Open Access Article

The Perception of Individuals' Privacy Concerning the Adoption of Smart City Healthcare Services: A Generic Model Development

Abdullah Aslam Alzawamri[1], Hairoladenan Kasim[2], Moamin Mahmoud[3]

[1] College of Graduate Studies, University Tenaga Nasional, Kajang, Malaysia

[2] College of Computing and Informatics, University Tenaga Nasional, Kajang, Malaysia

[3] Institute of Informatics and Computing in Energy, University Tenaga Nasional, Kajang, Malaysia

Abstract: With the continuous efforts to implement several smart cities, several challenges face these initiatives at the global level, the most prominent of which is data privacy. There is a lack of research on the factors that affect the perception of individuals' privacy, such as the risk of privacy, data sensitivity, privacy Awareness. In addition, it is not clear what those factors are, and they could swing people's intention to adopt smart services. Concerns about data privacy are categorized based on data activities to unauthorized retrieval, unauthorized use, unauthorized access, unauthorized sharing, insecure storage, and insecure transmission. Each of these issues might lead to a personal data breach and expose the data to be compromised, especially in the case of healthcare data. Therefore, this study aims to identify factors that affect the adoption of smart city healthcare services and subsequently propose a generic adoption model to focus on data and information privacy in this model, especially in health care. This model is developed based on two ways to extract the factors. First: the theories used are the Technology Acceptance Model (TAM), Unified Theory of Acceptance and Use of Technology (UTAUT), and Privacy calculus theory (PCT). Secondly: extract some factors from the literature review and studies related to this research. The model is expected will help to obtain the acceptance, adoption of smart city services and the extent of their impact on data and information privacy from the perspective of individuals and fill gaps. It also can be used in countries similar to Oman, such as in the Arabian Gulf countries.

Keywords: smart city, healthcare services, privacy, privacy concern, technology acceptance model.

關於採用智慧城市醫療保健服務的個人隱私感知：通用模型開發

摘要: 隨著多個智慧城市的不斷實施，這些舉措在全球範圍內面臨著幾個挑戰，其中最突出的是數據隱私。對影響個人隱私感知的因素，如隱私風險、數據敏感性、隱私意識等缺乏研究。此外，尚不清楚這些因素是什麼，它們可能會影響人們採用智能服務的意願。對數據隱私的擔憂根據數據活動分為未經授權的檢索、未經授權的使用、未經授權的訪問、未經授權的共享、不安全的存儲和不安全的傳輸。這些問題中的每一個都可能導致個人數據洩露並暴露數據，尤其是在醫療數據的情況下。因此，本研究旨在找出影響智慧城市醫療服務採用的因素，並隨後提出通用的採用模型，因此該模型中的重點將放在數據和信息隱私上，尤其是在醫療保健領域。該模型是基於兩種提取因素的方法開發的，第一：關於所使用的理論，即技術接受模型、技術接受和使用統一理論和隱私演算理論。其次：從與本研究相關的文獻綜述和研究中提取一些因素。該模型預計將有助於從個人的角度獲得智慧城市服務的接受、採用及其對數據和信息隱私的影響程度，並填補空白。也可用於類似阿曼的國家，如阿拉伯灣國家。

Received: August 17, 2021 / Revised: October 14, 2021 / Accepted: November 15, 2021 / Published: December 30, 2021

About the authors: Abdullah Aslam Alzawamri, College of Graduate Studies, University Tenaga Nasional, Kajang, Malaysia; Hairoladenan Kasim, College of Computing and Informatics, University Tenaga Nasional, Kajang, Malaysia; Moamin Mahmoud, Institute of Informatics and Computing in Energy, University Tenaga Nasional, Kajang, Malaysia

Corresponding authors Abdullah Aslam Alzawamri, abdullah.salim9999@gmail.com; Hairoladenan Kasim, hairol@uniten.edu.my; Moamin Mahmoud, moamin@uniten.edu.my

关键词：智慧城市、医疗保健服务、隐私、隐私关注、技术接受模型。

1. Introduction

Since the introduction of the smart city in 1994, the paradigm has attracted global attention from academia, industry, and policymakers. As projected and shown in Figure 1, smart cities are expected to quadruple globally by 2025. Despite smart city phenomenal growth, there is still no universally agreed definition as the conceptualization is rapidly evolving amid different conditions and needs of individual cities [1]. Smart City can be defined based on societal or technological perspectives based on the literature. The recent society-oriented definition of a smart city was provided by the Institute of Electrical and Electronics Engineers (IEEE) as a city that brings together society, government, and technology by enabling features such as smart living, a smart environment, smart mobility, smart living, smart government and smart economy [2]. From the technological point of view, a city is considered smart if it has available digital technologies across its breadth and width [3]. What is common to both perspectives is that a smart city is characterized by the advanced deployment of ICT, which allows the city to be livable, workable, and sustainable by the citizens.

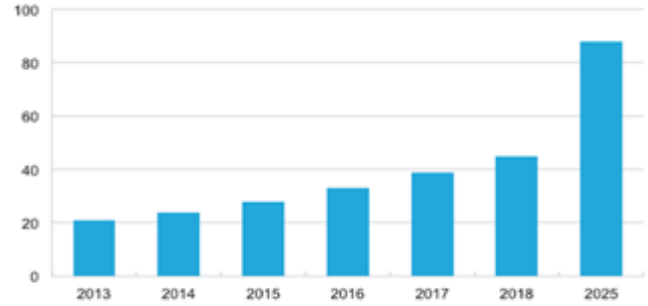

Fig. 1 Number of smart cities worldwide, as per HIS technology's definition [4]

Today, more than half of the world's population lives in the city with six or more devices connected to the internet. This suggests that many frameworks and numerous devices are connected in the city. The devices range from dividable to municipal systems such as street traffic, smart lighting, water, gas, and waste management to the smart healthcare system. Smart, innovative, and sustainable cities contribute to economic growth and promote social stability by enabling and encouraging both government and corporations to invest their expertise and resources in the new smart city projects by ensuring contentment and more economic growth for their people. Smart city services improve the citizens' living conditions and general well-being [5]. Since the people living with the city are the users of these services and there are concerns over information privacy, their perceptions and ideas must be considered during project conceptualization, planning, and execution [6].

A smart city is a modernized urban concept driven by technology that uses big data to improve quality of life through smart services in the home, transportation, health delivery, national grid, waste management, government operations, and increased infrastructure sustainability. Although smart cities make our urban communities livable, workable, and more sustainable, security and privacy concerns remain since smart city technology retrieves and process sensitive data from individuals and group [6]. Smart cities are conceived from assembling their national infrastructure and ICT to enhance smart living. This combination offers numerous advantages; however, it likewise presents numerous privacy challenges if not executed satisfactorily. Even though privacy risks and difficulties are inherent in any ICT system, its effectiveness enhances numerous services in an urban society in reality. A hacked email poses an individual data breach; however, it can turn chaos in the city or whole state [6, 7].

