ACCSCIENCE PUBLISHING

Design+

ARTICLE

Privacy and security concerns shaping smart city adoption: Evidence from Qatar

Dana Ahmad Al-Ali[1]*, Nadarajah Manivannan[1†], Ziad Hunaiti[2], and Yanmeng Xu[1†]

[1]Brunel Design School, College of Engineering, Design and Physical Sciences, Brunel University of London, London, United Kingdom

[2]Department of Electronic and Electrical Engineering, College of Engineering, Design and Physical Sciences, Brunel University of London, London, United Kingdom

Abstract

Information security remains a significant concern for the adoption of smart cities (SCs) worldwide, particularly in relation to the development and implementation of digital ecosystems. SCs entail the interconnectedness of networks and systems that collect and process huge volumes of diverse data. This study analyzes the impact of data privacy and data security issues on the citizens' willingness to adopt smart city environments. A critical review of the existing literature was conducted regarding the relationship between data privacy and security concerns and the adoption of the smart city ecosystem. The data collected from two sample groups, experts and citizens, were analyzed using statistical techniques, including independent samples *t*-tests and correlation analysis. The findings indicate that citizens and experts had significantly different perceptions of the characteristics of SCs. Still, both groups exhibited a strong positive correlation between key adoption variables and citizens' readiness to accept SCs. Based on the findings, several recommendations are proposed to increase citizens' acceptance of SCs.

Keywords: Data privacy; Smart city; Smart governance; Concerns; Readiness

[†]These authors contributed equally to this work.

***Corresponding author:**
Dana Ahmad Al-Ali
(danaahmadsm.al-ali@brunel.ac.uk)

Citation: Al-Ali DA, Manivannan N, Hunaiti Z, Xu Y. Privacy and security concerns shaping smart city adoption: Evidence from Qatar. *Design+*.
doi: 10.36922/DP025110017

Received: March 11, 2025

1st revised: July 16, 2025

2nd revised: July 29, 2025

Accepted: August 25, 2025

Published online: September 23, 2025

1. Introduction

1.1. Smart city and privacy issues

The adoption of smart cities (SCs) by many countries worldwide has significantly increased research interest in the role of digital technology in enhancing urban environments. A "smart city" is defined as "an urban area that integrates the use of the latest technologies to conduct data collection processes, then optimizes data usage to expand service operations within a city and improve the quality of life of local citizens."[1] This process leverages information technologies, artificial intelligence (AI), and the internet of things (IoT) to facilitate real-time decision-making, foster innovation and leadership, and enable interaction between humans, machines, and the urban environment.[2] However, the definition of an SC varies considerably across the literature. Some definitions emphasize technological innovation, while others underscore governance, social inclusion, financial development, and environmental sustainability as key elements.[3] The research notes that SCs are inherently multidimensional, with varying

conceptualizations shaped by a city's level of development, local priorities, resources, and citizen aspirations.[3] This plurality of views suggests that the SC concept cannot be reduced to technology alone but must be understood as a holistic framework encompassing digital, social, environmental, and economic transformation.[4] Smart city ecosystems (SCEs) rely on complex technological infrastructures, including interconnected networks, sensors, data platforms, and applications, to deliver a range of services, such as transportation, energy management, environmental monitoring, healthcare, financial services, and public safety.[5] Given their reliance on massive volumes of personal and sensitive data, these ecosystems also present significant challenges for data governance and privacy protection.[6] Thus, the implementation of SCs must have a balance between technological innovation and ethical and regulatory considerations regarding transparency, accountability, and citizen rights.

However, the widespread deployment of these technologies also raises significant concerns around data security and user privacy. SC systems routinely collect and process sensitive personal data, including biometric identifiers, health records, real-time location data, financial transactions, video surveillance feeds, and communication logs.[7] This exposes users to potential risks, such as unauthorized access, profiling, data breaches, and other cybersecurity threats.[8,9] Studies have shown a negative relationship between increased digital adoption and citizen trust in data privacy.[7,10] These concerns present an ongoing challenge for governments and service providers, who must build and maintain secure, resilient, and citizen-centered SC environments that promote trust while delivering the intended benefits of sustainability, efficiency, and quality of life.

1.2. Research rationale

The government of Qatar has long encouraged the adoption of SCEs, envisioning the use of advanced technologies to provide critical and regular services to citizens, including substantive deployments in healthcare, transportation, smart housing, environmental protection, and the overall sustainability of the living environment.[11] The concept of the SC has gained significant traction in Qatar, particularly through several initiatives, such as Msheireb Downtown Doha and Lusail City, which are Qatar's flagship SC projects. These developments have received national visibility and been promoted through government campaigns and strategic urban planning aligned with Qatar National Vision 2030.[12] The popularity of SC concepts in Qatar is increasing, particularly in major urban centers, such as Doha and Lusail, where digital technologies are being integrated into transportation, surveillance, energy, and municipal services. The government of Qatar has long supported the adoption of SCEs, envisioning the use of advanced technologies to deliver critical and routine services to citizens.[12,13] These include major initiatives in healthcare, transportation, smart housing, environmental protection, and overall urban sustainability.[11] However, it has also been recognized that the success of such efforts depends significantly on how effectively data privacy, security, and confidentiality concerns are addressed; any breach in data security could reduce citizen trust and lead to underutilization of smart services.[9,10]

Currently, as SC deployments in Qatar approach relative operational maturity,[14] there is a pressing need to assess the actual on-the-ground progress from the perspective of stakeholders. This includes examining whether SCs in Qatar represent a practical urban transformation or merely serve as an "urban brand identity."[15] Thus, this study is warranted to explore perceptions of data privacy and security among the general public and experts involved in SC projects, especially given Qatar's position as a leading national case study. Furthermore, it aims to investigate how data security-related factors influence citizens' willingness to adopt the SCE. This research contributes to the growing body of work on cybersecurity and SC adoption.

1.3. Study aim and objectives

The primary objective of the study is to investigate the relationship between factors related to data security in SCs and willingness to accept SCE in the context of Qatar. In line with this aim, the study seeks to achieve the following specific research objectives:

(i) To establish the privacy and data security concerns related to SCs among citizens and experts.
(ii) To analyze citizens' and experts' readiness to adopt SCs.
(iii) To investigate the relationship between privacy and data security concerns on readiness to adopt SCs.

1.4. Significance of the study

This study has both theoretical and practical implications. In terms of theoretical contributions, this study addresses the need for new research on data security and privacy issues in the context of SCs in Qatar. In addition, this study contributes to theoretical research from the perspective of general citizens and experts on SC projects. In terms of practical contribution, this study has the potential to generate useful insights that can be adopted by administrators of SC projects in various stages of project management. The findings of this study identify the need for stakeholder participation to ensure that SCEs meet all the data privacy and security expectations of users.

2. Literature review

This section of the paper reviews existing research on the interrelationship between data privacy and security concerns, as well as the adoption of SCs. It also examines key factors influencing SC adoption, particularly in the Qatari context, where large-scale SC developments, such as Lusail and Msheireb, have driven the implementation of interconnected technologies. These projects highlight local concerns around data handling, digital surveillance, and cybersecurity. Furthermore, the section discusses how privacy and security concerns are currently addressed in the context of SC. Building on this literature, the study constructs a theoretical framework based on established models, such as the Unified Theory of Acceptance and Use of Technology (UTAUT), integrating variables, including performance expectancy, effort expectancy, and facilitating conditions, to analyze adoption behavior in Qatar.

2.1. Impact of data privacy and security issues on SCs adoption

SCs have the potential to significantly improve residents' quality of life. However, there are growing concerns regarding the adoption of smart applications due to their vulnerability to cybercrimes, such as data and identity theft, ransomware, spam attacks, and even international cyber warfare.[1,8,16-18] These concerns are particularly relevant in Qatar, where the centralization of data and the digitization of public services have raised questions about how securely citizen data is stored and used.[14] Table 1 summarizes the SCEs considered most at risk from cybersecurity threats, based on expert assessments across three dimensions: technical vulnerability, impact of a successful attack, and interest of nation-state attackers. In cases where multiple technologies share the same ranking, for example, four technologies receiving a score of 9 under "Interest of nation-state attackers," which indicates either an equivalent level of perceived threat or limited differentiating data, as assessed by experts. The table reveals that the highest risks are associated with emergency and security alert systems, where breaches could have severe and immediate consequences.

