A Trust Based Smart City Adoption Model for the Australian Regional Cities: A Conceptual Framework

Research in Progress

Chiranjivi Neupane
School of Engineering and Technology
Central Queensland University
Rockhampton, Queensland
Email: chiranjivi.neupane@cqumail.com

Santoso Wibowo
School of Engineering and Technology
Central Queensland University
Melbourne, Victoria
Email: s.wibowo1@cqu.edu.au

Srimannarayan Grandhi
School of Engineering and Technology
Central Queensland University
Melbourne, Victoria
Email: s.grandhi@cqu.edu.au

Md Rahat Hossain
School of Engineering and Technology
Central Queensland University
Melbourne, Victoria
Email: m.hossain@cqu.edu.au

Abstract

With nearly half of the world's population living in the cities, many city and local governments are seeking to deploy smart solutions to their everyday city operations through the implementation of smart city services. However, the subject of smart city services has always been associated with trustworthiness of the services by its users due to security and privacy concerns. These issues may have a major impact on the smart city services adoption. The aim of this proposed research is to examine the technology, organisational, environment, and security determinants that influence stakeholders' trust towards their intention to adopt smart city services in Australian regional cities. For this, Technology-Organisation-Environment framework together with security related factors for ensuring stakeholders' trust will be tested using both quantitative and qualitative data. Structural equation modelling technique will be carried out using Smart PLS to test the presented hypotheses and the results will be finally discussed.

Keywords: Smart cities, adoption intention, security, trust, TOE framework, Australia regional cities.

1 INTRODUCTION

The worldwide urban population account to about 70% and this figure is expected to double in the next three decades (Braun et al. 2018). To address the problems that may arise due to the population growth and to improve the living standards of their citizens, local cities are transforming to smart cities (Dewi et al. 2016). Smart city services are ICT assisted intelligent services aimed at enhancing liveability, workability and sustainability by making the urban infrastructure and services efficient and integrated (Braun et al. 2018; Dewi et al. 2016). Literature highlights several benefits with smart city services. The benefits include smart energy, smart parks, smart precincts, smart lightings, smart transportations, smart water, smart governance, smart tourism, smart security and safety (Dewi et al. 2016; Zoonen 2016). Despite the benefits, there are security and privacy challenges that often influence the adoption of these smart city services. Saif Almuraqab and Jasimuddin (2017) point out that security challenges as a key factor towards the adoption of smart cities. This is further supported by Braun et al. (2018) and Dewi et al. (2018) who claim that security and privacy are major concerns for smart cities adoption. The use of innovative and smart technologies for smart city transformation is essential, but the intention to adopt the available technologies by its stakeholder is more important. According to Mayer et al. (1995) trust is the readiness to be vulnerable by the actions of another party. It is identified as a critical component for the technology adoption, as it addresses risk vulnerability and uncertainty (Gefen et al. 2003).

Trust and security are interrelated in adopting new technologies as individual's belief on security may have an influence on their adoption intention behaviour. In fact, previous studies considered trust as a factor in predicting intention behaviour (Belanche et al. 2012). Although, previous studies (Chourabi 2012; Dewi et al. 2016; Zoonen 2019) have been conducted on the importance of security and privacy for the adoption of smart cities through the development of a security model, these studies were limited to Technology, Organisation and Environmental factors, leaving the security and privacy implications behind. Literature presents limited evidence on smart cities adoption in Australian cities, let alone the effect of security and privacy on trust in the smart city services adoption by the Australian regional cities. Based on a report by the Australian government (2018), 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. Hence, it is critical for the government to plan for the future of regional cities by maximising their unique advantages and supporting their long-term growth through the development and implementation of smart city services whereby Australian regional cities can reach their full potential. Therefore, this study aims to provide a comprehensive review of factors that influence stakeholder's trust towards intention to adopt smart city services in the Australian regional cities. Furthermore, this paper proposes a conceptual framework by reviewing the models used for studying the users' adoption behaviour towards new innovations. This study aims to understand the role of security related factors in influencing stakeholders' trust towards their intention to adopt smart city services.

