ISSN 1816-6075 (Print), 1818-0523 (Online)
Journal of System and Management Sciences
Vol. 12 (2022) No. 5, pp. 311-342
DOI:10.33168/JSMS.2022.0519

Modeling Factors Influencing Individual's Adoption of Intelligence Healthcare Services in Smart Cities

Abdullah Aslam Alzawamri[1+], Hairoladenan Kasim[2], Moamin Mahmoud[3]
[1] College of Graduate Studies, University Tenaga Nasional, Malaysia
[2] College of Computing and Informatics, University Tenaga Nasional, Malaysia
[3] Institute of Informatics and Computing in Energy, University Tenaga Nasional, Malaysia

abdullah.salim9999@gmail.com (corresponding author), hairol@uniten.edu.my, moamin@uniten.edu.my

Abstract. Experience across the globe has proven how interdependent we are as people and how the community's well-being and health shape our individual well-being and health. A growing number of countries are creating smart communities and cities with the primary aim of improving the quality of life of people by integrating a huge amount of health data. In terms of health service deliveries, a city is considered smart only when people enjoy smart healthcare deliveries implemented purposefully to improve quality of life. However, the success of smart city healthcare deliveries depends on the staff and patients' acceptance and usage. Unfortunately, there has been little to no study on factors influencing end-users adoption of smart city healthcare services from Omani perspectives. This paper fills the gaps by examining the variables that affect people's perceptions of information privacy and the adoption of smart city services in Oman's Diwan of Royal Courte. In addition, Three hundred and forty-one questionnaires were administered among government employees who had completed the digital foundations for public services program. For empirical analysis, Structural Equation Modeling (SEM) approach was used. The findings show that perceived security, perceived usefulness, perceived ease of use, social influence, trust, privacy risk, information sensitivity, cultural norm, privacy awareness, and privacy concern are significant factors affecting an individual's intentions to adopt and actual adoption of health care services in smart cities in Oman. The results further prove that privacy concerns moderate the intention and adoption of intelligence healthcare services in Oman's smart cities. Finally, this study advises stakeholders like the government and health workers' managers to establish better privacy measures to protect people's health information, provide secured health data to meet consumers' requirements, and provide adequate techniques when confidentiality is breached for online health care services to be adopted successfully in Oman.

Keywords: smart city, healthcare services, privacy, privacy concern, TAM, UTAUT, PCT, SEM, intelligence.

1. Introduction

In a smart city, an unprecedented quantity of raw data is collected and stored in various private or governmental company databases, including personal information about residents, traffic and pollution circumstances, and humidity. Advanced technologies may improve intelligence healthcare services, but they also pose a risk to the privacy of its users. Thus before implementing the smart city service fully, personal information and data must be well protected. Recent developments in wireless sensor networks (WSNs) and widespread Internet of Things (IoT) adoption (Nam & Choi, 2022) have given rise to the concept of "smart health." It is a context-sensitive healthcare approach susceptible to greater security and privacy issues involving personal data. For instance, many people may need to be regularly checked for contact tracing to obtain the COVID-19 status and present location of infected residents, which may be a privacy infringement (Ding, Conti, & Solanas, 2016).

The privacy and security of patient data in a healthcare application system are among the rising discontent for adopting intelligence healthcare equipment, such as medical sensors, mobile gadgets, and wireless gateway access. To gather physiological data, sensor nodes are placed inside patients' bodies. In addition, the medical staff can access a wireless portal with verified access to retrieve the patient's data. (Deebak et al., 2019). In a smart city with intelligence healthcare delivery, information about the location of patients is regularly sent and updated at the hospitals, and this data assist medical professionals in delivering intelligence healthcare services. Patients' personal information, including lifestyle choices, frequently visited locations, and personal interests can be compromised by location data and timestamps alone. Therefore, it is crucial to keep the patient's whereabouts a secret (Natgunanathan, Mehmood, Xiang, & Member, 2019).

Smartphone health apps are a further application of smart health. The increasing usage of smartphones for healthcare monitoring makes patient data privacy vulnerable. Patients exhibit skepticism regarding the protection of their data by third-party companies in both cloud and fog computing, where issues about the privacy of personal health data are more frequently raised. Regulations and procedures can be put in place to ensure privacy. Only authorized individuals can access a patient's health information, and privacy refers to the circumstances under which a patient's data may be accessed, used, and revealed to a third party (Hathaliya & Tanwar, 2020). In addition, we conducted a preliminary study in the Diwan of the Royal Court, especially the Diwan Health Complex, which provides treatment for employees of the Diwan of Royal Court and their families. Therefore, the researcher spoke with some of this complex's employees to collect information that the researcher may rely on in this research.

Among the most prominent topics discussed are the goals of the healthcare center in the incoming period and what suggestions are available to develop it and provide a healthy environment suitable for patients and employees. The most important points that the researcher drew are: that the complex's management has the physical ability to develop and provide all the requirements that will advance the health services in this complex, and they also have the intention to apply the technology to help them to do so, and to keep pace with the global technical development, especially the techniques of the fourth industrial revolution, and it is in line with Oman Vision Objectives 2040. In this way, they decided to introduce or use technology to improve their health services. Wearable devices were chosen as the smart solution, to be placed on patients or even employees to monitor their health conditions or those with chronic diseases. In light of the spread of Covid-19, these devices will help greatly reduce the spread of the virus. Still, there is an obstacle preventing the implementation of this project, which is concern about the privacy of information and data related to patients and employees, and fear of leakage or loss of this data that may be of great importance to patients.

Several studies have indicated the existence of some challenges in health care, especially in smart cities. The most important is the privacy of the patient's data and how they will be protected from unauthorized access. Most studies have established patients' ambivalence toward wearable devices due to privacy concerns. Therefore, the field of this study will explore health care in smart cities to highlight challenges of the privacy of patient data and the use of smart cities' services and analyze from the perspective of the participants in this study. This study assumes that there is a smart city service, which will be applied to Diwan health employees. Knowing that the top management in the said health complex intends to improve healthcare service deliveries and use smart solutions such as wearable devices for patients and employees working in the health complex. However, they are reluctant to implement this solution because staff and patients have concerns about the privacy of their personal and medical records.

The success of smart city healthcare deliveries depends on the staff and patients' acceptance and usage. However, there has been little to no study on factors influencing end-users adoption of smart city healthcare services from Omani perspectives. This paper intends to fill the gaps by examining the variables that affect people's perceptions of information privacy and the adoption of smart city services in Oman's Diwan of Royal Courte. Data is collected using the questionnaire, and this study's conceptual hypotheses are tested. This study utilized pertinent items from prior studies to gather the data required to investigate the effects of the hypothesized constructs. In the questionnaire, the Likert scale is used. It represents a group of options for the answer, which can be numeric or verbal. It is mostly used in closed-end questions.

2. Literature Review

The research model is built by an extensive review of existing literature and theories such as Perceptual Control Theory (PCT), the Unified Theory of Acceptance and Use of Technology (UTAUT) (Zhang et al., 2021), and the Technology Acceptance Model (TAM) (Elvis & Kim, 2022). The main aim of this section is to explore the relationship between variables associated with privacy and acceptance in a smart city. There are twelve variables in the proposed model and will be considered as below:

2.1. Perceived security and smart city services adoption

Rahman, Taghizadeh, Ramayah, & Alam, (2017) suggested that many people have strong security concerns while using new technology. Before adopting new technology, citizens require a high level of enhanced security. According to their findings, the study hypothesizes that users' intention to use and perceived ease of use of UST positively correlate with perceived security (Sepasgozar et al., 2019). Walczuch, Lemmink, & Streukens, (2007) discovered that information security is a key element in accepting new technology, while lower new technology acceptance is associated with perceived security. As a result, a perceived security issue is positively correlated with perceived usability and intent to adopt smart city services.