Figure 1 depicts the technological and systemic factors that shape cybersecurity in SCs. The convergence of information and operational technology provides the technological ecosystem necessary to control different systems, but it also expands the scope of vulnerability to cyber threats.[20,21] Interoperability pertains to the protocol that enables integration and data exchange between new digital technologies and legacy systems, often with particular vulnerabilities due to disparate technology platforms. Finally, the integration of SC services with various interconnected technologies usually presents the challenge of cascading effects and catastrophic failures due to vulnerabilities or cyber-attacks in one or more systems.[20] For example, research on European countries found that a common feature of SC is the smart mobility system, which relies on automated vehicles and technology-controlled transportation systems.[10]

Table 1. Expert assessment of the cybersecurity of smart city technologies.[19]

Technology type	Ranking		
	Technical vulnerability	Impact of a successful attack	Interest of nation-state attackers
Emergency and security alert systems	1	1	1
Street video surveillance	2	3	2
Smart traffic lights/signals	3	2	3
Water consumption tracking	4	6	5
Smart tolling	5	7	8
Public transit open data	8	9	9
Gunshot detection	7	4	9
Smart waste or recycling bins	8	9	9
Satellite water leak detection	9	8	9

Cyber-attacks on such systems have the potential to cause widespread damage and loss of lives. Similarly, for IoT sensors, security threats, such as data confidentiality, insecure communication, and interception and jamming of communication, are present during their deployment in an SC environment.[10,21] Another key aspect is the digitization of healthcare records to facilitate a smooth delivery of healthcare services.[20] However, this also presents a vulnerability to hacking or cyber theft of the personal and medical records of the individuals, thereby posing a serious concern regarding the resilience. Here, resilience is defined as the capacity of infrastructure to withstand, absorb, recover from, and adapt to adverse conditions or cyber disruptions.[22,23] These aspects have also been highlighted in academic literature as security threats when relying on a digital ecosystem, especially in a wide range of services in the SCEs.[9,23,24]

Some studies related to cybersecurity threats in the context of SCs also argue for the need for a well-defined regulatory framework that can deter threats to privacy and limit excessive collection of personal data.[25,26] For instance, the European Union's General Data Protection Regulation restricts the collection of personal data and the uses to which it can be put. The regulation aims to achieve a fair balance between the interests of users and technology solution providers.[25] However, there are also challenges arising from

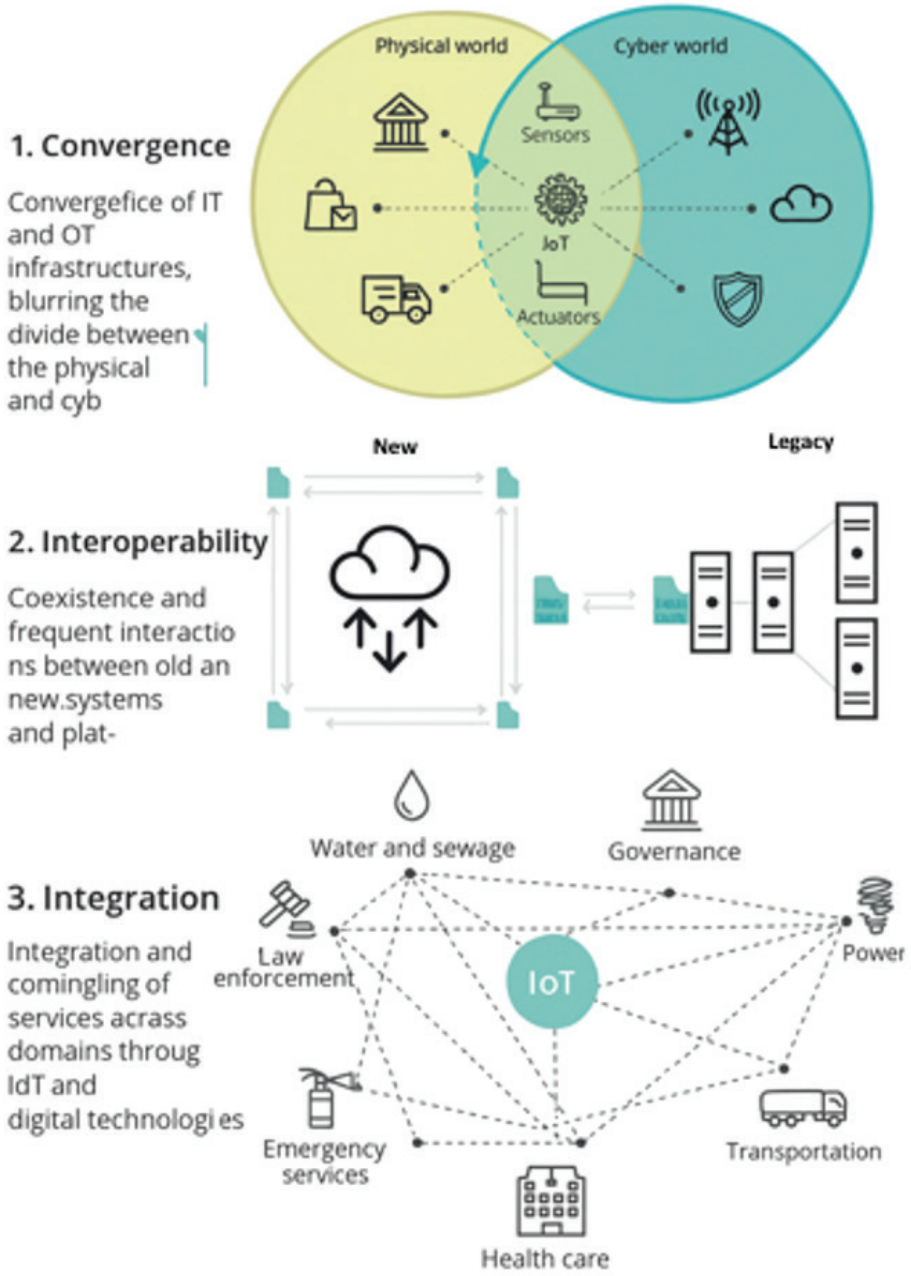

Figure 1. Key factors influencing cybersecurity in smart cities[20]
Abbreviations: IoT: Internet of Things; IT: Information technology; OT: Operational technology.

data collected by global positioning systems, cameras, and sensors, among other devices. These data collections pose a threat to individual privacy and expose them to malicious hackers.[26] Such challenges and threats are also present in smartphones used by citizens, which collect vast and far-reaching forms of personal and financial data that could be used for serious financial crimes, in addition to data theft.[5] Moreover, common standards that different countries can adopt to reduce privacy concerns are lacking.[23]

Consequently, it is challenging to determine the extent to which regulation and control are necessary and possible while using contemporary digital technologies, and it is becoming increasingly difficult for stakeholders in the SCE to establish consumer trust. In the case of Qatar, the National Cybersecurity Strategy has outlined specific regulatory mechanisms to manage these issues. These include mandatory risk assessments, incident reporting procedures, and security compliance standards

for organizations operating critical digital infrastructure.[14] Furthermore, Lusail SC initiatives are already implementing policy-led frameworks for data access, encryption, and operational transparency, thereby marking a practical move toward governance-led cybersecurity in Qatar's urban digital ecosystem.[14]

2.2. Key factors of smart city adoption related to information security

There has been considerable interest in the information security aspects in an SC context, in addition to the general use of systems. One of the key determinants for the adoption of SC services is the performance expectancy dimension, which refers to the individuals' level of belief in the extent to which using a system can be beneficial.[27,28] In the context of SCs, research on the performance expectancy of SC services in a mid-sized city in the south-eastern USA shows that it significantly affected app users' intentions to use services.[29] Research based on the UTAUT further notes that these benefits create performance expectations, which determine SC adoption.[30] Another key aspect related to performance expectancy is the scalability of services in an SC as the numbers of users increase.

In this regard, cloud services are needed to reduce reliance on physical servers while optimizing network, computing, and scalability requirements.[2] Bridging cloud and IoT can help administrators and architects of SC move to an integrated platform, offering seamless services in the SCEs.[2] The literature also shows that since most services of SCs in multiple disciplines, such as smart community, smart transportation, and smart healthcare, among others, have become data-driven, there is a need for higher processing power without compromising data integrity, scalability, and intelligent decision-making. Cloud computing fulfils these requirements and addresses the issue of information security.[31] However, it is also crucial that the technological architecture supports the adoption of cloud services and the integration of advanced technologies and data management.[22,24,32]

While scalability and performance issues can be addressed through rapid advances in technology, information security issues always remain at the forefront for users and the technology architects. In this regard, security and privacy concerns are quite common in the context of SC environments, primarily due to tools for monitoring the physical movement of citizens and the data collected while providing SC services. Such concerns can be addressed by increasing awareness of data security and privacy, as well as transparency within SCE governance.[33] There are also concerns that the interconnectedness of devices could facilitate unauthorized access, potentially leading to physical disruptions and bringing the entire connected infrastructure to a standstill.[9] Furthermore, advancements in technology, such as AI and IoT, have the potential to provide full connectivity and unprecedented improvements to human quality of life within the SCE but also raise challenges regarding security and privacy issues, thereby arguing the need for effective countermeasures.[21]

Another key aspect in the context of SC is the integrity of data, which refers to accuracy and validity.[34,35] The lack of data integrity defeats the purpose of interconnectedness of systems to provide an enhanced quality of services to citizens in an SC environment.[35] Hence, there is a need for SC projects to adopt advanced technologies, such as blockchain and big data frameworks, for processing data emanating from IoT devices. In addition, blockchain can be applied to provide a decentralized framework that records transactions, maintains data integrity, and enhances transaction efficiency through smart contracts.[34] Smart contracts are self-executing agreements coded on blockchain platforms that are generally considered trustworthy due to their transparency, immutability, and automation. They eliminate the need for third-party enforcement and reduce the risk of manipulation or fraud.[36]

Blockchain-based transactions in SCs also ensure data integrity and interoperability.[37] Furthermore, some analysts have recommended shifting to a decentralized big data auditing scheme for SC environments, which are driven by blockchain capabilities that can improve the reliability and stability of the systems, with additional benefits of lower computational costs.[38,39] Such systems not only reduce human interventions but also provide an accurate audit of the performance of AI data-driven analysis.

Effort expectancy is also crucial when exploring the adoption of SCs; it refers to the level of convenience for users when using any information system.[40] Study shows that effort expectancy significantly influences citizens' intention to use SCs.[30] The effort expectancy variable is a crucial component of UTAUT theory, wherein it has been reported that when users find a system convenient, they are more likely to use it regularly.[41,42]

Research on the adoption of AI-powered chatbots for public transport services in an Indian SC showed positive outcomes.[27] They observed that effort expectancy directly influenced the adoption intention of the chatbots, presenting a useful case for a convenient and user-friendly interface in availing daily-used services, such as transportation.[27] A study conducted in Malaysia also reported similar findings regarding the adoption of mobile healthcare applications, where the effort expectancy variable significantly influences the regular use of the mobile application.[43] These findings clearly highlight the

need to focus on the effort expectancy variable when designing public interface systems for higher adoption.