2 LITERATURE REVIEW

Smart city services have increasingly gained attention in academia, industry and governments in recent years (Braun et al. 2018). Although there is very limited research on trust-based adoption of smart city, literature presents various theories for the adoption of innovative technologies and factors such as trust and security have been widely used. Also, trust-based adoption of smart city services has not been studied using TOE framework. Scholars have proposed theories for the adoption of innovative technologies. Of these, most notable are Technology Adoption Model (TAM) (Davis 1989) and Technology, Organisation and Environment (TOE) model. TAM proposes that actual use intention of the technology is derived by the perceived ease of use and perceived usefulness of that technology (Davis 1989). Whereas, TOE model emphasises on studying the technology, organisation and environmental factors prior to new technology adoption (Tornatzky and Fleischer 1990). Interestingly, scholars (Gangwar and Ramaswamy 2015; Grandhi et al. 2019) presented the possibilities of adopting additional factors into the TOE model. This paper is backed by studies closely related to the context of the research. Using the original TOE model (Tornatzky and Fleischer 1990), this study presents a security related framework for the smart city adoption. Table 1 below presents previous studies using the TOE model.

Model	Study on adoption of technology	Authors
TOE	Adoption of ICT security culture in small, medium and micro enterprises	Mokwetli and Zuva 2018

Model	Study on adoption of technology	Authors
TOE	Influence of technology, organisation and environmental readiness towards smart city adoption decisions by local governments	Dewi et al. 2018
TOE and Human Organisation Technology (HOT)	Security determinants on cloud computing adoption by organisations. Study based on survey and interviews	Grandhi et al. 2019
Sec-TOE	Adoption of big data solutions by organisations	Salleh and Janczewski 2016
TOE	Decision making model for cloud computing adoption	Yoo and Kim 2018
TAM and TOE	Determinants of Cloud computing adoption	Gangwar and Ramaswamy 2015

Table 1. Previous Studies on Technology Adoption Models

2.1 Theoretical Framework

The theoretical framework developed in this study is based on the TOE model. The TOE model presents a number of dimensions that has influence towards adoption of innovation in organisations (Tornatzky and Fleischer 1990). Considering regional cities as public entities, the TOE model can be used to assess the determining factors towards an intention to adopt smart city services. Scholars have successfully used the TOE model to study the technology adoption intention. For example, Dewi et al. (2018) applied the TOE model to assess the influencing factors towards smart city adoption decision by public organisations. As this study aims to study the role of security related factors in influencing the stakeholders' intention to adopt smart city services in the Australian regional cities, the proposed TOE-based framework adopts information security related factors. Hence the framework in Figure 1 has been proposed as Technology-Organisation-Environment-Security (TOES) framework. Table 2 presents variables in this study and the sources.

