sustainability

MDPI

Article

Associated Information and Communication Technologies Challenges of Smart City Development

Mohammed Balfaqih [1,*] and Soltan Abed Alharbi [1,2,*]

[1] Department of Computer and Network Engineering, College of Computer Science and Engineering, University of Jeddah, Jeddah 23890, Saudi Arabia
[2] Department of Electrical and Electronic Engineering, College of Engineering, University of Jeddah, Jeddah 23890, Saudi Arabia
* Correspondence: mabalfaqih@uj.edu.sa (M.B.); salharbi@uj.edu.sa (S.A.A.)

Abstract: Smart cities development relies on information and communication technologies (ICTs) to improve all urban aspects, including governance, economy, mobility, and environment. The development is usually associated with several challenges and negative effects. This study relies on revealing ICTs challenges by firstly conducting a comprehensive literature review to identify the challenges that are most associated with ICTs. Then, a questionnaire survey was distributed among the Saudi population to study their expectations, perceptions, and concerns on the smart city concept and services. The questionnaire also investigated ICTs challenges identified from the literature review, including information security risks, privacy violation, incompatibility, and digital skill gaps. Consequently, semi-structured interviews were conducted to perceive the reasons for the incompatibility between different systems and digital skill gaps between the public. The findings show that the most likely challenges are information security risks and privacy violations, which are due to the increase in vulnerability, potential attacks, and lack of public awareness regarding personal data protection. The incompatibility between different systems and services in smart cities arouses worries among the public due to the expected high cost and difficulty of adaptation and utilization. Moreover, digital skill gaps arises between members of the population that have a low education level or are elderly persons.

Keywords: smart city; ICT challenges; information insecurity; privacy; compatibility; technology skills

Citation: Balfaqih, M.; Alharbi, S.A. Associated Information and Communication Technologies Challenges of Smart City Development. *Sustainability* **2022**, *14*, 16240. https://doi.org/10.3390/su142316240

Academic Editors: Orlando Troisi, Anna Visvizi, Wadee Alhalabi and Mara Grimaldi

Received: 18 October 2022
Accepted: 29 November 2022
Published: 5 December 2022

1. Introduction

The smart city concept was first proposed in the 1990s with the focus on employing information and communication technologies (ICTs) for developing modern infrastructure in cities [1]. Smart cities serve the well-being of the urban population with the aim of enhancing quality of life, fostering economy, resolving transportation and traffic problems, supporting a clean and sustainable environment, and providing accessible interactions with government authorities [2]. The six main basic dimensions for a smart city are smart governance, smart economy, smart mobility, smart environment, smart people, and smart living [3]. This will assist in achieving several sustainable development goals, such as sustainable cities and communities, quality education, good health, and well-being, along with industry, innovation, and infrastructure [4–6]. With the rapid growth of population and urban expansion, the smart city concept attracted significant attention and was quickly adopted worldwide. The number of smart cities with a clear smart city strategy over the world doubled from 87 in 2017 to more than 153 in 2019 [7]. Government authorities in Saudi Arabia have also initiated and established several high-profile economic cities, special zones, and 10 new smart cities across the country [8].

Although ICTs play a vital role in smart city development, they are only viewed as a solution towards specific problems in urban planning and management without the

consideration of their possible negative effects [9,10]. For example, systems and services could be vulnerable to information security issues such as cyberattacks, data breaches, and poor management and operation models [11]. In 2018, with the consideration that some companies report all data breaches, more than 148 million peculiar malware and 62,000 Internet of Things (IoT) attacks were found, and over 70 million personal records were stolen or leaked [12]. Another example of the negative effects is the isolation of the population who have a shortage of technical skills because of the rapid digital transformation of public services [13,14].

Systematic and empirical studies are essential for identifying potential challenges and required measures to reduce their negative effects. Different from existing studies that looked at the downsides of the involvement of ICTs in smart city development [15–18], this study investigates and analyzes these downsides within the context of a realistic sample. Although the study samples were the population of Saudi Arabia, the conclusion drawn from the study could be also applied to other countries, such as Gulf Cooperation Council (GCC) countries that are similar in terms of culture, economy, education, and other criteria. The study was carried out to systematically identify the associated challenges of smart city development from the literature as well as possible solutions. In addition, a questionnaire survey was distributed among residents of Saudi Arabia to study their perceptions about smart city development, including the challenges, expectations, and concerns. Then, the reasons for the incompatibility between different systems and the digital skill gaps between the public were further investigated through semi-structured interviews with 26 respondents. The main contributions of this paper are:

- A systematic literature review identifying the challenges of smart city development, their effects, and possible solutions. A total of 253 journal and conference articles were first obtained, which were scrutinized to 67 selected articles after disregarding the articles that were outside the scope of this study. Four major potential challenges have been identified from the literature, which are information security risks, privacy violation, incompatible systems, and digital skill gaps.
- A questionnaire survey investigating the perception of the Saudi Arabian population with respect to smart city development in terms of the associated challenges of smart city development, their severity level, and possible solutions. A simple random sampling was followed to obtain 234 valid questionnaires.
- Semi-structured interviews investigating the reasons for the incompatibility between different systems and the digital skill gaps between the public. The interview was based on a set of questions to obtain "why" rather than "how many" or "how much" [19].

The study included four phases, which were identifying associated challenges of smart city development, questionnaire design, data collection, and analysis methods, which are shown in Figure 1. In the first phase, the associated challenges of ICTs in smart city development, their effects, and their possible solutions were identified. In the second phase, a questionnaire survey and semi-structed interview were designed according to the findings to identify the perception of the population of Saudi Arabia. The data were collected in the third phase by carrying out the questionnaire survey and semi-structed interviews among residents in Saudi Arabia who were potential users of smart city services. Finally, the analysis was conducted by implementing several statistical methods to obtain the perspectives and preferences of the respondents on smart city services and the associated challenges that could be faced in developing smart city, including their causes, effects, and possible solutions.

The rest of the paper is organized as follows: Section 2 describes the considered case study, including the smart cities project in Saudi Arabia. The four phases of the methodology are described in Section 3. The subsections of the Methodology section describe the highlighted associated challenges of smart city development, their causes, and their effects as detailed in the literature; the Methodology subsections also describe the design of the questionnaire survey, semi-structured interviews, and data analysis. Section 4 discusses and

highlights the findings according to their scope and domain. The discussion of the practices that could help overcome the associated challenges is presented in Section 5. Finally, the paper is concluded in Section 6, highlighting open issues for future research works.

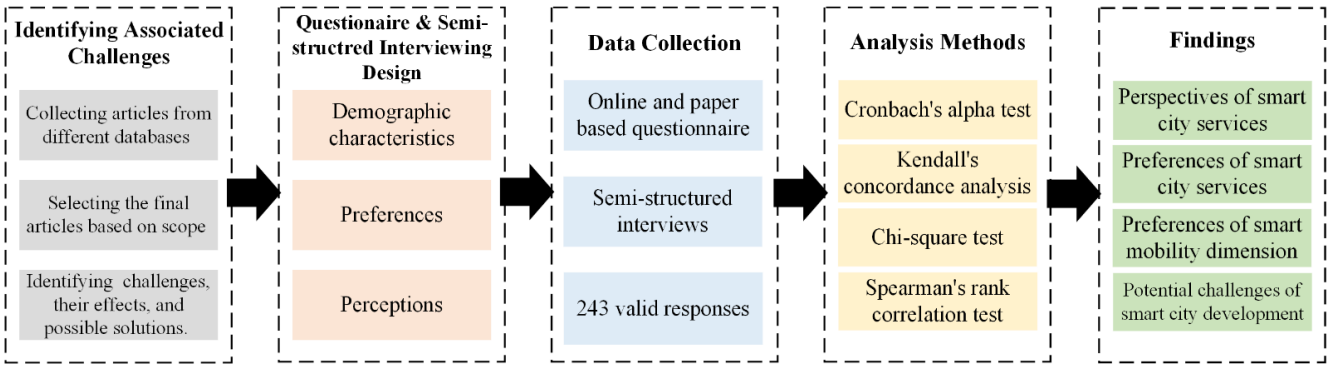

Figure 1. The main study phases.

2. Literature Review: Identifying Associated Challenges of Smart City Development

A comprehensive literature review was conducted based on content analysis of the Web of Science (WoS) database to retrieve relevant English literature from 2011 to 2022. This range of years was selected because most research studies related to smart cities and the challenges and risks associated with their development were published within this time period. A collection of words and Boolean connectors were used, including Smart City, Smart Cities, Challenges, and Risks, connected with "AND" and "OR". A total of 253 journal and conference articles were first obtained; however, only peer-reviewed journal articles were included in the study to ensure reliability and quality, resulting in a total of 104 articles. The articles were further scrutinized by considering the articles that studied and identified the potential challenges, causes, effects, and solutions in smart city development. This led to 67 selected articles after disregarding the articles that were outside the scope of this study. More than 70% of these articles were published between 2019 and 2022, which reflects the significant and recent interest in research related to smart cities. Four major potential challenges have been identified from the literature, which are information security risks, privacy violation, incompatible systems, and digital skill gaps, as shown in Table 1.

Table 1. Major potential challenges identified in the literature.

Research	Information Security	Privacy	Compatibility and Integration	Digital Skills
Yigitcanlar, T., et al., 2020 [20].	√	√	√	√
Allam, Z. and Dhunny, Z. A., 2019 [21].	√	√	√	-
Appio, F. P., 2019 [22].	√	√	√	√
Paiva, S., et al., 2021 [23].	√	√	√	-
Pundir, A., et. al., 2022 [24].	√	√	√	√
Ahmad, M., et al., 2021 [25].	√	√	√	√
Bilal, M., et al., 2020 [26].	√	√	-	-
Rao, P. M. and Deebak, B. D., 2022 [27].	√	√	√	√
Singh, S., et al., 2020 [28].	√	√	√	-
Sadik, S., et al., 2020 [29].	√	√	-	-
D'Amico, G., et al., 2020 [30].	√	√	√	-
Al Sharif, R. and Pokharel, S., 2021 [31].	√	√	√	√
Sharma, M., et al., 2020 [32].	√	√	√	√
Ismagilova, E., et al., 2020 [33]	√	√	√	-

2.1. Information Security Risks

Although the smart city concept brings a myriad of benefits, it increases the possibility of serious infrastructure and information security risks. Developing smart cities does not necessarily increase the threat, but it does increase the vulnerability and potential attacks. Hence, it is essential to support the smart city concept with mitigation measures against information security risks [34,35]. Several research works have considered information security as the greatest potential challenge of smart city development.

The main classes of security threats in smart cities are: (i) exploratory threats that aim at enumerating resources and credentials; (ii) infrastructure sabotage threats that aim to destroy or control smart city infrastructure via malware and overwhelm core resources; (iii) data manipulation threats that undermine data confidentiality and integrity; and (iv) third party vulnerabilities that target service providers in smart cities [36]. The authors in [37] studied the issues related to cybersecurity, privacy, and policy in the cyber-physical systems utilized in smart cities. The study found that the unification of smart cities services makes obtaining the jurisdiction of entities over the data difficult as it goes to several entities, states, and countries. Although developing and employing advanced cryptography and digital forensics improve privacy, it makes addressing legal disputes difficult. The study highlighted the need of secure data mashup techniques to combine organization datasets and obtain user consent before utilizing their data. Because the technical risks are related to technologies and their implementation, the risks of the top three technology-related risks in smart cities, which are IoT, big data, and blockchain, were discussed in [38]. Similarly, the risks of IoT, AI, and blockchain technologies were discussed in [31]. The common risks between these technologies are security risks in addition to unorganized data management and the integration of different technology standards. A four-layer cyber risk management framework was proposed in [34], which included cyber ecosystem, cyber infrastructure, cyber risk assessment, and cyber performance layers. The framework facilitates decisions by determining, quantifying, and ranking cyber risks. A linear programming model was also proposed to help managers make resource allocation decisions regarding multiple competing security projects. The major IoT security challenges for smart city applications were listed in [39] according to Activity-Network-Things (ANT)-centric architecture, which consists of the activity-centric, network-centric, and things-centric levels. The security challenges at the activity-centric level are edge security, secure storage, maintaining the quality of the security service, and secure integration. In the network-centric level, the challenges are authentication, identity management and access control, and secure communication environment; in things-centric, the challenges are ensuring secure updates and system resilience to attacks.