Another key factor is facilitating conditions, which refer to the extent to which an individual believes that the technical and organizational infrastructure can support the use of the system.[44] In the context of SCs, facilitating conditions can be enhanced by the use of advanced technologies, such as IoT, which help the administration to effectively process data and provide an interface for service delivery to citizens. Several studies acknowledged the need for a robust technological infrastructure that can mitigate risks to the system while providing efficient service delivery. However, studies conducted from the perspective of technology adoption have reported challenges in the facilitating conditions, considering the dynamic nature of the service delivery and the evolving ecosystem in the context of SCs.[44,45]

These challenges relate to privacy and data security, as well as scalability and interoperability.[45] The role of governance, along with technological infrastructure, has thus emerged as an effective measure of managing the challenges that arise in an SCE.[46] In addition, the behavioral intentions of adopting an information and communication technology (ICT) system play a crucial role in the success of adopting any ICT. In this case, behavioral intentions refer to the strength of any individual's intention to perform a behavior.[47] In the context of SCs, the behavioral intention to adopt services is dependent on various factors, such as ease of use, convenience, assurance of data privacy and security, trust in the system, facilitating conditions, and performance expectancy, among others.[48]

Research conducted in India found that perceived information and service quality influence the behavioral intentions of adoption of an ICT system in an SCE.[49] However, a counterargument is that even users who are aware of the different information systems and possess the requisite skills to use them express concerns regarding the utility, accessibility, security, and efficiency of SC services.[50] The findings are based on interdisciplinary SC research and highlight the need to address these factors to enhance the behavioral intentions of using SC services.

2.3. Addressing security and privacy concerns in SCs

The need to handle data from the perspectives of processing and security is one of the key challenges highlighted in several studies.[36,51,52] Researchers have proposed a new business model that integrates IoT with big data for data processing and analytics, enabling better informed decision-making in SC models.[36] Others have proposed using big data analytics when deciding and creating information technology (IT) infrastructure.[52] This approach ensures that SCs meet the needs of their inhabitants, with integrated systems that encompass smart home, water, and weather sensors, as well as surveillance equipment for data generation, collection, and analysis.[52]

However, evidence on the use of data analytics is often affected by challenges related to data collection and quality, the costs involved in data lifecycle management, as well as data security and privacy.[36] There are legitimate and serious concerns regarding these considerations, including the need to protect SC systems from malicious attacks or illegal access, which compromises individual rights and even the safety of city infrastructure.[36,51] A significant and growing body of research has focused on addressing such information security issues, and there have been various propositions on implementing security measures in an SC environment.

Researchers have mostly focused on the privacy of citizens, data security, and security measures in the interconnected networks.[35,53,54] Some commonly used measures for system security include biometric authentication, facial recognition, and multi-factor authentication.[19,46] While these measures are necessary, they are insufficient in themselves to copper-bottom SCE security in complex systems of interconnected networks. Figure 2 illustrates a comprehensive approach for SC data security and privacy, including SC conceptualization, security requirements, security challenges, privacy challenges, solutions and architectures, and open issues.

It can be seen from Figure 2 that the roadmap offers the benefit of providing an overarching framework, highlighting the different components of the technology ecosystem that require attention to prevent information security attacks, targeting systems and data. An additional layer of security can be imposed by utilizing blockchain technology, which can be integrated with smart devices to provide a secure communication platform.[56] However, it is also important to understand that the exponential rise in computing power brings about fundamental challenges that face the adoption of any system (e.g., financial costs), and there are increasingly critical potential vulnerabilities in increasingly vast systems, which can be exploited with malicious intent. The roadmap displayed in Figure 2 acknowledges the existential issues in this field, including secure data outsourcing, security risk management, and big data processing, all of which are integral parts of the SCE mix that need to be addressed to ensure robust security measures in SCs.[55,56]

2.4. Theoretical framework

The reviewed literature reveals that data privacy, information security, and network security are the main

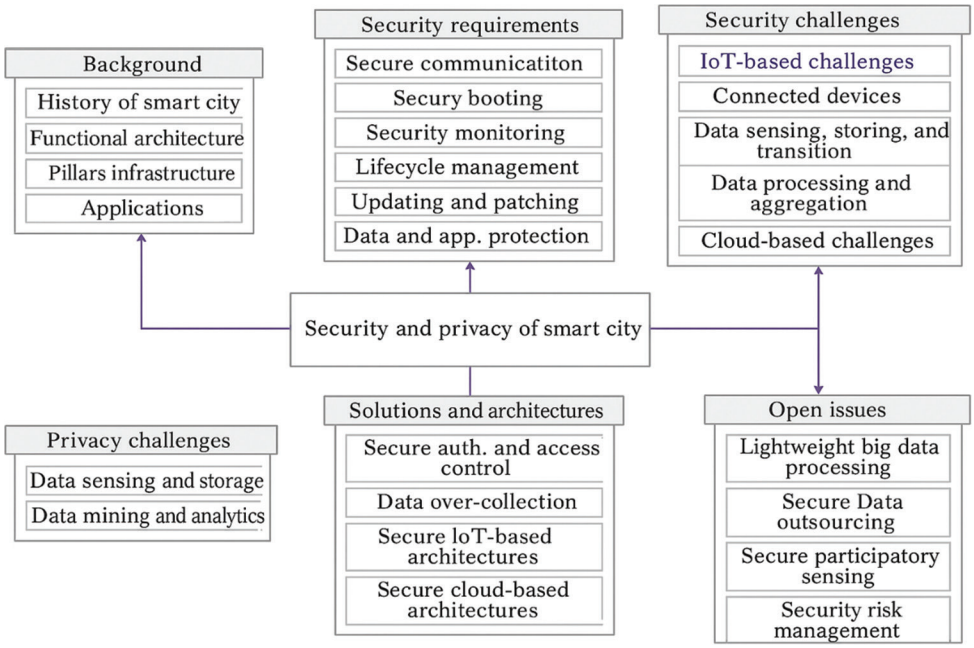

Figure 2. Roadmap for cybersecurity implementation in smart cities[55]
Abbreviations: Auth.: Authentication; IoT: Internet of things.

threats facing the technological ecosystem of SCs.[37,51,55] Specifically, these studies examine several dimensions of these threats, such as unauthorized access to personal data (privacy), system vulnerabilities and malware exposure (information security), and the susceptibility of interconnected communication networks to disruption or interception (network security). Moreover, ICT-related factors, such as effort expectancy, performance expectancy, and facilitating conditions, also play a crucial role in determining the adoption of the SC.[57] These factors are identified as independent variables, and their influence will be studied on the dependent variable, defined here as the willingness to adopt the SC environment. This construct is chosen because it reflects citizens' overall behavioral intention toward accepting and engaging with SC services, which is an outcome commonly used in technology acceptance models (TAMs), such as UTAUT, and supported in recent SC adoption literature.[4,30]

Figure 3 presents the theoretical framework underpinning this study, which integrates both behavioral and technical dimensions to explain citizens' willingness to adopt or perceive SCs. The framework comprises four key constructs: privacy of data, information security, network security, and IT acceptance. Each construct is grounded in technical components relevant to SCEs. The privacy of data refers to the extent to which individuals feel their personal information is protected within SC platforms, encompassing data anonymization techniques, consent management systems, and privacy-preserving

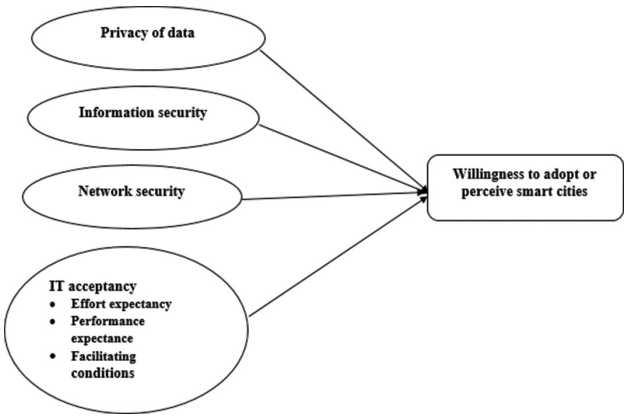

Figure 3. Conceptual framework for the willingness to adopt or perceive smart cities.

analytics that comply with data protection regulations, such as the GDPR.[3,6] Information security addresses the safeguarding of data during collection, storage, and processing through mechanisms, such as encryption algorithms, access control protocols, intrusion detection systems, and secure audit trails. Network security focuses on protecting communication infrastructure, particularly IoT and cloud-based systems, through secure communication protocols, firewalls, virtual private networks, and decentralized trust models, such as blockchain. The final construct, IT acceptance, draws on the UTAUT, incorporating effort expectancy, performance expectancy, and facilitating conditions. These factors relate

to the usability and perceived benefits of SC technologies, as well as the availability of technical support and system compatibility.