The literature has established that smart cities are vulnerable to data linkage and personal information tampering while digitally retrieving data, processing, and transmitting. The personal information in a smart city may contain users' location and identity in transportation, lifestyle inferred from intelligent surveillance, health records in hospitals, smart community, home, and waste. It would be a serious security breach for this private information to be disclosed to unauthorized or untrusted parties in any form [8]. Increased data collection on individuals is one of the major issues identified in many studies, particularly threats to individuals because of their data analysis using data mining techniques. Figure 2 displays the most dangerous privacy threats in smart cities [9]:

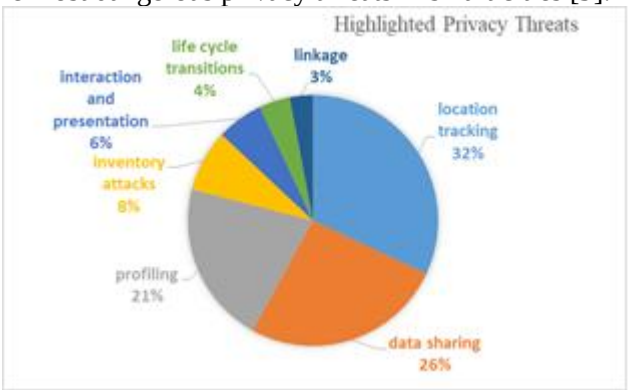

Fig. 2 Highlighted privacy threats

Recently, researchers and medical professionals have been studying consumers' mounting concerns about privacy and health risks of wearable technologies.

However, few studies have been carried out concerning the impact of that ambivalence on consumers' willingness to adopt these devices. The different themes identified in the literature are technology-focused, social acceptability, privacy and security, design, and user behavior. Figure 3 shows the number of smart wearables research themes [10].

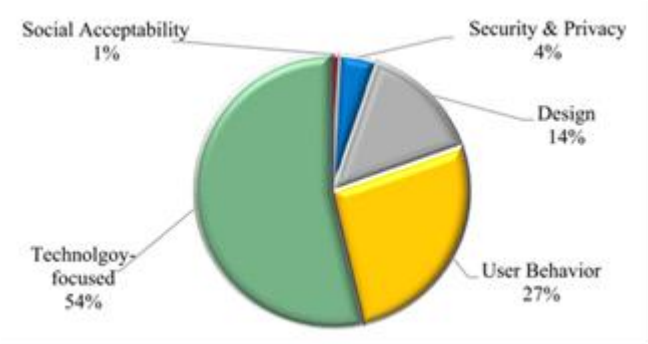

Fig. 3 Distribution of smart wearables themes

Every time a citizen registers for an email, buys an online product, uses or requests a service, enters into a contract, pays utility bills, or goes to your doctor, the citizen gives some personal data and information. Even without citizen knowledge and permission, personal information and data of citizens are captured and generated by agencies and companies that individuals are unlikely to have interacted with at no time. The only way people can trust businesses and government is the practice of effective data protection, with functional regulations to help reduce corporate and state surveillance and personal data unauthorized disclosure. Once data collection, processing, and analytics became widespread, citizens asked whether such data was collected and shared without their permission. Could their data be used to violate or discriminate against citizens' fundamental human rights? Who had the right to access it? Was it stored safely and accurately? Personal information privacy concerns grow amid a high proliferation of smart cities with data protection as mitigation measures.

Advocate for mitigation measures to protect personal information privacy in smart cities. Moreover, to let people enjoy the services of the smart cities trustingly. The traditional protection solution cannot be relied on in smart cities to withstand data over-collection and mashing. There is a substantial body of literature on information privacy issues concerning smart solutions such as smart grids, sensor networks, IoT enhanced surveillance cameras. However, the issues of personal information breach remain unresolved with yet to known factors affecting individual privacy perceptions and concerns [11].

2. Literature Review

2.1. Privacy Challenges

The lack of or limited understanding of smart cities' requirements and privacy challenges may prompt poor and unreliable execution and usage of the smart city. According to Sookhak *et al.* [13], one of the ways to ensure smart city data is the development of lightweight cryptographic methods for data decrypting and encrypting, and building a shared secret between nodes. However, such a security apparatus faces serious challenges due to heterogeneous devices used within the network. Privacy of data is a serious and crucial challenge in smart cities, which depends on gathering, analyzing, and sharing an enormous volume of data. As such, the viability of smart cities relies upon the effective deployment of big data applications in smart cities [13].

Consequently, personal information privacy breach needs to revolve around managing the security challenges posed instead of individual resistances. In this manner, transparent standards for protection will be essential to the successful transition of the smart city [14].

Despite the wide proliferation of smart cities across the globe, information privacy concerns are the issue raised in smart cities where advanced ICTs are deployed. Over 500 million personal information was stolen and exposed, and more than 430 million malicious malware was reported in 2015, an upsurge of about 36 percent from 2014 [15]. These numbers are becoming a new normal as online and real-life are no more distinguishable. The rapid public service digitalization often excludes part of the digitally illiterate society. Even the world's frontrunners are also experiencing crises with digitalization. These, among other things, proved that technology is on necessary but not sufficient component of smart cities. So, the urban environment smart is city transformation checked with suitable technologies and social and human resources deployment.

Another serious concern of the smart city is how data and information protection and privacy are managed. Previous works have studied the security and privacy issues in general without providing details of how data and information protection and privacy to be managed. Some other studies have recommended some solutions on data privacy. For example, Peters *et al.* [16] suggested applying the privacy zones framework to other smart spaces, for example, smart buildings, consequently ensuring privacy security for citizens depending on the level of their information sharing. Since smart cities are a work in progress, there are normally many chances to improve their security and privacy challenges [17]. The current security solutions, as of now, do not satisfy all security requirements in a smart city [18].

2.2. Privacy in Smart City Healthcare Services

In a smart city, an unusual amount of raw data like citizens' personal information, conditions of city traffic, pollution, and temperature are obtained and saved in different government or private companies' databases.

Despite potential healthcare services improvement by advanced technologies, citizens' information privacy could be breached, which means there should be adequate protection of personal information and data before full adoption of the smart city service. With recent advancements in wireless sensor networks (WSNs) and the high deployment of the Internet of Things (IoT), the concept of smart health has surfaced. A context-aware healthcare model, smart health can be prone to personal information security and privacy breaches. For instance, to get the COVID-19 status and current location of infected citizens, many citizens will have to be continuously monitored for contact tracing, which could be considered an invasion of privacy [19].

Privacy needs to be identified in the smart health context to protect citizens' personal information that accesses smart health services. The providers of smart health services make use of the patient identity to correlate individual health conditions or activities and records. In Ding *et al.* [16] construct, individual identity will be exposed when he/she contacts the city control center. Individuals' identities can be unlawfully used or stolen to retrieve sensitive personal data in the central database, such as lists of locations and health records. Hence, privacy could be breached. This is one of many personal information privacy concerns raised. To deal with this concern, individual identities are hidden by smart health service providers.

On the other hand, location privacy is about ensuring the physical location privacy of the people. When individuals choose optimal routes, they send their location to the city control center and allow the system provider to track their movements. Different techniques have been suggested for location privacy protection. The proposed methods show an approximate location that significantly hinders their service providers' location tracking [19].

Concerns about data privacy are categorized based on data activities to unauthorized retrieval, unauthorized use, unauthorized access, unauthorized sharing, insecure storage, and insecure transmission. Each of these issues might lead to a personal data breach and expose the data to be compromised, especially in the case of healthcare data [20].

A smart healthcare facility has a network of wireless medical sensors with lightweight resources limited in memory, processing power, and bandwidth. Medical sensors, such as elliptic curve cryptosystem, pulse oximeter, blood pressure, and temperature, are usually used in a patient's body to generate different wireless body area networks. They detect and obtain information about patients through a wireless system, generally provided to a medical practitioner, smart gadgets such as implantable medical devices, laptops, iPhones, and PDAs. Hence, it is believed that the medical practitioner may consider or read the evaluation for a thorough examination as and when it is required to process [21].