A possible mitigation measure for such risks is developing a good communication network monitoring system based on artificial intelligence (AI) for early recognition of threats, frauds, crimes, and accidents [20]. In [20,40,41], the authors proposed integrating blockchain and other encryption technologies with smart city systems to identify asymmetrical behavior, recognize the threat, and ensure data security. Achieving secure smart cities requires a holistic approach that acts in parallel with utilizing advanced technologies such as blockchain, software-defined networks (SDN), game theory, and ontology [42]. In [39], machine learning was suggested to be applied in IoT to provide systems with an automated/semi-automated security defense. The authors in [43] listed several requirements that should be considered when designing smart city systems to address the security and privacy issues. The requirements are: (i) privacy-aware communication for user data; (ii) lightweight and effective security solutions for data authenticity and integrity; and (iii) performing detailed risk assessment to obtain emerging attacks. Detection, prevention, and resolving cyber incidents were also emphasized during the data transmission and storage in the cloud, where the data are generated, processed, and stored in vulnerable environments [43–45]. Security controls and forensic readiness preserve forensically valuable evidence and consequently assist in preventing, detecting, and resolving cyber incidents. The obtained information during a forensic investigation can be fed into smart city security

systems to enhance the overall security infrastructure. Table 2 summarizes the possible causes, effects, and solutions of the main information security challenges.

Table 2. Information security challenge: possible causes, effects, and solutions from the literature.

Cause	Effect	Solution
• Weak security and encryption [37,46] • Cyberattacks [46,47]. • Difficult to guarantee end-to-end security due to large and interdependent systems [46]. • Design and operation errors [15,46,48]. • Inefficient management and operation models [15,47]. • Utilizing unsecure legacy systems and providing poor maintenance [46,47].	• Failure and unavailability of systems and services [48,49]. • Violation of information confidentiality [50]. • Economic losses [50,51].	• Implementing access control models that apply state-of the-art cryptography algorithms and security architectures [31]. • Employing/Developing strict standards for data security and privacy [52]. • Developing business models with enhanced security and privacy considerations [53]. • Enhancing security and transparency of financial systems by adopting emerging technologies such as blockchain [23]. • Developing/Implementing a management control strategy for operation and design [23]. • Developing/Implementing a cyber security strategy and recovery plan [48]. • Employing technical countermeasures such as backups, anti-virus software, and firewalls against intruders [48]. • Increasing security awareness and safeguard availability as well as performing continuous vulnerability assessments [48].

2.2. Privacy Violation

Privacy issues play a key role in the smart city context as the users interact ubiquitously and constantly with several ICT infrastructures and systems [54]. It was proven in recent years that user privacy may be threatened even upon adopting privacy-friendly naive solutions, such as anonymous multiple-ride tickets [55]. The growing utilization of smart city services on the cloud has increased privacy concerns [56]. In IoT-based systems, for instance, the majority of open-source IoT frameworks usually employ cloud platforms on Infrastructure-as-a-Service (IaaS) providers [57,58]. This in turn raises a serious threat to user privacy, channel security, and context security [59]. Moreover, several research studies proved that location trajectories are used to discover the identity of users or locate them [60–62]. Although location data is strategic information that enables a wide range of location-based services [63] and precise user profiling, it is considered sensitive data and may reveal habits that the user does not intend to share [64,65]. Artificial intelligence (AI) applications in smart cities, on the other hand, are associated with security and privacy risks that cause legal issues and require verification of compliance with existing laws related to fundamental rights protection [20,21].

As a mitigation measure, a comprehensive taxonomy of privacy metrics should be used by entities who are responsible for digital rights, ethical promises, and confidentiality. This ensures a unified metrics in investigating the privacy level of digital services. Using ad hoc privacy metrics instead of existing metrics when investigating privacy levels makes findings incomparable [66,67]. In addition, a new regulatory framework is needed to

manage the big data era, ensure data privacy, data security, and liability, and it is needed to validate the data to make the right decisions [68,69]. The authors in [70] proposed employing one of the most used privacy metrics, namely k-anonymity [71]; the authors also rely on data anonymization and generalization standard techniques standardized by the EU General Data Protection Regulation (GDPR) [72]. A decentralized governance platform for smart cities based on blockchain technology was proposed in [73] to address transparency concerning privacy and cost-efficiency. However, further studies are required to investigate the operational cost of blockchain-based applications in smart cities. Table 3 summarizes the possible causes, effects, and solutions of the main privacy challenges.

Table 3. Privacy challenge: possible causes, effects, and solutions from the literature.

Cause	Effect	Solution
• Data integrity between ubiquitous IoT-enabled systems without prior notification or permission from targeted users [46,48,74]. • Unauthorized access violations [50]. • Lack of knowledge and awareness of users on data privacy and protection [46]. • Insufficient regulations and standards of data privacy protection [75,76].	• Information disclosure and misuse [50,68]. • Risking reputation, trust, and liberty [33]. • Economic loss [77].	• Employing transparency-enhancing tools in smart city services [78]. • Identifying detailed policies and guidelines for access granting [31]. • Improving user privacy awareness and behavior by educating them about privacy-related topics [47]. • Establishing intensive regulations and standards to regulate data collection, sharing, and usage [31]. • Promoting collaborations between government and other regulating bodies to develop customized subscription models that improve the user experience [31]. • Balancing between privacy regulation and companies' rights to utilize user consumer data to avoid economic loss [77].

2.3. Incompatible Systems

The heterogeneity of the systems in smart cities raises the issue of compatibility and integration, which is the ability of different systems to function in harmony [30,32]. Different organizations and systems usually have different and incompatible standards and data formats due to expeditious and independent development. This hinders speedy technology adoption and most likely causes an additional cost. In Shenzhen, China, for instance, the Safe City project was halted because video data from incompatible surveillance systems in different districts could not be shared [79]. Several scholars proposed to formulate open standards for technologies and share interoperable protocols amongst tech suppliers [80]. This will facilitate the integration between stakeholders and data. Although data integration enables consolidating data from disparate sources, it may cause data alteration during transmission, data anonymity to third parties, or data access and privacy. The challenges related to the data integrity and quality of data generated from smart cities systems have been discussed in [30]. Another cause of the incompatibility is that several stakeholders are engaged in systems development with the possibility of insufficient communication or cooperation [80]. Moreover, some systems are independently developed with no integration plan for systems [81].

Incorporating new systems with existing interfaces and legacy systems to be implemented as a single application and to overcome the systems' incompatibility have been

proposed in [32]. The characteristics of enterprise collaborative systems and implementation issues for business firms have been described in [80]. The authors in [82] highlighted that establishing a smart city requires a state-led push for data centralization and a unified digital platform infrastructure. In this context, a holistic framework for e-learning systems in smart cities was proposed in [83]. The framework considers interdependence between infrastructure, data space, and learning space and includes an algorithm to detect privacy issues. The authors in [48,84] emphasized that the plan for systems and data integration and promotions of cross-sectional collaboration between different interfacing organizations must be conducted at the design stage. The possible causes and impacts of incompatible systems, as well as the proposed solutions in the literature are summarized in Table 4.

Table 4. Incompatible systems challenge: possible causes, effects, and solutions from the literature.

Cause	Effect	Solution
• Incompatible standards and data formats [75]. • Difficult to engage with several sectors and stakeholders [80]. • Develop systems independently without an integration plan [81]. • Lack of communication and cooperation between different sectors and stakeholders [80]. • Lack of supporting infrastructure, common information system, and unorganized data management [81]. • Difficulty of integrating data from legacy systems [81].	• Redundant construction and facilities, resource wastage; projects overlap [85]. • Poor data quality for analytics and decision-makers [81]. • Less effective smart cities [81].	• Develop open standards to improve data quality and services [80]. • Develop models to share infrastructure facilitating data sharing and cost reduction [31]. • Promote collaboration among different sectors and stakeholders to ensure cross-border integration [80]. • Develop a common information system and management solution for unorganized data [23]. • Consider the integration between systems and data during the design stage [48].

2.4. Digital Skill Gaps

Digitalization in smart cities increases inequality and social isolation because not everyone can access and utilize technology equally. This is referred to as the digital divide, which includes the inability to access technology or use it appropriately and consequently with respect to services and solutions provided by smart cities [86]. For instance, elderly people during COVID-19 were excluded from services because they are not familiar with technological services and devices [87–89]. Another skill gap is the lack of skilled labor that can handle sophisticated cyber-physical systems in smart cities. Cyber physical systems consist of thousands of IoT devices and sensors; hence, effectively managing them requires trained professionals [25]. Other causes lie in overly advanced services, poor digital literacy and skills, and personal attitude barriers [64,90]. Inactive engagement of participants in technology-driven services hinders the progress of these services [64]. Multicultural languages and different local languages in some cities could also cause a lack of accessibility to services [11]. Due to the loss of the potential value added to society, the issue of the digital skill gaps can cause high economic loss, social inequality, and exclusion [79]. Scholars have suggested that policymakers work towards liberating the process of digitization, which would increase the accessibility to services and improve digital literacy [66]. The inclusive use of technology and service delivery are significant issues that need to be considered by policymakers. Hence, Saudi Arabia's government agencies offer free Internet for some websites, places, and seasons to bridge the digital divide [91]. The possible causes and impacts of digital skill gaps, as well as the proposed solutions in the literature are summarized in Table 5.

Table 5. Digital skill gaps challenges: possible causes, effects, and solutions from the literature.

Cause	Effect	Solution
• Personal attitude hurdles and lack of awareness [64]. • Insufficient consideration for disadvantaged groups [64]. • Insufficient training program for unskilled people about applications and services [78]. • Insufficient societal involvement efforts [64].	• Expansion of the inequality level socially and economically [88]. • Less effective smart cities [81].	• Promote awareness about the benefits of smart city services and applications [21]. • Enhancing public services and information literacy to disadvantaged groups [64]. • Conducting essential education and training programs for the public and providing citizens in need with devices and Internet access [78]. • Establishing digital inclusion initiatives for citizens and entities [64].

3. Material and Methods

This section consists of four subsections. The first subsection describes the considered case study, including the smart cities project in Saudi Arabia. The other subsections describe the other three phases shown in Figure 1, including the questionnaire design, data collection, and analysis methods.

3.1. Case Study Background: Smart City Development in Saudi Arabia

The smart city development in Saudi Arabia was chosen due to its economic status and the significant ICT threats that are faced by its digital infrastructure. Saudi Arabia is the largest economy in the Middle East, one of the largest reserve currencies in the world, and the second largest sovereign investment fund in the world. It has a distinguished model for developing digital infrastructure, as it has invested about USD 4 billion with the aim of radically reshaping the economy and society. Nevertheless, according to a recent industry report, 95% of Saudi companies were exposed to cyberattacks in 2020 [92]. The report stated that 85% of study participants had seen a significant increase in the number of cyberattacks affecting businesses in the past two years.