3. Materials and methods

3.1. Study design

The authors used a survey research strategy to collect data from the recruited participants between May and July 2023. Primary data were collected from two groups of participants: (i) experts experienced in SC projects in Qatar and (ii) general Qatari citizens, defined in this study as adult residents of Qatar, both nationals and long-term expatriates, who live in urban areas and are potential users or beneficiaries of SC services. Unlike the expert group, these citizens were not required to have technical expertise but were expected to be aware of and impacted by urban digital services. An online link was circulated in a Facebook group created specifically to recruit participants for the study. The survey questionnaire comprised three sections. The first section was structured to collect demographic data, which provided information about the general characteristics of the samples included. The second section contained research-specific questions concerning respondents' SC-related data privacy and security concerns. The last section related to the respondents' readiness to adopt SCs. The responses in the second and third sections of the survey questionnaire were designed using five-point Likert scales.

3.2. Instrument

The survey questionnaire was designed to seek responses from the participants in the areas of "actual use of behavior in adopting cybersecurity," "availability of cybersecurity measures," "behavioral intention in adopting cybersecurity," "confidentiality of information," "effort expectancy," "facilitating conditions," "integrity of cybersecurity," "performance expectancy," "resilience of cybersecurity," "safety," and "social influence of cybersecurity." The survey questionnaire was prepared in these areas based on previous studies.[4,57] The broad research parameters selected in this study included three core domains: (i) technological determinants (such as the availability and integrity of cybersecurity systems, and resilience against attacks); (ii) behavioral and psychological factors (including effort expectancy, social influence, and behavioral intention); and (iii) information assurance aspects (such as confidentiality, performance reliability, and perceived safety). The authors selected broad research parameters to accommodate a holistic opinion of the participants regarding various aspects of data security. To gain a more holistic understanding of the data privacy and data security concerns of the respondents, the original survey questionnaire was adapted to be appropriate for the second group of participants—experts experienced working on SC projects, in addition to the original sample of citizens.[58]

3.3. Participant recruitment

The individual respondents appropriate for the study were selected based on specific inclusion criteria to ensure a valid representation of each group. General Qatari citizens were defined as adult residents of Qatar (aged 18 and above) living in urban areas and having at least basic awareness or interaction with SC services, such as digital public platforms, smart transport systems, or municipal applications. These individuals were identified, approached, and recruited through social media groups related to SCs in Qatar. The Facebook groups used for this purpose included "Qatar Living," "Life in Qatar," "Doha Qatar Online Place," "Residents of Qatar//Living in Qatar," "Qatar.com," "Doha Qatar City," "Lusail," and "Lusail Residents Network" (Lusail being Qatar's flagship SC initiative). These groups were selected for their broad and diverse user base, allowing access to a wide range of demographics reflective of the Qatari urban population. The study clearly stated that participation was voluntary, and participants were free to leave the survey or withdraw from the research at any time without providing a reason. For the expert group, the authors used purposive sampling. We contacted professionals with hands-on experience with SC projects in Qatar, particularly in areas such as cybersecurity, ICT development, urban planning, and public infrastructure management. Gatekeepers from relevant companies and agencies facilitated access to these experts. To maintain professionalism and privacy, all communications were carried out through the respondents' personal email addresses outside of working hours.

3.4. Sampling

The study used purposive sampling for the experts and convenience sampling for citizens. This approach was adopted to optimize the participation and selection of qualified respondents for the sample. Purposive and convenience sampling were based on the availability of respondents and the selection of participants with expert knowledge in cybersecurity, although the scope for generalization was limited. This strategy aligns with the principles of mixed-methods research, which often combines qualitative depth and contextual understanding (through purposive sampling) with broader, accessible participation (through convenience sampling), especially during exploratory phases or in studies addressing practical, real-world settings.[59,60] Mixed-methods designs value methodological flexibility and often prioritize contextual relevance over statistical generalizability when exploring

complex social or technological phenomena. Nonetheless, this approach suffers from a lack of generalizability of findings to the general population.[60] This research was not aimed at generalizing but rather was focused on a specific aspect (i.e., the influence of data privacy and security concerns on respondents' willingness to adopt SCs in the context of Qatar).

The primary inclusion criteria for the citizen groups were that they should be Qatari adult citizens (aged 18 and above), including residents and non-residents of SCs in the country, who were willing to participate in the online survey. The study collected data from 120 Qatari citizens regarding the impact of their concerns about data privacy and security on their readiness to adopt SCs. Participants in the expert group were subject to additional inclusion criteria of having experience in working on SC projects in Qatar.

3.5. Data analysis

The study collected data from 155 Qatari citizens. The data collected from the general public (hereinafter "public") (n = 120) and experts (n = 35) were analyzed using inferential, parametric, and non-parametric statistics. The authors aimed to establish potential statistically significant differences between the two groups of respondents. To assess group-level tendencies and enable comparison, the authors calculated the mean responses for each group on key variables. While averaging responses in relatively small samples carries the limitation of reduced generalizability, it is widely accepted in social science research as a method to detect central tendencies and significant patterns.[61] Before analysis, the datasets were screened for missing values and outliers, and reliability tests (Cronbach's alpha) were conducted to ensure internal consistency across scale items. The data were then cleaned and standardized using the Statistical Package for the Social Sciences (SPSS version 26, IBM, United States) software to ensure that responses across both groups were comparable. In this study, representativeness was approached through internal consistency within each group and the alignment of demographic distribution (e.g., age, gender, profession) with broader characteristics of the respective populations. For inferential testing, equal variance assumptions were evaluated through Levine's test, and both parametric (independent samples t-tests) and non-parametric methods were applied to validate robustness. Although not statistically representative in a probabilistic sense, the averaged results are analytically useful to highlight comparative differences between the two stakeholder categories. In addition, correlation tests were conducted separately for each group to avoid cross-sample bias and to ensure fair and meaningful comparisons.

4. Results

This section summarizes the results based on the data from 120 citizens and 35 experts. The first part presents data on the demographic characteristics of the participants, followed by the testing of the hypothesis and a discussion of the findings.

4.1. Demographic characteristics of samples

Collected demographic data included participants' age, sex, marital status, number of people in household, number of children in family, prior experience of living in an SC, and status of living in an SC. For the sample group comprising experts, the demographic data collected include age group, sex, marital status, current position in organization, prior experience in SC projects, duration of working on an SC project, and current status of employment in an SC project.

Table 2 shows the responses for the public, indicating relatively even distribution across the categories for demographic characteristics (age, sex, marital status, and family status), apart from the majority being male (60%), married (61%), and not having lived in an SC (81%). While 81% of the public group reported not having lived in SCs, and 78% indicated that they were not currently residing in one, the trustworthiness of the data remains valid due to the nature of the study's objectives. The research was designed not to assess the direct experience of users within a fully developed SC but rather to explore perceptions, attitudes, and concerns regarding the adoption of SC environments, including factors such as data privacy, cybersecurity, and service readiness. Perceived trust, intention to adopt, and awareness of potential benefits and risks are meaningful even in populations not yet embedded in SC contexts, as these perceptions heavily influence future adoption behaviors.[4] Furthermore, Qatar has introduced elements of SC services (e.g., smart transport, digital healthcare, e-government) that citizens interact with even outside formal SC zones, such as Lusail. Thus, although most respondents have not lived in a designated SC, they are nonetheless engaged with smart technologies, making their responses relevant and informative for this study.

The responses of the expert group are shown in Table 3. In contrast to the public group, there was a greater concentration of experts in the age cohort aged 35–45 (49%), followed by the oldest cohort aged 46 and above (34%), and an even sex distribution (with 57% male and 40% female). As with the public group, the majority of experts (63%) were married. The vast majority (91%) had worked directly on SC projects, and 69% were currently working on one, having direct experience in the field. Similar proportions worked as designers (20%), construction workers (29%), project managers (23%),

Table 2. Demographic characteristics of the public group

Question	Options	Frequency	Percentage
What is your age? (years)	18–25	24	20
	26–34	25	21
	35–45	33	28
	46+	38	32
What is your sex?	Male	72	60
	Female	40	33
	Prefer not to say	8	7
What is your marital status?	Single	27	23
	Married	73	61
	Divorced	10	8
	Other	10	8
How many people are there in your household?	1	15	13
	2	14	12
	3	26	22
	>3	65	54
How many children live in your household?	0	33	28
	1	24	20
	2	30	25
	3	7	6
	>3	26	22
Have you ever lived in an SC?	Yes	23	19
	No	97	81
How long have you lived in an SC? (years)	<1	9	8
	1–3	5	4
	4–6	5	4
	>6	4	3
	Have not lived in SC	97	81
Do you currently live in an SC?	Yes	16	13
	No	7	6
	Have not lived in SC	93	78

Abbreviation: SC: Smart city.

Table 3. Demographic characteristics of the expert group

Question	Options	Frequency	Percentage
What is your age? (years)	18–25	2	6
	26–34	4	11
	35–45	17	49
	46+	12	34
What is your sex?	Male	20	57
	Female	14	40
	Prefer not to say	1	3
What is your marital status?	Single	6	17
	Married	22	63
	Divorced	3	9
	Other	4	11
What is your position in your organization?	Designer	7	20
	Construction worker	10	29
	Project manager	8	23
	Managerial position	10	29
Have you ever worked on an SC project?	Yes	32	91
	No	3	9
How long have you worked on an SC project? (years)	<1	4	11
	1–3	9	26
	4–6	11	31
	>6	8	23
	Have not worked on an SC project	3	9
Do you currently work on an SC project?	Yes	24	69
	No	8	23
	Have not worked on an SC project	3	9

Abbreviation: SC: Smart city.

and in other managerial positions (29%). Hence, the sample represents a good mix to provide useful insights with respect to the different variables of SCs and citizen readiness to adopt an SCE.