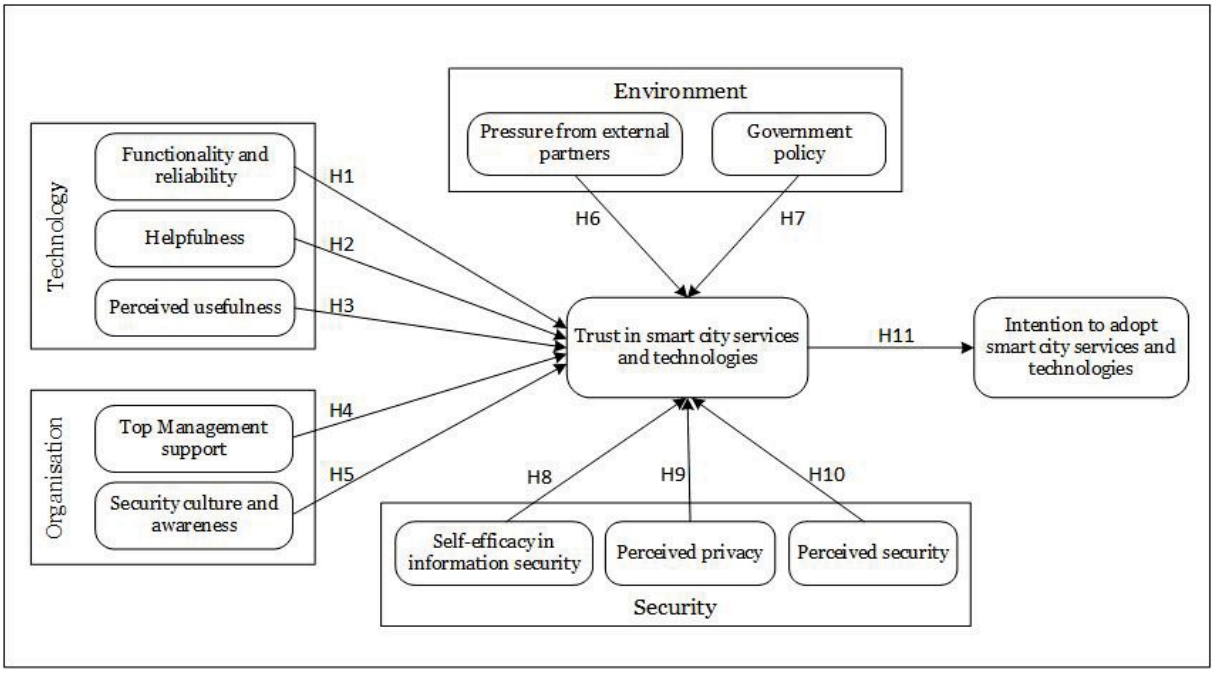

Figure 1: The research framework

2.2 Technology Related Factors

The technology can provide the required features and functions to perform a specific task (AlHogail 2018), but trusting a technology significantly depends on its ability to perform a task (Balasooriya et al. 2017). Helpfulness is the technology's ability and support to facilitate suitable, effective and responsive advice, which may be required to perform a task including guidelines and instructions (McKnight et al. 2011). The smart city stakeholders may perceive that new technologies would support them in performing tasks would incline towards adopting such technologies (AlHogail 2018). Perceived usefulness is the subjective probability of user's completion of a given task in an improved way (Guriting and Oly Ndubisi

2006). Jaafreh (2017) believes that the study of perceived usefulness and trust can have implication towards understanding the dynamic nature of trust and perceived usefulness. Earlier studies identified perceived usefulness as an important determinant in the new technology adoption intention (Colesca 2009). Hence, the following hypotheses have been presented:

H1: Functionality and reliability has positive influence towards trust in smart city services.

H2: Helpfulness positively influences trust in smart city services.

H3: Perceived usefulness of the smart city services positively influence stakeholder's intention to adopt smart city services.

2.3 Organisation Related Factors

Top management support refers to the commitment and involvement level of the senior management for smart city services adoption. Hu et al. (2012) demonstrated that top management support results in better organisational security policy enforcement and better security culture. Smart city projects require support from the strategic personnel and leaders during the decision-making process (Dewi et al. 2018). In an organisational context, information security awareness is an employee's knowledge and understanding about the information security policy and procedures (Bulgurcu et al. 2010). The security culture is created by instilling the concept of information security as usual duty of performance in the workplace. Therefore, it is reasonable to relate information security culture to the adoption of smart city services by its stakeholders.

H4: Top management support has positive influence towards trust on smart city services.

H5: Stakeholder's security culture and awareness positively influence stakeholder's trust in smart city services.

Factors	Definition	References
Functionality and reliability	It refers to capacity and ability of specific technology to provide the required features and functions for a specific task ensuring consistent and proper operations as predicted	AlHogail 2018; McKnight et al. 2011
Helpfulness	Technology's ability and support to facilitate suitable, effective and responsive advice, which may be required to perform a task including guidelines and instructions	AlHogail 2018; McKnight et al. 2011
Perceived usefulness	The extent of user's belief that use of technology would enrich their job performance	Davis 1989; McKnight et al. 2011; Saif Almuraqab and Jasimuddin 2017
Top management support	It refers to the extent of top management's commitment and involvement towards technology adoption decisions	Dewi et al. 2018; Hameed et al. 2012; Salleh and Janczewski 2016
Security culture and awareness	Information security culture is a subdomain of the organisation culture where it supports information security to become imminent part in employee's daily activities	Grandhi et al. 2019; Hameed and Arachchilge 2016; Saif Almuraqab and Jasimuddin 2017
Pressure from external partners	It refers to the pressure from other businesses such as partners or stakeholders in the supply chain that affects information security	Hashim et al. 2015; Ma and Ratnasingam 2008
Government policy	Government standards and regulations that may influence a business in terms of information security implementation	Balasooriya et al. 2017; Ma and Ratnasingam 2008
Self-efficacy in security	One's belief in capability to safeguard the information and system from unauthorised disclosure, manipulation, loss, destruction, and non-availability	Dewi et al. 2018; Rhee et al. 2009
Perceived security	The probability by which users or consumers believe that their sensitive information will not be tempered with by either viewing stored data or manipulated during transmission or storage by unauthorised persons	Chellappa and Pavlou 2002; Dewi et al. 2018; Hameed et al. 2012
Perceived privacy	The tendency to be concerned regarding submitted personal information to the services including safety of possible monitory transaction with services	Dewi et al. 2018; Rauniar et al. 2013; Zoonen 2016
Trust	Probability that a participant in a transaction will act in beneficial way or at least not harmful way to other participants so that they can cooperate later	AlHogail 2018; Saif Almuraqab and Jasimuddin 2017