Saudi Vision 2030 has set a series of goals to implement the smart city concept [93]. The Ministry of Municipal and Rural Affairs launched the project of implementing a smart city concept with the aim of boosting the competitiveness of Saudi cities and urban sustainability, enhancing the level of quality of life, improving the efficiency of city management, minimizing the negative environmental impact, attracting local and foreign investments, and creating job opportunities [94]. The ministry conducted a study in 2015 on 17 major Saudi cities to investigate their feasibility and eligibility to be transformed into smart cities based on the best smart practices in the world. The study findings indicated that all cities were at the same level of readiness to become a smart city [95]. Accordingly, 10 Saudi cities were selected to be converted into smart cities and build new economic cities and special zones. The implementation was started by preparing the infrastructure and establishing an integrated system to manage all of the city's facilities and services through a smart and interconnected electronic system. One of the most ambitious cities is NEOM City, in which its first phase will be completed by 2025. NEOM is a planned cross-border city in northwestern Saudi Arabia, Tabuk Province with the aim of having smart city technologies.

The development considers all six dimensions of smart cities, which are smart governance, smart economy, smart mobility, smart environment, smart people, and smart living [96]. For example, to achieve a smart environment and living, several slum removal and redevelopment projects have been recently conducted in these cities, such as in Makkah, Jeddah, and Alahsaa [97–100]. For smart mobility, the Saudi government aims to provide universal access and availability of transportation systems that are safe,

affordable, accessible, sustainable, and appropriate for all users, especially for women, children, people with disabilities, and the elderly. In addition, the government aims to improve road safety by expanding the scope of public transportation and reduce death and injury rates from road traffic accidents. In this context, the Haramain High-Speed Railway was opened on 20 March 2020 to link the Muslim holy cities of Medina and Mecca via King Abdullah Economic City to King Abdulaziz International Airport in Jeddah. Moreover, the Riyadh Metro project to build a rapid transit system in Riyadh is under construction, and it is expected to be operational at the end of 2022. To reduce death and injury rates from road traffic accidents, several accident detection systems are being developed globally and locally for configuration in cars [101].

3.2. Questionnaire Design

A questionnaire survey was carried out from February to September 2022 among 263 residents in Saudi Arabia who are potential users of smart city services. A pilot test was conducted before the formal survey to ensure that the questions were clear. The survey was distributed in online and paper formats; however, 20 of online responses were eliminated for further analysis due to missing or inconsistent answers. Accordingly, 234 questionnaires were valid, with an overall response rate of 88.97%. The questionnaire included three main parts as presented in Appendix A and took around 20 min to be completed. The first part consisted of four questions regarding the demographic characteristics including sex, age range, education level, and current city. The second part included 10 questions covering the respondents' perception and concerns of the smart city concept and services, as well as their use of such services. The third part investigated four associated challenges with smart city development, including information security, privacy, compatibility and integration, and technology skills that have been identified from the literature review. It consisted of three subparts, which were: (1) the likelihood of causes of each possible pitfall; (2) the severity of their effects; and (3) the effectiveness of mitigation measures. Five-point Likert-scale questions were used for the responses from 1 (very low) to 5 (very high). Most respondents (i.e., 77.35%) were in the ages ranged between 18 and 45 years, and most of the respondents had a bachelor's degree or higher (i.e., 65.81%). This is because these respondents are more easily accessible in the online questionnaire survey. The demographic information of the respondents is shown in Table 6.

3.3. Semi-Structured Interviews

The semi-structed interview was an interactive communication based on a predetermined thematic framework to identify "why" rather than "how many" [19]. It was also flexible because it was fine-tuned according to the interviewee's reaction. The semi-structured interviews were conducted with (i) stakeholders in the services and projects of smart cities to identify why they do not collaborate with other stakeholders to develop an integrated platform; (ii) disadvantaged groups to identify why they are not involved in smart city services. Table 7 shows the interviewees' profiles for their digital skill gaps.

3.4. Data Analysis

Statistical Packages for the Social Sciences (SPSS) software was used to implement several statistical methods, which were the Cronbach's alpha reliability test, Kendall's concordance analysis, chi-square test of association, and Spearman's rank correlation test. The Cronbach's alpha test was employed to examine the reliability of the questions based on a five-point Likert scale. These questions require a rating from respondents regarding the likelihood and severity of associated challenges of smart city development as well as the effectiveness of the mitigation measures. The obtained Cronbach's alpha coefficient ranged from 0.912 to 0.967, which satisfies the threshold level of 0.7, indicating that the responses on these questions are reliable and internally consistent [102]. The chi-square goodness-of-fit test was used to determine whether the sample percentage follows the population distribution in Saudi Arabia as shown in Table 8. According to the population

statistics [103], the results indicate that the sample proportions are consistent with the population proportions in terms of sex. This is because the *p*-value is not less than 0.05 (i.e., chi-square value = 0.071, *p*-value = 0.789) and, accordingly, there is no sufficient evidence that there is a difference between the sample and population proportions. However, there are differences between the proportions in terms of age, location, and education (i.e., *p*-value is less than 0.05) because the study sample included a greater number of the population aged between 18 and 45 years who were located in Jeddah with a bachelor's degree due to the approachability of these three population groups.

Spearman's rank correlation test was conducted to evaluate the association between involvement in the Saudi Arabian smart cities initiative and demographic variables (i.e., age and education level). The results showed a higher association degree with the population that had a higher education level, with a strong positive correlation ($\rho = 0.879$). On the other hand, the association degree was lower with age, with a weak positive correlation ($\rho = 0.050$).

Table 6. The demographic information of the respondents.

Demographic Criteria	Type	Number of Respondents	Percentage
Sex	Male	136	58.12%
	Female	98	41.88%
Age	18–30	89	38.03%
	31–45	92	39.32%
	46–60	42	17.95%
	More than 60	11	4.7%
Education level	Primary	12	15.1%
	Intermediate	29	12.4%
	Secondary	28	12%
	Diploma	33	14.1%
	Bachelor	92	39.3%
	Master or higher	40	17.1%

Table 7. The interviewees' profiles.

Demographic Criteria	Type	Number of Respondents	Percentage
Sex	Male	9	40.9%
	Female	2	9.1%
Highest Education level	Secondary	8	36.36%
	Diploma	2	9.1%
	Bachelor	1	4.5%

Table 8. Chi-square goodness-of-fit test of the sample compared with the population distribution in Saudi Arabia.

Attributes	Classification	Sample Proportion (%)	Population Proportion (%)	Chi-Square	*p*-Value
Sex	Male	58.12	56.8	0.071	0.789
	Female	41.88	43.2		
Age	18–30	38.03	23.57	11.743	0.008
	31–45	39.32	30.54		
	46–60	17.95	16.55		
	More than 60	4.7	5.86		
Location	Riyadh	21.4	19.12	89.786	0.000
	Jeddah	31.6	12.64		
	Medina	9.8	4.05		
	Dammam	9.4	3.33		
	Makkah	8.5	5.66		
	Yanbu	6.4	0.86		
	Al-Ahsa	3.8	3.84		
	Taif	2.6	2.14		
	Alqatif	1.3	0.28		
	Arar	1.3	0.73		
	Tabuk	1.3	1.21		
	Alkohbar	1.3	1.68		
	Abha	1.3	2.22		
Education	Primary	15.1	12.24	113.98	0.000
	Intermediate	12.4	14.97		
	Secondary school	12	22.4		
	Diploma	14.1	5.50		
	Bachelor	39.3	23.46		
	Master or higher	17.1	2.53		

4. Survey Findings

The next subsections discuss the findings according to their scope and domain. The perspectives and preferences of the respondents on smart city services are first analyzed. Then, the potentials of challenges that could be faced in developing smart cities are discussed, including their causes, effects, and possible solutions.

4.1. Perspectives on Smart City Services

The public understanding about the smart city was assessed to obtain the extent to which the government's vision agrees with the public's understanding of smart cities in Saudi Arabia. Initially, the participants were asked to self-assess their knowledge about the smart city concept in general. The responses indicated that 17.2% of the respondents knew nothing about smart city concept, whereas 24.35% had some knowledge. Most of the respondents, 58.45%, stated that they had some knowledge about the smart city concept. The participants were also questioned about their association and involvement with the Saudi smart cities initiative. The obtained results showed that 16.7% of the respondents had no idea about the smart cities initiative, whereas 31.2% of the participants heard about the initiative but had no interest in it. Around 23.1% of the respondents were very interested in smart city initiatives but were not involved. Only 15.8% of the respondents were involved in the smart city initiative by joining public forums about the initiative or through other means. However, more than 69% had knowledge about the underdevelopment of Saudi smart cities; for instance, 53.9% knew about NEOM City. It can be concluded that the smart city concept is not popular yet among the population of Saudi Arabia.

Most respondents, 59.95%, reported that the services that bring more stable and safer life are more useful and fulfill the population needs in smart cities. Around 31.1% agreed that services that benefit their interpersonal relationships with others are more significant, and 20.35% of the respondents believed that the more significant services are those related to personal development, self-esteem, and self-actualization. The findings reflect the

significance of safety and security services to the public. The relationships between the demographic characteristics of the respondents and their perception of the usefulness of the services were analyzed using Mood's median test because the data followed a non-normal distribution. The median of smart city perception ranged from 0 to 14, with a median value of 1. The findings indicated that there is no significant difference between the respondents' services perception and their sex ($p = 1.000$), age ($p = 0.518$), and location ($p = 0.845$). However, there was a significant statistical difference between the smart city perception and the education level of the respondents ($p = 0.018$). The results showed that 25% of the respondents with a secondary school degree reported the significance of personal development services, and a similar percentage was reported for services that are related to interpersonal relationships with others. On the other hand, 16.6% of postgraduate degree holders stated that personal development services are more useful and important, while the rest selected safety and security services.

4.2. Associated Challenges on Smart City Development

The main concerns of the public about smart city services that were obtained from the literature review were investigated. Information security risks (51.25%) and privacy violations (49.35%) were considered to be the top concerns, especially for the respondents who had a Master's degree or above. This could be because they are working with sensitive and confidential data due to their professional nature. The concerns of digital skill gaps (30.95%) as well as incompatibility between different systems (23.3%) were not considerably high. This is due to the noticeable success of the Human Capability Development Program under the umbrella of the Saudi Vision 2030 in preparing national human capabilities to compete globally, which has been accomplished by instilling values and developing basic and future skills and knowledge [104]. Moreover, several camps and fellowship programs have been organized by several government sectors and entities, such as the Saudi Digital Academy, Misk Academy, Tuwaiq Academy, and others to develop university graduates with essential skills that the labor market needs [105]. Participants who had no concern about smart city development only represents 10.25%, which indicates that the concerns are realistic and considerable and requires further investigation on the causes and solutions. In the following subsections, the findings of the five-point Likert-scale questions are discussed regarding the challenges, causes, effects, and solutions.

4.2.1. Information Security Risks

The main possible causes of information security risks are investigated in terms of occurrence likelihood and severity, as shown in Table 9. Using a mean score ranking, "cyberattacks" cause had the highest likelihood (3.31) with a severity of 3.54 among the other causes. This is due to the high rate of cyberattacks in Saudi Arabia, where 7 million cyberattacks hit the country in the first two months of 2021 [106]. The second highest occurrence likelihood was obtained by the "poor management and operation models of outsourcing products and services". The outsourcing of products and services is an effective management tool to reduce firm costs, focus more on the company's core competencies, and improve flexibility and performance by delegating some responsibilities to external companies. However, it brings significant risks that must be recognized and managed, including security and confidentiality, politics and reputation, delays in task completion, and performance degradation.