4.2. Statistical test for data analysis

For comparison of the two data sets, an independent sample *t*-test was carried out using SPSS statistical software. This test compares the means of two independent groups to detect any potentially significant difference between them.[62] The null and alternative hypothesis for this test is defined below:

H_0: The means of the two groups of the public and experts with respect to SC characteristics are not significantly different.

H_1: The means of the two groups of the public and experts with respect to SC characteristics are significantly different.

Considering the above, the output of the independent sample *t*-test is as shown in Table 4. The *t*-test for equality of means shows statistically significant results. This implies that the means of the two groups with respect to the perception of SC characteristics are significantly different. This difference is expected due to the participants' varying levels of exposure and expertise related to SC technologies. This is also evident in the different parameters of the survey questionnaire, i.e., actual use of behavior in adopting

privacy and data security in SCs, availability of privacy and data security, behavioral intention in adopting privacy and data security in SCs, confidentiality of privacy and data security, effort expectancy, facilitating conditions, integrity of privacy and data security, performance expectancy, resiliency of privacy and data security, and public readiness to accept SCs. Purposive sampling ensured that only individuals with relevant, hands-on experience in SC projects were included, thereby enhancing the depth and contextual relevance of expert insights. Similarly, the use of convenience sampling for citizens allowed for efficient data collection from a broad and diverse urban population. However, these non-probability sampling methods do not permit statistical generalization to the wider population and are potentially subject to selection bias.[61] For this study, the method was appropriate in exploratory or applied research contexts, where the goal is to compare stakeholder perceptions rather than produce generalizable metrics.

Hence, the null hypothesis is rejected. The differences in the mean are explained based on the argument that the public and experts have different levels of understanding regarding the SCE. The public's perception is primarily derived from personal experience and social communication, such as word of mouth, social media platforms, or public sources.[18] On the other hand, the perception of SCE among experts is derived based on their direct experience of working on SC systems.

A Pearson correlation test was conducted to test the linear association between the different parameters of SCE and citizens' readiness to accept SCs. The correlation test was conducted in two parts, one for the public and the other for experts. This is primarily due to the reasons that the means of perception for the two groups (the public and experts) regarding SC characteristics were found to be significantly different. The null and alternative hypotheses for conducting the correlation test are formulated below:

H_0: There is no significant correlation between the different parameters of SCE and public readiness to accept SCs.

H_1: There is a significant correlation between the different parameters of SCE and public readiness to accept SCs.

The statistical results from the public group are shown in Table 5. It can be observed that all variables representing the different characteristics of SCE from citizens' perspectives display statistically significant results, indicating a positive correlation with their readiness to accept SCs. The observed correlations, in descending order, are performance expectancy (r = 0.842, p<0.05), facilitating conditions (r = 0.814, p<0.05), confidentiality of privacy and data security (r = 0.794, p<0.05), resiliency of privacy and data security (r = 0.792, p<0.05), integrity of privacy and data security (r = 0.772, p<0.05), effort expectancy (r = 0.759, p<0.05), behavioral intention in adopting privacy and data security in SCs (r = 0.750, p<0.05), actual use of behavior in adopting privacy and data security in SCs (r = 0.745, p<0.05), and availability of privacy and data security (r = 0.714, p<0.05). Among these, performance expectancy shows the strongest correlation, suggesting that citizens are more willing to adopt SCs when they perceive clear benefits and efficiency gains. Facilitating conditions also ranked high, indicating that infrastructure and support systems significantly influence acceptance. These findings highlight that citizens' decisions are driven more by perceived utility and available support than by technical or behavioral aspects alone.

The statistical results from the expert group are shown in Table 6. All the variables representing the different

Table 4. Independent sample *t*-test between public and expert groups

Variable	Sig. (p<0.05)	Direction of difference
Actual use of behavior	Yes	Experts<public
Availability of privacy and data security	Yes	Experts<public
Behavioral intention	Yes	Experts<public
Confidentiality of privacy and data security	Yes	Experts<public
Effort expectancy	Yes	Experts<public
Facilitating conditions	Yes	Experts<public
Integrity of privacy and data security	Yes	Experts<public
Performance expectancy	Yes	Experts<public
Resiliency of privacy and data security	Yes	Experts<public
Readiness to accept SCs	Yes	Experts<public

Data source: Table A1.
Abbreviations: SCs: Smart cities; Sig.: Significance.

Table 5. Pearson correlation test of the public group

Variable	Correlation with readiness to accept SCs	Significance
Performance expectancy	0.842	p<0.05
Facilitating conditions	0.814	p<0.05
Confidentiality of privacy and data security	0.794	p<0.05
Resiliency of privacy and data security	0.792	p<0.05
Integrity of privacy and data security	0.772	p<0.05
Effort expectancy	0.759	p<0.05
Behavioral intention	0.750	p<0.05
Actual use of behavior	0.745	p<0.05
Availability of privacy and data security	0.714	p<0.05

Data source: Table A2.
Abbreviation: SCs: Smart cities.

characteristics of SCE from the experts' perspective display statistically significant results, indicating a positive correlation with public readiness to accept SCs. The observed correlations, in descending order, are performance expectancy (r = 0.893, p<0.05), confidentiality of privacy and data security (r = 0.891, p<0.05), resiliency of privacy and data security (r = 0.888, p<0.05), integrity of privacy and data security (r = 0.879, p<0.05), effort expectancy (r = 0.876, p<0.05), availability of privacy and data security (r = 0.865, p<0.05), actual use of behavior in adopting privacy and data security in SCs (r = 0.851, p<0.05), facilitating conditions (r = 0.844, p<0.05), and behavioral intention in adopting privacy and data security in SCs (r = 0.836, p<0.05). Performance expectancy remains at the top of the list, showing that experts also emphasize the importance of tangible improvements in service delivery. Interestingly, experts place slightly more importance on confidentiality and resilience of data systems, likely reflecting their deeper understanding of technical vulnerabilities. These insights suggest that while both groups value system performance, experts are more attuned to the foundational role of robust security infrastructure in citizen acceptance.

5. Discussion

The strong correlations demonstrated between the studied variables add support to previous studies. For the performance expectancy variable, a similar study in the United States reported that it had the highest influence on app-use intentions in the context of a service app.[29] A follow-up study also reported the positive influence of the performance expectancy variable on intention to use SC services.[30] These findings indicate that citizens familiar with the solutions offered in an SCE are more likely to adopt and use SC services regularly.

There has been considerable analysis in previous studies of the variables, including confidentiality, privacy, and data security.[8,9,33] These studies highlighted the concerns emanating from full connectivity and large volumes of data collection and analysis, facilitated by AI and intelligent systems, such as IoT. Hence, the findings of this study also concur with the need to redress the privacy and data security issues to enhance public readiness to accept SCs.

Table 6. Pearson correlation test of the expert group

Variable	Correlation with readiness to accept SCs	Significance
Performance expectancy	0.893	p<0.05
Confidentiality of privacy and data security	0.891	p<0.05
Resiliency of privacy and data security	0.888	p<0.05
Integrity of privacy and data security	0.879	p<0.05
Effort expectancy	0.876	p<0.05
Availability of privacy and data security	0.865	p<0.05
Actual use of behavior	0.851	p<0.05
Facilitating conditions	0.844	p<0.05
Behavioral intention	0.836	p<0.05

Data source: Table A3.
Abbreviation: SCs: Smart cities.

For the variable of resiliency of privacy and data security, the findings also affirm previous literature reporting that the interconnectedness of humans with digital devices requires voluminous data exchange, which means that SC systems need to be resilient to protect the privacy of users (i.e., the general public) and to ensure data security continuously.[9] Furthermore, although the literature shows that security and privacy concerns are common and fundamental in the context of SC environments,[33] there is a need for robust monitoring mechanisms to ensure resiliency of privacy and data security, which in turn enhances trust and public readiness to accept SCs. Hence, the findings of this study also concur with the need for resilient privacy and data security to enhance public acceptance of SCs.

The strong and positive correlation between the variable of integrity of privacy and data security is also closely related to the variables of privacy and data security, as well as the variable of confidentiality of privacy and data security, wherein strong support has been observed in literature with respect to influence on public readiness to accept SCs.[18,21,47,62] This is based on the axiomatic assumption that the public expects their data to be accurate when availing themselves of public services (e.g., medical health records). Prior research has also highlighted the use of advanced technologies, such as blockchain, to maintain data integrity in an SCE, enhancing trust and confidence among the residents of SCs.[35,37,58] In the context of Qatar, this concept is gaining traction, with several projects, such as Lusail SC and the Ministry of Communications and IT, promoting blockchain-based digital identity systems, smart healthcare platforms, and secure data-sharing protocols. These developments indicate a clear trend toward integrating advanced technologies as part of Qatar's National Vision 2030. However, full-scale implementation remains in progress, requiring continued policy alignment, technical capacity-building, and public engagement to ensure effective adoption.

