TEST Engineering & Management

January - February 2020
ISSN: 0193 - 4120 Page No. 12448 - 12456

Security Readiness Model of Public Organization in Smart Government: Conceptual Framework

Sulaiman Mohammed, Institute Technology Management and Entrepreneurship, Universiti Teknikal Malaysia Melaka, Melaka, Malaysia
Massila Kamalrudin, Associate Professor Doctor, Faculty of Information and Communication technology, Universiti Teknikal Malaysia Melaka, Melaka, Malaysia.
Samer Ali Al-shami Doctor, Institute Technology Management and Entrepreneurship, Universiti Teknikal Malaysia Melaka, Melaka, Malaysia
Halimaton Hakimi, Faculty of Information and Communication technology, Universiti Teknikal Malaysia Melaka, Melaka, Malaysia.
Safiah Sidek, Associate Professor Doctor, Institute Technology Management and Entrepreneurship, Universiti Teknikal Malaysia Melaka, Melaka, Malaysia

Article Info
Volume 82
Page Number: 12448 - 12456
Publication Issue:
January-February 2020

Article History
Article Received*: 18 May 2019*
Revised*: 14 July 2019*
Accepted*: 22 December 2019*
Publication*: 24 February 2020*

Abstract
Smart government are becoming one of the dominant and preferred sectors that intensely improving their service and facilities to attract public organization as well as to improve their delivering information. On top of that, security has become the main consent as it involves in every services and technology in smart government. This study aims to provide a new security readiness model of public organization in smart government. The proposed conceptual model for evaluating the level readiness of public organization in security of smart government. The proposed model will improve the security delivery of UAE government departments by enhancing the readiness towards public organization.

Keywords: *Big Security, Readiness Model, Public Organization, Smart Government*

I. INTRODUCTION

Smart governments need to provide effective security infrastructure and environment for better public organization. As the threat landscape on public organization continues to escalate, many organizations still lag behind in terms of protecting its critical infrastructure and electronic protected organization information as evident in the use of outdated technology and insecure internet. Therefore, improving the security in public organization is often the primary objective of the smart government to increase the security readiness level of organization change However, the smart government often impinge on the security public organization. It needs to be properly managed to public organization when they experience the security measures. It is necessary to consider readiness perspective to model security public organization in smart government in order to meet requirement in the future infrastructure of smart governments in order to meet the physical and emotional expectation of the public employee However, many studies have overlooked the aspect of security when it comes to the readiness model in. Likewise, the smart governments implemented at the United Arab Emirates is still at the infancy stage. Among of the issues faced by the organization are poor security management process. As the result, the organization faced the difficulty in terms of completing the procedure to change the readiness of security in public organization of smart government. In particular, readiness model remains largely unclear and definition and design of the underlying security readiness model of public organization in smart government is currently still missing, although various studies highlight the great demand and necessity for developing a renewing readiness model. Therefore, there are so far no security readiness model in public organization

January - February 2020
ISSN: 0193 - 4120 Page No. 12448 - 12456

designer for the smart government context. To fill in this research gap, this paper seeks to develop security readiness model of public organization smart government based on common findings of available readiness model for public organization perform self-assessment in determining its readiness to fight the security problem.

The rest of this paper is organized as follows: Section II presents the background and motivation. Section III presents the security readiness model in this paper. Section IV concludes the paper with some discussions about security readiness model and future works.

II. Background and Motivation

A. *Security of Public Organizations in Smart Governments*

In the context of smart government, the IT plays the important role to ensure the success of smart government implantation. The technology used are: Internet of Things (IoT), cloud computing, crowdsourcing, open data and others. Hence, the issues of security are also main problem in public organization.

The information security important for public organization which is enables the safe operation of application implemented on the organizations information technology system, protect the data the organizations collects and use at the organization and lastly is protect the organization's ability to function. This is because to protect the data, the organization will applied or install the appropriate software that will secure the data such as antivirus and others protected applications. So, information security is very important in an organization to protect the applications that implemented in organizations and protect the data store in computer as well. Besides protect the data, the application installed also need to be protect because it can contribute to information lost or damages.