The "human errors and negligent staff" cause had the third highest of occurrence likelihood (4.04), although its occurrence likelihood was ranked fourth (3.63). Most information breaches to an extent are related to the exploitation of committed errors or user behaviors of an organization staff; hence, the human factor is considered a key cause of security breaches [107]. It is essential for government and private entities to evaluate human factors and their impact on the vulnerability of the security system and notify individuals who were impacted by information security breaches. It is noticeable that "limited security sponsorship and management support" had the highest severity level (3.73) despite its

occurrence likelihood being the last among the other causes (2.95). This cause could occur in small and large entities; however, it has a low probability in Saudi entities. It mostly leads to other possible causes such as "weak security and encryption" or "poor management and operation models" [108].

Table 9. The likelihood and severity of the possible causes of information security risks from 1 (very low) to 5 (very high).

Possible Cause	Occurrence Likelihood (%)					Mean (Rank)	Severity (%)					Mean (Rank)
	1	2	3	4	5		1	2	3	4	5	
Limited security sponsorship and management support.	10.7	28.8	29.8	16.6	14.1	2.95 (6)	6.8	13.7	21	29.8	28.8	3.60 (1)
Poor management and operation models of outsourcing products and services.	9.9	22.3	28.7	26.2	12.9	3.10 (2)	6.3	11.2	24.3	34	24.3	3.59 (2)
Errors in systems design.	10.9	25.2	30.7	17.8	15.3	3.01 (5)	7	12.4	21.9	31.8	26.9	3.59 (2)
Human errors and negligent staff.	10.7	22.4	33.7	17.6	15.6	3.05 (3)	6.4	12.4	23.3	33.7	24.3	3.57 (3)
Cyberattacks.	9.5	16	30.5	22.5	21.5	3.31 (1)	7.4	13.4	24.8	26.7	27.7	3.54 (3)
Using unsecure legacy systems and poor maintenance.	11	24.5	32.5	16.5	15.5	3.01 (5)	6.8	16	18.9	35.9	22.3	3.51 (5)
Difficult to ensure end-to-end security due to large and interdependent systems with many stakeholders involved.	12.5	21	31	21	14.5	3.04 (4)	5.5	17.0	25.5	27	25	3.49 (4)
Weak security and encryption.	14.7	26.4	26.9	13.2	18.8	2.95 (6)	6	17.6	27.6	22.6	26.1	3.45 (5)

The effects of information security risks were also studied by measuring the mean scores of the severity level as presented in Table 10. The most severe effect was "breaching the confidentiality of user data" with a mean score of 3.31. Data confidentiality is an essential part of information security to prevent the stealing of personal data such as patient profiles, credit cards, or other information. Several cyberattacks have occurred worldwide, targeting personal data. In 2018, for example, 1.5 million patient profiles were stolen from Singapore health authorities and the details of 40,000 credit cards were obtained by accessing the data of 380,000 Hong Kong broadband network customers [88]. Moreover, the severity of "economic loss" and "system failure and non-availability of essential services" was followed by mean scores of 3.28 and 3.07, respectively. According to [109], the amount of cyberattacks increase every year; for instance, 19% of Saudi companies was affected by cyberattacks in 2012 while in 2018, it reached 31%, with a total cost of around USD 692 million.

Table 10. The effects of information security risks from 1 (very low) to 5 (very high).

Effect	Severity (%)					Mean
	1	2	3	4	5	
Breaching the confidentiality of user data.	7.6	14.2	35.5	24.4	18.3	3.31
Economic losses.	7.9	18.8	28.2	27.2	17.8	3.28
System failure and non-availability of essential services.	11.7	25	23.5	24	15.8	3.07

Table 11 presents the ranks of the solutions of information security risks in terms of effectiveness. The most effective solution is to develop a cybersecurity strategy and recovery plan (3.52), followed by implementing general technical countermeasures such as frequent backups, anti-virus programs, software updates, etc. (3.47). The cybersecurity strategy includes a series of objectives and principles that must be implemented. For instance, the National Cybersecurity Authority in Saudi Arabia have developed extensive cybersecurity policies and relevant practice guides to share them with relevant entities and have followed up on their compliance [110]. However, it is impossible to completely mitigate the security violations; hence, it is essential to prepare recovery plans to reduce the effect and damage of an incident. Other effective solutions include employing/developing

well-defined standards for developing and managing ICT services (3.47) and improving security awareness and availability safeguards and conducting continuous vulnerability assessment (3.37). Decision-makers should adopt standards that optimize the system security of smart cities where different standards for different scopes of work were proposed by different standardization organizations such as the ISO, IEEE, and ETSI.

Table 11. Solutions of information security risks from 1 (very low) to 5 (very high).

Solution	Effectiveness (%)					Mean
	1	2	3	4	5	
Developing a cybersecurity strategy and recovery plan.	5.8	12.6	28	30.9	22.7	3.52
General technical countermeasures such as frequent backups, anti-virus programs, software updates, and firewalls against intruders.	6.8	15	26.1	29	23.2	3.47
Employing/developing well-defined standards for developing and managing ICT services.	6.4	16.2	26.5	26.5	24.5	3.47
Improving security awareness and availability safeguards and conducting continuous vulnerability assessment.	8.3	15.6	25.9	31.2	19	3.37
Management controls over operation and design.	5.9	20	34.1	24.9	15.1	3.23

4.2.2. Privacy Violation

Privacy violation was rated as the second highest concern with 49.35% responses. Surprisingly, 92.36% of the participants who expressed their worry about privacy violations either never read disclaimers/conditions (58.81%) or read it sometimes (41.19%). On the other hand, around 7.64% of the respondents who expressed their worry about privacy violations always read disclaimers/conditions. The study also investigated if the respondents would stop using a system or installing an application if they do not accept disclaimers/conditions. Slightly less than half (45.2%) reported that they would stop using the application/system while the majority (48.4%) reported they might stop depending on the application/system. Only 6.5% of the respondents would stop using the application/system, which emphasizes the necessity of improving user privacy awareness and behavior by educating them about privacy-related topics. The ignorance of disclaimers/conditions could lead to the possible intrusion and misuse of personal information as most applications declare that user data will be used for other external/third parties or for other unknown purposes.

The study also investigated the types of information that the participants were unwilling to reveal during the downloading or usage of services and applications. The participants were asked about four common information types or any others, including location, email address, phone number, and social media accounts. Location gained the most negative responses (47.65%), followed by phone number (40.08%) and social media accounts (39.65%). This finding is possibly because sharing location could be used by unauthorized parties to track users or derive the users' behavior patterns based on location information during a period. Moreover, the users can be identified by their behavioral patterns and other information such as email address, resident address, and social media account. A small percentage (1.85%) of the participants were willing to reveal their information to use services/applications.

The findings of investigating the possible causes of privacy violation are presented in Table 12. The highest severity level could occur through "unauthorized access to systems" (3.67), with the third highest occurrence likelihood rank (3.02). Privacy violations represent any act against privacy rules and policies, which include the unauthorized access of data and systems, unauthorized copying or transferring of data, selling of data to a third party, or other instances [111,112]. The lack of knowledge and awareness on data protection was considered the second top severity cause of privacy violation (3.64). This cause had the highest likelihood (3.05), which emphasizes the necessity of improving public awareness. A recent study reported that 53.4% of the study respondents were not aware of cybersecurity laws in Saudi Arabia [113]. Several studies have shown that the level of

information security awareness has a positive relationship on the security-related behaviors of the individuals [114]. The absence of strict regulations to protect user data also had a high severity level (3.53); however, it had the lowest probability of occurrence (3.52). The wide use of big data technology, especially in smart cities, leads to a collection of excessive personal data and consequently the possibility of privacy violations. In such a case, individuals do not have strong control over their personal data.

Table 12. The likelihood and severity of the possible causes of privacy violation from 1 (very low) to 5 (very high).

Possible Cause	Occurrence Likelihood (%)					Mean	Severity (%)					Mean
	1	2	3	4	5	(Rank)	1	2	3	4	5	(Rank)
Unauthorized access to systems.	10.5	27.7	28.3	16.8	16.8	3.02 (3)	5	12	22	33	28	3.67 (1)
Users do not have enough knowledge and awareness on data protection.	11.7	25	28.6	16.3	18.4	3.05 (1)	6.5	11.5	24	27.5	30.5	3.64 (2)
No strict regulation to protect user data.	8.8	28.5	29	20.7	13	3.01 (4)	7.9	12.8	24.6	27.6	27.1	3.53 (3)
Integration and ubiquity of IoT-enabled systems in which personal data of users are utilized without prior permission or notice.	10.4	27.6	26	19.8	16.1	3.04 (2)	8.4	11.8	25.6	28.1	26.1	3.52 (4)

Due to the fact smart cities may pose threats to public privacy, decision-makers must pay more attention to privacy protection. The severity analysis of the effects of privacy violations, as presented in Table 13, has indicated that information exposure, citizen tracking, or impersonation has the most severe consequence (3.31), followed by economic loss (3.28) and risking public trust towards the society and posing threat to democracy (3.07).

Table 13. The severity effects of privacy violation from 1 (very low) to 5 (very high).

Effect	Severity (%)					Mean
	1	2	3	4	5	
Risking public trust towards the society and posing threat to democracy.	9.3	15.1	25.9	27.8	22	3.31
Economic losses.	6.5	13.5	29.5	26	24.5	3.28
Information exposure, citizen tracking, or impersonation.	6.8	16.6	27.3	27.3	22	3.07

According to Table 14, the most effective mitigation measure for protecting the public's privacy is to establish standards on how public data can be collected and used (3.45). The first federal Personal Data Protection Law (PDPL) to regulate the processing of personal data was issued in September 2021 and enforced starting March 2022. It is expected that organizations will make significant changes to operate according to the regulations. Date is collected ubiquitously in smart cities; hence, several solutions could be conducted along with privacy regulations to ensure privacy protection, including educating and training users to improve their knowledge and awareness of information privacy (3.44). The developers must also be educated and trained regarding their responsibilities and best practices. However, privacy regulations have a direct impact on privacy protection compared with improving public awareness, which is a long-term solution. The third effective solution is to conduct privacy impact assessments (PIA) to assist organizations in obtaining and managing privacy risks that might arise from new projects, initiatives, systems, processes, etc. (3.40).

4.2.3. Incompatibility between Different Systems

Different possible causes could lead to the incompatibility between different systems. The incompatibility issue arises from the management and planning slacks rather than the technology itself at the levels of either entities or country. As shown in Table 15, the analysis has indicated that the independent development and non-integrated services and applications have the highest severity level among the other causes (3.55), with an

occurrence likelihood of 2.98. The second highest risky cause (3.52) is that governments usually have information of a confidential nature and risk-averse policies, which had a possibility of occurrence of 3.06. This is reflected in policies, laws, and political force that could be enforced for project approval, resource monitoring, and management. The cause with the third highest severity is the incompatible data standards and formats, where the mean of severity level was 3.49 and the mean of occurrence likelihood was 2.95.

Table 14. Solutions of privacy violations from 1 (very low) to 5 (very high).

Solution	Effectiveness (%)					Mean
	1	2	3	4	5	
Establishing standards on how public data could be collected and used.	5.8	17	27.7	25.7	23.8	3.45
Legislation to allow users to control their own data and create a regulatory environment.	6.3	13.2	30.7	29.8	20	3.44
Utilizing education and training to help improve user knowledge and awareness of information privacy and informing developers of their responsibilities and best exercises.	7.2	15.9	27.5	28	21.3	3.40
Employing privacy by design (PbD).	6.9	15.7	32.4	26	19.1	3.35
Conducting privacy impact assessments (PIA).	7	16.5	34	29.5	13	3.25

Table 15. Likelihood and severity of the possible causes of incompatibility between systems from 1 (very low) to 5 (very high).