Hence, the findings of this study also concur with previous research in demonstrating that higher integrity of privacy and data security leads to enhanced readiness among the public to accept the SC environment. For the variable of effort expectancy, it is observed that there is a strong correlation with public readiness to accept SCs for both the public and experts. This is also consistent with

existing literature that reported the effort expectancy significantly influences citizens' intention to use SCs.[30] The strong correlation can be explained based on UTAUT, wherein users find a system convenient, they are more likely to use the system regularly.[22,46]

The strong correlation between the variable of facilitating conditions of public readiness to accept SCs is explained based on the argument that a robust technological architecture and infrastructure are necessary to support the services in SCs. Moreover, the advancements in technology also offer the scalability of services with ease, thereby ensuring that the technology infrastructure supports the citizen-centric services in SCE. These findings are also consistent with academic literature, which reports that robust technological infrastructure and governance enhance public participation in the SCE, thereby enabling an easy and efficient delivery of services by governments.[45,46]

Finally, for the variable of behavioral intention in adopting privacy and data security in SCs and the variable of actual use of behavior in adopting privacy and data security in SCs, it is observed that a strong correlation is demonstrated with public readiness to accept SCs for both the public and experts. This is because when the public understands the need for privacy and data security and trusts the ecosystem regarding privacy and data security measures, they are more likely to use the services in an SCE. These findings are also consistent with those in previous studies, which pointed out that the behavioral intention to adopt services is dependent on various factors, such as ease of use, convenience, assurance of data privacy and security, trust in the system, facilitating conditions, and performance expectancy.[48,49] In the public group, behavioral intention showed a correlation coefficient of $r = 0.750$ ($p<0.05$), and actual use of behavior showed $r = 0.745$ ($p<0.05$), indicating strong, statistically significant relationships with readiness to accept SCs. In the expert group, the same variables also revealed strong positive correlations of $r = 0.836$ and $r = 0.851$, respectively (both $p<0.05$). Hence, although the two groups are significantly different, the statistical results confirm a strong and positive correlation between the variables of SCs and public readiness to accept SCs.

6. Conclusion

6.1. Main outcomes

In the coming years, at varying paces in different global and regional contexts, the majority of current urban populations will live in SC environments. The use of technology in providing public services has become a common norm for government and corporate entities. However, the longstanding challenges of data security and privacy remain prevalent, concerning service users and providers. In this regard, this research focused on the effect of data privacy and data security issues on the public's willingness to adopt the SC environment. To achieve the research objectives, a critical review of previous academic literature was conducted regarding the interconnection between data privacy and security issues, as well as the adoption of SCs, key factors of SC adoption, and how security and privacy concerns are currently addressed in the SC context.

Based on the reviewed literature, this study developed a theoretical framework conceptualized to investigate perceptions of SC adoption variables for two representative samples, the "public" and "expert" groups. The findings revealed that the two samples differ in their responses, as observed from the output of the independent sample *t*-test. However, a strong positive correlation is observed between all variables of SC adoption, i.e., performance expectancy, facilitating conditions, confidentiality of privacy and data security, resiliency of privacy and data security, integrity of privacy and data security, effort expectancy, of behavioral intention in adopting privacy and data security in SCs, actual use of behavior in adopting privacy and data security in SCs, availability of privacy and data security, and public readiness to accept SCs.

The findings present useful insights into the importance of information security in an SC environment. Since the majority of systems are interconnected, it is imperative to set up strong administrative and governance control, which can mitigate the risk of vulnerabilities in an SC environment. Hence, some recommendations can be made based on this study for governmental authorities looking to increase public acceptance of SCs in Qatar and similar contexts.

First, concerns regarding privacy and data security need to be addressed both for the existing SCE paradigm and during the conceptualization of new SC models. For this purpose, previous studies[34,37] have suggested using advanced technologies, such as blockchain, big data, and IoT, to address network security, privacy, and data confidentiality. In Qatar, such implementation could build upon existing frameworks, such as the National Cybersecurity Strategy and Lusail SC's pilot initiatives in digital ID and data governance.[14] Practical steps include adopting permissioned blockchain systems for public service records (e.g., smart health or education) and creating a centralized trust authority under the Ministry of Communications and IT.

Second, the systems should be scalable to ensure public availability of the services. Prior research has suggested using cloud services to handle scalability and sustain system performance when managing large

volumes of data.[2,24,31] Since the SC environment spans multiple services, such as healthcare, transportation, and connectivity, there must be minimal downtime and enhanced service continuity. In the Qatar context, integrating scalable cloud infrastructure (e.g., through Qatar Cloud, Microsoft Azure Qatar Region) into government and municipal platforms would address performance bottlenecks while ensuring compliance with local data residency laws.

Third, the basic functionalities of services, such as performance expectations and effort expectations, must be adequately addressed when designing both the front end and the back end of SCE systems. This entails active stakeholder consultation and participation from the design stage onward, with continuous evaluation of deployed systems. The development of a Qatar-specific TAM could guide policymakers in measuring key predictors of adoption, such as perceived usefulness, trust, and ease of use, based on national user behavior studies. Such a model could be institutionalized by bodies like the Qatar Digital Government initiative.

Finally, the government should be aware of the factors inhibiting the adoption of SC services. This can be achieved through public education campaigns that increase trust in SC systems, thereby contributing to a positive behavioral intention toward using SC services regularly. Several initiatives, such as the "Digital Qatar" literacy programs and smart citizen apps, should be expanded to enhance transparency, raise cybersecurity awareness, and demystify SC technologies for ordinary residents. These efforts, combined with responsive feedback mechanisms, can bridge the gap between policy design and public trust.

6.2. Limitations

While this study has presented useful insights into data privacy and security in an SC environment, it was also conducted within a limited scope in the context of SCs in Qatar. The focus is also limited to data privacy and security and does not encompass a wider range of variables that potentially influence people's willingness to live in SC environments. Moreover, the data analysis, while suited to meeting the objectives of the current research (i.e., exploring stakeholder views), offers limited in-depth insights concerning important SC-related issues. This study has several limitations, including a small expert sample (n = 35) and potential sampling bias from Facebook-based citizen recruitment. The adapted survey lacked validation in the Qatari context, and parametric tests assumed equal variances without verification. Pearson's correlation indicates association but not causality. In addition, key UTAUT constructs, including social influence and habit, were excluded, limiting theoretical depth. Future research should address these concerns using longitudinal designs and broader model applications.

6.3. Suggestions

This study found clear and consistent relationships between cybersecurity-related factors and the willingness of both the public and experts to adopt SC systems in Qatar. Performance expectancy, data confidentiality, and system resiliency emerged as the most influential factors for both groups, with experts placing greater emphasis on data integrity and technical infrastructure. The analysis also showed meaningful differences in perception between the two groups, underlining the need for tailored strategies in SC planning and implementation. Future research should broaden the range of variables considered in SC adoption, with particular attention to models, such as TAM, and a complete use of the UTAUT framework, including dimensions like social influence and habit. It is also important to validate survey tools in the local context through pilot testing. Expanding the sample to include multiple cities and more diverse participants, and adopting longitudinal or experimental designs, would allow for a deeper understanding of how privacy and security concerns shape public adoption over time. These steps would strengthen both the theoretical and practical contributions of future work in this area.

Acknowledgments

The authors of this article would like to express their deep gratitude to their institution, Brunel University London. The present research complies with the open-access policy of Brunel University London. This research would not be possible without the support and guidance received from the University.

Funding

None.

Conflict of interest

The authors declare that they have no competing interests.

Author contributions

Conceptualization: All authors
Formal analysis: Dana Ahmad Al-Ali
Investigation: Dana Ahmad Al-Ali
Methodology: All authors
Supervision: Nadarajah Manivannan, Yanmeng Xu
Writing–original draft: Dana Ahmad Al-Ali
Writing–review & editing: All authors

Ethics approval and consent to participate

Informed consent was obtained from all subjects involved in the study. All procedures were performed in compliance with relevant laws and institutional guidelines and have been approved by the appropriate institutional committee: Research Ethics Committee of Brunel University London (Reference number: 38065-LR-Jul/2022-40874-2; date of approval: August 4, 2022).

Consent for publication

Informed consent for publication of anonymized participant data was obtained from all participants.

Availability of data

The research data are available at https://figshare.com/articles/journal_contribution/Untitled_It_b_Data_Privacy_and_Security_Concerns_and_Readiness_to_Accept_Smart_Cities_Empirical_Evidence_from_Qatar_b_em/25764780 (accessed on January 22, 2025).

References

1. Mak HWL, Lam YF. Comparative assessments and insights of data openness of 50 smart cities in air quality aspects. *Sustain Cities Soc*. 2021;69:102868.

   doi: 10.1016/j.scs.2021.102868

2. Petrolo R, Loscri V, Mitton N. Towards a smart city based on cloud of things, a survey on the smart city vision and paradigms. *Trans Emerg Telecommun Technol*. 2017;28(1):e2931.

   doi: 10.1002/ett.2931

3. Arora RU. Financial sector development and smart cities: The Indian case. *Sustain Cities Soc*. 2018;42:52-58.

   doi: 10.1016/j.scs.2017.12.049

4. Alhalafi N, Veeraraghavan P. Exploring the challenges and issues in adopting cybersecurity in Saudi smart cities: Conceptualization of the cybersecurity-based UTAUT model. *Smart Cities*. 2023;6(3):1523-1544.

   doi: 10.3390/smartcities6030072

5. Silva BN, Khan M, Han K. Towards sustainable smart cities: A review of trends, architectures, components, and open challenges in smart cities. *Sustain Cities Soc*. 2018;38:697-713.

   doi: 10.1016/j.scs.2018.01.053

6. Herath HMSS, Herath HMK, Madhusanka BGDA, Guruge LGPK. Data protection challenges in the processing of sensitive data. In: *Data Protection: The Wake of AI and Machine Learning*. Cham: Springer Nature Switzerland; 2024. p. 155-179.

   doi: 10.1007/978-3-031-76473-8_8

7. Rao PM, Deebak BD. Security and privacy issues in smart cities/industries: Technologies, applications, and challenges. *J Ambient Intell Humaniz Comput*. 2022;14(8):1-37.

   doi: 10.1007/s12652-022-03707-1

8. Cui L, Xie G, Qu Y, Gao L, Yang Y. Security and privacy in smart cities: Challenges and opportunities. *IEEE Access*. 2018;6:46134-46145.

   doi: 10.1109/ACCESS.2018.2853985

9. Elmaghraby AS, Losavio MM. Cyber security challenges in smart cities: Safety, security and privacy. *J Adv Res*. 2014;5(4):491-497.

   doi: 10.1016/j.jare.2014.02.006

10. Caragliu A, Del Bo C, Nijkamp P. Smart cities in Europe. *J Urban Technol*. 2011;18(2):65-82.

    doi: 10.1080/10630732.2011.601117

11. Novotný R, Kuchta R, Kadlec J. Smart city concept, applications and services. *J Telecommun Syst Manag*. 2014;3(2):1000117.

    doi: 10.4172/2167-0919.1000117

12. TASMU. *Technology-Led Initiatives Binding Five Different Sectors to Help Shape the Smart Qatar Roadmap*; 2025. Available from: https://tasmu.gov.qa/initiatives [Last accessed on 2025 Jul 28.

