sustainability

MDPI

Article

A Trust-Based Model for the Adoption of Smart City Technologies in Australian Regional Cities

Chiranjivi Neupane [1], Santoso Wibowo [1,*], Srimannarayana Grandhi [1] and Hepu Deng [2]

[1] School of Engineering & Technology, CQUniversity, Melbourne 3000, Australia; c.neupane@cqu.edu.au (C.N.); s.grandhi@cqu.edu.au (S.G.)
[2] School of Accounting, Info Sys & Supply Chain, RMIT University, Melbourne 3000, Australia; hepu.deng@rmit.edu.au
* Correspondence: s.wibowo1@cqu.edu.au

Abstract: This paper explores the role of stakeholders' trust in the adoption of smart city technologies, leading to the identification of the critical determinants for adopting smart city technologies in Australian regional cities. A comprehensive review of the related literature has been conducted. Such a review leads to the development of a trust-based research model for investigating the importance of trust in technology and its adoption. This model is then tested and validated with the use of a structural equation modeling technique on the survey data collected from ICT professionals in Australian regional cities. The study results show that perceived usefulness, perceived external pressure and perceived information security influence trust in smart city technologies. Further analysis highlights the significant relationship between stakeholders' trust and their intention to adopt smart city technologies. This study is unique, as it is one of a few studies that focus on exploring stakeholders' trust in the adoption of smart city technologies from the perspective of ICT professionals in Australia. The study results can be used by the government agencies to formulate appropriate policies to enhance the use of smart city technologies in the active pursuit of smart city development in Australia.

Keywords: trust; adoption intention; smart cities; Australia; technology

Citation: Neupane, C.; Wibowo, S.; Grandhi, S.; Deng, H. A Trust-Based Model for the Adoption of Smart City Technologies in Australian Regional Cities. *Sustainability* **2021**, *13*, 9316. https://doi.org/10.3390/su13169316

Academic Editor: Boris A. Portnov

Received: 31 July 2021
Accepted: 17 August 2021
Published: 19 August 2021

1. Introduction

The worldwide urban population accounts for about 70% and this figure is expected to double in the next three decades [1]. To address population growth and to improve the living standards of their citizens, local cities are increasingly being transformed into smart cities [2]. This is because smart cities utilize the latest information and communication technologies (ICT) to provide citizens with intelligent services for enhancing livability, workability, and sustainability [1,2]. Despite these benefits, there are security challenges that often influence the adoption of smart city technologies [3].

The use of innovative and smart technologies for smart city transformation is vital, however, the intention to adopt the available technologies by its stakeholders is more important. According to Mayer et al. [4], trust is the readiness to be vulnerable to the actions of another party. While security is considered critical in smart city technologies adoption, trust is identified as an important component for technology adoption, as it addresses risk vulnerability and uncertainty [5]. Belanche et al. [6] point out that trust and security are interrelated in adopting new technologies as individuals' belief in security may influence their adoption intention behavior. Previous studies considered trust as a factor in predicting intention behavior [3,6]. Although earlier studies have been conducted on the importance of security and privacy for the adoption of smart city technologies through the development of a security model, these studies were limited to technology, organization and environmental factors, leaving the security and privacy implications behind [2,7].

In addition, there is a limited study on smart city technologies adoption in Australian cities, let alone the effect of security and privacy on trust in the smart city technologies adoption by the Australian regional cities. The motivation of this study is that Australia is a developed nation with appropriate infrastructure. However, many regional cities are suffering from low or negative growth, as jobs lost in the manufacturing sector, or more recently the resources and energy sectors, are not replaced quickly enough [8]. Moreover, highly reputable organizations such as International Standards Organization (ISO, Geneva, Switzerland) presented requirements (ISO 37101:2016) of a management system for sustainable development in communities, including cities using a holistic approach, to ensure consistency with the sustainable development policy of communities. Hence, the government must plan for the future of regional cities by maximizing their unique advantages and supporting their long-term growth through the development and implementation of smart city technologies whereby Australian regional cities can reach their full potential.

To improve the livability, productivity and sustainability of cities and suburbs, the Australian government launched smart city initiatives, including the Smart Cities Plan, City Deals, the Smart Cities and Suburbs Program, and the National Cities Performance Framework to support the delivery of innovative smart city projects under the Smart Cities and Suburbs Program [8]. While the government has made a significant contribution to support adoption of smart city technologies, the value of the initiatives is unclear due to the lack of evidence on the rigorous assessment of these initiatives in the current literature. Therefore, this paper proposes and validates a trust-based model using structural equation modeling (SEM) for determining the key factors influencing stakeholders' trust towards their intention to adopt smart city technologies. This paper contributes to the information systems research domain by demonstrating how the concept of trust can be adopted for evaluating the relevant factors associated with the adoption smart city technologies. Moreover, this study provides a comprehensive review of factors that influence stakeholders' trust towards the adoption intention of smart city technologies in the Australian regional cities. In what follows, we first present an overview of the related research, leading to the development of a trust-based model. We then test and validate the proposed model. Finally, we present the research findings and their implications for smart city technologies adoption in the Australian regional cities.

2. Literature Review

2.1. Role of Trust in Technology Adoption

Smart city services have increasingly gained attention in academia, industry and governments in recent years [1]. A comprehensive review of various technology adoption models shows that technology, organization, environment, and security are the main factors in technology adoption decisions. Out of these four factors, the security factor has proven to be decisive, as users' perception of security may stop them from using new technologies. However, several studies [9–11] have shown that trust can play an important role in preparing individuals to accept unintended consequences posed by the security threats as it addresses risk vulnerability and uncertainty.

Kramer [12] explained that trust develops over time due to interpersonal relationships. Interestingly, trust can be significantly high even when the individuals have little knowledge. Baig et al. [13] argued that the trust developed through one's sense of security provided by guarantees, safety nets, or other impersonal structures may influence the decision to adopt new technologies. In this context, trust denotes the willingness of a user to assume the risk of information disclosure [4]. The representation of trust by Koller [14] as a function of an extent of risk of a certain situation can be alternatively viewed as a function of a particular smart service user's risk. This means, when there is minimum risk of security in the smart city technologies, there would be more trust towards such a technology.

Zhang et al. [15] and Yeh [11] have assessed the role of trust in technology adoption in various contexts. For example, Yeh [11] argue that technology trust is the individual's willingness to be vulnerable to new technology. This study on the role of trust in technology implementation reiterated the importance of trust. In the context of smart cities, trust is a user-initiated process based on their evaluation of smart technologies and associated risks, and user's willingness to adopt them for achieving specific goals. As trust in new technologies may influence users to accept risks and be exposed to vulnerabilities [16], it is considered an important factor in technology adoption [5]. Smart city services involve the use of smart devices and trust allows users to interact with smart devices and help differentiate trustworthy products and services from malicious ones [11].

This paper examines the role of technology, organizational, environmental and security factors on stakeholders' trust towards the adoption of smart city technologies. While literature [2,15] presents various technology adoption models, there is a lack of trust-based models that focus on technology, organizational, environmental and security facets concerning the adoption of smart city technologies. This warrants the need for further investigation. A trust-based Technology Adoption Model that helps identify users' needs and ways to fulfill these needs can significantly improve the adoption of smart city technologies. Hence, this study aims to fill this research gap by developing a trust-based model for smart city technologies adoption.