Possible Cause	Occurrence Likelihood (%)					Mean (Rank)	Severity (%)					Mean (Rank)
	1	2	3	4	5		1	2	3	4	5	
Independent development and non-integrated services and applications.	10.4	29.4	26.9	18.4	14.9	2.98 (2)	5.9	13.4	26.2	28.7	25.7	3.55 (1)
Governments have information of a confidential nature and risk-averse policies.	9.5	30.7	24.1	16.1	19.6	3.06 (1)	8.7	13.8	22.4	27	28.1	3.52 (2)
Incompatible data standards and formats.	10.4	27.7	33.2	14.4	14.4	2.95 (3)	6	13	29.5	29.5	22	3.49 (3)
Difficult to engage with a broad number of stakeholders.	10.8	27.6	34	14.8	12.8	2.91 (4)	6.9	16.3	23.2	32.5	21.2	3.45 (4)

The study of the severity level of the effects of incompatibility between different systems, as illustrated in Table 16, has shown that the most severe effect is reducing the efficiency of smart cities (3.36). This is followed by the severity of replicated facilities, resources wasting and overlapping, (3.33), and discomfort and dissatisfaction (3.29). For instance, developing different systems or platforms for the same service without integration could require the users to switch between these systems or platforms to search for relevant information.

Table 16. The severity effects of incompatibility between systems from 1 (very low) to 5 (very high).

Effect	Severity (%)					Mean
	1	2	3	4	5	
Reducing the efficiency of smart cities.	8	14.4	31.8	24.9	20.9	3.36
Discomfort and dissatisfaction	8.9	16.7	26.1	28.6	19.7	3.33
Replicated facilities, resources wasting, and overlapping.	9.4	15.3	28.7	29.7	16.8	3.29

Table 17 illustrates the findings of studying the solutions to address the issues arising from the incompatibility between different systems. The most effective solution is to formulate open standards and improve data quality (3.83). The open standards will facilitate using and transferring data across different systems and sectors, consequently enhancing the quality of services, especially services that require processing by multiple sectors. The second most effective solution is to plan the process of systems and data integration at

the design stage (3.58), where it ensures the compatibility between systems and devices proactively without compromising the functionality. It is also an effective solution for promoting cross-sectional collaboration between different interfacing organizations (3.57).

Table 17. The solutions of incompatibility between systems from 1 (very low) to 5 (very high).

Solution	Effectiveness (%)					Mean
	1	2	3	4	5	
Formulating open standards and improving data quality.	5.9	14.9	30.2	26.7	22.3	3.83
Planning the process of systems and data integration at the design stage.	7.4	11.8	32.4	25.5	23	3.58
Promoting cross-sectional collaboration among different interfacing organizations.	8.4	15.8	24.1	32.5	19.2	3.57
Sharing interoperable protocols among tech suppliers.	8.5	17	29	28.5	17	3.18

To identify the reasons of the incompatibility between different systems, five face-to-face interviews were conducted with stakeholders involved in smart city services. Four major concerns of compatibility and integration between services were identified as follows: (1) extra cost for facility procurement, legacy system upgrade, and extra manpower; (2) disclosing the information of systems and services may leak business conditions and other confidential information; (3) ownership of data in an integrated platform and services; and (4) developing their own platform and services to make more profits.

4.2.4. Digital Skill Gaps

The digital skill gaps concern was investigated by posing five-point Likert scale questions regarding the frequency and difficulty of using existing e-services such as online mapping, navigation systems, etc. The responses indicated that around 34.91% of the respondents were always using e-services in their daily life. Interestingly, only 7.6% of the respondents reported that they do not use e-services in their daily life. The other ratings were 22.5% for frequently, 20.14% for sometimes, and 14.85% for seldom. On the other hand, the rating percentage of the responses regarding the ease of utilizing e-services was 27.6% for very easy, 22.75% for easy, 18.3% for moderate, 14.85% for difficult, and 16.5% for very difficult. The proportion of elderly participants (more than 45 years old) who reported that using e-services was very difficult was 49%. Around 81.82% of the respondents who were more than 60 years old reported that using e-services was very difficult compared to the 16.67% reported by participants aged 45–60 years; on the other hand, this was reported by 20% of participants aged 31–35 years and 11.11% of participants aged 18–30 years. This indicates that the usage difficulty is higher in elderly groups than the younger ones. However, it can be generalized that e-services are sometimes used (mean = 2.89) and moderately (mean = 3.28), as the mean values are between 2.61 and 3.40.

Table 18 shows the analysis of the likelihood and severity of possible causes of digital skill gaps. The analysis of the possible causes of digital skill gaps has shown that the highest severity (3.65) could occur due to the lack of digital literacy skills, with a possibility of occurrence of 2.99. Different sectors could actively contribute to the learning process such as project building companies, non-profit organizations, and authorities. In this context, the Ministry of Communications and Information Technology in collaboration with public and private sectors have established Attaa Digital in 2018, which is a non-profit specialized initiative to overcome digital literacy and improve digital skills in all members of society [115]. The initiative until July 2021 presented more than 1900 training programs and reached more than 18 million beneficiaries. The initiative also supported 113,000 low-income families with more than 28,000 tablets and 110,000 data chips [116]. The second most risky cause was the poor quality of services (3.60), with a mean score of likelihood of 2.99. A recent study inspected the customer satisfaction of Saudi telecommunication companies by analyzing tweets related to their services including network coverage, quality of voice transmission, Internet speed, customer services, successful calls, etc. [117]. The results showed that the average level of customer satisfaction with the services of the three

companies is below 50%. Information and communications technologies are the backbone of smart cities development; hence, improving the services is necessary to meet the expectations of the public and requirements of developing smart cities. The third most risky cause was the lack of training programs for unskilled citizens (3.60), where the occurrence likelihood was 2.85. Despite the large number of academies and initiatives that have been established to provide training programs for unskilled citizens, more training programs are needed to build up the capability of enjoying the benefits brought by smart cities.

Table 18. Likelihood and severity of the possible causes of digital skill gaps from 1 (very low) to 5 (very high).

Possible Cause	Occurrence Likelihood (%)					Mean	Severity (%)					Mean
	1	2	3	4	5	(Rank)	1	2	3	4	5	(Rank)
Lack of digital literacy skills.	10.3	24.5	33.8	18.6	12.7	2.99 (2)	6.9	10.3	21.6	33.8	27.5	3.65 (1)
Poor quality of services.	9.3	27.3	31.7	18.5	13.2	2.99 (2)	6.4	12.3	24.1	29.6	27.6	3.60 (2)
Unavailability of Internet access and digital services.	12.9	30.8	28.4	13.9	13.9	2.85 (4)	6.5	11.5	25.5	29	27.5	3.60 (2)
Society does not participate in government initiatives.	10.3	28.1	28.6	16.3	16.7	3.01 (1)	8	14	22	30	26	3.52 (3)
Lack of training programs for unskilled citizens.	10.1	31.3	28.3	18.7	11.6	2.90 (3)	6.5	12.9	27.4	28.4	24.9	3.52 (3)
Lack of care for people with special needs.	11.6	36.7	23.6	15.6	12.6	2.81 (5)	8	10.9	26.9	30.8	23.4	3.51 (4)

The severity level of the effects of digital skill gaps indicated that the most severe effect is the economic and social inequality (3.25) followed by reducing the effectiveness of smart cities (3.23), as shown in Table 19. The smart cities in Saudi Arabia are still emerging and not all services are digitalized; thus, the severity of the effects was not ranked very high. The continued growth of smart cities could divide the public by providing access to more information and benefits for specific groups rather than for disadvantaged and excluded individuals.

Table 19. The severity effects of digital skill gaps from 1 (very low) to 5 (very high).

Effect	Severity (%)					Mean
	1	2	3	4	5	
Economic and social inequality	5.9	19.3	34.7	23.8	16.3	3.25
Reducing the effectiveness of smart cities.	7.9	19.3	30.7	25.7	16.3	3.23

According to Table 20, the most efficient solution is to provide financial support for computer acquisition or Internet access and decrease telecommunications charges (3.54). This is followed by mitigating the effect of digital skill gaps and providing education and training programs to unskilled people (3.51). Another effective solution is to motivate the public and private sectors to initiate and get involved in digital initiatives (3.49). Such solutions will overcome the attitude barriers and concerns dividing the public in aspects of service benefits.

Table 20. The solutions of digital skill gaps from 1 (very low) to 5 (very high).

Solution	Effectiveness (%)					Mean
	1	2	3	4	5	
Providing financial support for computer acquisition or Internet access and decreasing telecommunications charges.	6.4	13.7	22.1	34.8	23	3.54
Providing education and training and facilitate social learning for the public	6.8	11.7	27.7	31.1	22.8	3.51
Motivating digital inclusion initiatives of both citizens and private sectors.	5.9	12.3	29.6	31.5	20.7	3.49
Improving public services and enhancing their information literacy.	6.8	16.9	26.1	24.6	25.6	3.45
Increasing the penetration of digital devices.	5.9	22.1	30.4	25.5	16.2	3.24

To further investigate the reasons behind the digital skill gaps, the authors interviewed nine old males and two old females in the age range between 61 and 75 years old with different education levels. Eight of the interviewees owned smartphones, whereas only three owned dumbphones that could not run most applications and services. The interviewees were using electronic devices/services rarely, such as for calling, chatting, and sharing photos via the WhatsApp application. They were facing difficulty in using electronic devices due to either poor digital literacy or poor eyesight. Four participants expressed their interest in conducting training and workshops on how to use electronic devices. The other participants considered such training unnecessary as they usually asked for help from their family members and friends. Although the elderly seldom has needs for electronic devices and services in their daily life, it is better to educate them and improve digital literacy before more city services are digitalized.

5. Discussion

According to the findings, this section highlights the practices that could help overcome the associated challenges of smart city development by enriching the existing theory and by improving the managerial practice. One of the significant practices is the regular evaluation of the impact of organizations' staff on the vulnerability of the security system and accordingly conducting essential training and workshops. Such practices will significantly reduce the security breaches from the exploitation of committed errors or user behaviors of an organization's staff. Globally, each national cybersecurity authority should develop and implement extensive cybersecurity policies and relevant practice guides that must be followed by the relevant groups and individuals. Moreover, all authorities should emphasize adopting standards that optimize system security and reduce the incompatibility between smart city systems.

Another practice that could significantly enhance privacy is developing regulations on how public data can be collected and used. Simultaneously, educating and training users about these regulations will improve their knowledge and awareness of information privacy. Promoting and supporting cross-sectional collaboration between different interfacing organizations and accordingly considering the integration between their systems at the design stage are effective practices for mitigating the incompatibility between different smart city systems. Financial support for computer acquisition and Internet access is the most effective practice for promoting the utilization of digital technologies and consequently the digital skill gaps.

6. Conclusions

Information and communication technologies play a key role in the development of smart cities; however, it is only viewed as a solution towards specific problems in urban planning and management without taking into consideration the several challenges and negative effects. This paper revealed these challenges by conducting a comprehensive literature review and event-based research on the Saudi Arabian population. According to the findings, information security risks, privacy violation, incompatibility between systems, and digital skill gaps are the major challenges. Implementing a cybersecurity strategy (e.g., the National Cybersecurity Authority in Saudi Arabia) and recovery plan to reduce the effect and damage of any possible incident are effective solutions for mitigating information security risks. Privacy violations could be addressed by regulating how public data can be collected and used in addition to improving the public's knowledge and awareness of information privacy. Formulating open standards and planning the process of systems and data integration at the design stage facilitate the usage and transferring of data across different systems and ensure the compatibility between systems and devices. Digital skill gaps could be addressed by providing financial support for computer acquisition and Internet access, as well as providing education and training programs. However, the limitation of this study is that some questionnaire items do not consider some personal determinant factors such as the difference in terms of ICT knowledge, smart cities awareness, and personal

innovativeness. Thus, it is encouraged in future studies to examine how the differences between the public in terms of ICT knowledge, personal innovativeness, and awareness about the smart city concept could affect their preferences and perceptions.