In a system of healthcare application, the privacy and security of patients' data are one of the growing concerns to adopting smart healthcare devices, namely medical sensors, mobile computing devices, and wireless gateway access. Sensor nodes in healthcare are used directly in the body of patients to obtain physiological information. The medical team can retrieve the patent's data by the verified access of a wireless gateway [21].

A report from Price water- house Coopers' Health Research Initiative (HRI) in 2014 noted that nearly one-third of users who possess a wearable device use it daily, while privacy is one of the critical uneasiness of customers. Eighty-two percent of respondents were worried that wearable technologies would intrude on their privacy. Besides, to fully use these technologies in shaping the new health economy, it would be imperative to address consumers' privacy concerns. Thus, from an industrial perspective, there is an urgent need to examine the privacy of medical wearable technologies. The issue of data privacy plays a vital role in shaping the intention of patients to adopt health information technology (HIT). This is because of the more significant health information sensitivity [22].

Another smart health usage is found in smartphone health applications. The extensive use of smartphones for monitoring healthcare is susceptible to patient data privacy. In fog and cloud computing, personal health data privacy concerns are reported, and patients express ambivalence about third-party companies' data security. Privacy can be achieved with the implementation of regulations and policies. Privacy means only authorized users can access the patient's health information and in which situation patient data might be accessed, utilized, and disclosed to a third-party [23]. These authors report a three-layer e-Health architecture of patients and caregivers where the three layers are: back end, communication layer, and front end, as displayed in Figure 4.

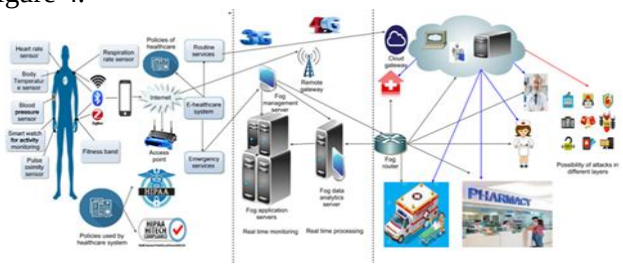

Fig. 4 The basic architecture of healthcare in smart city

Table 1 Summary of healthcare studies

Service used	The function	Privacy issue	Reference
Smart-Health Application	The developed application assists patients with special conditions such as respiratory ailments and babies.	Identity privacy, Query privacy, Location privacy, Owner privacy, and Footprint privacy	[19]

Service used	The function	Privacy issue	Reference
Smart In-Home Emergency Health Service (SIHEHS)	The system is used for in-Home Patients to take care of older people through smart technologies.	Unauthorized access, Unauthorized sharing, Unauthorized use, Unauthorized collection, Insecure storage, and Insecure transmission	[20]
Internet of Medical Things (IoM) application system.	The developed system is used to analyses health performance and security issues with the following compositions: system database, medical sensors, medical practitioner/professional, server, gateway, and patient.	The privacy protection and security of health data	[21]
Location privacy protection system (Trusted Third Party)	The system is used for the collection of data about patients' location	Location privacy	[24]
Privacy-Aware Smart Health Access Control System (PASH)	The system is built to solve user privacy and data security issues by incorporating smart health cloud (SHC) to keep smart-health records (SHRs)	Attribute privacy, Decryption test efficiency, Expressiveness, and full security	[25]
Smart Health Devices Integration	An integrated privacy scheme to upgrade preservation of privacy together with computing similarity without exposing sensitive information.	Privacy during access and authentication Data access control Privacy preservation	[26]
Healthcare wearable devices	The device is used to minimize healthcare costs and improve the efficiency of healthcare delivery.	Personal information privacy	[22]
Healthcare 4.0	Healthcare 4.0 keeps and monitors the patient's record through implantable medical devices (MDs) and wearable devices (WDs)	Privacy and security issues	[23]

3. Related Works

In this section, the researcher will discuss previous studies related to the individuals' information privacy perceptions and their intention to adopt smart city services. Most of these studies are recent, and they were extracted from several databases such as Science Direct, Scopus, IEEE, and google scholar. The researcher first extracted studies about acceptance and adoption models in smart cities, followed by studies on privacy in different areas such as e-commerce, wearable devices, and social network sites, as shown in Table 2 summary of related work studies. The study proposed model will be based on the literature.

3.1. Models of Acceptance and Adoption in Smart Cities

Park [27] examines the important factors affecting individuals' intention to use smart services using a model, principally developed through the expectation-confirmation model (ECM) and the technology acceptance model (TAM). The study reveals the effect of individual confirmation on perceived enjoyment, usefulness, and ease of use but not satisfaction. The confirmation indirectly affects satisfaction via perceived enjoyment, usefulness and ease of use, and user acceptance of hedonic information systems. These results indicate that individuals have more hedonic and utilitarian values when users' expectations are established at smart devices usage. Subsequently, the positive relationship between the values accounts for more individual intention and satisfaction of smart services [27].

Another study by Gunawan and Smart [28] sought to find factors affecting the adoption of smart city services in the local government area of Yogyakarta. However, the city administrators have not carried out an empirical study on the perception of Yogyakarta people and their readiness to use the service. Using the Unified Theory of Acceptance and Use of Technology (UTAUT) model, the study found that the level of trust and familiarity with the system affect citizens' eagerness toward the smart city. Other factors such as social influence and facilitating conditions do not affect people's intention toward smart city services. Therefore, the study concludes that the most important factor determining people's adoption rate is the ease of use of smart city devices [28].

The study of Sepasgozar *et al.* [29] delved into the cultural dimension for future smart cities developments. The authors posit that the first task in developing a smart city is to select culturally aligned devices, followed by technology adaptation, and management of technology acceptance is the final and difficult task [29]. Structural equation modeling was used to explore further the technology acceptance. The study found that relative compatibility and advantage factors, operation, work facilitation, and self-efficacy played important roles in users' intention to adopt smart city services. By developing Urban Services Technology Acceptance Model (USTAM) through a rigorous process, urban communities with heterogeneous cultural attributes and identities can use the model.

According to Manfreda *et al.* [30], smart city development relies majorly on technological trends. Their work highlighted the importance of factors affecting smart mobility. Autonomous vehicles' perceived benefits are important in the adoption of the technology. However, the autonomous vehicle perceived security challenges do not influence peoples' intention to adopt the vehicle [30].

Shuhaiber and Mashal [31] have explored key elements influencing residents' smart home usage and

acceptance by using TAM. Their results show that perceived trust, attitude towards use, and usefulness affect intention to adopt a smart home positively and significantly. Also, perceived usefulness is a function of perceived ease of use. Furthermore, perceived enjoyment, perceived ease of use, perceived usefulness, trust, and awareness significantly influence intention to use smart homes. Other explanatory variables have been found to have affected intention to use smart homes positively and significantly. For illustrative purposes, peoples' awareness of the smart home significantly influences their intention to adopt [31].

Buyle *et al.* [32] focused on the influence of decision-makers' attributes on their intention to adopt certain data records and description rules (data standards). The study finds key elements influencing altitude toward data standards usage and proposes implementation criteria for the data rules in government institutions. It is found that individual innovativeness positively influences individual altitude toward data standards. However, personal attributes do not affect the perceived ease of use and usefulness of data standards. By implication, the authors suggest that organizational bottleneck and network governance will play an important role in improving the adoption rate of data standards and possibly increase complex ecosystem interoperability [32].