2.2. Perceived usefulness and smart city services adoption

Perceived usefulness is related to a user's belief that technologies will be needed for increasing daily performance tasks (Sepasgozar, Hawken, Sargolzaei, & Foroozanfa, 2019). The degree to which a person is persuaded that smart homes would improve their quality of life is influenced by perceived usefulness (Shuhaiber & Mashal, 2019). Consequently, there can be a connection between the intention to employ urban service technology and perceived utility (UST). According to Shuhaiber & Mashal's research in 2019, users' perceptions of the usefulness of smart homes have a favorable and significant impact on their intention to utilize the technology (Rahman et al., 2017; Schmidthuber et al., 2018).

2.3. Perceived ease of use and smart city services adoption

A user's belief that technology will be helpful in their daily chores is related to perceived ease of use (Kabbiri et al.,2018). The degree to which someone is persuaded that smart homes would improve their mental and physical well-being depends on how easy they perceive them to be (Shuhaiber and Mashal, 2019). People in the city might believe using and learning UST requires much work. Understanding government e-portals' embrace of other technologies depends on this (Schmidthuber et al., 2018).

2.4. Social influence and smart city services adoption

According to Gunawan & Smart (2019), Perceived social influence has little impact on a person's behavior, including their willingness to embrace smart city technology.

There may be a difference between societies from one country to another, so the researcher will assume social have a positive impact on the Intention to Adopt Smart City Services.

2.5. Trust and smart city services adoption

The association between trust and mindset toward smart houses is favorable and significant. The more faith someone has in smart homes, the better they feel about them. (Shuhaiber & Mashal, 2019). A person's internal perception of smart homes must be competent, manageable, and reliable to convey their faith in them (Luor, Lu, Yu, & Lu, 2015). As a result, trust greatly impacts people's intentions to use smart city services.

2.6. Privacy risk and smart city services adoption

Private concern has been proven to have a positive and considerable impact on private risk, according to Chellappa and Sin (2005). The degree of a person's worry for online privacy was also found to affect privacy risk in their model positively. Perceived risk positively influenced privacy concerns, as demonstrated by Xu et al. (2008) and Dinev & Hart (2004). Additionally, it was discovered that privacy risk (Xu, Michael, & Chen, 2013) significantly impacted privacy concerns.

2.7. Information sensitivity and smart city services adoption

Phelps et al. (2001) divided personal information into three categories: financial information about oneself, demographic data, and information about one's way of life and purchases. People are more sensitive to certain information, such as personal identification numbers, financial information, and medical information, than other types of information, such as lifestyle choices, purchasing patterns, and demographic data (Li, Wu, Gao, & Shi, 2016). Users are not necessarily willing to divulge more sensitive information online, according to Malhotra et al. (2004). However, people typically opt out of participating if it would require them to reveal more sensitive information. In addition, health information sensitivity has a considerable impact on users' privacy risk for healthcare wearable devices, according to research by Li H. et al. (2016). Consequently, there is a positive correlation between information sensitivity and privacy concerns.

2.8. Cultural norm and smart city services adoption

Milberg et al. (2000) found cultural norms as a key element in impacting users' privacy concerns, which indirectly affect the corporate management of a country's constitutional approach toward privacy protection. Furthermore, societal norms may be complicated concerning privacy concerns and e-commerce adoption of users within the community, which is affected by cultural values. (Mohammed & Tejay,2017). Therefore, there is a positive relationship between cultural norms and privacy concerns.

2.9. Privacy awareness and smart city services adoption

Privacy awareness shows the individual know-how about privacy policies and practices, information, and how to preserve his private space (Jiang, 2011). Dinev and Hart (2006) established that users with high social awareness would generally relate to privacy issues. Individuals' attitudes depend on the user's beliefs, so their privacy concerns will also depend on their privacy awareness. Privacy awareness gauge the level of personal knowledge about privacy violations and issues. Social networking services (SNS) providers and government administrators must ensure to protect individual privacy. It has been determined that a person's awareness has a significant role in determining the various levels of privacy concerns (Balapour, Nikkhah, & Sabherwal, 2020). Smith et al. (2011) also argue that citizens who know that some applications and websites may, without their knowledge, collect their information always have more concerns about privacy than users who are unaware of such dubious exercises. Privacy awareness reduces or raises the relationship strength between security and privacy concerns. For instance, individuals with a greater privacy awareness level think mobile apps possess lower security. This is because customers may have read or heard more about instances of illegal user information disclosure and are aware that such occurrences usually involve unsecured mobile apps (Balapour et al., 2020). As a result, the study assumes that privacy knowledge and concern are significantly related.

2.10. Privacy concerns and trust and smart city services adoption

According to Wottrich, van Reijmersdal, and Smit's (2018) research, users of mobile applications in Western Europe have privacy concerns, which negatively affect their intentions to agree to application permissions to access their personal data information. Consumer behavior and behavior towards the intention to use the service may be a negative impact due to privacy concerns, so it should be mitigated privacy concerns by the service provider (G.R. Milne & M. Boza,1999, J. Phelps et al.,2001). Studies on Internet usage have also shown that privacy concerns affect users' intentions to use the internet (T. Dinev & P. Hart, 2005). According to Dhagarra, Goswami, and Kumar (2020), researchers must comprehend the worries about consumer data and information privacy, which act as a barrier to accepting the use of health care technologies. Kim (2008) studied the effects of privacy and security at the collective and individual levels on e-vendors trust-related issues. The study found that privacy affects trust negatively. The low levels of trust among users affected a significant negative in the transactions and commercial and social activities via the Internet due to privacy concerns that led to losses in business between companies and users (Xu et al., 2013). Therefore, the hypotheses will be as follows:

2.11. Intention to adopt Smart City Services and Actual Smart City Services Adoption

Although many previous behavioral pieces of literature primarily employ the intention to adopt as a proxy for behavior (Y. Li, 2014; T. Wang et al., 2014), other studies have argued that behavioral intention is not a sufficient determinant of behavior in some specific contexts. However, users in the healthcare wearable device study (T. Dinev et al., 2013) are more observant of their healthcare problems and more motivated to accept developing technologies to optimize their health. Li et al. (2016)'s research has thus confirmed that the adoption intention is strongly and favorably associated with the adoption itself. Thus, these studies indicate a favorable correlation between the intention to adopt smart city services and the actual acceptance of these services.

3. Methodology

3.1. Research model and hypothesis

The factors affecting smart city service adoption are as diverse as findings from previous literature. This research empirically investigated the relationship among the factors of perceived security, perceived usefulness, perceived ease of use, social influence, trust, privacy risk, information sensitivity, cultural norm, privacy awareness, privacy concerns, and intention to adopt smart city services. Based on the previous literature and theories, the research model is developed as shown in fig. 1

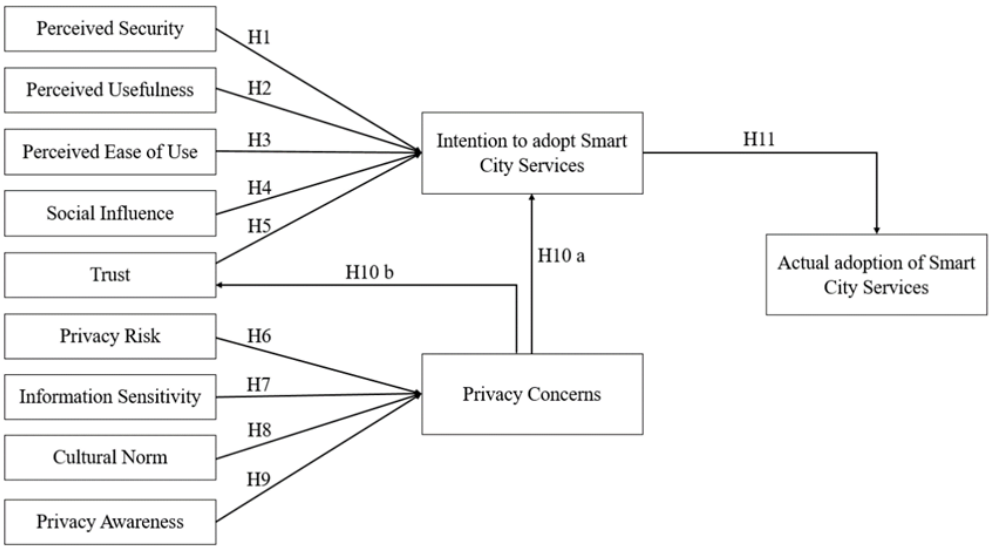

Fig. 1: Research model.