Author Contributions: Conceptualization, M.B. and S.A.A.; methodology, M.B. and S.A.A.; validation, S.A.A. and M.B.; writing—original draft preparation, M.B.; writing—review and editing, M.B. and S.A.A.; project administration, S.A.A.; funding acquisition, S.A.A. and M.B. All authors have read and agreed to the published version of the manuscript.

Funding: The authors extend their appreciation to the Deputyship for Research & Innovation, Ministry of Education in Saudi Arabia for funding this research work through project number MoE-IF-G-20-10.

Institutional Review Board Statement: The study was conducted in accordance with the Declaration of Helsinki, and approved by the Bioethics of Scientific and Medica Research of University of Jeddah (protocol code HAP-02-J-094 and date of approval 31 August 2022).

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A Perceptions, and Concerns of Population on Smart City Concept

The smart city concept employs information and communication technologies to enhance quality of life by facilitating the more efficient and sustainable management of cities. This survey questionnaire aims to understand perceptions and concerns of the population regarding the smart city concept and services. The questionnaire includes three main parts as presented and takes around 20 min to be completed. The first part consists of four questions regarding the demographic characteristics, including sex, age range, education level, and current city. The second part includes 10 questions covering the respondents' perception and concerns of the smart city concept and services, as well as their use of such services. The third part investigates four associated challenges with smart city development, including information security risks, privacy violation, incompatibility between different systems, and digital skill gaps that have been identified from the literature review. It consists of three subparts, which are: (1) the likelihood of causes of each possible pitfall; (2) the severity of their effects; and (3) the effectiveness of mitigation measures.

PART A. Demographic Information.

1.	What is your sex?					
(a)	Male	(b) Female				
2.	What is your age range?					
(a)	18–30	(b) 31–45	(c) 46–60			(d) More than 60
3.	What is your education level?					
(a)	Primary	(b) Intermediate	(c) Secondary	(d) Diploma	(e) Bachelor	(f) Master or higher
4.	What is your current city?					
(a)	Riyadh	(b) Jeddah	(c) Makkah	(d) Madinah	(e) Yonbu	(f) Dammam
(g) Alahsa		(h) Other, please specify _____.				

PART B. Smart City Concept and Services.

5.	How much do you know about the smart city concept?			
(a)	No idea	(b) Very little	(c) Some knowledge	(d) Very well
6.	Name any smart city project you know about (if any):			
_____.				
7.	Smart city aims to improve quality of life using information and communication technologies. What are your concerns regarding the smart city concept? (may choose multiple answers)			
(a)	Information security (e.g., cyberattacks, system break-down)	(b) Privacy of personal data.	(c) Integration and compatibility between different systems and devices.	(d) Skills shortage of using advanced technologies.
(e) No concerns.	(f) Other, please specify _____.			
8.	How would you rate your participation and involvement in Saudi smart cities initiative?			
(a)	I have no idea about it.	(b) I heard but am not interested about it.	(c) I am very interested but not involved.	(d) I participated in public forums about the initiative.
(e) Other, please specify _____.				
9.	What is the type of smart city services that you think are more useful and fulfill population needs?			
(a)	Services that bring more stable and safer life.	(b) Services that contribute to my relationship with other people.	(c) Services that are conducive to my personal development, self-esteem, and self-actualization.	
10.	How often do you use e-services in your daily life such as online mapping, navigation systems, etc.?			
	1 = never ⟶ 5 = always			
(a)	1 (b) 2	(c) 3	(d) 4	(e) 5
11.	How you usually feel when you use e-services such as online mapping, navigation systems, etc.?			
	1 = never ⟶ 5 = always			
(a)	1 (b) 2	(c) 3	(d) 4	(e) 5
12.	Do you read the disclaimers/conditions when you use a new device or application?			
(a)	Never.	(b) Yes, sometimes.	(c) Yes, always.	
13.	Will you stop using a device or installing an application because you do not accept the disclaimers/conditions?			
(a)	Never.	(b) Yes, sometimes.	(c) Yes, always.	
14.	What is the personal information that you will not give when you use a device or an application? (May choose multiple answers)			
(a)	Location (tracking)	(b) Email address	(c) Phone number	(d) Social media accounts
(e) Other, please specify _____.				

PART C. Likelihood and Severity of Associated Challenges of Smart City Development.

(1) **Likelihood of possible causes**

Please rate the likelihood and severity of each possible pitfall from 1 (very low) to 5 (very high).

Associated Pitfall	Possible Cause	Occurrence Likelihood						Severity					
		Don't know	1	2	3	4	5	Don't know	1	2	3	4	5
Information security	Weak security and encryption.												
	Cyberattacks.												
	Difficult to ensure end-to-end security due to large and interdependent systems with many stakeholders involved.												
	Errors in systems design.												
	Poor management and operation models of outsourcing product and services.												
	Limited security sponsorship and management support.												
	Using unsecure legacy systems and poor maintenance.												
	Human errors and negligent staff.												
	Other, please specify.												
Privacy	Integration and ubiquity of IoT-enabled systems in which personal data of users are utilized without prior permission or notice.												
	Unauthorized access to systems.												
	Users do not have enough knowledge and awareness of data protection.												
	No strict regulations to protect user data.												
	Other, please specify.												
Compatibility and integration	Incompatible data standards and formats.												
	Difficult to engage with a broad number of stakeholders.												
	Independent development and non-integrated services and applications.												
	Governments have information of a confidential nature and risk-averse policies.												
	Other, please specify.												
Technology skills	Unavailability of Internet access and digital services.												
	Lack of digital literacy skills.												
	Poor quality of services.												
	Lack of care for people with special needs.												
	Lack of training programs for unskilled citizens.												
	Society does not participate in government initiatives.												
	Other, please specify.												

(2) **Effects of challenges**

Please rate the severity of each pitfall from 1 (very low) to 5 (very high).

Associated Pitfall	Effect	Severity					
		Don't know	1	2	3	4	5
Information security	System failure and non-availability of essential services.						
	Breaching the confidentiality of user data.						
	Economic losses.						
	Other, please specify.						
Privacy	Information exposure, citizen tracking, or impersonation.						
	Risking public trust towards the society and posing a threat to democracy.						
	Economic losses.						
	Other, please specify.						
Compatibility and integration	Replicated facilities, resources wasting, and overlapping.						
	Reducing the efficiency of smart cities.						
	Discomfort and dissatisfaction						
	Other, please specify.						
Technology skills	Economic and social inequality						
	Reducing the effectiveness of smart cities.						
	Other, please specify.						

(3) **Effectiveness of mitigation measures**

Please rate the effectiveness of the following mitigation measures for smart city development from 1 (very low) to 5 (very high).

Associated Pitfall	Solution	Effectiveness					
		Don't know	1	2	3	4	5
Information security	Management controls over operation and design.						
	General technical countermeasures such as frequent backups, anti-virus programs, software updates, and firewalls against intruders.						
	Employing/developing well-defined standards for developing and managing ICT services.						
	Improving security awareness and availability safeguards and conducting continuous vulnerability assessments.						
	Developing a cyber security strategy and recovery plan.						
	Other, please specify.						
Privacy	Establishing standards on how public data could be collected and used.						
	Utilizing education and training to help improve user knowledge and awareness of information privacy; informing developers of their responsibilities and best practices.						
	Legislation to allow users to control their own data and create a regulatory environment.						
	Employing privacy by design (PbD).						
	Conducting privacy impact assessments (PIA).						
	Other, please specify.						
Compatibility and integration	Sharing interoperable protocols among tech suppliers.						
	Formulating open standards and improving data quality.						
	Promoting cross-sectional collaboration among different interfacing organizations.						
	Planning the process of systems and data integration at the design stage.						
	Other, please specify.						
Technology skills	Increasing the penetration of digital devices.						
	Providing financial support for computer acquisition or Internet access and decreasing telecommunications charges.						
	Providing education and training, facilitate social learning to the public						
	Improving public services and enhancing their information literacy.						
	Motivating digital inclusion initiatives for both citizens and private sectors.						
	Other, please specify.						