Based Kim *et al.* [33] study aims to investigate the causal relationship between the cause and effect of the usefulness, informativeness, entertainment, accommodation capacity, and smart-environment technologies. A single model was developed by considering the interactions among the TAM, HAM, and smart TAM to verify the effects of advertising through mobile on the overall attitudes toward advertising. It was found that the entertainment did not impact the usefulness (perceived) nor the SDET significantly, indicating that the entertainment provided by the smartphone attenuates the entertainment provided by a mobile advertisement. The study also found that the attitude toward an advertisement is not affected by the perceived ease of use. However, the results revealed the effects of the perceived ease of use on the value of an advertisement and on the intention to use advertising. The value of an advertisement on the attitude toward the advertisement, and the attitude toward an advertisement on the intention to use the advertisement. Although their study showed that the perceived ease of use does not affect the attitude toward an advertisement, the influence of the perceived ease of use should not be neglected because the perceived ease of use may positively impact the overall attitude toward an advertisement [34].

Belanche-Gracia *et al.* [35] presented a theoretical model and developed security and privacy factors affecting citizens' intentions to use smartcards continuously. Their framework results show the extent to which people's concerns are important for smartcard service consolidation. First, their study does not support the hypothesis on the relationships between continuance intentions, perceived usefulness, and privacy. This has been said to be due to very limited personal information on the card. Another important justification could be because local administration directly manages local services with a high level of security standards other than being managed and controlled by private companies. Despite insignificant effects, public administrators are encouraged to uphold a high level of security standards service deliveries, given the sensitivity and amount of personal information collected, processed, and stored. Their results affirm people's perceptions of the smartcard as a system of payment that comes along with more financial applications and services. Hence, smartcard developers and city administrators are encouraged to ensure smartcard security for service optimization [35].

3.2. Models of Privacy in Different Domains

Balapour *et al.* [36] examined the effects of privacy-related perceptions, such as privacy policy effectiveness and privacy risk, on users' perceptions of mobile app security. They found perceived security to be negatively influenced by the perceived privacy risk of mobile apps. The perceived privacy policy effectiveness significantly affects users' perceived mobile app security. Privacy awareness perception has moderated the relationship between privacy risk perception and security of mobile apps perception. Based on the sensitivity of the information of the mobile apps, it is found that users perceived privacy-security differed [36].

Mohammed and Tejay [37] examined the moderating effect of national culture on the privacy of information and the adoption of e-commerce in developing countries. The authors argued that despite the economic development and technological advancement of a society, the national culture to be the key element in determining individuals' privacy of information and the adoption of e-commerce. They found that cultural background affects multiple factors, influencing individuals' attitudes towards e-commerce adoption and online transaction. However, society's cultural background does not affect individual privacy concerns. Overall, the perceived safety of the internet and acceptance of e-commerce strongly influence individuals' willingness to do online transactions. While cultural values do not influence privacy concerns, cultural values do impact other factors that influence the use of e-commerce [37].

Li *et al.* [22] developed a model based on the calculus theory of privacy to examine how healthcare wearable devices are adopted. The analyses of risk-benefit influence the decision of citizens to adopt healthcare wearable gadgets. Sensitivity to health information, legislative protection, perceived prestige, and personal innovativeness form individuals' privacy risk perceptions. The study found that their functional

congruence and informativeness perceptions influence peoples' benefit perceptions [10].

Fortes and Rita [38] proved that online purchase intentions reflect internet privacy concerns. The study on 900 online surveys found that internet privacy concerns negatively influenced individuals' perceptions of e-commerce. The study reported how risk perceptions were negatively impacted by trust concerning relationships between beliefs. Although ease of use perception positively affects usefulness perception, e-commerce use suffered from diverse beliefs [38].

Xu *et al.* [39] studied how privacy concerns can be reduced while maintaining an online social network and transactions. Information control and risk perception were found to have positively impacted privacy concerns. While subjective norm, the sensitivity of the information and the level of privacy concern relationships were insignificant. Their results further elaborated the effects of risk perception orchestrated by the data breach, unapproved leakage of personal data leakage has devastating effects on individual privacy concerns. Another interesting finding from their work is that, unlike privacy concerns, perceived benefits proved to be a key element in determining the behavior of individuals on personal information self-disclosure [39].

Table 2 Summary of related work

No	Authors	Model Used	Factors to Examine	Findings
1	[20]	ECM &TAM.	Satisfaction, confirmation, service and system quality, perceived ease of use, enjoyment, usefulness, flow state, cost	These results indicate that individuals have more hedonic and utilitarian values when users' expectations are established at smart devices usage. Subsequently, the positive relationship between the values accounts for more individual intention and satisfaction of smart services.
2	[36]	CPM theory	Perceived privacy, perceived effectiveness perceived security, privacy awareness, information sensitivity	Privacy awareness perception has moderated the relationship between privacy risk perception and security of mobile apps perception. Based on the sensitivity of the information of the mobile apps, it is found that users perceived privacy-security differed. .
3	[28]	UTAUT	Performance Expectancy, Facilitating Conditions, Social Influence Effort Expectancy	The study concludes that the most important factor determining people's adoption rate is the ease of use of smart city devices.
4	[29]	TAM & SCT	Security Perception, Ease of use Perception, Relative advantages, Usefulness Perceived, Reliability, Compatibility, Quality Services, Self-efficacy, facilitated work, Cost reduction, Energy-saving, Time-saving.	The study found that relative compatibility and advantage factors, operation, work facilitation, and self-efficacy played important roles in users' intention to adopt smart city services.
5	[30]	TAM & UTAUT	AV adoption, Technologically minded individuals, legal and Technological concerns, Societal and personal benefits, Mobility efficiencies, Security and safety concerns	Their work highlighted the importance of factors affecting smart mobility. Autonomous vehicles' perceived benefits are important in the adoption of the technology.
6	[31]	TAM	Usefulness perception, Ease of use perception, Intention to use, Attitude toward use, Trust, Awareness, Risk, and enjoyment perception	Perceived enjoyment, perceived ease of use, perceived usefulness, trust, and awareness significantly influence intention to use smart homes. Other explanatory variables have been found to have affected intention to use smart homes positively and significantly.
7	[32]	TAM & TRI	Discomfort, Perceived ease of use, Optimism, Perceived innovativeness, Usefulness of data insecurity, intention to use data	It is found that individual innovativeness positively influences individual altitude toward data standards. However, personal attributes do not affect the perceived ease of use and usefulness of data standards.
8	[37]	privacy calculus model & TAM	Perceived Safety, E-commerce acceptance, Privacy concerns, Personal interest, Willingness to transact	They found that cultural background affects multiple factors, influencing individuals' attitudes towards e-commerce adoption and online transaction. However, society's cultural background does not affect individual privacy concerns.
9	[33]	TAM & HAM	Entertainment, Informative, Ease of use perceptions, Perceived usefulness, Smart environments, Mobile advertising value, Mobile advertising attitude, Intention to adopt	The results revealed the effects of the perceived ease of use on the value of an advertisement and on the intention to use advertising. The value of an advertisement on the attitude toward the advertisement, and the attitude toward an advertisement on the intention to use the advertisement.
10	[22]	Privacy calculus theory	Sensitivity health information, Personal innovativeness, Legislative protection, Prestige Perceptions, In informativeness Perceptions, Functional congruence, Privacy risk Perceptions, Benefit Perceptions, Adoption intention, Actual	The study found that their functional congruence and informativeness perceptions influence peoples' benefit perceptions.