2.2. Technology Adoption Models

Various frameworks have been developed for the adoption of innovative technologies, with the most notable being Technology Adoption Model (TAM) [17] and Technology, Organization and Environment (TOE) [18] framework. TAM proposes that the actual use intention of the technology is derived from the perceived ease of use and perceived usefulness of that technology [17]. On the contrary, the TOE model categorizes technology adoption related attributes into three dimensions, namely, technology, organization and environment [18]. The TOE model has been used widely to study the technology adoption intention and acceptance of new technologies. It identifies technology, organization and environmental factors as influencing factors in technology adoption decisions in organizations [18]. The technology factor explains adoption in terms of functionality and reliability as well as their perceived usefulness. The environmental context refers to pressure from external partners and government policy. The TOE model considers social and behavioral aspects to determine the interaction among technology development in an organization setting influenced by the surrounding environment [5,19].

As cities and towns are public entities, the TOE model can be useful in assessing the smart city technologies adoption intention [2,15]. For instance, Dewi et al. [2] successfully used the TOE model to assess the influencing factors towards smart city technologies adoption decisions. Meanwhile, Gangwar et al. [19] used the TOE model to study key determinants of cloud computing adoption in organizations. While the TOE model offers a valid ground for studying technology adoption intention, it does not consider the security context in technology adoption decisions [20].

Despite these benefits, there are security challenges with deploying technologies in smart cities [2,15]. The security challenges often influence the adoption of technologies. For instance, Saif Almuraqab et al. [21] suggested security challenges as a key factor towards the adoption of IoT technology, which is the enabler technology for smart cities. Security and privacy have been indicated as major concerns for smart cities adoption [1].

Several studies have been conducted on the role of trust on technology adoption. AlHogail [20] and Yeh [11] highlight the positive impact of trust in new technology adoption even in volatile situations. Ratten [22] proved the role of trust in influencing users' behavioral intention to adopt technological innovations. AlHogail [20] concluded that consumer trust improved the technology adoption rate. Hence, trust is an important factor in adopting smart city technologies. Table 1 outlines the research context, strengths and limitations of trust-based models.

Table 1. Strengths and Limitations of Trust-based Technology Adoption Models.

Research Context	Strengths	Limitations	
Role of security and trust in technology adoption	Presented several issues relating to trust and security in smart cities.	Lack of discussion on specific issues	Braun et al. [1]
Influence of technology trust towards implementation of HR information system	Framework details determinants of technology trust using technology, organization and user dimensions.	Lack of discussion on environment and security dimensions and their influence on trust	Lippert and Swiercz [23]
Role of trust in adopting mobile payment solutions	Introduced trust factor in original TAM model to develop trust enhanced TAM model.	Unable to establish the validity and reliability of the proposed model	Dahlberg et al. [10]
Role of trust, innovation and performance in technology adoption	Compared two (USA and China) different cultural contexts to understand the behavioral attitude towards technological innovations.	Self-reported data were collected that may mean there is a respondent bias	Ratten [22]
Determinants of acceptance of ICT-based smart city services and their effect on the quality of life	Presented a user acceptance model for the adoption of ICT-based smart city services using the diffusion of innovation theory. Trust is found to have a significant influence on user acceptance of smart city services.	Control variables (gender, education and age can have different influences on different smart city service domains)	Yeh [11]
IoT adoption by improving consumer trust	Considered security-related factors as determinants of trust towards IoT adoption.	Environmental and organisational domains are not considered as determinants of trust	AlHogail [20]

3. A Trust-Based Model

This study presents a trust-based model for smart city technologies adoption. In addition, considering the importance of security-related factors in promoting trust, the proposed model adopts information security-related factors. The security context in the presented model relates to perceived privacy, perceived information security, and self-efficacy in information security. Since there is a handful of prior research that explored the adoption of smart cities, this paper is backed by studies closely related to the context of the research. The following subsections detail the factors under each dimension in the proposed model.

3.1. Technology-Related Factors

Technology provides the required features and functions to perform a specific task [20], but trusting a technology significantly depends on its ability to perform a task [11]. The technology perspective considers the functional reliability aspects and the usefulness of the new technology. In fact, Dewi et al. [2] believed that these technology-related factors influence stakeholders' trust towards their intention to adopt smart city technologies.

3.1.1. Functionality and Reliability

It refers to whether technology can provide the required features and functions to perform a specific task or fulfill a task requirement as expected [20]. Trusting a new technology significantly depends on its ability to perform a task and proven to show a positive influence towards trust as well as the adoption of smart city technologies such as IoT [24]. Similarly, Ratten [22] proposed trust as a function of functionality, reliability, and helpfulness. The authors found a positive relationship between them. This means individuals' trusting beliefs are influenced by the functionality and reliability of the specific technology. Based on these prior outcomes, functionality and reliability have been proposed as technology-related factors and are hypothesized as:

Hypothesis 1 (H1). *Functionality and reliability have a positive influence on stakeholders' trust in smart city technologies.*

3.1.2. Perceived Usefulness

Perceived usefulness is the subjective probability of users' completion of a given task in an improved way [25]. Lin and Dong [16] believed that perceived usefulness and trust can have an implication towards understanding the dynamic nature of trust and perceived usefulness during different phases of users' encounters with e-services. Goldfinch et al. [25] found that perceived usefulness enhances the trust level in e-government services. Meanwhile, Saif Almuraqab et al. [21] noticed that there is a direct positive impact of perceived usefulness towards perceived trust in their study to examine the influence of perceived trust towards their intention to adopt an online trading system. Similarly, Lin and Dong [16] stated the positive influence of perceived usefulness towards the adoption of IoT in small and medium-sized enterprises. Accordingly, the following hypothesis is proposed for perceived usefulness:

Hypothesis 2 (H2). *Perceived usefulness of smart city technologies positively influences stakeholders' intention to adopt them.*

3.2. Organization Related Factors

The organizational factor refers to the characteristics that represent an organization in terms of its strategies, culture, structure and policies [26,27]. According to von Solms [28], information security can be established by developing an information security culture in organizations. Moreover, ensuring the development of an information security culture can enable trust towards new technology.

Information Security Culture

Information security culture is a subdomain of the organization culture where it supports information security to become an imminent part of employees' daily activities [26]. Information security culture is also linked to the belief of individual employees towards compliance with the organizational policies and standards related to information security [11]. Van Zoonen [7] believed that the security culture of the employees in an organization can be created by instilling the concept of information security in every employee as part of their routine in the workplace. Meanwhile, AlKalbani et al. [3] stated that a higher level of information security compliance can be achieved by having an effective information security culture. Belanche et al. [6] claimed that employees' understanding of appropriate information security culture results from effective training and awareness programs. In an organizational context, information security awareness is an employee's knowledge and understanding about the information security policy and procedures of the organization, but in general, information security depicts an employee's overall understanding and knowledge about the information security issues and their ramification [29,30]. Therefore, the following hypothesis has been proposed:

Hypothesis 3 (H3). *Information security culture positively influences stakeholders' trust in smart city technologies.*

3.3. Environment Related Factors

The environmental context refers to the domain, where an organization conducts its business and involves its industry, competitors, access to outside resources and is related to government's influence [9,18,31]. This domain fundamentally infers that the adoption of innovative technologies by an organization is influenced by the environment in which the organization operates. Chang et al. [32] pointed out that pressure from external partners and government policies are the key reasons for technology adoption.