Next, security is important to protect the data organization collects and used. If information is left unprotected, the information can be accessed by anyone. If the information falls into the wrong hands, it can destroy lives, dropping business and can also be used to do harm. Information security programs will ensure that appropriate information is protected both business and legal requirements by taken steps to protect the organizations data. In addition, taken steps to protect organizations information is a matter of maintaining privacy and will help prevent identity theft.

In public organization, information is important business assets and essential for the business and thus need appropriate protected. This is especially important in a business environment increasingly interconnected, in which information is now exposed to a growing number and a wider variety of threats and vulnerabilities. Cause damage such as malicious code, computer hacking, and denial of service attacks have become more common, more ambitious, and more sophisticated. So, by implemented the information security in an organization, it can protect the technology assets in use at the organization. However, the readiness of security is still not investigating in the public organization of smart government

Smart government is a complex concept, which involves not only the adoption of an innovation or sophisticated technology, but also involving the government and society as the parties that adopt the innovation. In addition, the adoption of smart city concept is a huge investment, in terms of providing smart technology, IT professionals, and also in designing procedures and ICT plans that must be tailored to the goals of both central and local government. Therefore, before adopting smart government concept, every leader needs to assess the barriers and benefits, as well as the readiness of their city, either from internal or external organization. Lou (2010) defines the concept of electronic readiness (e-readiness) as the ability of a country, company, or organizational unit to prepare, use, and take a benefit from the adoption of a new innovation, such as e-business, e-government, e-procurement, e-learning, etc. Based on the definition, the concept of smart government readiness is defined as the ability of the local government to prepare itself in adopting and implementing smart government optimally, so that the purpose of the smart government adoption

January - February 2020
ISSN: 0193 - 4120 Page No. 12448 - 12456

can be achieved well. Assessment of internal readiness when adopting smart government can provide an overview of the current position and state of the local government. In addition, it also can be a guideline to prepare all requirements needed in adopting smart government concept in public organization. Thus, smart government strategy or implementation plan can be done smoothly and solve various security problems in public organization.

B. What is readiness in the context of public organization?

Expressions, such as organizational readiness or organizational preparedness have the same meaning and they are focus more on the micro level, which is organization level. On the other hand, addition expression can be found, such as e-readiness which is more focused on macro level. “E-readiness (electronic readiness) is a measure of the degree to which a country, nation or economy may be ready, willing or prepared to obtain benefits which arise from information and communication technologies” (Dada, 2006, p. 1). The most practical definition of organizational readiness/preparedness from our stand point of view is the one proposed by Hartman, Sifonis, and Kador (2000) and refers to the “level at which an organization has optimized key attributes required to successfully implement Internet-enabled business strategies and initiatives“. Without first addressing its readiness, an organization’s IT initiatives may fail.

Organizational readiness is a journey, not a destination. Through continuous improvement an organizational can more easily deploy and use ICT enabled business processes that are focused, accountable and measurable. Together the four pillar can help drive organizational success. If the foundation of one pillar is not as strong as the others, the organization may falter on its path on long term success.

C. The Factors to Determine Readiness of Security in Public Organization.

There are many works done to enhance the security in public organization. For example, (Tarimo, 2006) have developed a new approach for ICT security readiness checklist for developing countries. They are conducted quantitative approach to measure the effectiveness of security for developing countries. The measurement item focus in information security which is confidentiality, integrity and availability. However this research more focusing on developing countries rather than focus on organization.

Next, Upadhyaya et al., (2012) developed E-government security readiness assessment for developing countries. In this studies, they are use mixed research method in which both qualitative and quantitative methods and techniques are used in the overall study. They are use two sets of questions were prepared. The first set was targeted for IT department heads, and security experts or system administrators because they manage all the information systems functionalities including its security while the security experts or system administrators make sure that the systems are functioning as per the required policy, procedures, organization's requirement, etc. The second set was a general security related questions targeted for any employee of that organization to understand whether information systems users in the organizations to know the awareness of IS security, policies and procedures, training they received, etc. Questionnaires that were targeted to the IT department heads were designed based on the ISO audit checklist customized and ICT security readiness checklist addressing the main components to assess the IS security readiness and audit of a given organization. Even though, this study focusses on the security readiness in organization. But they are doing not focus on public organization.