This paper set twelve hypotheses based on the review in section 2 between independent variables and actual adoption of smart city services. The following 12 hypotheses are as follows;

H1: Perceived security positively affects Intention to Adopt Smart City Services.

H2: Perceived usefulness has a positive and significant impact on Intention to Adopt Smart City Services

H3: Perceived ease of use positively and significantly impacts Intention to Adopt Smart City Services.

H4: Social influence positively impacts Intention to Adopt Smart City Services.

H5: Trust has a significant positive impact on the Intention to Adopt Smart City Services.

H6: Privacy risk has a positive influence on privacy concern

H7: Information sensitivity positively affects the level of privacy concern.

H8: Cultural Norm have a positive influence on privacy concerns.

H9: Privacy awareness positively affects the level of privacy concern.

H10a: Privacy concerns have a negative impact on Intention to Adopt Smart City Services.

H10b: Privacy concerns have a negative impact on trust.

H11: Intention to adopt Smart City Services significantly positively impacts actual adoption of Smart City Services.

3.2. Measurement instruments of variables

The research instrument will be designed in the English language. Although there more than one language in Oman, its official is Arabic. To include persons who might not be able to speak English in the study, it is crucial to make sure the instrument is available in both Arabic and English. The instrument will be translated carefully into Arabic without altering its conceptual meaning in this case. The development will pass through four main steps. The first step is selecting instrument items, followed by the validation of the instruments. Then a group of academic experts will check the validity and receive comments from them. The fourth step is measuring the reliability of the instrument by carrying out a pilot study. The measurement instruments consist of eleven variables which are shown in Table 1.

Table 1: Measurement instruments of variables.

	Questions	Factor To Test	Adapted From
	I would feel secure using Healthcare Services in Smart Cities (HSSC) if it had enough security.	Perceived Security	Balapour et al.(2020); Sepasgozar et al. (2019)
	I would have the confidence that legal and technological mechanisms are appropriately protecting me from online hackers.		
	I believe that HSSC operators would assume full liability for any form of transactional security lapse.		
	When using HSSC, I'd feel secure in the security of my transaction.		
	Using HSSC would allow me to finish work much more quickly.	Perceived Usefulness	(Shuhaiber & Mashal, 2019); (Sepasgozar et al., 2019)Sepasgozar et al. (2019)
	My life would be better if I use HSSC.		
	HSSC would be a useful tool for communicating with businesses and government organizations.		
	I would have more control with HSSC.		
	Overall, I think utilizing HSSC is advantageous.		
	I believe I would have no trouble learning how to use HSSC.	Perceived Ease of Use	(Shuhaiber & Mashal, 2019); (Sepasgozar et al., 2019)Sepasgozar et al. (2019)
	I believe HSSC would be simple to use.		
	I believe my dealings with the HSSC would be easy to comprehend.		
	I believe I could easily persuade the HSSC to perform the task I need.		
	People who have the power to affect my behavior believe I should utilize HSSC.	Social Influence	(Venkatesh et al., 2003).
	My essential friends and family believe that I should use the HSSC.		
	Senior management in the company would promote the usage of HSSC.		
	Many employees in my firm believe that HSSC is crucial.		
	I feel HSSC would be trustworthy	Trust	(Shuhaiber & Mashal, 2019); (Xu et al., 2013)
	I feel HSSC would be reliable		
	I feel HSSC would be controllable		
	I have faith that HSSC will not utilize my personal information unlawfully.		
	Regarding HSSC, there could be many privacy concerns.	Privacy Risk	(Xu et al., 2013); (Fortes & Rita, 2016)
	HSSC could fraudulently use personal information		

	Using HSSC with my personal data would result in many unforeseen problems.		
	In general, providing personal information to HSSC would be dangerous.		
	I think HSSC would request personal information that is very sensitive	Information Sensitivity	(Li et al., 2016); (Xu et al., 2013)
	I would feel uncomfortable with the type of HSSC information that is required from me		
	I believe that HSSC would learn more sensitive information about me.		
	When utilizing HSSC, the health information I supply will be of the utmost importance to me.		
	People who have the power to affect my decisions could believe that maintaining personal information is crucial.	Cultural Norm	(Xu et al., 2013) Adapt from related work
	My colleagues might think I should be cautious about maintaining my privacy.		
	People who matter to me advise me to use caution when disclosing personal information.		
	My neighborhood might think that I should be cautious about protecting my privacy.		
	Companies collecting personal data online should be transparent about how it will be handled, processed, and used.	Privacy Awareness	(Balapour et al., 2020)
	Very clear disclosure of HSSC's privacy practices is required.		
	Knowing how my personal information will be used is crucial to me.		
	I believe it is crucial that I understand how my personal data will be handled.		
	I am concerned that HSSC will gather excessive amounts of personal data about me.	Privacy Concerns	(Fortes & Rita, 2016);(Pentina, Zhang, Bata, & Chen, 2016); (Xu et al., 2013)
	I am worried that HSSC may hold my confidential information improperly.		
	I am anxious that illegal individuals might have access to my personal data.		
	I am afraid that my personal data will be utilized for purposes other than healthcare.		

	I am concerned that an authorized person would find my private information in HSSC		
	Overall, I am concerned about submitting my personal information to HSSC		
	I intend to use HSSC	Intention to adopt Smart City Services	(Shuhaiber & Mashal, 2019); (Sepasgozar et al., 2019)
	I am willing to use HSSC in the near future		
	I would recommend HSSC to others		
	I would use HSSC	Actual adoption of Smart City Services	(Li et al., 2016)
	I would use HSSC as the platform to create a healthy living		
	I would often use HSSC to get health information		

3.3. Reliability measurement of variables

The researcher will also conduct a pilot study before publishing the final questionnaire and collecting data to ensure that the questionnaire is free of errors and its clarity, understanding, and accuracy. The questionnaire will be published to a small sample of employees, whose number may range from 20 to 30, then ensure their feedback. If any, after confirming the accuracy of the questionnaire, the questionnaire will be distributed to the entire sample. The researcher distributed the questionnaire to a group of approximately 35 employees. Thirty-one out of them filled out the questionnaire. The data was analyzed to prove the reliability of all variables using Cronbach's Alpha, and the result for each variable should be more than 0.7. Table 2 shows the variables, numbers of items, and Cronbach's Alpha results. Reliability analysis is implemented for evaluating the internal consistency of items by using the most widely used method called Cronbach's Alpha.

Table 2: Reliability measurement of variables.

Variables	No. Items	Cronbach's Alpha
Perceived Security	4	0.796
Perceived Usefulness	5	0.766
Perceived Ease of Use	4	0.812
Social Influence	4	0.770
Trust	4	0.766
Privacy Risk	4	0.771
Information Sensitivity	4	0.715
Cultural Norm	4	0.846
Privacy Awareness	4	0.718
Privacy concerns	6	0.887
Intention to adopt Smart City Services	3	0.917
Actual adoption of Smart City Services	3	0.887

4. Data Analysis

As explained earlier in chapter three, the major measures were built on existing instruments. The latent version of the research variables measurement items and the summary version of the research variables measurement items are presented in Table 3.