Table 2. Factors and Definitions

2.4 Environment Related Factors

Pressure from external partners and government policy are environmental related factors under consideration in this study. In many cases, an organisation may adopt a technology due to influences exerted by its business partners. This adoption of a new technology can significantly be influenced by external pressure, particularly when this technology directly affects the competition and is a strategic necessity. In this situation, the pressure to adopt new smart city services quickly is to provide better services and gain strategic advantages. However, the decision to do so may result in an unexpected security concern (AlHogail 2018). In relation to government policy, Zoonen (2019) believes that smart city services need to adhere strictly to the existing government policy, as non-compliance may result in additional transaction costs and potential legal outcomes. This is supported by Balasooriya et al. (2017) who found that government policies have a positive impact on organisations trying to adopt new information systems technology. Hence the following hypotheses have been presented:

H6: Perceived external pressure negatively influences trust on smart city services.

H7: Government policies have positive influence towards trust on smart city services.

2.5 Security Related Factors

Self -efficacy, being an important paradigm of social cognitive theory, proximally determines individual behaviour (Bandura 1986). individuals with higher level of self-efficacy tend to have better motivation, cognitive resources and ability to mobilise themselves towards successful execution of a task (Stajkovic and Luthans 1998). Rhee et al. (2009) define self-efficacy in context of information security as a belief in one's capacity to protect information and information systems from unauthorised disclosure, modification, loss, destruction, and lack of availability. Self-efficacy therefore is considered as a possible factor towards adoption of smart city services in terms of information security. Perceived information security is the probability by which users or consumers believe that their sensitive information will not be tampered with by either viewing stored data or manipulated during transmission or storage by unauthorised persons (Chellappa and Pavlou 2002). Security has been identified as a factor having significant concern towards the intention to adopt risky technologies that used internet (Saif Almuraqab and Jasimuddin 2017). Goldfinch et al. (2009) found security of government's electronic services is an important factor towards its adoption by citizens. Hence, it can be generalised that intention to adopt new technology is fairly determined by its end user's trust over the security and privacy of that technology. Chourabi et al. (2012) identified privacy and security as the influencing factor in the smart city initiative model. Privacy can also play a major role determining trust by the users or stakeholders of smart cities because smart cities are made up of multiple digital services (Belanger and Hiller 2006). Developing trust between smart city service providers and its users is vital (Schurr and Ozanne 1985) as it represents the willingness to assume the risk of information disclosure (Mayer et al. 1995). When there is minimal risk of security in the smart city services, there would be more trust towards such service or system. Tolbert and Mossberger (2006) categorised trust into two categories, process-based and institution-based trust. Based on the discussion, the following hypotheses have been presented.

H8: Self-efficacy in information security positively influences stakeholder's trust in smart city services.

H9: Perceived information security of the smart city services positively influences stakeholder's trust in smart city services.

H10: Perceived privacy of the smart city services positively influences stakeholder's trust towards smart city services.

H11: Trust in smart city's digital services positively influences stakeholder's intention to adopt smart city services.