Mijnhardt et al., (2016) developed Information Security Focus Area Maturity for Small Medium Enterprise SME information security as cornerstone in the development of an assessment too for tailor-made, fast, and easy-to-use information security

January - February 2020
ISSN: 0193 - 4120 Page No. 12448 - 12456

advice for SMEs. They evaluate the model with the expert it ICT. They evaluate based on these two important factors in the security which are information security and security policy. This another seven previous studies also mentioned that information security and security policy are important in the security of organization (Choi and Lee, 2015) (Kautsarina and Gautama, 2014) (Antoniou, 2018) (Sohrabi et al., 2016) (Soomro et al., 2016)(Singh, 2017)(Kirlappos et al., 2015). This work describes exploratory research into the field of adaptive IS assessments targeted at SMEs. They performed a systematic literature review and assembled a total of 75 organizational factors. By grouping factors and removing factors not adhering to set criteria, we identified a long list of 26 OCs for IS in SMEs. For each of these OCs, the levels of measurement were defined and a number of iterative interviews were held. Even though this study focus on the security maturity but they more focusing on the measurement security in SME rather than public organization.

Furthermore (Al-izki and Weir, 2016) conducted survey to assess the information security posture within Omani public sector organization, as well as the Omani manager's attitude towards Security. In the survey, they targeted four dimensions of security in public organization which are 1. Organization's Information Security Policy 2. Organization's compliance with IS best practices 3. Information Security Training and Awareness 4. Managerial attitude towards Information Security. These four dimensions were specified as aspects of Information Security. The survey, was conducted anonymously and was disseminated electronically via the Internet to all participants. Questions were written in Arabic and English to accommodate the native language and working language of participants. However, this study those not cater on the security readiness in the public organization.

(Almubayedh et al., 2019) discussed on the security issues in Saudi Arabia Small Organization. The studies more emphasize that the precise awareness of information security policy, its aspects and practices is a significant point that organizations must pay attention to prevent potential security threats. However, some Saudi organizations lack the security awareness. They represents some previous studies that were conducted to evaluate the state of policy, information security awareness and security training (Sari and Nurshabrina, 2016) (Singh, 2014) (Maynard et al., 2013) (Kraemer et al., 2009) and application in a Saudi organization. They consider a small Saudi organization to perform a case study, to audit its state and describe the possible risk scenarios that may take place. Most information about the company was gathered by interviewing its CEO. The audit found five possible risk scenarios, named lack of security policy, personal information leakage from the website, the risk of damage of the CEO's device and two scenarios related to outsourcing companies. Therefore, they provided some recommendations to the audited organization which may serve other organizations that have the same characteristics, which are adopting and documenting a comprehensive security policy and procedures from beginning stages of a company, ensure that the employees are aware of these documents and the required practices to secure sensitive information. In addition, introduce a mechanism to ensure that security controls are met and to secure personal information transmitted over their website and recommending to regularly checks that the website is bugs free. Additionally, recommends considering more security details on the outsourcing contracts and involve a specialized attorney on it. Also, prefer short-term out- sourcing contracts and take possible alternatives third-party companies into consideration as a precaution.

In the nutshell, the comparison of all above-mentioned related works and the summarization of factor to determine readiness of security in public organization in Table 1.