Table 3. List of Constructs and Measurement Indicators

S/N	First Order Construct	Number of Indicators (49)
1	Perceived Security (PS)	4
2	Perceived Usefulness (PU)	5
3	Perceived Ease of Use (PEU)	4
4	Social Influence (SI)	4
5	Trust	4
6	Privacy Risk (PR)	4
7	Information Sensitivity (IS)	4
8	Cultural Norm (CN)	4
9	Privacy Awareness(PA)	4
10	Privacy Concern (PC)	6
11	Intention to adopt (ITASCS)	3
12	Actual adoption of Smart City Services (AAOSCS)	3

The study further checked the data set for extreme values. According to (Tabachnick & Fidell, 2007), outliers are unreasonable observations with extreme values in one variable or a combination of distinct variables from the rest of the data. For this research, the study employed a univariate method of the standardized score of each variable. A variable becomes an outlier if the z score is between -4.0 and +4.0 or beyond (Hair et al. 2006).

Table 4. Result of univariate outlier based on standardized values.

S/N	Construct	Indicators	Standardized Value z score	
			Lower Bound	Upper Bound
1	Perceived Security (PS)	PS1	-2.37865	1.69278
		PS2	-3.14637	1.32669
		PS3	-2.90807	1.32323
		PS4	-3.02562	1.30334
2	Perceived Usefulness	PU1	-2.31684	1.47065
		PU2*	-4.97571	1.13981
		PU3	-4.29889	1.1653
		PU4*	-4.81686	1.27794
		PU5	-2.16083	1.44048
3	Perceived Ease of Use	PEU1	-3.89149	1.27044

		PEU2	-3.24647	1.36694
		PEU3	-2.73679	1.36105
		PEU4*	-4.09799	1.4522
4	Social Influence	SI1*	-4.26738	1.57605
		SI2	-2.79642	1.89652
		SI3	-3.07871	1.70658
		SI4	-3.23807	1.46113
5	Trust	Trust1	-3.4244	1.59086
		Trust2	-3.8473	1.4209
		Trust3	-2.50319	1.48761
		Trust4	-3.40322	1.55499
6	Privacy Risk	PR1	-2.75717	1.38973
		PR2	-2.59577	1.48434
		PR3	-1.92019	1.69353
		PR4	-2.2514	1.81423
7	Information Sensitivity	IS1	-1.85879	1.85214
		IS2	-1.99603	1.77312
		IS3	-1.88601	1.93393
		IS4	-2.24499	1.56842
8	Cultural Norm	CN1	-2.07853	1.6329
		CN2	-2.09785	1.55267
		CN3	-3.54937	1.27535
		CN4	-3.4248	1.28219
9	Privacy Awareness	PA1*	-4.14725	1.27869
		PA2	-3.25415	0.91535
		PA3	-3.71857	0.82514
		PA4*	-4.09123	0.70479
10	Privacy Concern	PC1	-3.8297	0.67868
		PC2	-2.07482	1.56019
		PC3	-1.99145	1.53626
		PC4	-2.30709	1.23447
		PC5	-2.22768	1.20614
		PC6	-2.16831	1.26408
11	Intention to Adopt Smart City Services	ITASCS1	-1.9086	1.45632
		ITASCS2	-3.79549	1.47944
		ITASCS3*	-4.16242	1.5654
12	Actual Adoption of Smart City Services	AAOSCS1	-3.70964	1.46531
		AAOSCS2*	-4.19635	1.52874
		AAOSCS3	-2.40977	1.42116

***** *indicate outliers scores.*

From Table 4. above, the results of the lower and upper bound of the standardized z score show that only eight items out of 49 indicators exhibit a score less than -4 at the lower bound. The eight items include the perceived usefulness 2, 3, and 4 items

(PU2, PU3 & PU4) with lower extreme bound scores of -4.97551, -4.22889, and -4.81686, respectively. In addition, under perceived ease of use indicators, only item 4 (PEU4) shows an extremely lower bound score of -4.09799.

The result also shows that an extreme indicator under social influence constructs a score of -4.26738. Moreover, under the perceived awareness indicators, two outliers cases were established for perceived awareness 1 and 2 with lower bound scores -4.14725 and -4.09123. In addition, under the Intention to Adopt Smart City Services construct, the third item shows an outlier score of -4.16242 at the lower bound. The last outlier is item two under Actual adoption of smart city services (AAOSCS 2) with an extreme value of -4.19625. All eight items were subsequently removed to ensure the data sets' accuracy.

The skewness and kurtosis of distribution values were also employed in this study to evaluate the normalcy of the data sets. An indication of a distribution's symmetry is its skewness, and in comparison to a normal distribution, how peaked distribution is near its mode is indicated by its kurtosis. Skewness and kurtosis both demonstrate how far from normal a distribution deviates. It is acceptable to have skewness or kurtosis values in the +2.0 to -2.0 range, according to Hair et al. (2006). Table 5 presents the results of the Normality Test.

Table 5: Assessment of normality of all items.

	N	Skewness		Kurtosis	
	Statistic	Statistic	Std. Error	Statistic	Std. Error
PS1	279	.543	.146	.968	.291
PS2	279	-.901	.146	.857	.291
PS3	279	-.689	.146	-.060	.291
PS4	279	-.713	.146	.004	.291
PU1	279	-.660	.146	.307	.291
PU2*	279	-.937	.146	2.657	.291
PU3*	279	-.956	.146	2.093	.291
PU4*	279	-.950	.146	3.385	.291
PU5	279	-.615	.146	1.069	.291
PEU1	279	-.437	.146	1.282	.291
PEU2	279	-.587	.146	1.162	.291
PEU3	279	-.670	.146	.730	.291
PEU4	279	-.801	.146	1.813	.291
SI1	279	-.780	.146	1.744	.291
SI2	279	-.404	.146	-.214	.291
SI3	279	-.551	.146	.161	.291
SI4	279	-.603	.146	.560	.291
TRUST1	279	-.507	.146	.188	.291
TRUST2	279	-.910	.146	1.627	.291
TRUST3	279	-.365	.146	-.046	.291
TRUST4	279	-.664	.146	.556	.291

PR1	279	-.702	.146	.240	.291
PR2	279	-.438	.146	-.543	.291
PR3	279	-.266	.146	-.940	.291
PR4	279	-.192	.146	-.781	.291
IS1	279	.028	.146	-.912	.291
IS2	279	-.220	.146	-.943	.291
IS3	279	.126	.146	-.918	.291
IS4	279	-.336	.146	-.648	.291
CN1	279	-.195	.146	-.899	.291
CN2	279	-.546	.146	-.090	.291
CN3	279	-.884	.146	.798	.291
CN4	279	-.890	.146	.655	.291
PA1	279	-.905	.146	1.646	.291
PA2	279	-1.207	.146	1.170	.291
PA3	279	-1.042	.146	.896	.291
PA4	279	-1.291	.146	1.380	.291
PC1	279	-1.544	.146	1.498	.291
PC2	279	-.156	.146	-.997	.291
PC3	279	-.193	.146	-1.005	.291
PC4	279	-.597	.146	-.543	.291
PC5	279	-.610	.146	-.619	.291
PC6	279	-.546	.146	-.698	.291
ITASCS1	279	-.158	.146	-1.185	.291
ITASCS2*	279	-.939	.146	2.154	.291
ITASCS3	279	-.637	.146	1.242	.291
AAOSCS1	279	-.567	.146	.747	.291
AAOSCS2*	279	-.862	.146	2.568	.291
AAOSCS3	279	-.907	.146	1.654	.291

The result shows that all 49 variables are normally distributed except five. The indicators exceed the Kurtosis threshold by being greater than 2. The items are three perceived usefulness indicators (PU2, PU3 & PU4) and one item each under Intention to adopt smart city services (ITASCS2) and actual adoption of smart city services (AAOSCS2). For all other indicators, the skewness ranged between -0.126 and 1.544, while the Kurtosis ranged between -0.004 and 1.8113, which are acceptable normality thresholds.