No	Authors	Model Used	Factors to Examine	Findings
			adoption behavior	
11	[38]	TPB and TAM	Trust, Privacy concerns, Risk Perceptions, Usefulness Perceptions, Ease of Use Perceptions, Control Perceptions, attitude towards, intention to use EC	The study on 900 online surveys found that internet privacy concerns negatively influenced individuals' perceptions of e-commerce. The study reported how risk perceptions were negatively impacted by trust concerning relationships between beliefs.
12	[35]	TAM	Security, Ease-of-use, Usefulness perceptions, Privacy, Continuance intentions	Their study does not support the hypothesis on the relationships between continuance intentions, perceived usefulness, and privacy. This has been said to be due to very limited personal information on the card. Another important justification could be because local administration directly manages local services with a high level of security standards other than being managed and controlled by private companies.
13	[39]	Privacy calculus theory & TPB	Information Control, Trust and Privacy Concerns, Privacy Sensitivity, Subjective Norm, Privacy Risk	Their results further elaborated the effects of risk perception orchestrated by the data breach, unapproved leakage of personal data leakage has devastating effects on individual privacy concerns.

4. The Proposed Model Development

Through this section, the researcher will explain the steps that would be followed to develop the proposed model through theories and extensive literature reviewed in the previous section:

4.1. Theories Selections

4.1.1. Technology Acceptance Model (TAM)

TAM is one of the most popular and widely used models in the literature for explaining and predicting individual acceptance and usage behaviors toward new technology. In TAM, four key constructs always deployed are ease-of-use perception, usefulness perception, intention to use, and actual use [40]. The main aim of TAM is to allow the decision-makers to know the potential impact of some external factors on the individual attitude, beliefs, and intentions to use new technology [41]. Figure 5 displays the conceptual model of TAM.

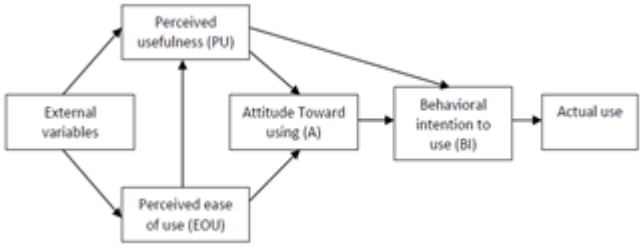

Fig. 5 Technology acceptance model [42]

4.1.2. Unified Theory of Acceptance and Use of Technology (UTAUT) Model

The UTAUT model is defined as a model used to understand the individual intention to accept new information technology [42]. UTAUT model is developed by combining eight existing models. The combined model is Theory of Planned Behavior (TPB), Social Cognitive Theory (SCT), Theory of Reasoned Action (TRA), Innovation Diffusion Theory (IDT) and TPB (C-TAM-TPB), Model of PC Utilization (MPCU), Motivational Model (MM), and TAM. UTAUT model has four variable factors that are key elements of acceptance and use [28]. The social Influence factor and UTAUT conceptual model used in this study are shown in Figure 6.

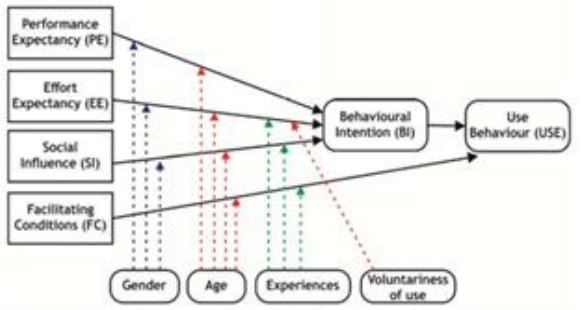

Fig. 6 UTAUT model

4.1.3. Privacy Calculus Theory (PCT)

PCT is believed as one of the most widely used frameworks to investigate contemporary perceived privacy. The calculus information privacy perspective handles the combined effects of benefits perceptions and perceived risks on privacy and privacy-protective behaviors [43]. PCT theory posits that the privacy concept cannot be viewed in isolation but rather seen from economic terms. Users from the model viewpoint can, at the same time, have beliefs that are strong about information disclosure on benefits and costs [44]. Individuals usually behave in ways to minimize negative results and maximize positive results. Users can disclose information in return for specific social and economic benefits with the pre-conditions that their data will be used judiciously, without future negative consequences. Loss of privacy with information disclosure is allowable so far that it guarantees certain benefits, and the level of risk is minimal [43]. Among the most important factors contained in PCT and will be used in this study are privacy concerns, risk perceptions, and trust, shown as in Figure 7.

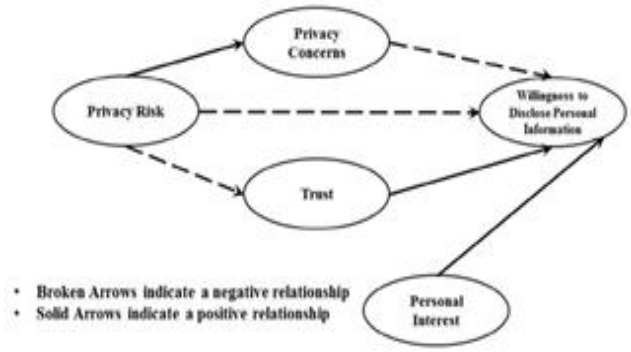

Fig. 7 Extended privacy calculus model [44]

4.2. Selection Factors

Factors in previous studies do have similarities. For instance, in the UTAUT model, there are similar factors among several models combined to develop UTAUT. Morris *et al.* [40] summarize the factors considered the same or similar [40]. Table 3 shows the root constructs that have been adopted by Venkatesh *et al.* [42] in UTAUT model development.

Table 3 The root factors of UTAUT model

#	Factors	Root Constructs
1	Performance expectancy	Relative advantage, Extrinsic motivation, Usefulness perceptions, Job-fit,
2	Effort expectancy	Easy to use perceptions, Complexity
3	Social influence	Social factors, Subjective norm, Image
4	Facilitating Conditions	Behavioral control perceptions, Compatibility, Facilitating conditions.

This study will consider factors similarity, as discussed earlier, in line with extant literature. Therefore, Table 4 displays the factors with their sources and their similarities. These factors will be used to develop the conceptual model of this study. The choice of the factors is also based on the privacy calculus theory, the UTAUT, and the theory of the TAM.

Social influence is adopted from UTAUT, WHILE Usefulness and ease of use are taken from TAM, and privacy concerns, privacy risk, and trust from the extended privacy calculus model. Other variables include perceived security, information sensitivity, privacy awareness, intention to adopt smart city services, and actual adoption of smart city services from related works. The cultural norm is a factor that was extracted from previous studies. Since cultural beliefs differ from one country to another [37], and since this study will be applied in Oman, this factor must be added and tested on privacy concerns.

Table 4 Factor with similar functions

	Factors	Frequency	Similar function/meaning	Sources
1	Perceived Security	2	Insecurity, security, safety, Safety perceptions	[32], [37]
2	Perceived Usefulness	7	Relative advantages, Services quality, Self-efficacy, Personal interest, Perceived benefit, Service and system quality, Satisfaction, Perceived effectiveness, Performance, Expectancy, Mobility-related efficiencies, Technologically minded individuals	TAM
3	Ease of Use Perceptions	7	Enjoyment perceptions, Enjoyment, Confirmation, Effort Expectancy	TAM
4	Social Influence	1	Subjective Norm, Personal and societal benefits	UTAUT
5	Trust	3	Optimism	[45]
6	Privacy Risk	2	Perceived risk, Perceived privacy risk	PCT
7	Information Sensitivity	2	Health information sensitivity, Privacy Information Sensitivity	[22], [39]
8	Cultural Norm	-	-	[37]
9	Privacy Awareness	1	Awareness	[31]
10	Privacy Concerns	3	Perceived privacy, technological and legal concerns, concerns, privacy, discomfort	[30], [45]
11	Intention to adopt	2	Intention to use data, Willingness to transact, Intention to use mobile advertising, intention to use e-commerce	TAM [37]
12	Actual adoption	1	-	[22]

Figure 8 illustrates the proposed model that the researcher relied on to extract the variables. First: the theories used, which are UTAUT, PCT, and TAM. Secondly: extract some variables from the literature review and studies related to this research. Table 5 displays the classification of variables.