3.3.1. Pressure from External Partners

Organizations are sensitive to changes in the external environment. Wibowo and Mubarak [9] claimed that pressure from external partners and organizations' desire to maintain competitive advantage drives organizations to adopt new technologies. Yeh [11] presented various examples of organizations achieving competitive advantage through the adoption of innovative technologies. In essence, the adoption of new technology can significantly be influenced by external pressure, particularly when this technology directly affects the competition and is of a strategic necessity. In this situation, the pressure to adopt new smart city technologies quickly is to provide better services and gain strategic advantages. However, the decision to adopt new technologies may result in an unexpected security concern [20]. Hence, the following hypothesis has been proposed to validate the influence of external pressure towards trust:

Hypothesis 4 (H4). *Perceived external pressure positively influences stakeholders' trust in smart city technologies.*

3.3.2. Government Policy

The government policy factor refers to the way a government plans to support the implementation and adoption of innovative technologies in the region. In relation to government policy, Van Zoonen [7] believed that smart city technologies need to strictly adhere to the existing government policy, as non-compliance may result in additional transaction costs and potential legal outcomes. This is supported by Chang et al. [32] who found that government policies have a positive impact on organizations trying to adopt new information systems technology. Similarly, Wibowo and Mubarak [9] explained that not all government policies on public services influence trust. However, their study found a significant positive influence of government policies on users' or citizens' trust

towards new technologies. Their study justified the need to consider government policy in enhancing stakeholders' trust in technology-related services. Based on the facts above, the following hypothesis has been presented:

Hypothesis 5 (H5). *Government policies have a positive influence on stakeholders' trust in smart city technologies*.

3.4. Security-Related Factors

Security factors have always been associated with the adoption of innovative technologies such as big data and IoT [2,26]. Wu et al. [30] pointed out that security challenges are a key factor towards the adoption of IoT technology, which is one of the enabler technologies for smart cities. Security and privacy have been indicated as major concerns for smart cities' adoption [1,11]. The context of security here refers to the goal to protect information from attacks, viruses, frauds, and various malicious activities that may cause distress to the information or the infrastructure in the smart cities [15]. The security domain is the main focus of the research, which consists of three factors: perceived privacy, perceived information security and self-efficacy in information security. The following subsections discuss the factors related to the security domain of the theoretical model of the research.

3.4.1. Perceived Privacy

Information privacy is the individual's right to control over their personal information, including how their information is collected, shared and used [31]. In the smart city context, privacy is the fundamental right of the individual which should be guaranteed by any system, including smart city technologies. Perceived privacy is the individual's perception of control over their personal information [32]. Van Zoonen [7] identified privacy and security as influencing factors in the smart city initiative model, where privacy and security factors are related to the built infrastructure domain of the smart city. Privacy challenges in the digital environment are a major threat to the success of initiatives such as e-government because of the mistrust and skepticism of such services by citizens [5]. Privacy can also play a major role in determining trust by the users or stakeholders of smart cities because smart cities are made up of multiple digital services. In view of earlier studies, the following hypothesis is proposed:

Hypothesis 6 (H6). *Perceived privacy of the smart city technologies positively influences stakeholders' trust in smart city technologies.*

3.4.2. Perceived Information Security

Perceived information security is defined as the probability by which users or consumers believe that their sensitive information will not be tampered with or manipulated during transmission or storage by unauthorized persons [13]. The perceived information security in the smart city technologies is the extent to which the expectation of users or city inhabitants are met to ensure their confidential information is not breached or misused. Chellappa and Pavlou [33] suggested that online consumers' perception towards information security is determined by the mechanism of robust security technologies such as encryption, protection, verification and authentication. However, the perceived information security may be determined by different factors depending on the information technology environment. Goldfinch et al. [25] found that the security of government's electronic services is an important factor towards its adoption by citizens. Hence, it can be generalized that intention to adopt new technology is fairly determined by its end users' trust over the security and privacy of that technology. It is, however, important to know the relationship between the perception of information security and stakeholders' trust in smart city technologies, and the subsequent intention to adopt smart city technologies. Therefore, the hypothesis has been proposed as:

Hypothesis 7 (H7). *Perceived information security of the smart city technologies positively influence stakeholders' trust in smart city technologies.*

3.4.3. Self-Efficacy in Information Security

Rhee et al. [26] defined self-efficacy in information security as a belief in one's capacity to protect information and information systems from unauthorized disclosure, modification, loss and destruction. However, self-efficacy has been differentiated into various types such as general computer self-efficacy and specific self-efficacy as one related to the safe and appropriate use of internet transactions [4]. Rhee et al. [26] pointed out that users' intention to apply security effort is significantly influenced by self-efficacy in information security. Another study by Sarabdeen et al. [34] identified self-efficacy as the key factor in e-government adoption. Self-efficacy is therefore considered to be a contributing factor for building stakeholders' trust leading to the adoption of smart city technologies. In addition, it may have an indirect influence on adoption intention. Therefore, the following hypothesis to relate information security self-efficacy and trust is proposed as:

Hypothesis 8 (H8). *Self-efficacy in information security positively influence stakeholders' trust in smart city technologies.*

3.5. Trust in Smart City Technologies

Information security and trust towards an information system are believed to be interrelated [33]. Developing trust between smart city services and their stakeholders is important, as trust plays an important role in consumer behavior [34]. Trust also represents the willingness to assume the risk of information disclosure [4]. This means when there is minimal risk of security in the smart services, there would be more trust towards such service or a system. Various studies tested the relationship between perceived information security and trust [35]. The study of trust-based determinants in the smart city technologies adoption in the case of smart city services may generate an important outcome by identifying the most influencing determinants towards stakeholders' trust in smart city technologies and their intention to adopt the smart services motivated by this trust. Tolbert and Mossberger [36] categorized trust in governments' electronic services into process-based trust and institution-based trust. This process-based trust depends on the government's responsiveness via improved communication, increased citizens' participation and enhanced efficiency and effectiveness of e-government services. Institution-based trust is created by transparency, responsibility, increased participation, efficiency and effectiveness of the government's electronic services [33,36,37]. The following hypothesis is proposed to investigate the relationship between stakeholders' trust in smart city technologies and their adoption intention:

Hypothesis 9 (H9). *Trust in smart city technologies positively influences stakeholders' intention to adopt smart city technologies.*

4. Research Design

The proposed research model presented in Figure 1 consists of 9 hypotheses, which are tested by using Structured Equation Modeling (SEM) Partial Least Square (PLS), where the structural relationship between dependent and independent variables are studied by looking at the combined result of factor analysis and multiple regression.