Table 6 shows descriptive statistics such as the frequency, minimum, maximum, mean, variance, standard deviation, and standard error of issues relating to perceived security. As displayed in the table, the minimum and maximum values of all items under perceived security are 6 and 18, respectively. The mean of perceived security is 13.5269. This reveals that the respondents are strongly concerned that healthcare services providers in the smart city will take full responsibility for any security breach during any transaction. While for perceived usefulness, the minimum and the maximum values of all items range between 4 and 10, with an average value of 7.8065

and a standard error of 0.07647. This indicates that many respondents believe that a smart city's healthcare delivery will benefit them.

Regarding perceived ease of use, all items' minimum and maximum values range from 7 to 15, with an increased mean value of 12.3763. The statistic values of variance, standard deviation, and standard error are 2.581, 1.60651, and 0.09618, respectively. With these measures of dispersion value, it can be reported that many respondents believed that smart city healthcare services would be easy to use when finally adopted. However, as can be observed from Table 6, the mean of social influence indicates a strong role of the encouragement from top government officers and senior management in the organization to the influence of important people around the respondents with less than one standard error. There is a strong indication that people around them highly influence the respondents.

Trust can be viewed as the respondent's strong belief in the HSSC transparency and reliability. The statistics from Table 6 reveal the mean value of trust along with other important statistics. Respondents are more concerned about service reliability than any other trust-related issues. The risk of private risk being comprised is another important construct with respondents concerned with a high potential breach of personal information while using HSSC.

Safeguarding sensitive information is considered very important in preventing data compromise. The descriptive statistics show how concerned respondents are with personal health information in the face of HSSC. The mean score is for the sensitivity of personal information provided by respondents, people important to respondents warn against revealing personal information online, and individuals want to know how their personal information is being used and by whom. On the other hand, standard deviation shows the dispersion index revealing how respondents under each item differ from the item mean.

Table 6. Descriptive statistics.

Constructs	N Statistic	Minimum Statistic	Maximum Statistic	Mean Statistic	Std. Error	Std. Deviation Statistic	Variance Statistic
Perceived Security (PS)	279	6.00	18.00	13.5269	.13821	2.30853	5.329
Perceived Usefulness (PU)	279	4.00	10.00	7.8065	.07647	1.27729	1.631
Perceived Ease of Use (PEU)	279	7.00	15.00	12.3763	.09618	1.60651	2.581
Social Influence (SI)	279	3.00	15.00	10.7133	.11979	2.00095	4.004
Trust	279	6.00	20.00	15.2796	.14480	2.41860	5.850
Privacy Risk (PR)	279	6.00	20.00	13.5448	.15306	2.55669	6.537
Information Sensitivity (IS)	279	4.00	20.00	12.4516	.19703	3.29109	10.831
Cultural Norm (CN)	279	7.00	20.00	14.8172	.15675	2.61820	6.855

Privacy Awareness(PA)	279	4.00	10.00	8.5771	.08236	1.37565	1.892
Privacy Concern (PC)	279	10.00	30.00	21.8172	.29068	4.85535	23.574
Intention to adopt Smart City Services(ITASCS)	279	2.00	10.00	7.1470	.07402	1.23640	1.529
Actual adoption of Smart City Services (AAOSCS)	279	2.00	10.00	7.7993	.08257	1.37914	1.902
Valid N (listwise)	279						

And finally, the descriptive statistics on actual adoption of smart city services with regard to whether the respondent would use intelligence healthcare services in smart cities to get health information and create a healthy living. The minimum and maximum values of actual adoption are 2 and 10, respectively, with a mean average of 7.7993. The dispersion measures reveal that most respondents would like to adopt the new technology. Generally, values of standard deviation are very low compared to their respective mean, as seen in Figure 2.

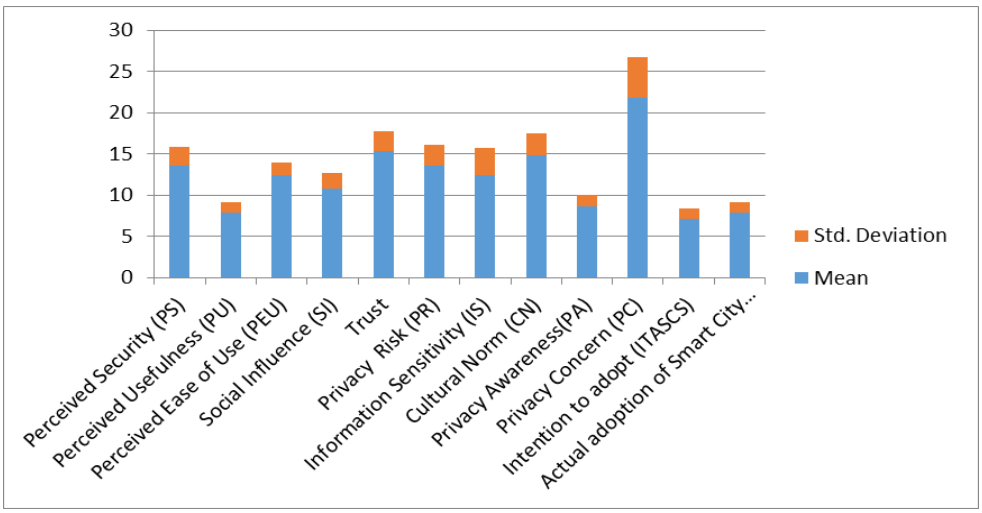

Fig. 2: Mean and standard deviation.

The socio-demographical attributes of respondents are relevant to respondents' intention to adopt healthcare services in a smart city. Table 7. shows that a total of 279 respondents participated in the survey. The result indicates that a total of 188 males, equivalent to around 67 percent of the total participants of the study, while females only accounted for the remaining 33 percent (91). Not surprisingly, around 94 percent (263) of the respondents are of Omani nationality, while only about 6 percent (16) are not Omanis. These results indicate that our findings can be applied to Oman since most of our respondents are Omanis. The age distribution of the respondents shows that individuals within the range of 30-39 are the highest, with a

total of 169 (60.6 percent) followed by respondents within the 40-49 age group. Those over 50 are next, with adults in their 20s the least during this survey. Therefore, it is important to note that substantial percentage of our respondents are aged 30 and above. About 85 percent of respondents in our survey are either bachelor's degree holders, master's, or Ph.D., with a total of 236 out of 279. While around 12 percent of the respondents hold diploma certificates, only seven respondents hold a secondary school leaving certificate.

More than one-quarter of the respondents accounting for 78 (28 percent), are administrators according to their occupational status, while more than one-fifth, 64 (23 percent), are Information Technologists. Educators and medical practitioners recorded 33 (11.8 percent) and 32 (11.5 percent), respectively. About 10 percent (28) of the respondents are finance experts, while the remaining 15.7 percent (44) are of professions other than those mentioned above. Regarding computer skills, most respondents have moderate computer skills, with a total of 207 (74.2 percent), followed by those who rated their computer skills as experts, with only 20.8 percent (58) respondents. Only 14 respondents claim to be novices.

Table 7: Socio-demographic characteristics of the respondents

		Frequency	Percent
Gender	Male	188	67.4
	Female	91	32.6
Nationality	Omani	263	94.3
	Non-Omani	16	5.7
Age	20-29 years	6	2.2
	30-39 years	169	60.6
	40-49 years	95	34.0
	over 50 years	9	3.2
Educational Level	Secondary Education	7	2.5
	Diploma	34	12.2
	Bachelor	118	42.3
	Postgraduate	118	42.3
	Others	2	0.7
Field of Work	Administration	78	28.0
	Finance	28	10.0
	Information Technology	64	23.0
	Medical	33	11.8
	Education	32	11.5

	Others	44	15.7
Computer Skills	Novice	14	5.0
	Moderate	207	74.2
	Expert	58	20.8

Source: Author's

As previously stated, the path coefficients of the constructs were used to evaluate the structural equation model. The path coefficients described the relationships between dependent and independent constructs that have been theorized. Finally, the structural equation model tests the direct causal effects between the constructs.