Table 5 Classification of variables

Independent variables	Mediator	Dependent variable
Perceived Security Perceived Usefulness Ease of Use Perceptions Social Influence Trust Privacy Risk Information Sensitivity Cultural Norm Privacy Awareness	Intention to adopt Privacy Concerns	Actual adoption

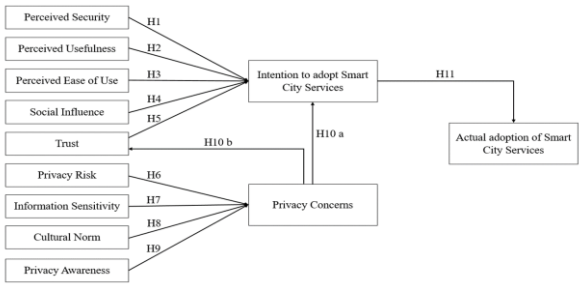

Fig. 8 Proposed model

5. Conclusion

This study addressed privacy in the healthcare domain, especially wearable medical devices services in smart cities, to propose a model that would increase the

adoption rate with different security policies that may require new data and information privacy. Researchers believe an unresolved privacy issue in smart cities is based on recent studies in the last few years. They also recommended the need for further studies on this challenge. It is revealed in the literature that there are insufficient privacy studies in smart cities from the users' perspectives, most of the available studies are technical studies, and there is little privacy model for smart city services. Therefore, this study intends to find out factors affecting individual privacy perception adopting smart city services, a behavior that may threaten the future of smart cities.

This paper determined the research problem by analyzing previous studies and determining the issues and factors from reviewing the literature. The outputs of this stage are the generic model for this study. It also provides an in-depth literature review of the privacy challenges of the smart city and privacy in Healthcare Services and related work in which the researcher discussed previous studies related to individuals' perceptions about the privacy of their information and their intention to adopt smart city services. The proposed model that the researcher relied on two ways to extract the variables, first: about the theories used, which are UTAUT, PCT, and TAM. Secondly: extract some factors from the literature review and studies related to this research. About selection of factors, factors in previous studies do have similarities. For instance, in the UTAUT model, there are similar factors among several models combined to develop UTAUT. Therefore, this study considered factors similarity and frequency extracted from the related studies discussed earlier. For all the factors extracted from the related studies, the result was twelve factors: Social influence is adopted from UTAUT, while usefulness and ease of use are taken from TAM, privacy concerns, privacy risk, and trust from the extended privacy calculus model. Other factors include perceived security, information sensitivity, privacy awareness, intention to adopt smart city services, and actual adoption of smart city services from related works. The cultural norm is a factor that was extracted from previous studies. Since cultural beliefs differ from one country to another, and since this study will be applied in Oman, this factor must be added and tested on privacy concerns. Finally, we have presented the adopted factors in this study and the proposed generic model.

As previously mentioned by the researcher that the smart city services like wearable devices are still under study in the health complex and were not applied until now in reality. Therefore, the researcher was assumed that these devices were present for the sample participating in the study, but in reality, they did not use yet, so it could affect the result slightly, so the study was done on the employees who participated who had undergone the program of Digital Foundations for Public Services. Eventually, this study should be repeated after these services are applied in the health complex, and it may also include information security and privacy and the extent of their impact on the local community in Oman. Also, this study can be used in other countries that differ from Oman in terms of customs and traditions, and it has its policy and orientations regarding the adoption of smart city services, with the use of other methodological methods such as the qualitative method and the results may be significant in the research field.

References

[1] LAM, P.T.I., and MA, R. Potential pitfalls in developing smart cities and mitigation measures: An exploratory study. *Cities*, 2017, 91(December): 146–156.

[2] IEEE. *Smart Cities*, 2015.

[3] SMART CITIES COUNCIL. *Smart City Definitions and Overviews*, 2014.

[4] IHS TECHNOLOGY. *Smart Cities to rising Fourfold in Number from 2013 to 2025*, 2014.

[5] YEH, H. The effects of successful ICT-based smart city services: From citizens' perspectives. *Government Information Quarterly*, 2017, 34(3): 556–565.

[6] GHARAIBEH, A. Smart cities: A survey on data management, security, and enabling technologies. *IEEE Explore*, 2017, 19(4): 2456–2501.

[7] VAN ZOONEN, L. Privacy concerns in smart cities. *Government Information Quarterly*, 2016, 33(3): 472–480.

[8] MCCLUSKEY, S., ECKHOFF, D., and WAGNER, I. Privacy in the Smart City - Applications, Technologies, Challenges, and Solutions. *IEEE Explore*, 2017, 19(1): 2456–2501.

[9] ALEISA, N., and RENAUD, K. Privacy of the Internet of Things: A Systematic Literature Review. *Proceedings of the 50th Hawaii International Conference on System Sciences*, 2017: 1–10.

[10] MARAKHIMOV, A., and JOO, J. Computers in Human Behavior Consumer adaptation and infusion of wearable devices for healthcare. *Computers in Human Behavior*, 2017, 76: 135–148.

[11] MA, R., LAM, P.T.I., and LEUNG, C.K. Potential pitfalls of smart city development: A study on mobile parking applications (apps) in Hong Kong. *Telematics and Informatics*, 2018, 35(6): 1580–1592.

[12] SOOKHAK, M., TANG, H., HE, Y., and YU, F.R. Security and Privacy of Smart Cities: A Survey, Research Issues, and Challenges. *IEEE Communications Surveys & Tutorials*, 2019, 21(2): 1718–1743.

[13] SOOKHAK, M., TANG, H., and YU, F.R. Security and Privacy of Smart Cities: Issues and Challenge. *Proceedings of the 20th IEEE International Conference on High-Performance Computing and Communications; 16th IEEE International Conference on Smart City; 4th IEEE International Conference on Data Science and Systems, HPCC/SmartCity/DSS*, 2019: 1350–1357.

[14] BRAUN, T., FUNG, B.C.M., IQBAL, F., and SHAH, B. Security and privacy challenges in smart cities. *Sustainable Cities and Society*, 2018, 39(August): 499–507.

[15] SYMANTEC. Internet security threat report. *Network Security*, 2016, 21(2): 1–3.