Questionnaire Development

A close-ended questionnaire with three sections is developed for data collection. The first section includes research aims, key terms in the questionnaire and the researchers' contact details. The next section contains questions for collecting respondents' demographic data. The final section consists of questions for assessing and validating the research model.

Based on the literature review, a total of 34 questions are developed for this study. A five-point 'Likert' scale is used for collecting stakeholders' perceptions towards their intention to adopt smart city technologies. In the five-point Likert scale used in this study, the value "1" represents "strongly disagree" and the value "5" represents "strongly agree". The questionnaire was developed based on the conceptual model of the research as shown in Figure 1, where each item was taken from the previous survey-based studies, to ensure the reliability of the indicators. The questionnaire was pilot tested using subject matter experts, smart city practitioners, fellow researchers, and smart city users for ensuring the questionnaire validity. The survey questionnaire was then emailed to the city councils and ICT professionals in Australia regional cities, requesting them to complete the online survey. Table 2 presents the factors and the relevant indicators adopted for this study.

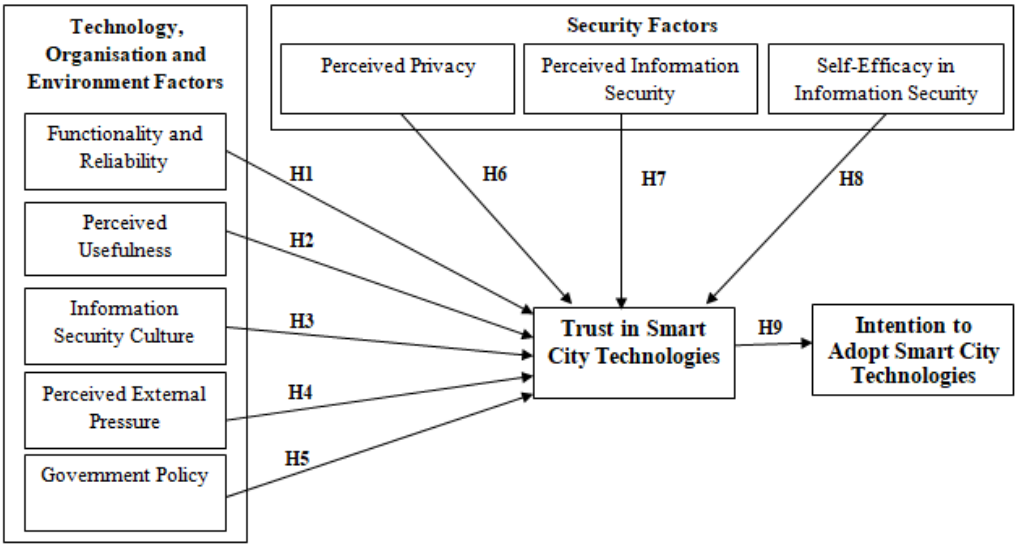

Figure 1. Research Model.

Table 2. Summary of Factors and Indicators in the Research Model.

Dimension	Factors	Indicators
Technology	Perceived Usefulness	Will not create harassment [38] Services are convenient [38] Services give greater control [17]
	Functionality and Reliability	Technical capacity to ensure data will not be intercepted by hackers [37] Sufficient technical capacity to ensure data cannot be modified by a third party [37]
Organisation	Information Security Culture	Familiarity with the information security policies of the organization [34] Individual's role for escalating information security incidents [29] Awareness of the information security responsibilities [3]
Environment	Perceived External Pressure	Smart city services are an effective way to interact with the government [30] The use of smart services will improve the efficiency of obtaining services [26]
	Government Policy	Aware of the potential damage to the information system by hacker threats [26] The use of smart services will improve the efficiency of obtaining services [26]
Security	Perceived Privacy	There will be no loss of data from an agency behaving opportunistically in smart city services [30] Feel safe when I send personal information [22] Feel confident about privacy with regards to the smart city services [34]
	Perceived Information Security	Smart services provided are reliable [34] Concern for the privacy of its users [34] The transaction is secure while using the smart services [37] Information I provide to the council will not be manipulated [37]

Table 2. *Cont.*

Dimension	Factors	Indicators
	Self-Efficacy in Information Security	Confidence in handling virus-infected files [26] Confidence in understanding terms relating to information security [26] Confidence in learning the method to protect information and information system [26] Confidence in managing files in computer [26] Confidence in setting the Web browser to different security levels [26] Confidence in using different programs to protect my information and information system [26] Confidence in updating security patches to the operating system [26] Confidence in following the 'user guide' when help is needed to protect my information [26]
	Trust	Councils and other relevant authorities can be trusted to carry out online transactions faithfully [38] Legal and technological structures adequately protect from problems on the internet [38] Smart city services would provide a valuable service for residents in our city council [38] The responsible of taking full responsibility for any type of insecurity [38]
	Intention to Adopt	Confidence in the technology used in smart city's services [38] Not concerned that the information submitted online could be misused [37] Believe that smart city services are safe to interact with for financial purposes [15]

5. Data Analysis

5.1. Sample Demographics

A total of 229 people completed the survey. The survey participants are ICT professionals working in the Australian regional cities. About 13% of respondents were aged 18–24, 27% aged 25–34, 26% aged 35–44, 10% aged 55–64. and 5% aged 65–74. In total, 15.6% of respondents have less than 2 years of ICT related experience, 28% have 2 to 5 years of ICT related experience, 28% have 5 to 10 years of ICT related experience and the remaining 28.4% have more than 10 years of ICT related experience. Within the ICT job domain, a majority of respondents (29.3%) work in the business process area. The remaining respondents in this domain work in education and training (24%), technology (20%), research and development (13.3%), consulting (6.6%), leadership (5.7%), and other areas (2%).

5.2. Structural Equation Modeling

This study adopted the structural equation modeling (SEM) technique to test the research model and used IBM SPSS and SmartPLS software tools. Figure 2 shows the measurement model. A summary of the measurement model indicators is shown in Table 3.

During the data screening stage, four survey responses from 229 samples were found to be less than 10% complete. These were excluded from the final study, as none of these four questionnaires consisted of data about variables other than the respondents' demographics. A total of 225 samples were used to conduct normality tests for studying data distribution through kurtosis and skewness, identifying outliers using Mahalanobis distance, evaluating multicollinearity using variance inflation factor (VIF) and Tolerance and identifying non-response bias with independent sample *t*-test. The normality test results indicate that the data are normally distributed. The multivariate outlier was evaluated by calculating Mahalanobis distance (D2) divided by degrees of freedom (df) (number of items in this case) for each factor individually [38]. The results showed all instances had D2/df values below 4.0. Therefore, no multivariate outlier was identified in the data. Initial evaluation

of multicollinearity [39] is done using an item-to-item correlation matrix. Results showed no higher correlation between items in the correlation matrix. VIF values obtained from SmartPLS version 3.2.7 for all factors show no values higher than 5.0. Moreover, the observed results showed five items with VIF between 2.0 and 2.5, and all other items had VIF less than 2.0. Therefore, no multicollinearity was observed as per the threshold suggested by Hair et al. [39]. With a size of 225, it would be impractical to divide the samples equally. Hence, the dataset was split into two groups. The first group consisted of the first 112 samples and the second group consisted of the last 112 samples. The samples were then analyzed for a two-sample independent *t*-test at a 5% significance level. The results show no significant difference in mean for the first and the second wave of responses. The *t*-test results indicate that there is no non-response bias.