In this study, the hypothesized path coefficients are 12, which are H1, H2, H3, H4, H5, H6, H7, H8, H9, H10a, H10b, and H11.

Table 8. Examining results of hypothesized causal & direct effects of the constructs.

	Path		Path Coefficient	Standard Error	T-Value	P-Value
PS	→	ITASCS	0.475*	0.091	5.220	0.000
PU	→	ITASCS	0.529*	0.048	11.020	0.000
PE	→	ITASCSU	0.495*	0.062	7.984	0.000
SI	→	ITASCS	0.434*	0.081	5.358	0.000
TRUST	→	ITASCS	0.623*	0.088	7.080	0.000
IS	→	PC	0.597*	0.033	17.545	0.000
PR	→	PC	0.442*	0.028	15.785	0.000
CN	→	PC	0.459*	0.029	15.828	0.000
PA	→	PC	0.165*	0.017	9.706	0.005
PC	→	ITASCS	-0.268*	0.016	16.750	0.000
PC	→	TRUST	0.02	0.024	0.833	0.675
ITASCS	→	AAOSCS	0.765*	0.039	19.615	0.000

**p< 0.05 , **p< 0.01, ***p< 0.001*

As presented in Table 8. all the paths coefficient were statistically significant because their p-values were below the standard significance level of 0.05 except the path of privacy concern to trust, which exhibit a p-value of 0.675. As a result, all the hypotheses H1, H2, H3, H4, H5, H6, H7, H8, H9, H10a, and H11 were supported, while H10b was rejected.

5. Discussion on Research Hypothesis Test

One of the objectives of this research is to discover the factors that affect individual privacy perceptions when it comes to accepting smart city services, a behavior that

could endanger the future of smart cities. The results of path analysis are discussed in connection to the structural model's hypotheses in this section:

H1: Perceived security has a positive effect on Intention to Adopt Smart City Services.

On the intention to adopt services for smart cities, perceived security is thought to have a favorable impact. The t-value and p-value of the perceived security are 5.220 and 0.000, respectively, as given in Table 4.9. Additionally, a favorable influence was indicated by the path coefficient of 0.475. This indicates that the intention to adopt smart city services is significantly positively influenced by perceived security. H1 is therefore supported. As a result, the intention to use smart city services will increase by 0.475 for every standard deviation increase in perceived security. This straightforward fact can be interpreted as meaning that in Oman, perceptions of security affect decisions about whether to use smart city services. The outcome is in line with earlier research by Sepasgozar et al. (2019) and Walczuch, Lemmink, and Streukens (2007).

H**2**: Perceived usefulness has a positive and significant impact on Intention to Adopt Smart City Services.

Another study hypothesis is that the intention to use smart city services in Oman is positively and significantly influenced by perceived usefulness. For example, the path coefficient of perceived usefulness was 0.529, and the t-value and P-value were 11.020 and 0.000, respectively, as shown in Table 4.9, Section 4. H2 is therefore supported. This indicates that the perceived utility significantly impacts the propensity to embrace smart city services in Oman. Additionally, it suggests that an increase of one standard deviation in perceived usefulness in Oman will result in an increase of around 0.529 in intentions to use smart city services. The outcome is consistent with earlier research by Shuhaiber and Mashal (2019).

H**3**: Perceived ease of use has a positive and significant impact on Intention to Adopt Smart City Services.

The study also advanced the hypothesis that perceived ease of use significantly and favorably affects people's intentions to use smart city services. According to Table 4.9, the t-value and p-value of perceived ease of use in predicting the intention to adopt smart city services were 7.984 and 0.000, respectively. It implies a 0.000 chance of obtaining an absolute t-value of 7.984. To put it another way, the regression weight for perceived ease of use (PEU) in predicting the intention to adopt smart city services is significantly different from zero at the 0.05 level. As a result, H3 was consequently supported. The path coefficient of 0.495 further revealed a positive link. Intention to Adopt Smart City Services (IATSCS) increases by 0.495 standard deviations for every standard deviation improvement in perceived Ease of Use (PEU). This implies that the desire to embrace smart city services in Oman would depend on

perceived ease of usage. This finding supports Schmidthuber et al.'s (2018) research outcomes.

H**4**: Social influence has a positive impact on Intention to Adopt Smart City Services.

Social factors influence the intention to implement smart city services in Oman. The t-value and p-value of social impact in predicting intention to adopt smart city services, as shown in Table 4.9, were 5.358 and 0.000, respectively. This indicates a 0.000 chance of obtaining a t-value with an absolute value of up to 5.358. This suggests that hypothesis H4 was supported because there is a substantial difference between zero and the effect of social influence on the intention to embrace smart cities. The path coefficient, which indicates a beneficial effect, was 0.434. An increase in social influence of one standard deviation will result in a 0.434 increase in Oman's intention to adopt smart cities. Therefore, social influences affect people's eagerness to use smart cities. The outcome contrasts with that of Gunawan and Smart (2019). This implies that a person's geographic location may have an impact on the social influence they experience.

H**5**: Trust has a significant positive impact on Intention to Adopt Smart City Services.

Table 4.9 also shows the impact of trust on the decision to use smart city services. The path coefficient was 0.623, and the t-value and p-value values were 7.080 and 0.000, respectively. This indicates a 0.000 chance that the t-value will be as high as 7.080. As a result, the regression weight for trust in estimating the likelihood of adopting smart cities differs significantly from zero. Additionally, the outcome displays a path coefficient of 0.623, showing a favorable impact. Accordingly, a rise of 1 standard deviation in the trust will result in 0.623 standard deviations in Oman’s to adopt smart cities.

H6: Privacy risk has a positive influence on privacy concerns.

Table 4.9 also shows the impact of trust on the decision to use smart city services. The path coefficient was 0.623, and the t-value and p-value were 7.080 and 0.000, respectively. This indicates a 0.000 chance that the t-value will be as high as 7.080. As a result, the regression weight for trust in estimating the likelihood of adopting smart cities differs significantly from zero. Additionally, the outcome displays a path coefficient of 0.623, showing a favorable impact. Accordingly, one standard deviation in trust will increase by 0.623 in Oman's intention to adopt smart cities. With a path coefficient of 0.442, the outcome similarly demonstrates a favorable relationship between privacy risk and privacy worry. It means that for every increase in privacy risk (PR) of 1 standard deviation, privacy worry rises by 0.442 standard deviations. In other words, privacy concerns increase as privacy risks do. As a result, hypothesis H6 is confirmed. The findings support those of studies conducted by Xu et al. in 2008, Dinev & Hart in 2004, and Xu et al. in 2013.

H7: Information sensitivity has a positive effect on the level of privacy concern.

Information sensitivity influences the level of privacy concern is another hypothesis in the study symbolized by H7. This result is also shown in Table 4.9, with the path coefficient of 0.597, t-value of 17.545, and p-value of 0.000. From the path coefficient result, it means that information sensitivity exerts a positive impact on privacy concerns. For example, a one standard deviation increase in information sensitivity increases privacy concern with a 0.597 standard deviation value. The result also indicates that the probability of getting a t-value as large as 17.545 in absolute terms is 0.000. This indicates that the regression weight for information sensitivity in the prediction of privacy concerns is significantly different from zero. Hence, hypothesis is correct. The higher the Information sensitivity, the higher the privacy concern of people. The result supported the finding of Li et. al., (2016).

H8: Cultural Norm have a positive influence on privacy concerns.