[16] PETERS, F., HANVEY, S., VELURU, S., MADY, A.E.D., BOUBEKEUR, M., and NUSEIBEH, B. Generating

Privacy Zones in Smart Cities. *The Fourth IEEE Annual International Smart Cities Conference (ISC2 2018)*, 2019: 1–8.
[17] CUI, L., XIE, G., QU, Y., GAO, L., and YANG, Y. Security and privacy in smart cities: Challenges and opportunities. *IEEE Access*, 2018, 6(February): 46134–46145.
[18] ATI, M., and BASMAJI, T. Framework for managing smart cities security and privacy applications. *ISCAIE 2018 - 2018 IEEE Symposium on Computer Applications and Industrial Electronics*, 2018: 191–194.
[19] DING, D., CONTI, M., and SOLANAS, A. A smart health application and its related privacy issues. *Proceedings 2016 Smart City Security and Privacy Workshop*, 2016: 11–15.
[20] ALGHANIM, A.A., RAHMAN, S.M.M., and HOSSAIN, M.A. Privacy Analysis of Smart City Healthcare Services. *Proceedings of 2017 IEEE International Symposium on Multimedia*, 2017, (January): 394–398.
[21] DEEBAK, B.D., AL-TURJMAN, F., ALOQAILY, M., and ALFANDI, O. Special Section on Security and Privacy in Emerging Decentralized an Authentic-Based Privacy Preservation Protocol for Smart e-Healthcare Systems in IoT. *IEEE Access*, 2019, 7: 135632–135649.
[22] LI, H., WU, J., GAO, Y., and SHI, Y. Examining individuals' adoption of healthcare wearable devices: An empirical study from a privacy calculus perspective. *International Journal of Medical Informatics*, 2016, 88(555): 8–17.
[23] HATHALIYA, J.J., and TANWAR, S. An exhaustive survey on security and privacy issues in Healthcare 4.0. *Computer Communications*, 2020, 153(January): 311–335.
[24] NATGUNANATHAN, I., MEHMOOD, A., XIANG, Y., and MEMBER, S. Location Privacy Protection in Smart Health Care System. *IEEE Internet of Things Journal*, 2019, 6(2): 3055–3069.
[25] ZHANG, Y., ZHENG, D., and DENG, R.H. Security and Privacy in Smart Health: Efficient Access Control. *IEEE Internet of Things Journal*, 2018, 5(3): 2130–2145.
[26] LIU, H., YAO, X., YANG, T., and NING, H. Cooperative Privacy Preservation for Wearable Devices in Hybrid Computing-Based Smart Health. *IEEE Internet of Things Journal*, 2019, 6(2): 1352–1362.
[27] PARK, E. User acceptance of smart wearable devices: An expectation-confirmation model approach. *Telematics and Informatics*, 2020, 47(October).
[28] GUNAWAN, H., and SMART, A. Identifying Factors Affecting Smart City Adoption Using the Unified Theory of Acceptance and Use of Technology Method. *2018 International Conference on Orange Technologies*, 2019: 1–4.
[29] SEPASGOZAR, S.M.E., HAWKEN, S., SARGOLZAEI, S., and FOROOZANFA, M. Implementing citizen-centric technology in developing smart cities: A model for predicting the acceptance of urban technologies. *Technological Forecasting and Social Change*, 2019, 142(December): 105–116.
[30] MANFREDA, A., LJUBI, K., and GROZNIK, A. Autonomous vehicles in the smart city era: An empirical study of adoption factors important for millennials. *The International Journal of Information Management*, 2019, March: 102050.
[31] SHUHAIBER, A., and MASHAL, I. Understanding users' acceptance of smart homes. *Technology in Society*, 2019, 58(January): 101110.
[32] BUYLE, R., VAN COMPERNOLLE, M., VLASSENROOT, E., VANLISHOUT, Z., MECHANT, P., and MANNENS, E. Technology readiness and acceptance model' as a predictor for the use intention of data standards in smart cities. *Media and Communication*, 2018, 6(4): 127–139.
[33] KIM, Y.B., JOO, H.C., and LEE, B.G. How to forecast behavioral effects on mobile advertising in the smart environment using the technology acceptance and web advertising effect models. *KSII Transactions on Internet and Information Systems*, 2016, 10(10): 4997–5013.
[34] KIM, Y.B., JOO, H.C., and LEE, B.G. How to Forecast Behavioral Effects on Mobile Advertising in the Smart Environment using the Technology Acceptance Model and Web Advertising Effect Model. *KSII Transactions on Internet and Information Systems*, 2016, 10(10): 4997–5014.
[35] BELANCHE-GRACIA, D., CASALÓ-ARIÑO, L.V., and PÉREZ-RUEDA, A. Determinants of multi-service smartcard success for smart cities development: A study based on citizens' privacy and security perceptions. *Government Information Quarterly*, 2015, 32(2): 154–163.
[36] BALAPOUR, A., NIKKHAH, H.R., and SABHERWAL, R. Mobile application security: Role of perceived privacy as the predictor of security perceptions. *The International Journal of Information Management*, 2020, November: 102063.
[37] MOHAMMED, Z.A., and TEJAY, G.P. Examining privacy concerns and eCommerce adoption in developing countries: The impact of culture in shaping individuals' perceptions toward technology. *Computers & Security*, 2017, 67: 254–265.
[38] FORTES, Z., and RITA, P. Privacy concerns and online purchasing behavior: Towards an integrated model. *European Research on Management and Business Economics*, 2016, 22(3): 167–176.
[39] XU, F., MICHAEL, K., and CHEN, X. Factors affecting privacy disclosure on social network sites: an integrated model. *Electronic Commerce Research*, 2013: 151–168.
[40] MORRIS, M.G., HALL, M., DAVIS, G.B., DAVIS, F.D., and WALTON, S.M. User Acceptance of Information Technology: Toward a Unified View. *Institutions & Transition Economics: Microeconomic Issues eJournal*, 2003, 27(3): 425–478.
[41] MARCHEWKA, J.T., LIU, C., and KOSTIWA, K. An Application of the UTAUT Model for Understanding Student Perceptions Using Course Management Software. *Communications of the IIMA*, 2007, 7: 10.
[42] VENKATESH, V., MORRIS, M.G., and DAVIS, F.D. User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 2003, 27(3): 425-478.
[43] LAUFER, R.S., and WOLFE, M. Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory. *Journal of Social Issues*, 1977, 33: 22-42.
[44] DINEV, T., and HART, T.P. Privacy Concerns and Levels of Information Exchange: An Empirical Investigation of Intended e-Services Use. *e-Service Journal*, 2006, 4: 25-59.
[45] PARASURAMAN, A. Technology Readiness Index (TRI) is a multiple-item scale to measure readiness to embrace new technologies. *Journal of Service Research*, 2000, 2(4).

参考文:

[1] LAM, P.T.I., 和 MA, R. 智慧城市發展中的潛在陷阱和緩解措施：一項探索性研究。城市，2017，91（十二月）：146-156。

[2] 电气与电子工程师协会。智慧城市，2015。

[3] 智慧城市委員會。智慧城市定義和概述，2014。

[4] 国际健康保险协会技術。從 2013 到 2025，2014，智慧城市的數量將增加四倍。

[5] YEH, H. 成功的基於 信息通信技術的智慧城市服務的影響：從公民的角度。政府信息季刊，2017，34(3)：556–565。

[6] GHARAIBEH, A. 智慧城市：關於數據管理、安全和支持技術的調查。电气与电子工程师协会探索，2017，19(4)：2456–2501。

[7] VAN ZOONEN, L. 智慧城市中的隱私問題。政府信息季刊，2016，33(3)：472–480。

[8] MCCLUSKEY, S.、ECKHOFF, D., 和 WAGNER, I. 智能城市中的隱私 - 應用、技術、挑戰和解決方案。 电气与电子工程师协会探索，2017，19(1)：2456–2501。

[9] ALEISA, N., 和 RENAUD, K. 物聯網隱私：系統文獻綜述。第 50 屆夏威夷國際系統科學會議論文集，2017：1-10。

[10] MARAKHIMOV, A., 和 JOO, J. 人類行為中的計算機消費者適應和可穿戴設備註入醫療保健。人類行為中的計算機，2017，76：135-148。

[11] MA, R., LAM, P.T.I., 和 LEUNG, C.K.智慧城市發展的潛在陷阱：關於香港停車移動應用程序（應用程序）的研究。遠程信息處理和信息學，2018，35（6）：1580-1592。