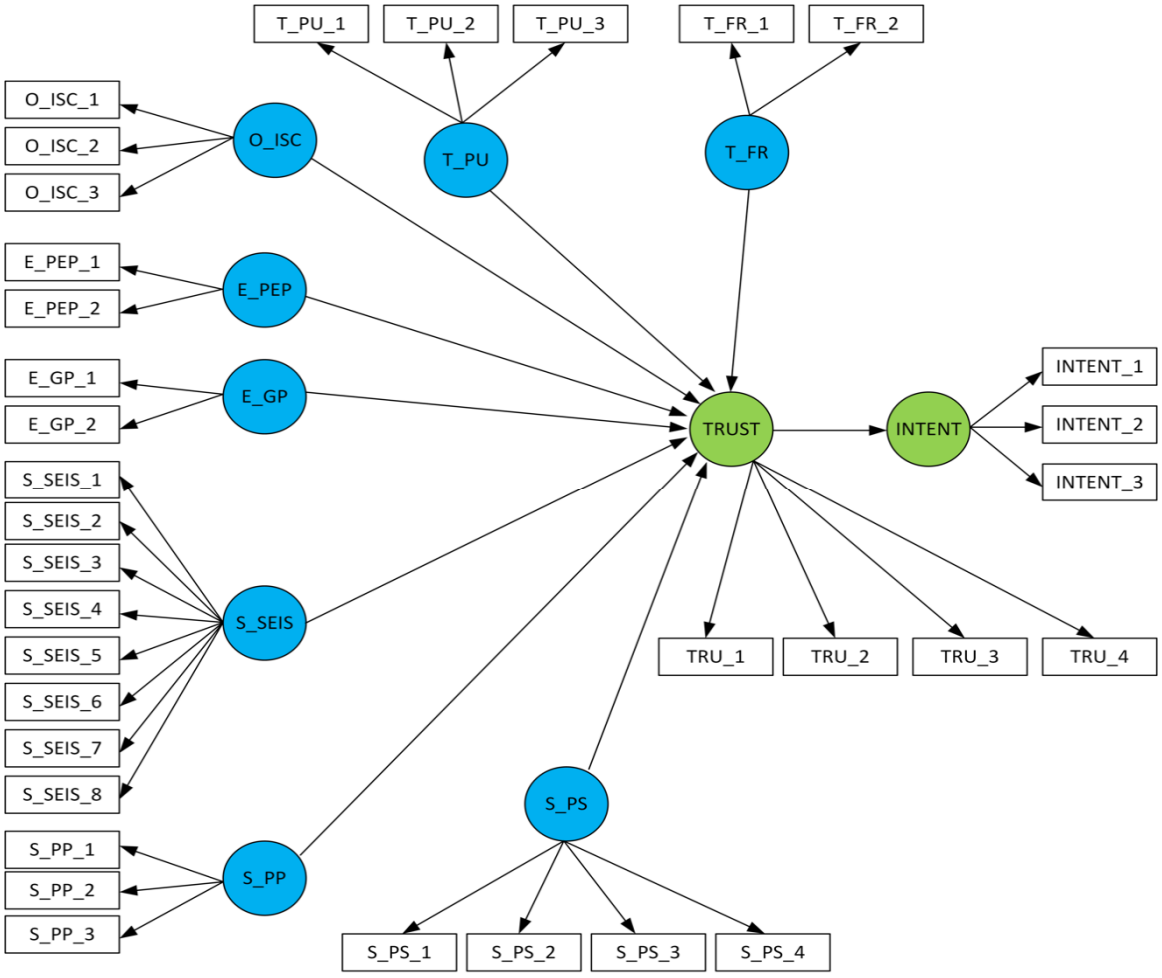

Figure 2. The Measurement Model.

Table 3. Summary of the Measurement Model Indicators.

Functionality and reliability		Perceived privacy	
T_FR_1	Technical capacity to ensure data will not be intercepted by hackers	S_PP_1	There will be no loss of data from an agency behaving opportunistically
T_FR_2	Sufficient technical capacity to ensure data cannot be modified by a third party	S_PP_2	Feel safe when I send personal information to councils
Perceived Usefulness		S_PP_3	Feel confident about privacy with regards to the smart city services
T_PU_1	Will not create harassment	Self-Efficacy in Information Security	
T_PU_2	Services are convenient	S_SEIS_1	Confidence in handling virus-infected files
T_PU_3	Services give greater control		
Information Security Culture		S_SEIS_2	Confidence in understanding terms relating to information security
O_ISC_1	Familiarity with the information security policies of the organisation	S_SEIS_3	Confidence in learning the method to protect information and information system
O_ISC_2	Individual's role for escalating information security incidents	S_SEIS_4	Confidence in managing files in a computer
O_ISC_3	Awareness of the information security responsibilities	S_SEIS_5	Confidence in setting the Web browser to different security levels
Pressure from External Partners		S_SEIS_6	Confidence in using different programs to protect my information
E_PEP_1	An effective way to interact with government	S_SEIS_7	Confidence in updating security patches to the operating system
E_PEP_1	will improve the efficiency of obtaining services	S_SEIS_8	Confidence in following the 'user guide' when help is needed to protect information
Government Policy		Trust	
E_GP_1	Aware of the potential damage to the information system by hacker threats	TRU_1	Smart city services would provide a valuable service for residents
E_GP_2	The use of smart services will improve the efficiency of obtaining services	TRU_1	Councils can be trusted to carry out online transactions faithfully
Perceived Information Security		TRU_1	Legal and technological structures protect from problems on internet
S_PS_1	Smart services provided are reliable	TRU_1	The responsible firm providing services will take full responsibility for insecurity
S_PS_2	Council shows concern for the privacy of users	Intention to Adopt	
S_PS_3	The transaction is secure while using the smart services	INTENT_1	Confidence in the technology used in smart city's services
S_PS_4	Information I provide to council will not be manipulated	INTENT_1	Not concerned that the information submitted online could be misused
		INTENT_1	Believe that smart city services are safe to interact with for financial purposes

5.3. Instrument Validation

In scientific research, all the instruments must be validated to minimize measurement errors [39]. Thus, this study has adopted a systematic approach for validating the instrument through content validity, reliability analysis, convergent validity and discriminant validity before assessing the structural model.

The instruments developed for this study followed an appropriate process suggested by Hair et al. [39] to ensure content validity. This study conducted an extensive literature review on technology adoption models before considering the TOE model to ensure content validity. The results presented in Table 4 show that the AVE value of above 0.5, Composite reliability (CR) values above 0.7 and Cronbach's alpha values were above 0.5. These values indicate the reliability of the measurement instrument [40].

Table 4. Reliability Scores of the Factors.