January - February 2020
ISSN: 0193 - 4120 Page No. 12448 - 12456

Table 1: Factor of Security in Public Organization

Author	Factor									Domain
	Information Security			Security Policy	Security Standard	Security Processed	Security Training	Culture	Awareness	
	Availability	Integrity	Confidentiality							
(Tarimo, 2006)	x	x	x							IT
(Upadhyaya et al., 2012)				x	x	X				E-Government
(Mijnhardt et al., 2016)	x	x	x	x						SME
(Choi and Lee, 2015)	x	x	x	x						Cloud System
(Kautsarina and Gautama, 2014)	x	x	x	x	x					IT
(Al-izki and Weir, 2016)				x			x		x	Public organization
(Antoniou, 2018)	x	x	x	x	x					Public Organization
(Almubayedh et al., 2019)				x	x	X	x			Organization
(Felipe, 2017)				x						Organization
(Almubayedh et al., 2019)				x			x		x	Organization
(Sari and Nurshabrina, 2016)				x			x		x	Education
(Lange et al., 2016)				x						Organization
(Singh, 2014)				x			x	x	x	Organization
(Madini O. Alassafi, Abdulrahman Alharthi, Robert J Walters, 2015)								x		Organization
(Maynard et al., 2013)									x	SME
(Sohrabi et al., 2016)	x	x	x	x						Organization
(Soomro et al., 2016)	x	x	x	x			x		x	
(Singh, 2017)	x	x	x	x			x		x	Services organization
(Kirlappos et al., 2015)	x	x	x	x					x	Learning Organization
(Kraemer et al., 2009)							x		x	Organization
Total	**9**			**16**	**4**	**2**	**8**		**9**	

Altogether, seven important factors were identified from a total of 20 studies to the factors involved in security in public organization. Based on the Table 1 above, we found that *Security Policy* is most important factor which account 16 studies. This is followed by *Information security and Awareness* of security with nine studies and *security training with eight* studies. The rest of this studies brief of description of these findings.

As a conclusion, although *Security policy, Information security and Awareness* is the most concerned factor identified in this review, the weightage of applying the factor influence is different. It shows that all attributes four *Security Policy, Information Security, Awareness and Security Training* are gained more crucial and attention in security of public organization. Therefore, in Table 1 and Table 2, we explain in general and operational definition of four factors of security in public organization.

January - February 2020
ISSN: 0193 - 4120 Page No. 12448 - 12456

Table 2: The Definition of Factor in security of organization

Element	Operational Definition
Security Policy	A set of rules and practices that specify or regulate on how a system or organization provides security services to protect sensitive and critical system resources.
Security Information	The practice of protection information such as confidentiality, integrity and availability from unauthorized access, use, disclosure, alert, inspection and recording or damage.
Security Training	formal process for educating employees about computer security
Awareness	Knowledge and attitude members of an organization possess regarding the protection of the physical, and especially informational, assets of that organization. Many organizations require formal security awareness training for all workers when they join the organization and periodically thereafter, usually annually

III. CONCEPTUAL FRAMEWORK

Figure 1 shows the conceptual framework of security readiness model of public organization in smart government. The model is developed based on the literature review. The model consists of dimension of security readiness and dimension of readiness model. The developments of the model start with determination of dimensions of security readiness of smart governments. The purpose of developing a new security readiness model of public organization in smart governments as reference for top management to measure the readiness of organization for level security. Based on the literature review conducted, we found that there are four dimensions of security of organization which are security policy, security information, security training and awareness. These four dimensions have relationship with security readiness in public organizations. The detailed description of the conceptual frameworks is explained in below:

Motivated from the gaps described by the literature and determine factor of security readiness in section II(c), we propose to overcome the gaps through proposing a security readiness model of public organization in smart governments. This security readiness model will employ the concept of readiness model design as per described in Section II. This is because it found that readiness model able to incorporate human perspective and technology for better change in public organization of smart UAE government. Figure 1 shows the conceptual framework proposed for this study. As shown in Figure 1, the security readiness model in public organization.

Based on the research conceptual model, the specifically hypothesis following are formulated in this research and shown in Table 3.

Table 3: Formulation Research Hypothesis

H1	H_1:	There is a significant relationship information security and security readiness
	H_0:	There is no significant relationship between information security and security readiness
H2	H_1:	H_1: There is a significant relationship between security policy and security readiness
	H_0:	There is no significant relationship between security policy and security readiness
H3	H_1:	There is significant relationship between security training and security readiness
	H_0:	There is no significant relationship between security training and security readiness
H4	H_1:	There is a significant relationship between awareness and security readiness
	H_0:	There is no significant relationship between awareness and security

January - February 2020
ISSN: 0193 - 4120 Page No. 12448 - 12456

		readiness
H5	H_1:	There is a significant relationship between trust and security readiness
	H_0:	There is no significant relationship between trust and security readiness
H6	H_1:	There is a significant relationship between usability and security readiness
	H_0:	There is no significant relationship between usability and security readiness
H7	H_1:	There is a significant relationship between knowledge and security readiness
	H_0:	There is no significant relationship between knowledge and security readiness

IV. CONCLUSION AND FUTURE RESEARCH DIRECTION

This study contributes on new factor of security readiness for public organization in UAE, organization can use this model for reference in developing the successful public organization.