13. Communications Regulatory Authority (CRA). *Smart Cities*. CRA Website; 2025. Available from: https://www.cra.gov.qa/en/services/emerging-technologies/smart-cities [Last accessed on 2025 Jul 28].

14. AlAli D, Manivannan N, Xu Y. A framework for effective design thinking based smart cities projects in Qatar. *Smart Cities*. 2023;6(1):531-562.

    doi: 10.3390/smartcities6010025

15. Syed M, Aina YA, Yigitcanlar T. Smart and sustainable Doha? From Urban brand identity to factual veracity. *Urban Sci*. 2024;8(4):241.

    doi: 10.3390/urbansci8040241

16. Barns S, Cosgrave E, Acuto M, McNeill D. Digital infrastructures and urban governance. *Urban Policy Res*. 2017;35(1):20-31.

    doi: 10.1080/08111146.2016.1235032

17. Khatoun R, Zeadally S. Cybersecurity and privacy solutions in smart cities. *IEEE Commun Mag*. 2017;55(3):51-59.

    doi: 10.1109/MCOM.2017.1600297CM

18. Baldi G, Megaro A, Carrubbo L. Small-town citizens' technology acceptance of smart and sustainable city development. *Sustainability*. 2022;15(1):325.

    doi: 10.3390/su15010325

19. Frick KT, Abreu GM, Malkin N, Pan A, Post AE. *The Cybersecurity Risks of Smart City Technologies: What*

do the Experts Think? UC Berkeley Centre for Long-Term Cybersecurity; 2021. Available from: https://cltc.berkeley.edu/wp/content/uploads/2021/03/smart_city_cybersecurity.pdf [Last accessed on 2024 Dec 26].

20. Pandey P, Goldern D, Peasley S, Kelkar M. *Making Smart Cities Cybersecure: Ways to Address Distinct Risks in an Increasingly Connected Urban Future*. Deloitte Insights; 2019. Available from: https://www2.deloitte.com/us/en/insights/focus/smart/city/making/smart/cities/cyber/secure.html [Last accessed on 2024 Dec 26].

21. Braun T, Fung BC, Iqbal F, Shah B. Security and privacy challenges in smart cities. *Sustain Cities Soc*. 2018;39:499-507.

doi: 10.1016/j.scs.2018.02.039

22. Chen D, Wawrzynski P, Lv Z. Cybersecurity in smart cities: A review of deep learning-based applications and case studies. *Sustain Cities Soc*. 2021;66:102655.

doi: 10.1016/j.scs.2020.102655

23. Nayyar A, Jain R, Mahapatra B, Singh A. Cybersecurity challenges for smart cities. In: Ahuja K, Khosla A, editors. *Driving the Development, Management, and Sustainability of Cognitive Cities. New York: IGI Global*; 2019. p. 27-54.

doi: 10.4018/978-1-5225-8085-0

24. Chen J, Ramanathan L, Alazab M. Holistic big data integrated artificial intelligent modeling to improve privacy and security in data management of smart cities. *Microprocess Microsyst*. 2021;81:103722.

doi: 10.1016/j.micpro.2020.103722

25. Hoofnagle CJ, Van Der Sloot B, Borgesius FZ. The European Union general data protection regulation: What it is and what it means. *Inf Commun Technol Law*. 2019;28(1):65-98.

doi: 10.1080/13600834.2019.1573501

26. Ismagilova E, Hughes L, Dwivedi YK, Raman KR. Smart cities: Advances in research-an information systems perspective. *Int J Inf Manage*. 2019;47:88-100.

doi: 10.1016/j.ijinfomgt.2019.01.004

27. Kuberkar S, Singhal TK. Factors influencing adoption intention of AI powered chatbot for public transport services within a smart city. *Int J Emerg Technol Learn*. 2020;11(3):948-958.

28. Beştepe F, Yildirim SÖ. Acceptance of IoT-based and sustainability-oriented smart city services: A mixed methods study. *Sustain Cities Soc*. 2022;80:103794.

doi: 10.1016/j.scs.2022.103794

29. Hou J, Arpan L, Wu Y, Feiock R, Ozguven E, Arghandeh R. The road toward smart cities: A study of citizens' acceptance of mobile applications for city services. *Energies*. 2020;13(10):2496.

doi: 10.3390/en13102496

30. Habib A, Alsmadi D, Prybutok VR. Factors that determine residents' acceptance of smart city technologies. *Behav Inf Technol*. 2020;39(6):610-623.

doi: 10.1080/0144929X.2019.1693629

31. Enayet A, Razzaque MA, Hassan MM, Alamri A, Fortino G. A mobility-aware optimal resource allocation architecture for big data task execution on mobile cloud in smart cities. *IEEE Commun Mag*. 2018;56(2):110-117.

doi: 10.1109/MCOM.2018.1700293

32. Badidi E, Mahrez Z, Sabir E. Fog computing for smart cities' big data management and analytics: A review. *Fut Int*. 2020;12(11):190.

doi: 10.3390/fi12110190

33. Zhang K, Ni J, Yang K, Liang X, Ren J, Shen XS. Security and privacy in smart city applications: Challenges and solutions. *IEEE Commun Mag*. 2017;55(1):122-129.

doi: 10.1109/MCOM.2017.1600267CM

34. Altulyan M, Yao L, Kanhere SS, Wang X, Huang C. A unified framework for data integrity protection in people-centric smart cities. *Multimed Tools Appl*. 2020;79:4989-5002.

doi: 10.1007/s11042-019-7182-7

35. Alam T. Blockchain-based big data integrity service framework for IoT devices data processing in smart cities. *Mindanao J Sci Technol*. 2021;19(1):137-162.

doi: 10.61310/mndjsteect.1030.21

36. Hashem IAT, Chang V, Anuar NB, *et al*. The role of big data in smart city. *Int J Inf Manage*. 2016;36(5):748-758.

doi: 10.1016/j.ijinfomgt.2016.05.002

37. Rahman MS, Chamikara MAP, Khalil I, Bouras A. Blockchain-of-blockchains: An interoperable blockchain platform for ensuring IoT data integrity in smart city. *J Ind Inf Integr*. 2022;30:100408.

doi: 10.1016/j.jii.2022.100408

38. Rahi S, Mansour MMO, Alghizzawi M, Alnaser FM. Integration of UTAUT model in internet banking adoption context: The mediating role of performance expectancy and effort expectancy. *J Res Interact Mark*. 2019;13(3):411-435.

doi: 10.1108/JRIM-02-2018-0032

39. Yu H, Yang Z, Sinnott RO. Decentralized big data auditing for smart city environments leveraging blockchain technology. *IEEE Access*. 2018;7:6288-6296.

doi: 10.1109/ACCESS.2018.2888940

40. Oh S, Lehto XY, Park J. Travelers' intent to use mobile technologies as a function of effort and performance expectancy. *J Hosp Mark Manag*. 2009;18(8):765-781.

doi: 10.1080/19368620903235795

41. Onaolapo S, Oyewole O. Performance expectancy, effort

expectancy, and facilitating conditions as factors influencing smartphones use for mobile learning by postgraduate students of the University of Ibadan, Nigeria. *Interdiscip J E Skills Lifelong Learn*. 2018;14:95-115.

42. Utomo P, Kurniasari F, Purnamaningsih P. The effects of performance expectancy, effort expectancy, facilitating condition, and habit on behaviour intention in using mobile healthcare application. *Int J Community Serv Engagem*. 2021;2(4):183-197.

    doi: 10.47747/ijcse.v2i4.529

43. Leong GW, Ping TA, Muthuveloo R. Antecedents of behavioural intention to adopt internet of things in the context of smart city in Malaysia. *Glob Bus Manag Res*. 2017;9:515-528.