References

1. Alawadhi, S.; Aldama-Nalda, A.; Chourabi, H.; Gil-Garcia, J.R.; Leung, S.; Mellouli, S.; Nam, T.; Pardo, T.A.; Scholl, H.J.; Walker, S. Building understanding of smart city initiatives. In *International Conference on Electronic Government*; Springer: Berlin/Heidelberg, Germany, 2012; pp. 40–53.
2. Ismagilova, E.; Hughes, L.; Dwivedi, Y.K.; Raman, K.R. Smart cities: Advances in research—An information systems perspective. *Int. J. Inf. Manag.* **2019**, *47*, 88–100. [CrossRef]
3. Giffinger, R.; Fertner, C.; Kramar, H.; Meijers, E. City-ranking of European medium-sized cities. *Cent. Reg. Sci. Vienna UT* **2007**, *9*, 1–12.
4. Sallam, A.; Almohammedi, A.A.; Gaid, A.S.; Shihab, Y.A.; Sadeq, M.; Abdulaziz, S.E.; Abduasalam, S.; Abdulhaleem, Y.; Shepelev, V. Performance Evaluation of Fog-Computing Based on IoT Healthcare Application. In Proceedings of the 2021 International Conference of Technology, Science and Administration (ICTSA), Taiz, Yemen, 22–24 March 2021; pp. 1–6.
5. Yusof, M.H.M.; Zin, A.M.; Satar, N.S.M. Behavioral Intrusion Prediction Model on Bayesian Network over Healthcare Infrastructure. *CMC Comput. Mater. Contin.* **2022**, *72*, 2445–2466.
6. Balfaqih, H.; Yunus, B. Supply chain performance in electronics manufacturing industry. In *Applied Mechanics and Materials*; Trans Tech Publications Ltd.: Stafa-Zurich, Switzerland, 2014; Volume 554, pp. 633–637.
7. Mittereder, M. Smart City Index: Vienna and London Lead the Worldwide Ranking. Roland Berger. 2019. Available online: https://www.rolandberger.com/en/Media/Smart-City-Index-Vienna-and-London-lead-the-worldwide-ranking.html (accessed on 1 May 2022).
8. Siemens. 2016. Available online: http://www.siemens.com.sa/pool/about/Smart_cities_Saudi_Arabia_study.pdf (accessed on 1 May 2022).
9. Golubchikov, O.; Thornbush, M. Artificial intelligence and robotics in smart city strategies and planned smart development. *Smart Cities* **2020**, *3*, 56. [CrossRef]
10. Edwards, L. Privacy, security and data protection in smart cities: A critical EU law perspective. *Eur. Data Prot. L. Rev.* **2016**, *2*, 28. [CrossRef]
11. Townsend, A.M. *Smart Cities: Big Data, Civic Hackers, and the Quest for a New Utopia*; WW Norton & Company: New York, NY, USA, 2013.
12. Symantec. Internet Security Threat Report. 2019. Available online: https://docs.broadcom.com/doc/istr-24-2019-en (accessed on 23 February 2022).
13. House of Commons. Digital Skills Crisis: Second Report of Session 2016–17. 2016. Available online: https://www.publications.parliament.uk/pa/cm201617/cmselect/cmsctech/270/270.pdf (accessed on 23 February 2022).
14. Caragliu, A.; Del Bo, C.; Nijkamp, P. *Smart Cities in Europe*; Routledge: London, UK, 2013; pp. 185–207.
15. Ma, R.; Lam, P.T.; Leung, C.K. Potential pitfalls of smart city development: A study on parking mobile applications (apps) in Hong Kong. *Telemat. Inform.* **2018**, *35*, 1580–1592. [CrossRef]
16. Lam, P.T.; Yang, W. Factors influencing the consideration of Public-Private Partnerships (PPP) for smart city projects: Evidence from Hong Kong. *Cities* **2020**, *99*, 102606. [CrossRef]
17. Hasan, M.K.; Akhtaruzzaman, M.; Kabir, S.R.; Gadekallu, T.R.; Islam, S.; Magalingam, P.; Hassan, R.; Alazab, M.; Alazab, M.A. Evolution of industry and blockchain era: Monitoring price hike and corruption using BIoT for smart government and industry 4.0. *IEEE Trans. Ind. Inform.* **2022**, *18*, 9153–9161. [CrossRef]
18. Chang, I.C.C.; Jou, S.C.; Chung, M.K. Provincialising smart urbanism in Taipei: The smart city as a strategy for urban regime transition. *Urban Stud.* **2021**, *58*, 559–580. [CrossRef]
19. Fylan, F. Semi-structured interviewing. *Handb. Res. Methods Clin. Health Psychol.* **2005**, *5*, 65–78.
20. Yigitcanlar, T.; Desouza, K.C.; Butler, L.; Roozkhosh, F. Contributions and risks of artificial intelligence (AI) in building smarter cities: Insights from a systematic review of the literature. *Energies* **2020**, *13*, 1473. [CrossRef]
21. Allam, Z.; Dhunny, Z.A. On big data, artificial intelligence and smart cities. *Cities* **2019**, *89*, 80–91. [CrossRef]
22. Appio, F.P.; Lima, M.; Paroutis, S. Understanding Smart Cities: Innovation ecosystems, technological advancements, and societal challenges. *Technol. Forecast. Soc. Change* **2019**, *142*, 1–14. [CrossRef]
23. Paiva, S.; Ahad, M.A.; Tripathi, G.; Feroz, N.; Casalino, G. Enabling technologies for urban smart mobility: Recent trends, opportunities and challenges. *Sensors* **2021**, *21*, 2143. [CrossRef]
24. Pundir, A.; Singh, S.; Kumar, M.; Bafila, A.; Saxena, G.J. Cyber-Physical Systems Enabled Transport Networks in Smart Cities: Challenges and Enabling Technologies of the New Mobility Era. *IEEE Access* **2022**, *10*, 16350–16364. [CrossRef]
25. Ahmad, M.; Ahad, M.A.; Alam, M.A.; Siddiqui, F.; Casalino, G. Cyber-Physical Systems and Smart Cities in India: Opportunities, Issues, and Challenges. *Sensors* **2021**, *21*, 7714. [CrossRef] [PubMed]
26. Bilal, M.; Usmani, R.S.A.; Tayyab, M.; Mahmoud, A.A.; Abdalla, R.M.; Marjani, M.; Pillai, T.R.; Targio Hashem, I.A. Smart cities data: Framework, applications, and challenges. *Handb. Smart Cities* **2020**, 1–29. [CrossRef]
27. Rao, P.M.; Deebak, B.D. Security and privacy issues in smart cities/industries: Technologies, applications, and challenges. *J. Ambient. Intell. Humaniz. Comput.* **2022**, 1–37. [CrossRef]
28. Singh, S.; Sharma, P.K.; Yoon, B.; Shojafar, M.; Cho, G.H.; Ra, I.H. Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city. *Sustain. Cities Soc.* **2020**, *63*, 102364. [CrossRef]
29. Sadik, S.; Ahmed, M.; Sikos, L.F.; Islam, A.K.M. Toward a sustainable cybersecurity ecosystem. *Computers* **2020**, *9*, 74. [CrossRef]
30. D'Amico, G.; L'Abbate, P.; Liao, W.; Yigitcanlar, T.; Ioppolo, G. Understanding sensor cities: Insights from technology giant company driven smart urbanism practices. *Sensors* **2020**, *20*, 4391. [CrossRef] [PubMed]
31. Al Sharif, R.; Pokharel, S. Smart City Dimensions and Associated Risks: Review of literature. *Sustain. Cities Soc.* **2021**, *77*, 103542. [CrossRef]

32. Sharma, M.; Joshi, S.; Kannan, D.; Govindan, K.; Singh, R.; Purohit, H.C. Internet of Things (IoT) adoption barriers of smart cities' waste management: An Indian context. *J. Clean. Prod.* **2020**, *270*, 122047. [CrossRef]
33. Ismagilova, E.; Hughes, L.; Rana, N.P.; Dwivedi, Y.K. Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework. *Inf. Syst. Front.* **2020**, *24*, 1–22. [CrossRef] [PubMed]
34. Lee, I. Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management. *Future Internet* **2020**, *12*, 157. [CrossRef]
35. Ande, R.; Adebisi, B.; Hammoudeh, M.; Saleem, J. Internet of Things: Evolution and technologies from a security perspective. *Sustain. Cities Soc.* **2020**, *54*, 101728. [CrossRef]
36. Neshenko, N. Illuminating Cyber Threats for Smart Cities: A Data-Driven Approach for Cyber Attack Detection with Visual Capabilities. Ph.D. Thesis, Florida Atlantic University, Boca Raton, FL, USA, 2021.
37. Habibzadeh, H.; Nussbaum, B.H.; Anjomshoa, F.; Kantarci, B.; Soyata, T. A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities. *Sustain. Cities Soc.* **2019**, *50*, 101660. [CrossRef]
38. Ullah, F.; Qayyum, S.; Thaheem, M.J.; Al-Turjman, F.; Sepasgozar, S.M. Risk management in sustainable smart cities governance: A TOE framework. *Technol. Forecast. Soc. Change* **2021**, *167*, 120743. [CrossRef]
39. Fan, J.; Yang, W.; Lam, K.Y. Cybersecurity Challenges Of IoT-enabled Smart Cities: A Survey. *arXiv* **2022**, arXiv:2202.05023.
40. Botello, J.V.; Mesa, A.P.; Rodríguez, F.A.; Díaz-López, D.; Nespoli, P.; Mármol, F.G. BlockSIEM: Protecting smart city services through a blockchain-based and distributed SIEM. *Sensors* **2020**, *20*, 4636. [CrossRef]
41. Priyanka, E.B.; Thangavel, S. Influence of Internet of Things (IoT) In Association of Data Mining Towards the Development Smart Cities-A Review Analysis. *J. Eng. Sci. Technol. Rev.* **2020**, *13*, 1–21. [CrossRef]
42. 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. [CrossRef]
43. 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*, 16–24. [CrossRef]
44. Baig, Z.A.; Szewczyk, P.; Valli, C.; Rabadia, P.; Hannay, P.; Chernyshev, M.; Johnstone, M.; Kerai, P.; Ibrahim, A.; Sansurooah, K. Future challenges for smart cities: Cyber-security and digital forensics. *Digit. Investig.* **2017**, *22*, 3–13. [CrossRef]
45. Wu, Y.C.; Sun, R.; Wu, Y.J. Smart city development in Taiwan: From the perspective of the information security policy. *Sustainability* **2020**, *12*, 2916. [CrossRef]
46. Jo, J.H.; Sharma, P.K.; Sicato, J.C.S.; Park, J.H. Emerging technologies for sustainable smart city network security: Issues, challenges, and countermeasures. *J. Inf. Process. Syst.* **2019**, *15*, 765–784.
47. Kitchin, R.; Dodge, M. The (in) security of smart cities: Vulnerabilities, risks, mitigation, and prevention. *J. Urban Technol.* **2019**, *26*, 47–65. [CrossRef]
48. Lam, P.T.; Ma, R. Potential pitfalls in the development of smart cities and mitigation measures: An exploratory study. *Cities* **2019**, *91*, 146–156. [CrossRef]
49. Hindy, H.; Brosset, D.; Bayne, E.; Seeam, A.K.; Tachtatzis, C.; Atkinson, R.; Bellekens, X. A taxonomy of network threats and the effect of current datasets on intrusion detection systems. *IEEE Access* **2020**, *8*, 104650–104675. [CrossRef]
50. Procopiou, A.; Chen, T.M. Security Challenges and Solutions in IoT Networks for the Smart Cities. In *Internet of Things*; CRC Press: Boca Raton, FL, USA, 2022; pp. 161–204.
51. Meyers, R. Data highway and the digital transformation: Arguments for secure, centralised log management. *Netw. Secur.* **2020**, *2020*, 17–19. [CrossRef]
52. Elahi, H.; Wang, G.; Peng, T.; Chen, J. On transparency and accountability of smart assistants in smart cities. *Appl. Sci.* **2019**, *9*, 5344. [CrossRef]
53. Kirimtat, A.; Krejcar, O.; Kertesz, A.; Tasgetiren, M.F. Future trends and current state of smart city concepts: A survey. *IEEE Access* **2020**, *8*, 86448–86467. [CrossRef]
54. Eckhoff, D.; Wagner, I. Privacy in the smart city—Applications, technologies, challenges, and solutions. *IEEE Commun. Surv. Tutor.* **2017**, *20*, 489–516. [CrossRef]
55. Avoine, G.; Calderoni, L.; Delvaux, J.; Maio, D.; Palmieri, P. Passengers information in public transport and privacy: Can anonymous tickets prevent tracking? *Int. J. Inf. Manag.* **2014**, *34*, 682–688. [CrossRef]
56. Gebru, K.; Casetti, C.; Chiasserini, C.F.; Giaccone, P. IoT-based mobility tracking for smart city applications. In Proceedings of the 2020 European Conference on Networks and Communications (EuCNC), Dubrovnik, Croatia, 15–18 June 2020; pp. 326–330.
57. Calderoni, L.; Magnani, A.; Maio, D. IoT Manager: An open-source IoT framework for smart cities. *J. Syst. Archit.* **2019**, *98*, 413–423. [CrossRef]
58. Calderoni, L.; Magnani, A.; Maio, D. Iot manager: A case study of the design and implementation of an open source iot platform. In Proceedings of the 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), Limerick, Ireland, 15–18 April 2019; pp. 749–754.
59. Calderoni, L. Preserving context security in AWS IoT Core. In Proceedings of the 14th International Conference on Availability, Reliability and Security, Canterbury, UK, 26–29 August 2019; pp. 1–5.
60. Gambs, S.; Killijian, M.O.; del Prado Cortez, M.N. De-anonymization attack on geolocated data. *J. Comput. Syst. Sci.* **2014**, *80*, 1597–1614. [CrossRef]
61. Ji, S.; Li, W.; Srivatsa, M.; He, J.S.; Beyah, R. General graph data de-anonymization: From mobility traces to social networks. *ACM Trans. Inf. Syst. Secur. (TISSEC)* **2016**, *18*, 1–29. [CrossRef]