The intention was to develop security readiness model to help guide the top management in the public organization to measure readiness of security according employee expectation. For future work, we will evaluate the security readiness model with our potential respondent that working in public organization at the UAE smart governments.

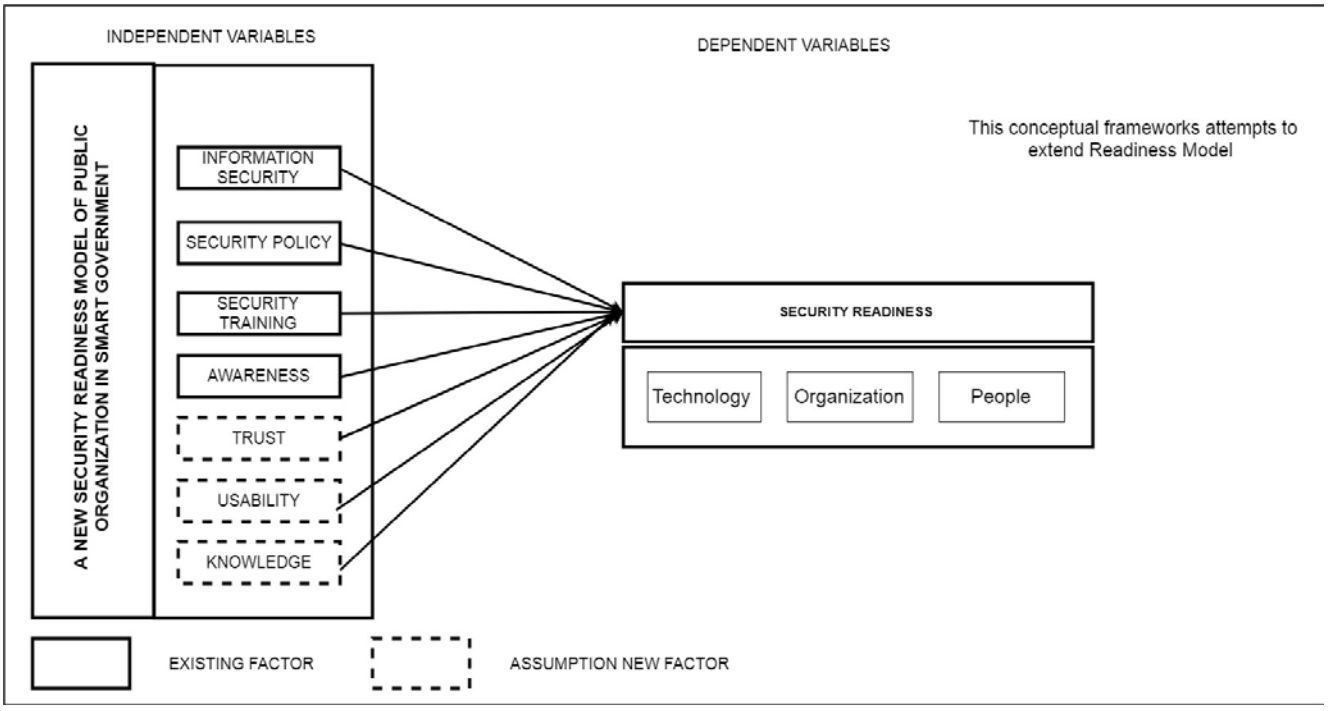

Fig. 1. The proposed conceptual framework

ACKNOWLEDGMENT

The authors are grateful to those who have assisted directly or indirectly to complete this study at Universiti Teknikal Malaysia Melaka.

.

REFERENCES

[1] Alam, F. & Paul, A., 2016. A Computational model for Trust and Reputation relationship in Social Network. s.l., IEEE, pp. 1-6.

[2] Almarabeh, T. & Abu Ali, A., 2010. A General Framework for E-Government: Definition Maturity Challenges, Opportunities, and Success.. European J. of Scientific Research, 39(1), pp. 29-42.