The test of the hypothesis on cultural norms having a positive influence on privacy concerns is also shown in Table 4.9. The result established that their cultural norm directly influences privacy concerns in Oman. This is concluded based on the output of the path coefficient of 0.459, the t-value of 15.825, and the P-value of 0.000. The result also indicates that the an increase of standard deviation in cultural norms leads to 0.459 standard deviation increase in privacy concern. The result of the t-value and the corresponding p-value justified that regression weight for cultural norm in the prediction of privacy concerns is significantly different from zero. Therefore, the study failed to reject the hypothesis (H8) based on the valid results established. Hence, cultural norm exerts a significant positive effect on privacy concern. This result corroborates the study of Milberg et al. (2000), who found cultural norms as a crucial component in impacting users' privacy concerns.

H9: Privacy awareness has a positive effect on the level of privacy concern.

Another hypothesis examined in this study was the effect of privacy knowledge on the degree of privacy worry. The outcome reveals that the t-value and p-value were respectively 9.705 and 0.005. At the 0.05 threshold of significance, the result differs considerably from zero. This implies that there is a 0.005 percent chance that the t-value will be as high as 9.705. Additionally, the path coefficient score was 0.165, which ,shows that privacy knowledge positively impacts privacy concerns

The investigation validated the hypothesis in light of the established results (H9). As a result, the study draws the conclusion that privacy knowledge positively affects the degree of privacy worry. As a result, the amount of privacy concern increases as privacy policies and practises become more well known. This finding supports the assertion made by Balapour et al. (2020) that individual awareness has a significant role in influencing the degree to which privacy concerns are raised.

H10a: Privacy concerns have negative impact on Intention to Adopt Smart City Services.

The hypothesis that privacy concerns have a detrimental impact on intention to embrace smart city services was explored based on the results shown in Table 4.9. The p-value was 0.000 and the t-value was 16.750, respectively. This indicates that there is a 0.000 chance that the t-value will be as high as 16.750. Additionally, it shows that the regression weight for privacy concern is considerably different from zero when predicting changes in intention to employ smart city services. The outcome also reveals that the path coefficient was -0.268, indicating a detrimental effect of privacy concerns on the intention to use smart city services. According to earlier studies in the literature, privacy concerns have the opposite effect on the inclination to use smart city services. This study thus provides evidence in favor of the hypothesis that, in Oman, individual intentions to embrace smart city services are lower the more privacy issues there are. The outcome supports the findings of Dinev & Hart's (2005), which found that privacy concerns have a detrimental impact on people's intentions to use the internet.

H10b: Privacy concerns have a negative impact on trust.

The investigation of the impact of privacy issues on trust, which guided the formation of hypothesis H10b, is another area of concern and interest for this study. It is established that the t-value and the p-value were 0.833 and 0.675, as indicated in Table 4.9. This indicates a 0.675 percent chance that the t-value will be as high as 0.833. This indicates that the outcome is not significant at a threshold of significance of 0.01 percent. The path coefficient is 0.02, indicating a favorable influence as opposed to the anticipated adverse effect. These proven results lead this study to reject the hypothesis and conclude that privacy concerns negatively impact trust in Oman. This runs counter to Kim's (2008) study, which found that privacy concerns significantly adversely affected trust.

H11: Intention to adopt Smart City Services has a significant positive impact on actual adoption of Smart City Services.

According to the study's hypotheses, the decision to use smart city services is significantly influenced by one's intention to do so. The outcome of the analysis is shown in Table 4.9, where the t-value and p-value are 19.615 and 0.000, respectively. This indicates a 0.000 chance that the t-value will be as high as 19.615. The outcome also suggests a substantial difference between zero and the regression weight for the intention to embrace smart city services in predicting the actual adoption of smart city services in Oman.

A positive influence on actual adoption is indicated by the path coefficient of intention to adopt smart city services (ITAOSCS), which is 0.765. The results of this study thus provide credence to the idea that having the goal to adopt smart city services influences that adoption significantly. The outcome is consistent with the research by Li et al. (2016), who found a strong and favorable relationship between the desire to adopt and the actual adoption of new technology.

6. Conclusive Remarks

The smart city model in the health domain was formulated based on the conceptual theories reviewed in the literature. The proposed model was later tested and validated by using the structural equation method of analysis. This is because SEM considers the hypothesis systemic relationship among variables as a whole and the fundamental links between different variables. SEM allows for both confirmatory and exploratory modeling, therefore was used for both theory testing and theory creation

One of the main drivers of this research is the lack of studies on privacy cconcerns in smart city services. Therefore, this study significantly adds to the body of knowledge about adoption of smart city services with a strong emphasis on privacy issues. This study adds to the body of knowledge in four distinct ways:

i. In this study, three (3) theoretical models - UTAUT, PCT, and TAM were combined and used to improve the final model's predictive capability. To successfully deploy smart city services in the Oman health sector, the conceptual model was created by incorporating all ideas that are pertinent to addressing the issues in Oman. The model integrates the constructs of privacy concern (privacy risk, information sensitivity, cultural norm, and privacy awareness) with the constructions of intention to embrace smart city services (perceived security, perceived ease of use, and perceived utility). This study is expected to pique the interest of researchers and health-care stakeholders, allowing them to dig further into and investigate the framework for related research, particularly in relation to smart cities and other user-initiated models. However, additional investigations outside of the health sector may be able to validate the approach.

ii. One of the main issues with the smart city is how data and information security and privacy are maintained. Previous research acknowledged security and privacy concerns in general but did not go into detail about how to handle data and information privacy.

iii. In this study, the moderating factor between privacy risk, information sensitivity, cultural norms, privacy awareness, trust, and intention to adopt smart cities was privacy concern. It demonstrates that the effects of privacy risk, information sensitivity, cultural norm, and privacy awareness have a strong negative impact on people's intentions to adopt smart cities.

iv. This research leads to the development of a well-structured survey on smart city adoption in connection to privacy concerns, which is the first of its kind in the health sector in Oman. The designed instrument had gone through a range of evaluation processes with the help of panellists. pre-testing, pilot testing, validity, and reliability assessment are some of the stages and activities included in the instrument development process. This instrument

can be researched and examined further by future researchers in related investigations.

v. This research is considered as one of the first empirical studies that used privacy concern as moderating variable on intention to adopt smart city services in the health sector in Oman.

This study has been carried out with mainly government employees, so, the generalization for the whole country is one of the limitation of this study. Private health care providers adoption of smart city services could vary due to their unique characteristics. This might be due to their level of education and IT knowledge.

Acknowledgement

This paper research is supported by the TNB SEED FUND with Grant Code: (U-TL-RD-21)

References

Balapour, A., Nikkhah, H. R., & Sabherwal, R. (2020). Mobile application security: Role of perceived privacy as the predictor of security perceptions. *International Journal of Information Management*, (November), 102063. DOI: https://doi.org/10.1016/j.ijinfomgt.2019.102063.

Chellappa, R. K., & Sin, R. (2005). Personalization versus privacy: An empirical examination of the online consumer's dilemma. Information *Technology and Management*, 6(2), 181–202

Deebak, B. D., Al-turjman, F., Aloqaily, M., & Alfandi, O. (2019). Special section on security and privacy in emerging decentralized an authentic-based privacy preservation protocol for smart e-healthcare systems in IoT. IEEE Access, 7, 135632–135649. DOI: https://doi.org/10.1109/ACCESS.2019.2941575.

Dhagarra, D., Goswami, M., & Kumar, G. (2020). International journal of medical informatics impact of trust and privacy concerns on technology acceptance in healthcare: An Indian perspective. Int*ernational Journal of Medical Informatics*, 141(February), 104164. DOI: https://doi.org/10.1016/j.ijmedinf.2020.104164.

Dinev, T. & Hart, P. (2004). Privacy concerns and Internet use—a model of trade-off factors. Paper read at Working Paper, Department of Information Technology and Operations Management at Florida Atlantic University.

Dinev, T. & Hart, P. (2005). Internet privacy concerns and social awareness as determinants of intention to transact. *International Journal of Electronic Commerce*.