62. Francia, M.; Gallinucci, E.; Golfarelli, M.; Santolini, N. DART: De-Anonymization of personal gazetteers through social trajectories. *J. Inf. Secur. Appl.* **2020**, *55*, 102634. [CrossRef]
63. Chon, Y.; Talipov, E.; Shin, H.; Cha, H. Smart DC: Mobility prediction-based adaptive duty cycling for everyday location monitoring. *IEEE Trans. Mob. Comput.* **2013**, *13*, 512–525. [CrossRef]
64. Primault, V.; Boutet, A.; Mokhtar, S.B.; Brunie, L. The long road to computational location privacy: A survey. *IEEE Commun. Surv. Tutor.* **2018**, *21*, 2772–2793. [CrossRef]
65. Van Zoonen, L. Privacy concerns in smart cities. *Gov. Inf. Q.* **2016**, *33*, 472–480. [CrossRef]
66. Hassankhani, M.; Alidadi, M.; Sharifi, A.; Azhdari, A. Smart city and crisis management: Lessons for the COVID-19 pandemic. *Int. J. Environ. Res. Public Health* **2021**, *18*, 7736. [CrossRef] [PubMed]
67. Wagner, I.; Eckhoff, D. Technical privacy metrics: A systematic survey. *ACM Comput. Surv. (CSUR)* **2018**, *51*, 1–38. [CrossRef]
68. Machin, J.; Batista, E.; Martínez-Ballesté, A.; Solanas, A. Privacy and security in cognitive cities: A systematic review. *Appl. Sci.* **2021**, *11*, 4471. [CrossRef]
69. Silva, B.N.; Khan, M.; Han, K. Integration of Big Data analytics embedded smart city architecture with RESTful web of things for efficient service provision and energy management. *Future Gener. Comput. Syst.* **2020**, *107*, 975–987. [CrossRef]
70. Righini, S.; Calderoni, L.; Maio, D. A privacy-aware zero interaction smart mobility system. *IEEE Access* **2022**, *10*, 11924–11937. [CrossRef]
71. Sweeney, L. k-anonymity: A model for protecting privacy. *Int. J. Uncertain. Fuzziness Knowl. Based Syst.* **2022**, *10*, 557–570. [CrossRef]
72. Party, D.P.W. Opinion 05/2014 on Anonymisation Techniques. *Diunduh Dari* **2014**. [CrossRef]
73. Coelho, V.N.; Oliveira, T.A.; Tavares, W.; Coelho, I.M. Smart accounts for decentralized governance on smart cities. *Smart Cities* **2021**, *4*, 45. [CrossRef]
74. Mothukuri, V.; Parizi, R.M.; Pouriyeh, S.; Huang, Y.; Dehghantanha, A.; Srivastava, G. A survey on security and privacy of federated learning. *Future Gener. Comput. Syst.* **2021**, *115*, 619–640. [CrossRef]
75. Martens, C.D.P.; da Silva, L.F.; Silva, D.F.; Martens, M.L. Challenges in the implementation of internet of things projects and actions to overcome them. *Technovation* **2021**, *118*, 102427. [CrossRef]
76. Zhang, T.; Gao, L.; He, C.; Zhang, M.; Krishnamachari, B.; Avestimehr, A.S. Federated Learning for the Internet of Things: Applications, Challenges, and Opportunities. *IEEE Internet Things Mag.* **2022**, *5*, 24–29. [CrossRef]
77. Schmitt, J.; Miller, K.M.; Skiera, B. The impact of privacy laws on online user behavior. *arXiv*, 2020; arXiv:arXiv.org/abs/2101.11366v2.
78. Nižetić, S.; Šolić, P.; González-de, D.L.D.I.; Patrono, L. Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future. *J. Clean. Prod.* **2020**, *274*, 122877. [CrossRef] [PubMed]
79. Shen, L.; Huang, Z.; Wong, S.W.; Liao, S.; Lou, Y. A holistic evaluation of smart city performance in the context of China. *J. Clean. Prod.* **2018**, *200*, 667–679. [CrossRef]
80. Prakash, S.; Joshi, S.; Bhatia, T.; Sharma, S.; Samadhiya, D.; Shah, R.R.; Kaiwartya, O.; Prasad, M. Characteristic of enterprise collaboration system and its implementation issues in business management. *Int. J. Bus. Intell. Data Min.* **2020**, *16*, 49–65. [CrossRef]
81. Raghavan, S.; Simon, B.Y.L.; Lee, Y.L.; Tan, W.L.; Kee, K.K. Data integration for smart cities: Opportunities and challenges. *Comput. Sci. Technol.* **2020**, *603*, 393–403.
82. Große-Bley, J.; Kostka, G. Big Data Dreams and Reality in Shenzhen: An Investigation of Smart City Implementation in China. *Big Data Soc.* **2021**, *8*, 20539517211045171. [CrossRef]
83. Caviglione, L.; Coccoli, M. A holistic model for security of learning applications in smart cities. *J. E Learn. Knowl. Soc.* **2020**, *16*, 1–10.
84. Balfagih, Z.; Mohamed, N.; Mahmud, M. A framework for quality assurance of electronic commerce websites. *E Commer.* **2012**, 143–163. [CrossRef]
85. Adnan, Y.M.; Hamzah, H.; Dali, M.M.; Daud, M.N.; Alias, A. Comparative Overview of Smart Cities Initiatives: Singapore and Seoul. 2016. Available online: https://www.academia.edu/25534867/Comparative_Overview_of_Smart_Cities_Initiatives_Singapore_and_Seoul (accessed on 23 February 2022).
86. Watts, G. COVID-19 and the digital divide in the UK. *Lancet Digit. Health* **2020**, *2*, e395–e396. [CrossRef]
87. Seifert, A. The digital exclusion of older adults during the COVID-19 pandemic. *J. Gerontol. Soc. Work.* **2020**, *63*, 674–676. [CrossRef]
88. Ma, R. A Study of Potential Pitfalls in the Development of Smart Cities and Mitigation Measures. 2019. Available online: https://theses.lib.polyu.edu.hk/bitstream/200/9997/1/991022232431503411.pdf (accessed on 23 February 2022).
89. Troisi, O.; Fenza, G.; Grimaldi, M.; Loia, F. COVID-19 sentiments in smart cities: The role of technology anxiety before and during the pandemic. *Comput. Hum. Behav.* **2022**, *126*, 106986. [CrossRef] [PubMed]
90. Hawash, B.; Mokhtar, U.A.; Yusof, Z.M.; Mukred, M.; Gaid, A.S. Factors affecting Internet of Things (IoT) adoption in the Yemeni oil and gas sector. In Proceedings of the 2021 International Conference of Technology, Science and Administration (ICTSA), Taiz, Yemen, 22–24 March 2021; pp. 1–7.
91. Balfagih, Z.; Balfaqih, M. Simulating and Epidemic Prediction of COVID-19 Transmission in Universities Considering Different Interventions. In *The International Research & Innovation Forum*; Springer: Cham, Switzerland, 2020; pp. 565–575.
92. Tenable. The Rise of The Business-Aligned Security Executive. Forrester Thought Leadership Paper: A Custom Study Commissioned. Available online: https://securityleaders.com.br/download/Arthur_Capella_tenable_Final.pdf (accessed on 23 February 2022).
93. Saudi Vision. 2017. Available online: http://vision2030.gov.sa/en/foreword (accessed on 23 February 2022).
94. Doheim, R.M.; Farag, A.A.; Badawi, S. Smart city vision and practices across the Kingdom of Saudi Arabia—A review. *Smart Cities Issues Chall.* **2019**, 309–332. [CrossRef]

95. World Economic Forum. Saudi Arabia Is Building a Mega-City that Will Run on 100% Renewable Energy. 2017. Available online: http://www.weforum.org/agenda/2017/10/Saudi-arabia-is-going-to-build-a-500-billion-mega-city (accessed on 21 June 2022).
96. Balfaqih, M.; Ismail, M.; Nordin, R.; Balfaqih, Z. Handover performance analysis of distributed mobility management in vehicular networks. In Proceedings of the 2015 IEEE 12th Malaysia International Conference on Communications (MICC), Kuching, Malaysia, 23–25 November 2015; pp. 145–150.
97. Almubarak, A. The Emergence of Slums in Makkah, Saudi Arabia, and the Saudi Government Response. School of Design, University of Pennsylvania. 2014. Available online: https://fac.ksu.edu.sa/sites/default/files/ali-almubarak-cpln626-final-paper.pdf (accessed on 26 June 2022).
98. Saudi Gazette Report. Second Phase of Slum Removal Ends in Makkah's Al-Nakasa District. 2022. Available online: https://Saudigazette.com.sa/article/616619/SAUDI-ARABIA/Second-phase-of-slum-removal-ends-in-Makkahs-Al-Nakasa-district (accessed on 21 June 2022).
99. Saudi Gazette Report. Jeddah Municipality Reveals Slums Removal's Completion Dates. 2022. Available online: https://www.Saudigazette.com.sa/article/619195 (accessed on 21 June 2022).
100. Saudi Gazette Report. King Salman Orders Establishing Commissions to Develop Taif, Al-Ahsa. 2022. Available online: https://Saudigazette.com.sa/article/620122/SAUDI-ARABIA/Royal-order-establishes-commissions-for-development-of-Taif-Al-Ahsa (accessed on 21 June 2022).
101. Balfaqih, M.; Alharbi, S.A.; Alzain, M.; Alqurashi, F.; Almilad, S. An Accident Detection and Classification System Using Internet of Things and Machine Learning towards Smart City. *Sustainability* **2021**, *14*, 210. [CrossRef]
102. Santos, J.R.A. Cronbach's alpha: A tool for assessing the reliability of scales. *J. Ext.* **1999**, *37*, 1–5.
103. General Authority for Statistics. Population Estimates in the Midyear of 2021. 2022. Available online: https://www.stats.gov.sa/sites/default/files/POP%20SEM2021E.pdf (accessed on 18 July 2022).
104. Saudi Vision 2030. Human Capability Development Program. 2022. Available online: https://www.vision2030.gov.sa/v2030/vrps/hcdp/ (accessed on 21 July 2022).
105. Qimam. QIMAM: Empowering High-Potential University Students in Saudi Arabia. 2022. Available online: https://www.qimam.com/en/ (accessed on 18 July 2022).
106. Ruba Obais. Saudi Arabia had 7 Million Cyberattacks in 2021. 2021. Available online: https://www.arabnews.com/node/1832526/Saudi-arabia (accessed on 25 July 2022).
107. Hughes-Lartey, K.; Li, M.; Botchey, F.E.; Qin, Z. Human factor, a critical weak point in the information security of an organization's Internet of things. *Heliyon* **2021**, *7*, e06522. [CrossRef]
108. Johnson, M.E.; Goetz, E. Embedding information security into the organization. *IEEE Secur. Priv.* **2007**, *5*, 16–24. [CrossRef]
109. Alharbi, F.; Alsulami, M.; Al-Solami, A.; Al-Otaibi, Y.; Al-Osimi, M.; Al-Qanor, F.; Al-Otaibi, K. The Impact of Cybersecurity Practices on Cyberattack Damage: The Perspective of Small Enterprises in Saudi Arabia. *Sensors* **2021**, *21*, 6901. [CrossRef]
110. National Cybersecurity Authority. Controls and Guidelines. 2022. Available online: https://nca.gov.sa/en/legislation (accessed on 27 July 2022).
111. Hu, Q.; Xu, Z.; Dinev, T.; Ling, H. Methods for evaluating and effectively managing the security behavior of employees. *Commun. ACM* **2011**, *54*, 54–60. [CrossRef]
112. Alsewari, A.A.; Poston, R.; Zamli, K.Z.; Balfaqih, M.; Aloufi, K.S. Combinatorial test list generation based on Harmony Search Algorithm. *J. Ambient. Intell. Humaniz. Comput.* **2020**, *13*, 1–17. [CrossRef]
113. Aljabri, S. Cybersecurity Awareness In Saudi Arabia. *Int. J. Res. Publ. Rev.* **2021**, *2582*, 7421.
114. AlMindeel, R.; Martins, J.T. Information security awareness in a developing country context: Insights from the government sector in Saudi Arabia. *Inf. Technol. People* **2020**, *34*, 770–788. [CrossRef]
115. Saudi Arabia Ministry of Communications and Information. Atta Digital. 2022. Available online: https://attaa.sa/ (accessed on 27 July 2022).
116. Saudi Press Agency. MCIT Honors 30 Ambassadors and 20 Partners in the "Attaa Digital" Initiative. 2021. Available online: Shorturl.at/bgMZ2 (accessed on 27 July 2022).
117. Almuqren, L. Twitter Analysis to Predict the Satisfaction of Saudi Telecommunication Companies' Customers. Ph.D. Thesis, Durham University, Durham, UK, 2021.