January - February 2020
ISSN: 0193 - 4120 Page No. 12448 - 12456

[3] Almuraqab, N. S., 2016. M-Government Adoption Factors in the United Arab Emirates: A Partial Least-Squares Approach. International Journal of Business and Information, 11(4), pp. 404-431.

[4] Anthopoulos, L. G., 2017. Smart Government: A New Adjective to Government Transformation or a Trick?. In: Understanding Smart Cities: A Tool for Smart Government or an Industrial Trick?. s.l.:Springer International Publishing, pp. 293-293.

[5] Antrhopolous, L. & Reddick, C. G., 2016. Smart City and Smart Government: Synonymous or Complementary?. MOntreal, Quebec, s.n.

[6] Bartle, C., Avineri, E. & Chatterjee, K., 2013. Online information-sharing: A qualitative analysis of community, trust and social influence amongst commuter cyclists in the UK. Transportation Research Part F, pp. 16, pp. 60–72.

[7] Bingham, L. B., Nabatchi, T. & O'Leary, R., 2005. . The new governance: Practices and processes for stakeholder and citizen participation in the work of government. Public Administration Review, pp. 65(5), 547–558.

[8] Cheng, H.-H. & Fu, T.-J., 2018. The Determinants of Online Shopping Behavior. Singapore, s.n.

[9] Chen, Y.-F. & Lan, Y.-C., 2014. An Empirical Study of the Factors Affecting Mobile Shopping in Taiwan. International Journal of Technology and Human Interaction, 10(1), pp. 19-30.

[10] Clohessy, T., Acton, T. & Morgan , L., 2014. Smart city as a service - A future roadmap for e-government smart city cloud computing initiatives. s.l., IEE/ACM.

[11] Fong, S., Zhuang, Y., Yu, M. & Ma, I., 2012. Quantitative Analysis of Trust Factors on Social Network using Data Mining Approach. London, s.n.

[12] Gil-Garcia, J. R., Helbig, N. & Ojo, A., 2014. Being smart: Emerging technologies and innovation in the public sector. Government Information Quarterly, 31(1), pp. 11-18.

[13] Gil-GArcia, J. R., Pardo, T. A. & Nam, T., 2015. What makes a city smart? Identifying core components and proposing an integrative and comprehensive conceptualization.. Information Polity, 20(1), pp. 61-87.

[14] Gil-Garcia, J. R., Zhang, J. & Puron-Cid, G., 2016. Conceptualizing smartness in government: An integrative and multi-dimensional view. Government Information Quarterly, 33(3), pp. 524-534.

[15] Habibi, M. R., Laroche, M. & Richard, M.-O., 2014. The roles of brand community and community engagement in building brand trust on social media. Computers in Human Behavior, 37(1), pp. 152-161.

[16] Hajli, N., 2018. Ethical Environment in the Online Communities by Information Ethical Environment in the Online Communities by Information. J Bus Ethics , 149(1), pp. 799-810.

[17] Hallikainen, H. & Laukkanen, T., 2018. National culture and consumer trust in e-commerce. International Journal of Information Management, 38(1), pp. 97-106.

[18] Harsh, A. & Ischalkaranje, N., 2015. Transforming e-government to smart government: A South Australian perspective. Advances in intelligent Systems and Computing, pp. 1, 9-16.

[19] Hoffmann, C., Lutz, C. & Meckel, M., 2014. The Impact of User Characteristics on Online Trust. Journal of Management Information Systems, 31(3), pp. 138-171.

[20] Hsu, M.-H., Chuang, L.-W. & Hsu Cheng, S., 2014. Understanding online shopping intention: the roles of four types of trust and their antecedents, Internet Research, pp. Vol. 24 Issue 3, pp.332-352.

[21] Jafarpour, H. & Andalib, A., 2016. A New Method for Determination of Effective Criteria to Evaluate Electronic Trust (E-Trust) of Online Customers. s.l., s.n., pp. 1-6.

[22] Janowski, T., 2015. Digital government evolution: From transformation to contextualization. Government Information Quarterly, pp. 221-236.