3 RESEARCH DESIGN

This research aims to test the role of technology, organisation and security determinants that influence stakeholders' trust towards their intention to adopt smart city services in the Australian regional cities. A two-step mixed method is adopted in this research. In the initial step, a quantitative study using survey questionnaire will be conducted to test the conceptual framework and the subsequent hypotheses. Then the qualitative study based on semi-structured interviews will be conducted to clarify the results from the quantitative study. The target recipients of the study are IT professionals working in the Australian regional cities, who are knowledgeable about smart city services. SmartPLS software will be used to employ the structural equation modellings technique, as it helps to reveal the relationships between the measured variables and the latent constructs.

4 CONCLUSION

There are limited studies on trust-based adoption model of smart city services. The initiation and acceptance of smart city services need to be adopted by its stakeholders for the success of such services. This research study thus aims to provide empirical evidence regarding influences of technology, organisation, environment, and security related factors towards trust in smart city adoption intention by its stakeholders. So, conclusive goal of this study is to identify security related concerns that influence towards adoption of smart city services. The findings from this study have both theoretical and practical implications. The findings can be beneficial for academia, IT professionals and local governments for considering most influencing factors for adoption decision of smart city services in a region.

5 REFERENCES

AlHogail, A. 2018. "Improving IoT Technology Adoption through Improving Consumer Trust," *Technologies* (6:1), July, pp. 64-73.

Australian Government, DITCRD (2018), "Smart Cities Plan". https://www.infrastructure.gov.au/cities/smart-cities/plan/index.aspx Retrieved 12 May 2019.

Balasooriya, P., Wibowo, S., Grandhi, S., and Wells, M. 2017. "The Impact of Security Concerns on Personal Innovativeness, Behavioural and Adoption Intentions of Cloud Technology," *Software Networking* (1:1), pp. 265-290.

Bandura, A. 1986. *Social Foundations of Thought and Action*. Englewood Cliffs, NJ: Prentice-Hall.

Belanche, D., Casal, L.V., and Flavian, C. (2012). "Integrating trust and personal values into the Technology Acceptance Model: The case of e-government services adoption," *Cuadernos de Economia Direccion de la Empresa* (15:4), pp. 192-204.

Belanger, F., and Hiller, J.S. 2006. "A Framework for E-Government: Privacy Implications," *Business Process Management Journal* (12:1), January, pp. 48-60.

Braun, T., Fung, C.M., Iqbal, F., and Shah, B. 2018. "Security and Privacy Challenges in Smart Cities," *Sustainable Cities and Society* (39:1), March, pp. 499-507.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. 2010. "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS Quarterly* (34:3), September, pp. 523-548.

Chellappa, R.K., and Pavlou, P.A. 2002. "Perceived Information Security, Financial Liability and Consumer Trust in Electronic Commerce Transactions," *Logistics Information Management* (15:1), December, pp. 358-368.

Chourabi, H., Nam, T., Walker, S., Gil-Garcia, J.R., Mellouli, S., Nahon, K., Pardo, T.A., and Scholl, H.J. 2012. "Understanding Smart Cities: An Integrative Framework," (HICSS), The 45th Hawaii International Conference on System Science, IEEE, pp. 2289-2297.

Colesca, S.E. 2009. "Understanding Trust in E-Government," *Inzinerine Ekonomika-Engineering Economics* (3:3), pp. 7-15.

Davis, F.D., 1989. "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology," *MIS Quarterly* (13:3), September, pp.319-340.

Dewi, M.A.A., Hidayanto, A.N., Purwandari, B., Kosandi, M. and Budi, N.F.A., 2018. "Smart City Readiness Model Based on Technology-Organization-Environment (TOE) Framework and Its Effect on Adoption Decision," The 22nd Pacific Asia Conference on Information Systems, pp. 1-7.

Gangwar, H., and Ramaswamy, R. 2015. "Understanding Determinants of Cloud Computing Adoption Using an Integrated TAM-TOE Model," *Journal of Enterprise Information Management* (28:1), February, pp. 107-130.

Gefen, D., Karahanna, E., and Straub, D. 2003. "Trust and TAM in online shopping: an integrated model," *MIS Quarterly* (27:1), pp. 51-90.