Dimension	Factors	AVE	CR	α
Technology	Perceived usefulness (T_PU)	0.584	0.808	0.64
	Functionality and reliability (T_FR)	0.804	0.891	0.76
Organisation	Information security culture (O_ISC)	0.688	0.868	0.77
Environment	Government policy (E_GP)	0.699	0.822	0.57
	Pressure from external partners (E_PEP)	0.754	0.860	0.67
Security	Self-efficacy in information security (S_SEIS)	0.535	0.898	0.87
	Perceived privacy (S_PP)	0.522	0.758	0.54
	Perceived security (S_PS)	0.506	0.803	0.68
Trust	Trust (TRU)	0.558	0.834	0.73
Adoption Intention	Intention to adopt (INT)	0.546	0.779	0.60

To ensure that factor analysis is appropriate for the data, Bartlett's Test of Sphericity [41] and the Kaiser-Meyer-Olkin (KMO) test are carried out. The test results indicate that the KMO values are above 0.5. The *p*-values obtained through Bartlett's Test of Sphericity are below 0.05. Hair et al. [39] suggest that CR values above 0.7 and AVE values of at least 0.5 indicate sufficient convergent validity. The AVE values above 0.5 and the CR values above 0.7 for the factors in the research model suggest sufficient convergent validity.

Fornell and Larcker [42] presented various approaches for assessing discriminant validity. Out of these approaches, the Fornell and Larcker criterion is commonly used to assess discriminant validity. However, this approach has been discouraged in recent times because it fails to establish a distinction between the factors in a micro-level [43]. The other approach, the Heterotrait–Monotrait (HTMT) ratio of correlation, is considered superior and highly recommended for assessing discriminant validity. Henseler et al. [43] explain that the HTMT values 0.9 or below are required to establish discriminant validity. The HTMT test results presented in Table 5 indicate that the values are within the acceptable threshold establishing discriminant validity.

Table 5. Heterotrait–Monotrait (HTMT) Ratio of Correlations.

	E_GP	E_PEP	INTENT	O_ISC	S_PP	S_PS	S_SEIS	TRUST	T_FR
E_PEP	0.35								
INTENT	0.35	0.55							
O_ISC	0.88	0.64	0.61						
S_PP	0.48	0.49	0.9	0.43					
S_PS	0.47	0.53	0.74	0.65	0.75				
S_SEIS	0.73	0.51	0.52	0.78	0.51	0.67			
TRUST	0.58	0.81	0.74	0.74	0.68	0.81	0.62		
T_FR	0.40	0.52	0.77	0.61	0.83	0.74	0.56	0.62	
T_PU	0.31	0.89	0.84	0.53	0.68	0.54	0.38	0.80	0.65

5.4. Structural Model Assessment

The structural model consists of exogenous (which have no arrows pointing towards them from any factors) and endogenous (which have arrows pointed toward them in the structural path relationships) factors. Figure 2 shows the structural path model of the study.

Assessment of R^2, Q^2 and f^2

A coefficient of determination (R^2) value represents the extent of variation in the regression model from the baseline (0) [39]. The threshold of R^2 values for endogenous factors indicated by Chin [44] are 0.67, 0.33 and 0.19 depicting substantial, moderate and weak. Table 6 shows that R^2 values for Trust is 0.582, which means 58.2% of the variance in trust is explained by exogenous factors. Similarly, adoption intention, with a variance of 27.9% explained by the factor trust, has a small variance.

Table 6. R^2 and Q^2 Values for the Endogenous Factors.

	R^2	SSO	SSE	Q^2	SD	T-Statistics	*p*-Values
INTENT	0.279	675	580.41	0.14	0.056	4.989	0.00
TRUST	0.582	900	636.32	0.293	0.046	12.739	0.00

The values of f^2 and Q^2 are used to measure the quality criteria of the structural model [45]. All relationships indicate a small f^2 effect size except trust and intent to adopt relationship, which has a large effect size with a value of 0.387. Table 7 shows the f^2 values for the paths in the structural model.

Table 7. f^2 Values for the Paths in the Structural Model.

Factors Influence	f^2 Values	Sample Mean (M)	Std. Dev.
E_GP -> TRUST	0.013	0.019	0.02
E_PEP -> TRUST	0.057	0.063	0.04
O_ISC -> TRUST	0.024	0.033	0.03
S_PP -> TRUST	0.018	0.025	0.02
S_PS -> TRUST	0.084	0.093	0.05
S_SEIS -> TRUST	0.004	0.011	0.01
TRUST -> INTENT	0.387	0.408	0.11
T_FR -> TRUST	0.00	0.007	0.01
T_PU -> TRUST	0.067	0.077	0.04

The structural model is assessed by using Stone–Geisser's Q^2. The Q^2 value is only applicable to the endogenous variables, where a positive value indicates predictive relevance [39]. The Q^2 values obtained for trust and adoption intention in this study are above 0, which confirm the predictive relevance of endogenous factors in the structural model.

5.5. Hypotheses Evaluation

To test the significance of the path of the measurement model, the bootstrapping method was used in PLS-SEM. It is a recommended way of producing better approximation when the sample size is small [46]. For hypothesis testing, the critical t-values for the two-tailed test are regarded as 1.65, 1.96 and 2.58 for 10%, 5% and 1% level of significance, respectively, and the VIF values for each item should be below 5 [39]. The results presented in Table 8 show that four hypotheses have been supported.

Table 8. Results for the Hypothesized Relationships.

Hypothesis	β	*t*-Value	*p*-Value	Remarks
H1: Functionality and reliability → Trust	−0.02	0.292	0.77	Rejected
H2: Perceived usefulness → Trust	0.224	3.65	0.000	Supported
H3: Information security culture → Trust	0.16	1.8	0.072	Rejected
H4: Perceived external pressure → Trust	0.20	2.99	0.003	Supported
H5: Government policy → Trust	0.093	1.5	0.134	Rejected
H6: Perceived privacy → Trust	0.117	1.8	0.07	Rejected
H7: Perceived information security → Trust	0.25	3.88	0.000	Supported
H8: Self-efficacy in information security → Trust	0.529	0.72	0.47	Rejected
H9: Trust in smart city technologies → Adoption intention	0.528	9.69	0.000	Supported

6. Results and Discussion

The results show there is no significant impact of functionality and reliability toward stakeholders' trust in smart city technologies. There is a slight negative influence observed with a negative path coefficient value, but the observed β value is close to zero, and the result is not significant, as the *p*-value is higher than 0.05. Hence, hypothesis H1 is rejected. This result contradicts the finding of AlHogail [20], which identified functionality and reliability as a positively influencing factor towards building trust. The results concerning H2 indicate that the findings are in line with the recent study of Zhang et al. [15], where the authors hypothesized that perceived usefulness influences trust. Similarly, the relationship between trust and perceived usefulness has been found to be significant in earlier studies [16,37]. Thus, the validated outcome suggests stakeholders' perception of the usefulness of smart city services increases the adoption of smart city technologies by stakeholders in the regional Australian cities.