[23] Jiménez,, C. E. et al., 2014. Smart government: opportunities and challenges in smart cities development. In: Handbook of research and democratic strategies and citizen-centred e-government services. Hershey: IGI Global, pp. 1-19.

[24] Kavanaugh, A. et al., 2016. The Use and Impact of Social Media during the 2011 Tunisian Revolution. Shaghai, China, s.n.

[25] Kay, T. & We, C., 2009. Smart IT. IEEE IT Pro, pp. 20-23.

[26] Kiliroor, C. C. & Valliyammai, C., 2016. Trust Analysis on Social Networks for Identifying Authenticated Users. s.l., s.n.

January - February 2020
ISSN: 0193 - 4120 Page No. 12448 - 12456

[27] Kim, S. & Park, H., 2013. Effects of various characteristics of social commerce (s-commerce) on consumers' trust and trust performance. International Journal of Information Management, Volume 33, pp. 318-332.

[28] Kliksberg, B., 2000. Rebuilding the state for social development: Towards "smart governmenr".. International Review of Administrative Sciences, pp. 66(2), 241-257.

[29] Kostagiolas, P., Korfiatis, N., Kourouthanasis, P. & Alexias, G., 2014. Work-related factors influencing doctors search behaviors and trusttoward medical information resources. International Journal of Information Management, pp. 34, pp.80–88.

[30] Liu, M. & Yuan, Q., 2015. The Evolution of Information and Communication Technology in Public Administration. Public Administration and Development, 35(2), pp. 140-151.

[31] Li, Y., Wang, X., Lin, X. & Hajli, M., 2018. Seeking and sharing health information on social media: A net valence model and cross-cultural comparison. Technological Forecasting & Social Change, 126(1), pp. 24-40.

[32] Mellouli, S., Luna-Reyes, L. F. & Zhang, J., 2014. Smart government, citizen participation and open data. Information Polity, pp. 19, 1-4.

[33] Meskaran, F., Ismail, Z. & Shanmugam, B., 2013. Online Purchase Intention: Effects of Trust and Security Perception. Australian Journal of Basic and Applied Sciences, 7(6), pp. 307-315.

[34] Nishioka, D., Saito, Y. & Murayama, Y., 2014. The influence of knowledge level in information security onto the factors of Anshin for online shopping users. Hawaii, s.n.

[35] Noor, A. D., Sulaiman, R. & Abu Bakar, A., 2014. A Review of Factors that Influenced Online Trust in Social Commerce. Putrajaya, Malaysia, s.n.

[36] Paek, H.-J. & Hove, T., 2014. Determinants of Vertical and Horizontal Online Health Information Behavior. Hawaii , IEEE Computer Society, pp. 1-10.

[37] Pal, D., Funilkul, S., Charoenkitkarn, N. & Khantamanin, P., 2018. Internet-of-Things and Smart Homes for Elderly Healthcare: An End User Perspective. SPECIAL SECTION ON HUMAN-CENTERED SMART SYSTEMS AND TECHNOLOGIES, IEEE Translations, Volume 6, pp. 10483-10496.

[38] Ponte, E., Carvajal-Trujillo, E. & Escobar-Rodríguez, T., 2015. Influence of trust and perceived value on the intention to purchase travel online: Integrating the effects of assurance on trust antecedents. Tourism Management, pp. 47, pp. 286-302.

[39] Salvodelli, A., Codagnone, C. & Misuraca, G., 2014. Understanding the e-government paradox: Learning from literature and practice on barriers to adoption.. Government Information Quarterly, pp. 31, 63-71.

[40] Scholl, H. J. & Scholl, M. C., 2014. Smart Governance: A Roadmap for Research and Practice. Berlin, Germany, s.n., pp. 1-17.

[41] Sparks, B., Perkins, H. & Buckley, R., 2013. Online travel reviews as persuasive communication: The effects of content type, source, and certification logos on consumer behavior. Tourism Management, pp. 39, pp. 1-9.

[42] Wang, S. & wang, X., 2008. Factors Impacting Chinese Consumers' Macro-Level Trust on B2C E-Ecommerce: An Empirical Study. Taipei, Taiwan, s.n.