Goldfinch, S., Gauld, R., and Herbison, P. 2009. "The Participation Divide? Political Participation, Trust in Government, and E- Government in Australia and New Zealand," *Australian Journal of Public Administration* (68:1), August, pp. 333-350.

Grandhi, S., Wibowo, S., and Balasooriya, P. 2019. "Sec-HOTE-Fit Framework for Assessing Key Security Determinants in Cloud Computing Adoption," The 23rd Pacific Asia Conference on Information Systems, pp. 1-7.

Guriting, P., and Oly Ndubisi, N. 2006. "Borneo Online Banking: Evaluating Customer Perceptions and Behavioural Intention," *Management Research News* (29:1), January, pp. 6-15.

Hameed, M.A., Counsell, S., and Swift, S. 2012. "A Meta-analysis of Relationships between Organisational Characteristics and IT Innovation Adoption in Organisations," *Information and Management* (49:5), July, pp 218-232.

Hashim, H.S., Bin Hassan, Z., and Hashim, A.S. 2015. "Factors Influence the Adoption of Cloud Computing: A Comprehensive Review," *International Journal of Education and Research* (3:7), July, pp. 295-306.

Hu, Q., Dinev, T., Hart, P., and Cooke, D. 2012. "Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture," *Decision Sciences* (43:4), August, pp. 615-660.

Jaafreh, A.B. 2017. "Electronic Business Adoption and the National Culture: Conceptual Framework in the Saudi Arabia," *International Journal of Research in IT and Management* (7:1), pp. 48-56.

McKnight, D., Carter, M., Thatcher, J., and Clay, P. 2011. Trust in a Specific Technology: An Investigation of its Components and Measures," *ACM Transactions on Management Information Systems* (2:2), June, pp. 12-24.

Ma, Q., and Ratnasingam, P. 1995. "Factors Affecting the Objectives of Information Security Management," Proceedings of CONF-IRM 2008, pp. 29-35.

Mayer, R.C., Davis, J.H., and Schoorman, F.D. 1995. "An Integrative Model of Organizational Trust," *Academy of Management Review* (20:3), July, pp. 709-734.

Mokwetli, M., and Zuva, T. 2018. "Adoption of the ICT Security Culture in SMME's in the Gauteng Province, South Africa," International Conference on Advances in Big Data, pp. 1-7.

Rauniar, R., Rawski, G., Yang, J. 2013. "Social Media User Satisfaction - Theory Development and Research Findings," *Journal of Internet Commerce* (12:2), May, pp. 195-224.

Rhee, S.K., Kim, C., and Ryu, Y.U. 2009. "Self-efficacy in Information Security: Its Influence on End Users' Information Security Practice Behavior," *Computers & Security* (28:8), pp. 816-826.

Saif Almuraqab, N., and Jasimuddin S. 2017. "Factors that Influence End-Users' Adoption of Smart Government Services in the UAE: A Conceptual Framework," *The Electronic Journal Information Systems Evaluation* (20:1), pp. 11-23.

Salleh, K. A., and Janczewski, L. 2016. "Adoption of Big Data Solutions: A Study on its Security Determinants Using Sec-TOE Framework," Proceedings of the CONF-IRM 2016, pp. 1-12.

Schurr, P.H., and Ozanne, J.L. 1985. "Influences on Exchange Processes: Buyers' Preconceptions of a Seller's Trustworthiness and Bargaining Toughness," *Journal of Consumer Research* (11:4), February, pp. 939-953.

Stajkovic, A.D., and Luthans, F. 1998. "Self-Efficacy and Work-Related Performance: A Meta-Analysis," *Psychological Bulletin* (124:2), September, pp. 240-261.

Tolbert, C.J., and Mossberger, K. 2006. "The Effects of E- Government on Trust and Confidence in Government," *Public Administration Review* (66:1), May, pp. 354-369.

Tornatzky, L.G., and Fleischer, M. 1990. *The Processes of Technological Innovation*. Massachusetts: Lexington Books.

Yoo, S.K., and Kim, B.Y. 2018. "A Decision-Making Model for Adopting a Cloud Computing System," *Sustainability* (10:1), August, pp. 2952-2967.

Zoonen, L. 2016 Privacy Concerns in Smart Cities," *Government Information Quarterly* (33:3). July, pp. 472-480.