Dinev, T. & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, 17(1), 61–80. DOI: https://doi.org/10.1287/ isre.1060.0080.

Dinev, T., Xu, H., Smith, J. H., & Hart, P. (2013). Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts, *Eur. J. Inform. Syst*. 22, 295–316.

Ding, D., Conti, M., & Solanas, A. (2016). A smart health application and its related privacy issues. *Proceedings of the 2016 Smart City Security and Privacy Workshop, SCSP-W 2016*, 11–15. DOI: https://doi.org/10.1109/SCSPW.2016.7509558.

Elvis, T. E. & Kim, H. (2022). Unified perspective of technology readiness index (TRI) and technology acceptance model (TAM) for adoption of digital pills. *Journal of System and Management Sciences*, 12(4), 101–114. DOI: https://doi.org/10.33168/JSMS.2022.0407.

Fortes, N., & Rita, P. (2016). Privacy concerns and online purchasing behaviour: Towards an integrated model ☪. *European Research on Management and Business Economics*, 22(3), 167–176. DOI: https://doi.org/10.1016/j.iedeen.2016.04.002.

Gunawan, H. & Smart, A. (2019). Identifying factors affecting smart city adoption using the unified theory of acceptance and use of technology (UTAUT) method. *2018 International Conference on Orange Technologies (ICOT)*, 1–4.

Hair.Jr., J. F., Black., W. C., Babin., B. J., Anderson., R. E., & L.Tatham., R. (2006). Multivariant data analysis. New Jersey: Pearson International Edition.

Hathaliya, J. J. & Tanwar, S. (2020). An exhaustive survey on security and privacy issues in Healthcare 4 . 0. Computer communications, 153(January), 311–335. DOI: https://doi.org/10.1016/j.comcom.2020.02.018.

Jiang, X. (2011). Privacy concern toward using social networking services : A conceptual model. *2011 2nd International Conference on Artificial Intelligence, Management Science and Electronic Commerce (AIMSEC)*, 3180–3183. DOI: https://doi.org/10.1109/AIMSEC.2011.6011395.

Kabbiri, R., Dora, M., Kumar, V., Elepu, G., Gellynck, X., 2018. Mobile phone adoption in agri-food sector: Are farmers in Sub-Saharan Africa connected? *Technol. Forecast. Soc. Chang*. 131, 253–261.

Kim, D. J. (2008). Self-perception-based versus transference-based trust determinants in computer-mediated transactions: A cross-cultural comparison study. *Journal of Management Information Systems*, 24(4), 13–45. DOI: https://doi.org/10.2753/mis0742- 1222240401.

Li, H., Wu, J., Gao, Y., & Shi, Y. (2016). Examining individuals' adoption of healthcare wearable devices: An empirical study from privacy calculus perspective. *International Journal of Medical Informatics*, 88(555), 8–17. DOI:https://doi.org/10.1016/j.ijmedinf.2015.12.010.

Li, Y. (2014). The impact of disposition to privacy, website reputation and website familiarity on information privacy concerns. *Decis. Support Syst*. 57, 343–354.

Luor, T., Lu, H. P., Yu, H., & Lu, Y. (2015). Exploring the critical quality attributes and models of smart homes. Maturitas, 82(4), 377–386. DOI: https://doi.org/10.1016/j.maturitas.2015.07.025.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems 87 Research*, 15(4), 336–355.

Milberg, S. J., Smith, H. J., & Burke, S. J. (2000). Information privacy: Corporate management and national regulations. *Organ Sci*, 11(1), 35–57.

Milne, G. R. & Boza, M. (1999). Trust and concern in consumers' perceptions of marketing information management practices. *Journal of Interactive Marketing*, 13(1), 5–24.

Mohammed, Z. A. & Tejay, G. P. (2017). Examining privacy concerns and ecommerce adoption in developing countries: The impact of culture in shaping individuals ' perceptions toward technology. *Computers & Security*, 67, 254–265. DOI: https://doi.org/10.1016/j.cose.2017.03.001.

Nam, J., & Choi, M. (2022). IoT edge cloud platform with revocatable blockchain smart contract. *Journal of Logistics, Informatics and Service Science*, 9(2), 131–144. DOI: https://doi.org/10.33168/LISS.2022.0208.

Natgunanathan, I., Mehmood, A., Xiang, Y., & Member, S. (2019). Location privacy protection in smart health care system, 6(2), 3055–3069.

Niraula, S. R. (2019). A review of research process, data collection and analysis. 1–6.

Pallant, J. (2013). SPSS survival manual: A step by step guide to data analysis using SPSS for Windows (5th ed.). Maidenhead, England; New York: McGraw Hill/Open University Press.

Pentina, I., Zhang, L., Bata, H., & Chen, Y. (2016). Computers in human behavior exploring privacy paradox in information-sensitive mobile app adoption : A cross-cultural comparison. *Computers in Human Behavior*, 65, 409–419. DOI: https://doi.org/10.1016/j.chb.2016.09.005.

Phelps, J., D'Souza, G. & Nowak, G. J. (2001). Antecedents and consequences of consumer privacy concerns: An empirical investigation. *Journal of Interactive Marketing*, 15(4), 2–17.

Rahman, S. A., Taghizadeh, S. K., Ramayah, T., & Alam, M. M. D. (2017). Technology acceptance among micro-entrepreneurs in marginalized social strata: The case of social innovation in Bangladesh. *Technological Forecasting and Social Change*, 118, 236–245. DOI: https://doi.org/10.1016/j.techfore.2017.01.027.

Schmidthuber, L., Maresch, D., Ginner, M., 2018. Disruptive technologies and abundance in the service sector - toward a refined technology acceptance model. *Technol. Forecast. Soc. Chang*. 1–11.

Sepasgozar, S. M. E., Hawken, S., Sargolzaei, S., & Foroozanfa, M. (2019). Implementing citizen centric technology in developing smart cities: A model for predicting the acceptance of urban technologies. *Technological Forecasting and Social Change*, 142(December 2017), 105–116. DOI: https://doi.org/10.1016/j.techfore.2018.09.012.

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

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An inter-disciplinary review. *MIS Quarterly*, 35(4), 989–1016. DOI: https://doi.org/10.2307/41409970.

Tabachnick, B.G., Fidell, L.S., 2007. Using multivariate statistics, 5th ed. Pearson International, Boston.

Venkatesh, V., Morris, M. G. & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 27(3), 425-478.

Walczuch, R., Lemmink, J., Streukens, S. (2007). The effect of service employees' technology readiness on technology acceptance. *Inf. Manag*. 44(2), 206–215.

Wang, T., Jung, C.-H., Kang, M.-H., & Chung, Y.-S. (2014). Exploring determinants of adoption intentions towards Enterprise 2.0 applications: An empirical study. *Behav. Inform. Technol*, 33, 1048–1064.

Wottrich, V. M., van Reijmersdal, E. A., & Smit, E. G. (2018). The privacy trade-off for mobile app downloads: The roles of app value, intrusiveness, and privacy concerns. *Decision Support Systems*, 106, 44–52. DOI: https://doi.org/10.1016/j.dss.2017.12.003.

Xu, F., Michael, K., & Chen, X. (2013). Factors affecting privacy disclosure on social network sites : an integrated model, 151–168. DOI: https://doi.org/10.1007/s10660-013-9111-6.

Xu, H., Dinev, T., Smith, H. J., & Hart, P. (2008). Examining the formation of individual's information privacy concerns: toward an Integrative view. Paper read at 29th Annual International Conference on Information Systems (ICIS), at Paris, France.

Zhang, Y. B., Zhang, L. L., & Kim, H. K. (2021). The effect of UTAUT2 on use intention and use behavior in online learning platform. *Journal of Logistics, Informatics and Service Science*, 8(1), 67–81. DOI: https://doi.org/10.33168/LISS.2021.0105.