Hypothesis 'H3' is developed to understand the relationship between information security culture and trust in smart city technologies. Based on the *p*-value, the hypothesis is rejected. This means the influence of information security culture is not significant towards building trust in smart city technologies. Interestingly, Chang et al. [32] stated that trust can be increased by having appropriate information security culture. This is opposite to what the current research results show. The result of the current study means further research is required to assess how information security culture influences stakeholders' trust towards their intention to adopt smart city technologies. The test results suggest hypothesis H4 is supported. This means external pressure positively influences stakeholders' trust in smart city technologies. However, the low value of the path coefficient indicates the influence of perceived external pressure on stakeholders' trust is less significant. Smart city technologies are not limited to within a single organization, and this pressure from internal and external sources can be challenging to distinguish. While the results are in line with Belanche et al. [6] study, where they found a significant direct influence of external pressure on perceived trust for the adoption of innovative technology, distinguishing between different types of external pressure is important to understand how different sources of pressure influence on trust. The results indicate that the government policies have no significant influence over stakeholders' trust in smart city technologies. Meanwhile, Knack and Zak [47] believed that only a few public policies by the government have an impact on stakeholders' trust. The study outcome shows stakeholders are not convinced that government policy influences their level of trust in smart services. Future studies in a similar setting may offer further details into the influence of government policies on stakeholders' trust.

The results suggest that perceived privacy influences trust, even though the results are not significant. Based on the *p*-value, the hypothesis is rejected. Earlier studies conducted by Sarabdeen et al. [34] on technology adoption found a positive influence of perceived privacy on trust. However, the non-significant positive impact of perceived privacy on trust found in this study is supported by the study of Lippert and Swiercz [23] on user acceptance of the online system, where the researcher attempted to test the influence

of perceived privacy and perceived security on trust. The results suggest that there is a significant impact of perceived information security towards stakeholders' trust. The results are in conjunction with the results of several prior studies such as AlHogail [20], and Wibowo and Mubarak [9]. Prior studies related to trust in any ICT services have been regarded as comparable to the trust in ICT led smart city technologies. Security factors have a positive influence on stakeholders' trust when it comes to IoT technologies, which are also an enabling technology for smart cities [20]. Lin and Dong [16] also found a significant positive influence of perceived security on users' trust using internet-based services. The positive coefficient value for the path Information Security Self-efficacy to Trust is not supported by the relevant *p*-value. This means the hypothesis is rejected, depicting that self-efficacy in information security does not have a positive influence on stakeholders' trust in smart city technologies. A study by Saif Almuraqab et al. [21] found that a positive relationship between trust and self-efficacy is related to safe and proper use of internet-based services.

The result indicates stakeholders' trust in smart city technologies positively influence their intention to adopt. The Q2 values of 0.14 and 0.29 for the endogenous factors, including 'trust' and 'intention to adopt', further support the predicted positive influence of trust on intention to adopt. The factors on trust and adoption have been previously studied by a number of studies on technology adoption [9,11]. The results from this study are consistent with the prior research study by Belanche et al. [6]. In their study, they found a significant influence of perceived trust on the adoption of an innovative e-commerce platform. Further, the outcome of the current study is also in line with the study of Alharbi et al. [37], which strongly supports that the trustworthiness of the smart city technologies used in smart cities promotes adoption by the stakeholders. The results of this study suggest that the trustworthiness of the individual services needs to be ensured to maximize the adoption of smart city technologies.

7. Conclusions

This paper presented and substantiated a trust-based model to study the stakeholders' intention to adopt smart city services and technologies. The study results show that perceived usefulness, perceived external pressure and perceived information security influence trust in smart city technologies. Further analysis highlights the significant relationship between stakeholders' trust and their intention to adopt smart city technologies. It is therefore critical for government agencies to formulate appropriate policies to enhance the use of smart city technologies.

From a theoretical point of view, this study contributes to the literature on smart cities. In particular, this study provides an in-depth understanding of the influence of technology, organization, environment and security factors on stakeholders' trust. Moreover, this study elaborates on how trust can be used for the successful adoption of new technologies such as smart city technologies. From a practical point of view, the study results can be used by government entities for transforming regional cities with smart technologies to improve the livability, productivity and sustainability of cities and suburbs. However, this study is not free from limitations: the proposed model was tested using the data collected from the Australian regional cities. Hence, the outcome of this research may not be directly applicable in contexts that are different to the scope of this study; this study attempted to validate various propositions made in the paper with limited supporting evidence, highlighting the need for future research into testing a trust-based smart city technologies adoption model. The data collection is based on an online survey. Future research could include interviews for a better understanding of the role of stakeholders' intention to adopt smart city services and technologies.

Author Contributions: Conceptualization, C.N. and S.W.; methodology, C.N., S.W. and S.G.; writing—original draft preparation, C.N.; writing—review and editing, S.W., S.G. and H.D.; supervision, S.W. and S.G. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: The study was conducted according to the guidelines of Human Research Ethics Committee and approved by the Ethics Committee of CQUniversity (Ethics number 21284, 20/06/2019).

