualitative and quantitative research. Nephrology Nursing Journal, 45(2), 209-213.
[20] Lee, Y., Kozar, K. A., & Larsen, K. R. (2003). The technology acceptance model: Past, present, and future. Communications of the Association for information systems, 12(1), 50.
[21] Legris, P., Ingham, J., & Collerette, P. (2003). Why do people use information technology? A critical review of the technology acceptance model. Information & management, 40(3), 191-204.
[22] Chen, S. C., Shing-Han, L., & Chien-Yi, L. (2011). Recent related research in technology acceptance model: A literature review. Australian journal of business and management research, 1(9), 124.
[23] Cannizzaro, S., Procter, R., Ma, S., & Maple, C. (2020). Trust in the smart home: Findings from a nationally representative survey in the UK. Plos one, 15(5), e0231615.
[24] Muzafar, S., & Jhanjhi, N. Z. (2020). Success Stories of ICT Implementation in Saudi Arabia. In Employing Recent Technologies for Improved Digital Governance (pp. 151-163). IGI Global.
[25] VanVoorhis, C. W., & Morgan, B. L. (2007). Understanding power and rules of thumb for determining sample sizes. Tutorials in quantitative methods for psychology, 3(2), 43-50.
Sumaya M. Author is with the Dept. of IS, College of Computing and Information Technology, University of Bisha, Bisha, KSA (e-mail: 440804862@ub.edu.sa).
Rasha J. Author is with the Dept. of IS, College of Computing and Information Technology, University of Bisha, Bisha, KSA (e-mail: rashahilal@ub.edu.sa).