[12] SOOKHAK, M.、TANG, H.、HE, Y., 和 YU, F.R.智慧城市的安全和隱私：調查、研究問題和挑戰。 人類行為中的計算機通信調查與教程，2019，21(2)：1718–1743。

[13] SOOKHAK, M.、TANG, H., 和 YU, F.R.智慧城市的安全和隱私：問題和挑戰。第 20 屆人類行為中的計算機高性能計算與通信國際會議論文集；第 16 屆人類行為中的計算機智慧城市國際會議；第四屆 人類行為中的計算機數據科學與系統國際會議，2019：1350–1357。

[14] BRAUN, T.、FUNG, B.C.M.、IQBAL, F., 和 SHAH, B. 智慧城市中的安全和隱私挑戰。可持續城市與社會，2018，39（八月）：499-507。

[15] 賽門鐵克。互聯網安全威脅報告。網絡安全, 2016, 21(2): 1–3。

[16] PETERS, F.、HANVEY, S.、VELURU, S.、MADY, A.E.D.、BOUBEKEUR, M., 和 NUSEIBEH, B. 在智慧城市中生成隱私區。第四屆 电气与电子工程师协会年度國際智慧城市會議，2019：1-8。

[17] CUI, L., XIE, G., QU, Y., GAO, L., 和 YANG, Y. 智慧城市的安全與隱私：挑戰與機遇。电气与电子工程师协会訪問，2018，6 月（二月）：46134–46145。

[18] ATI, M., 和 BASMAJI, T. 管理智慧城市安全和隱私應用程序的框架。伊斯卡伊 2018 - 2018 电气与电子工程师协会計算機應用和工業電子研討會，2018：191–194。

[19] DING, D.、CONTI, M., 和 SOLANAS, A. 智能健康應用程序及其相關隱私問題。2016 年智能城市安全和隱私研討會論文集，2016：11-15。

[20] ALGHANIM, A.A. 、 RAHMAN, S.M.M., 和 HOSSAIN, M.A. 智慧城市醫療保健服務的隱私分析。2017 电气与电子工程师协会國際多媒體研討會論文集，2017，（1 月）：394–398。

[21] DEEBAK, B.D.、AL-TURJMAN, F.、ALOQAILY, M., 和 ALFANDI, O. 新興分散式安全和隱私特別部分為物聯網中的智能電子醫療保健系統提供了基於真實的隱私保護協議。 电气与电子工程师协会訪問，2019，7：135632–135649。

[22] LI, H., WU, J., GAO, Y., 和 SHI, Y. 檢查個人對醫療保健的採用可穿戴設備：從隱私演算角度進行的實證研究。國際醫學信息學雜誌，2016，88（555）：8-17。

[23] HATHALIYA, J.J., 和 TANWAR, S. 對醫療保健 4.0 中安全和隱私問題的詳盡調查。計算機通信，2020，153（一月）：311-335。

[24] NATGUNANATHAN, I.、MEHMOOD, A.、XIANG, Y., 和 MEMBER, S. 智能醫療保健系統中的位置隱私保護。 电气与电子工程师协会物聯網期刊，2019，6(2)：3055–3069。

[25] ZHANG, Y.、ZHENG, D., 和 DENG, R.H. 智能健康中的安全和隱私：高效訪問控制。 电气与电子工程师协会物聯網期刊，2018，5(3)：2130–2145。

[26] LIU, H., YAO, X., YANG, T., 和 NING, H. 基於混合計算的智能健康中可穿戴設備的合作隱私保護。 电气与电子工程师协会物聯網期刊，2019，6(2)：1352–1362。

[27] PARK, E. 用戶對智能可穿戴設備的接受度：一種期望-確認模型方法。遠程信息處理與信息學，2020，47（10 月）。

[28] GUNAWAN, H., 和 SMART, A. 使用統一的技術接受和使用理論識別影響智能城市採用的因素。2018 橙色技術國際會議，2019：1-4。

[29] SEPASGOZAR, S.M.E., HAWKEN, S., SARGOLZAEI, S., 和 FOROOZANFA, M. 在開發智慧城市中實施以公民為中心的技術：預測城市技術接受度的模型。技術預測與社會變革，2019，142（十二月）：105-116。

[30] MANFREDA, A.、LJUBI, K., 和 GROZNIK, A. 智慧城市時代的自動駕駛汽車：對千禧一代重要的採用因素的實證研究。國際信息管理雜誌，2019，3 月：102050。

[31] SHUHAIBER, A., 和 MASHAL, I. 了解用戶對智能家居的接受程度。社會技術, 2019, 58(1 月): 101110.

[32] BUYLE, R., VAN COMPERNOLLE, M., VLASSENROOT, E., VANLISHOUT, Z., MECHANT, P., 和 MANNENS, E. 技術準備和接受模型作為數據標準使用意圖的預測在智慧城市。媒體與傳播，2018，6(4)：127–139。

[33] KIM, Y.B., JOO, H.C., 和 LEE, B.G.如何利用技術接受模型和網絡廣告效果模型預測智能環境下移動廣告的行為效果。 國際汽聯互聯網和信息系統交易，2016，10(10)：4997–5013。

[34] KIM, Y.B., JOO, H.C., 和 LEE, B.G.如何使用技術接受模型和網絡廣告效果模型預測智能環境中移動廣告的行為效果。 國際汽聯互聯網和信息系統交易，2016，10(10)：4997–5014。

[35] BELANCHE-GRACIA, D.、CASALÓ-ARIÑO, L.V., 和 PÉREZ-RUEDA, A. 智慧城市發展中多服務智能卡成功的決定因素：一項基於公民隱私和安全認知的研究。政府信息季刊，2015，32(2)：154–163。

[36] BALAPOUR, A. 、NIKKHAH, H.R., 和 SABHERWAL, R. 移動應用程序安全性：感知隱私作為安全感知預測器的作用。國際信息管理雜誌，2020，11 月：102063。

[37] MOHAMMED, Z.A., 和 TEJAY, G.P. 檢查發展中國家的隱私問題和電子商務採用：文化在塑造個人對技術的看法方面的影響。計算機與安全，2017，67：254-265。

[38] FORTES, Z., 和 RITA, P. 隱私問題和在線購買行為：邁向集成模型。歐洲管理和商業經濟學研究，2016，22(3)：167–176。

[39] XU, F., MICHAEL, K., 和 CHEN, X. 影響社交網站隱私披露的因素：綜合模型。電子商務研究，2013：151-168。

[40] MORRIS, M.G.、HALL, M.、DAVIS, G.B.、DAVIS, F.D., 和 WALTON, S.M. 用戶對信息技術的接受：走向統一的觀點。制度與轉型經濟學：微觀經濟問題電子期刊，2003，27(3)：425–478。

[41] MARCHEWKA, J.T., LIU, C., 和 KOSTIWA, K. 使用課程管理軟件了解學生感知的 猶他州模型的應用。 國際醫學會通訊，2007，7:10。

[42] VENKATESH, V.、MORRIS, M.G., 和 DAVIS, F.D. 用戶對信息技術的接受：走向統一的觀點。 什麼季刊，2003，27(3)：425-478。

[43] LAUFER, R.S., 和 WOLFE, M. 作為概念和社會問題的隱私：多維發展理論。社會問題雜誌，1977，33：22-42。

[44] DINEV, T., 和 HART, T.P. 隱私問題和信息交換水平：預期電子服務使用的實證調查。電子服務雜誌，2006，4：25-59。

[45] PARASURAMAN, A. 技術準備指數是一種多項目量表，用於衡量接受新技術的準備情況。服務研究雜誌, 2000, 2(4)。