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

References

1. Braun, T.; Fung, B.C.; Iqbal, F.; Shah, B. Security and privacy challenges in smart cities. *Sustain. Cities Soc.* **2018**, *39*, 499–507. [CrossRef]
2. Dewi, M.A.; Hidayanto, A.N.; Purwandari, B.; Kosandi, M.; Budi, N.A. Smart city readiness model based on technology-organization-environment (toe) framework and its effect on adoption decision. In Proceedings of the Pacific Asia Conference Information System, Yokohama, Japan, 26–30 June 2018.
3. AlKalbani, A.; Deng, H.; Kam, B. Organisational security culture and information security compliance for E-government development: The moderating effect of social pressure. In Proceedings of the Pacific Asia Conference on Information Systems, Singapore, 5–9 July 2015.
4. Mayer, R.C.; Davis, J.H.; Schoorman, F.D. An integrative model of organizational trust. *Acad. Manag. Rev.* **1995**, *20*, 709–734. [CrossRef]
5. Gefen, D.; Karahanna, E.; Straub, D.W. Trust and TAM in online shopping: An integrated model. *MIS Q.* **2003**, *27*, 51–90. [CrossRef]
6. Belanche, D.; Casaló, L.V.; Flavián, C. Integrating trust and personal values into the technology acceptance model: The case of E-government services adoption. *Cuad. Econ. Dir. Empresa* **2012**, *15*, 192–204. [CrossRef]
7. Van Zoonen, L. Privacy concerns in smart cities. *Govern. Inf. Q.* **2016**, *33*, 472–480. [CrossRef]
8. Australian Government. "Smart Cities and Suburbs", Department of Infrastructure. 2020. Available online: https://www.infrastructure.gov.au/cities/Sustainable-Development-Goal-11.aspx (accessed on 11 November 2020).
9. Wibowo, S.; Mubarak, S. Exploring stakeholders perceived risk and trust towards their intention to adopt cloud computing: A theoretical framework. In Proceedings of the Twenty-Third Pacific Asia Conference on Information Systems, Dubai, United Arab Emirates, 22–24 June 2020.
10. Dahlberg, T.; Mallat, N.; Öörni, A. Trust enhanced technology acceptance model consumer acceptance of mobile payment solutions: Tentative evidence. *Stockh. Mobil. Roundtable* **2003**, *22*, 1–19.
11. Yeh, H. The Effects of successful ICT-based smart city services: From citizens' perspectives. *Govern. Inf. Q.* **2017**, *34*, 556–565. [CrossRef]
12. Kramer, R.M. The sinister attribution error: Paranoid cognition and collective distrust in organizations. *Motiv. Emot.* **1994**, *18*, 199–230. [CrossRef]
13. 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]
14. Koller, M. Risk as a determinant of trust. *Basic Appl. Soc. Psych.* **1988**, *9*, 265–276. [CrossRef]
15. Zhang, K.; Ni, J.; Yang, K.; Liang, X.; Ren, J.; Shen, X.S. Security and privacy in smart city applications: Challenges and solutions. *IEEE Commun. Mag.* **2017**, *55*, 122–129. [CrossRef]
16. Lin, Z.; Dong, L. Clarifying trust in social internet of things. *IEEE Trans. Knowl. Data Eng.* **2018**, *30*, 234–248. [CrossRef]
17. Davis, F.D. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Q.* **1989**, *13*, 319–340. [CrossRef]
18. Tornatzky, L.G.; Fleischer, M. *The Process of Technological Innovation*; Lexington Books: Lexington, MA, USA, 1990.
19. Gangwar, H.; Date, H.; Ramaswamy, R. Understanding determinants of cloud computing adoption using an integrated TAM-TOE model. *J. Enterp. Inf. Manag.* **2015**, *28*, 107–130. [CrossRef]
20. Alhogail, A. Improving IoT technology adoption through improving consumer trust. *Technologies* **2018**, *6*, 64. [CrossRef]
21. Saif Almuraqab, N.; Jasimuddin, S. Factors that influence end-users' adoption of smart government services in the UAE: A conceptual framework. *Electron. J. Inf. Syst. Eval.* **2017**, *20*, 11–23.
22. Ratten, V. Behavioral intentions to adopt technological innovations: The role of trust, innovation and performance. *Int. J. Enterp. Inf. Syst.* **2014**, *10*, 1–12. [CrossRef]
23. Lippert, S.K.; Swiercz, P.M. Human resource information systems (HRIS) and technology trust. *J. Inf. Sci.* **2005**, *31*, 340–353. [CrossRef]
24. Li, C.; Dai, Z.; Liu, X.; Sun, W. Evaluation system: Evaluation of smart city shareable framework and its applications in china. *Sustainability* **2020**, *12*, 2957. [CrossRef]
25. Goldfinch, S.; Gauld, R.; Herbison, P. The participation divide? political participation, trust in government, and E-government in Australia and New Zealand. *Aust. J. Publ. Admin.* **2009**, *68*, 333–350. [CrossRef]
26. Rhee, H.S.; Kim, C.; Ryu, Y.U. Self-efficacy in information security: Its influence on end users' information security practice behavior. *Comput. Secur.* **2009**, *28*, 816–826. [CrossRef]

27. Teo, T.S.; Ranganathan, C.; Dhaliwal, J. Key dimensions of inhibitors for the deployment commerce. *IEEE Trans. Eng. Manag.* **2006**, *53*, 395–411. [CrossRef]
28. Von Solms, B. Information security—The third wave? *Comput. Secur.* **2000**, *19*, 615–620.
29. Bulgurcu, B.; Cavusoglu, H.; Benbasat, I. Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Q.* **2010**, *34*, 523–548. [CrossRef]
30. 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]
31. Grandhi, L.S.; Grandhi, S.; Wibowo, S. A security-UTAUT framework for evaluating key security determinants in smart city adoption by the Australian city councils. In Proceedings of the 21st ACIS International Winter Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, Ho Chi Minh City, Vietnam, 28–30 January 2021; pp. 17–22.
32. Chang, Y.; Wong, S.F.; Libaque-Saenz, C.F.; Lee, H. The role of privacy policy on consumers' perceived privacy. *Gov. Inf. Q.* **2018**, *35*, 445–449. [CrossRef]
33. Chellappa, R.K.; Pavlou, P.A. Perceived information security, financial liability and consumer trust in electronic commerce transactions. *Logist. Inf. Manag.* **2002**, *15*, 358–368. [CrossRef]
34. Sarabdeen, J.; Rodrigues, G.; Balasubramanian, S. E-government users' privacy and security concerns and availability of laws in Dubai. *Int. Rev. Law Comput. Technol.* **2014**, *28*, 261–276. [CrossRef]
35. Nikitas, A.; Michalakopoulou, K.; Njoya, E.T.; Karampatzakis, D. Artificial intelligence, transport and the smart city: Definitions and dimensions of a new mobility Era. *Sustainability* **2020**, *12*, 2789. [CrossRef]
36. Tolbert, C.J.; Mossberger, K. The effects of E-government on trust and confidence in government. *Pub. Admin. Rev.* **2006**, *66*, 354–369. [CrossRef]
37. Alharbi, N.; Papadaki, M.; Dowland, P. The impact of security and its antecedents in behaviour intention of using E-government services. *Behav. Inf. Technol.* **2017**, *36*, 620–636. [CrossRef]
38. Neupane, C.; Wibowo, S.; Grandhi, S.; Hossain, R. A Trust based smart city adoption model for the Australian regional cities: A conceptual framework. In Proceedings of the ACIS, Perth, Australia, 9–11 December 2019.
39. Hair, J.F.; Sarstedt, M.; Hopkins, L.; Kuppelwieser, V.G. Partial least squares structural equation modeling (PLS-SEM). *Eur. Bus. Rev.* **2014**, *26*, 106–121. [CrossRef]
40. Lew, Y.K.; Sinkovics, R.R. Crossing borders and industry sectors: Behavioral governance in strategic alliances and product innovation for competitive advantage. *Long Range Plan.* **2012**, *46*, 13–38. [CrossRef]
41. Lewis, B.R.; Templeton, G.F.; Byrd, T.A. A methodology for construct development in MIS research. *Eur. J. Inf. Syst.* **2005**, *14*, 388–400. [CrossRef]
42. Fornell, C.; Larcker, D.F. Evaluating structural equation models with unobservable variables and measurement error. *J. Mark. Res.* **1981**, *18*, 39–50. [CrossRef]
43. Henseler, J.; Ringle, C.M.; Sarstedt, M. A new criterion for assessing discriminant validity in variance-based structural equation modeling. *J. Acad. Mark. Sci.* **2015**, *43*, 115–135. [CrossRef]
44. Chin, W.W. The partial least squares approach to structural equation modeling. *Mod. Methods Bus. Res.* **1998**, *29*, 295–336.
45. Peng, D.X.; Lai, F. Using partial least squares in operations management research: A practical guideline and summary of past research. *J. Oper. Manag.* **2012**, *30*, 467–480. [CrossRef]
46. Schmidheiny, K. Clustering in the linear model. *Short Guides Microeconometrics-Univ. Basel* **2012**, *1*, 7–11.
47. Knack, S.; Zak, P.K. Building trust: Public policy, interpersonal trust, and economic development. *Supreme Court. Econ. Rev.* **2003**, *10*, 91–107. [CrossRef]