44. Oliveira VAT, Santos GD. Information technology acceptance in public safety in smart sustainable cities: A qualitative analysis. *Procedia Manuf*. 2019;39(4):1929-1936.

    doi: 10.1016/j.promfg.2020.01.239

45. Dirsehan T, Van Zoonen L. Smart city technologies from the perspective of technology acceptance. *IET Smart Cities*. 2022;4(3):197-210.

    doi: 10.1049/smc2.12040

46. Yeop MA, Yaakob MFM, Wong KT, Don Y, Zain FM. Implementation of ICT policy (blended learning approach): Investigating factors of behavioural intention and use behaviour. *Int J Instr*. 2019;12(1):767-782.

    doi: 10.29333/iji.2019.12149a

47. Yeh H. The effects of successful ICT-based smart city services: From citizens' perspectives. *Gov Inf Q*. 2017;34(3):556-565.

    doi: 10.1016/j.giq.2017.05.001

48. Chatterjee S, Kar AK, Gupta MP. Success of IoT in smart cities of India: An empirical analysis. Gov Inf Q. 2018;35(3):349-361.

    doi: 10.1016/j.giq.2018.05.002

49. Lytras MD, Visvizi A. Who uses smart city services and what to make of it: Toward interdisciplinary smart cities research. *Sustainability*. 2018;10(6):1998.

    doi: 10.3390/su10061998

50. Al Nuaimi E, Al Neyadi H, Mohamed N, Al-Jaroodi J. Applications of big data to smart cities. *J Internet Serv Appl*. 2015;6:25.

    doi: 10.1186/s13174-015-0041-5

51. Rathore MM, Ahmad A, Paul A, Rho S. Urban planning and building smart cities based on the internet of things using big data analytics. *Comput Netw*. 2016;101(6):63-80.

    doi: 10.1016/j.comnet.2015.12.023

52. Ijaz S, Shah MA, Khan A, Ahmed M. Smart cities: A survey on security concerns. *Int J Adv Comput Sci Appl*. 2016;7(2):612-625.

    doi: 10.14569/IJACSA.2016.070277

53. Mehmood Y, Ahmad F, Yaqoob I, Adnane A, Imran M, Guizani S. Internet-of-things-based smart cities: Recent advances and challenges. *IEEE Commun Mag*. 2017;55(9):16-24.

    doi: 10.1109/MCOM.2017.1600514

54. Shakya DS. Collaboration of smart city services with appropriate resource management and privacy protection. *J Ubiquitous Comput Commun Technol*. 2021;3(1):43-51.

    doi: 10.36548/jucct.2021.1.005

55. Biswas K, Muthukkumarasamy V. Securing smart cities using blockchain technology. In: IEEE 18th *International Conference on High Performance Computing and Communications*. United States: IEEE; 2016. p. 1392-1393.

    doi: 10.1109/HPCC-SmartCity-DSS.2016.0198

56. Sookhak M, Tang H, He Y, Yu FR. Security and privacy of smart cities: A survey, research issues and challenges. *IEEE Commun Surv Tutor*. 2018;21(2):1718-1743.

    doi: 10.1109/COMST.2018.2867288

57. Arpaci I, Sevinc K. Development of the cybersecurity scale (CS-S): Evidence of validity and reliability. *Inform Dev*. 2022;38(2):218-226.

    doi: 10.1177/0266666921997512

58. Denscombe M. Communities of practice: A research paradigm for the mixed methods approach. *J Mixed Methods Res*. 2008;2(3):270-283.

    doi: 10.1177/1558689808316807

59. Johnson RB, Onwuegbuzie AJ, Turner LA. Toward a definition of mixed methods research. *J Mixed Methods Res*. 2007;1(2):112-133.

    doi: 10.1177/1558689806298224

60. Rasch D, Teuscher F, Guiard V. How robust are tests for two independent samples? *J Stat Plan Inference*. 2007;137(8):2706-2720.

    doi: 10.1016/j.jspi.2006.04.011

61. Saunders M, Lewis P, Thornhill A. *Research Methods for Business Students*. London: Pearson Education; 2019.

62. Macke J, Casagrande RM, Sarate JAR, Silva KA. Smart city and quality of life: Citizens' perception in a Brazilian case study. *J Clean Prod*. 2018;182:717-726.

    doi: 10.1016/j.jclepro.2018.02.078

Appendix

Table A1. Independent sample *t*-test

EV	Levine's test for equality of variances		*t*-test for equality of means					95% CID	
	F	Sig.	*t*	df	S2T	MD	SED	Lower	Upper
Actual use of behavior in adopting privacy and data security in SCs									
Ad.	0.664	0.417	−2.570	153.000	0.011	−0.527	0.205	−0.933	−0.122
NAd.			−2.751	61.676	0.008	−0.527	0.192	−0.910	−0.144
Availability of privacy and data security									
Ad.	2.856	0.093	−3.106	153.000	0.002	−0.642	0.207	−1.050	−0.234
NAd.			−3.509	68.061	0.001	−0.642	0.183	−1.006	−0.277
Behavioral intention in adopting privacy and data security in SCs									
Ad.	0.784	0.377	−2.732	153.000	0.007	−0.568	0.208	−0.979	−0.157
NAd.			−2.842	58.833	0.006	−0.568	0.200	−0.968	−0.168
Confidentiality of privacy and data security									
Ad.	0.070	0.791	−3.042	153.000	0.003	−0.631	0.207	−1.041	−0.221
NAd.			−3.055	55.735	0.003	−0.631	0.207	−1.045	−0.217
Effort expectancy									
Ad.	0.135	0.714	−2.670	153.000	0.008	−0.570	0.214	−0.992	−0.148
NAd.			−2.708	56.548	0.009	−0.570	0.211	−0.992	−0.148
Facilitating conditions									
Ad.	0.807	0.370	−2.325	153.000	0.021	−0.473	0.204	−0.875	−0.071
NAd.			−2.441	59.742	0.018	−0.473	0.194	−0.861	−0.085
Integrity of privacy and data security									
Ad.	0.656	0.419	−2.717	153.000	0.007	−0.560	0.206	−0.967	−0.153
NAd.			−2.819	58.600	0.007	−0.560	0.199	−0.957	−0.162
Performance expectancy									
Ad.	1.246	0.266	−2.843	153.000	0.005	−0.604	0.212	−1.024	−0.184
NAd.			−2.958	58.857	0.004	−0.604	0.204	−1.013	−0.196
Resiliency of privacy and data security									
Ad.	0.044	0.833	−3.243	153.000	0.001	−0.661	0.204	−1.063	−0.258
NAd.			−3.273	56.133	0.002	−0.661	0.202	−1.065	−0.256
Public readiness to accept SCs									
Ad.	11.615	0.001	−3.132	153.000	0.002	−0.649	0.207	−1.058	−0.240
NAd.			−3.712	75.033	0.000	−0.649	0.175	−0.997	−0.301

Abbreviations: Ad.: Assumed; CID: Confidence interval of the difference; df: Degree of freedom; EV: Equal variances; MD: Mean difference; NAd.: Not assumed; S2T: Significance (2-tailed); SCs: Smart cities; SED: Standard error difference.

Table A2. Pearson correlation test of the public group

Variables	1	2	3	4	5	6	7	8	9	10
1. Actual use of behavior in adopting privacy and data security in SCs	1	0.822**	0.832**	0.861**	0.817**	0.853**	0.832**	0.822**	0.840**	0.745**
2. Availability of privacy and data security	0.822**	1	0.895**	0.874**	0.834**	0.850**	0.820**	0.837**	0.800**	0.714**
3. Behavioral intention in adopting privacy and data security in SCs	0.832**	0.895**	1	0.926**	0.875**	0.886**	0.821**	0.855**	0.800**	0.750**
4. Confidentiality of privacy and data security	0.861**	0.874**	0.926**	1	0.909**	0.926**	0.873**	0.888**	0.885**	0.794**
5. Effort expectancy	0.817**	0.834**	0.875**	0.909**	1	0.910**	0.852**	0.858**	0.807**	0.759**
6. Facilitating conditions	0.853**	0.850**	0.886**	0.926**	0.910**	1	0.870**	0.920**	0.886**	0.814**
7. Integrity of privacy and data security	0.832**	0.820**	0.821**	0.873**	0.852**	0.870**	1	0.872**	0.876**	0.772**
8. Performance expectancy	0.822**	0.837**	0.855**	0.888**	0.858**	0.920**	0.872**	1	0.893**	0.842**
9. Resiliency of privacy and data security	0.840**	0.800**	0.800**	0.885**	0.807**	0.886**	0.876**	0.893**	1	0.792**
10. Public readiness to accept SCs	0.745**	0.714**	0.750**	0.794**	0.759**	0.814**	0.772**	0.842**	0.792**	1

Note: **Correlation is significant at the 0.01 level (2-tailed).
Abbreviation: SCs: Smart cities.

Table A3. Pearson correlation test of the expert group

Variables	1	2	3	4	5	6	7	8	9	10
1. Actual use of behavior	1	0.922**	0.886**	0.919**	0.937**	0.880**	0.940**	0.902**	0.910**	0.851**
2. Availability of privacy and data security	0.922**	1	0.881**	0.901**	0.896**	0.863**	0.912**	0.877**	0.916**	0.865**
3. Behavioral intention	0.886**	0.881**	1	0.929**	0.925**	0.926**	0.944**	0.890**	0.920**	0.836**
4. Confidentiality of privacy and data security	0.919**	0.901**	0.929**	1	0.934**	0.895**	0.952**	0.902**	0.914**	0.891**
5. Effort expectancy	0.937**	0.896**	0.925**	0.934**	1	0.932**	0.957**	0.927**	0.934**	0.876**
6. Facilitating conditions	0.880**	0.863**	0.926**	0.895**	0.932**	1	0.938**	0.904**	0.918**	0.844**
7. Integrity of privacy and data security	0.940**	0.912**	0.944**	0.952**	0.957**	0.938**	1	0.934**	0.960**	0.879**
8. Performance expectancy	0.902**	0.877**	0.890**	0.902**	0.927**	0.904**	0.934**	1	0.954**	0.893**
9. Resiliency of privacy and data security	0.910**	0.916**	0.920**	0.914**	0.934**	0.918**	0.960**	0.954**	1	0.888**
10. Public readiness to accept SCs	0.851**	0.865**	0.836**	0.891**	0.876**	0.844**	0.879**	0.893**	0.888**	1

Note: **Correlation is significant at the 0.01 level (2-tailed).
Abbreviation: SCs: Smart cities.