Sec-HOTE-Fit Framework for Assessing Key Security Determinants in Cloud Computing Adoption

Research-in-Progress

Srimannarayana Grandhi

Santoso Wibowo

Prasanna Balasooriya

Abstract

The use of Cloud computing has been growing steadily due to its support to businesses and individuals in cost saving and service improvements. Despite the benefits, there are concerns such as security and privacy during its adoption. The purpose of this proposed research is to examine the security determinants by focusing on the influence of technological factors in security, organisational security view and security related environmental factors. To accomplish this goal, the Technological-Organisational-Environmental (TOE) and the Human-Organisation-Technology (HOT-fit) frameworks are adopted into the main research framework. This research will be conducted using a Sequential Explanatory Mixed Method approach. The online survey questionnaires will be used to collect data. Then, the result of this first quantitative process will be further explored and complemented with semi-structured interviews. Results generated from both phases will then be triangulated and a cross-study synthesis will be conducted to form the final result and discussion.

Keywords: Cloud Computing, Adoption, Security, Sec-HOTE-fit Framework, Determinants

Introduction

Cloud computing or cloud services are one of the important technologies for businesses to maintain competitiveness in the marketplace. In fact, it has emerged as a powerful platform for organisations that prefer to delink management of software systems from their core functions (Motiwalla and Thompson 2012; Grandhi and Wibowo 2015). This model allows to host resources outside their organisation and provide them with flexibility and on-demand access to virtualised resources via networks (Mell and Grance 2011). It empowers users with online data storage and software services options through networks (Saedi 2016). Cloud computing can be defined as a model for achieving a flexible, on-demand network access to a range of virtualised IT resources including servers, applications, networks, data storage and services that are located outside the organisation (Mell and Grance 2011; Shayan et al. 2014). It allows users to share and access the resources online via subscriptions. Moreover, cloud computing permits organisations to breakdown their systems and services into smaller components, which can be distributed across the network.

The ease of access and the cost of owning resources made cloud computing popular (Motiwalla and Thompson 2012). Over the years, businesses have adopted various technologies to benefit from cloud computing. A recent study by KPMG (2016) predicts that more than $3 billion savings achieved through cloud computing adoption by Australian organisations will make an additional contribution to the Australian GDP. Hashemi (2013) points out that cloud computing helps businesses to reduce their operational costs by providing access to critical information and resources. Due to numerous benefits, more than 40% of European organisations have adopted cloud services to achieve cost and efficiency related benefits. In fact, recent studies highlight the potential increase in IT spending for acquiring technologies to enable public or private cloud services (Habjan and Pucihar 2017). Despite these benefits, the adoption rate of cloud computing is growing very slowly due to security and privacy concerns (Hashemi 2013). The Cloud computing poses several security risks with storing data outside of the organisation. Poor security may lead to attacks from hackers, malware infections, loss of intellectual property and loss of control over information systems altogether. Due to security concerns on sensitive data, organisations limit the use of cloud computing services. Security breaches can cause loss of control over sensitive data, availability and performance (Ray 2016; Wibowo and Grandhi 2019). Singh et al. (2015) explain that security breaches were the main reason in limiting the adoption of cloud computing by European organisations. Although cloud computing is still evolving, it is important to ensure and address data security and the privacy of the users' data on the cloud.

This study identified two research gaps. First, despite significant literature on cloud computing, there are limited studies into the security factors associated with cloud computing adoption (Lian, Yen and Wang 2014; Priyadarshinee et al. 2017; Saleh and Janczewski 2016). Moreover, some of these studies are inconclusive due to limited data (Saleh and Janczewski 2016). Second, Australia was ranked 5 globally with a score of 80.61 for cloud computing adoption. While there is significant interest among public and private entities in adopting cloud computing, there are limited number of studies (Al Ismaili et al. 2016; Senarathna et al. 2018) on security implications of cloud computing. Hence, this paper assesses the security determinants for the adoption of cloud computing by organisations.

This paper reviews the two theoretical frameworks, Technology-Organisation-Environment framework and Human-Organisation-Technology framework for cloud adoption, and develops a research framework based on previous studies presented in table 1 to examine the security determinants for cloud computing adoption. This paper is organised into five sections. Section two provides a literature review on cloud computing adoption framework and the two prominent frameworks, namely TOE and HOT-fit. Then the research framework and the research questions are presented. Section three presents the proposed research hypotheses. Section four presents the proposed research design and Section five concludes the paper with expected contributions of the research.

Literature Review and Research Framework

This section provides a brief overview on cloud computing adoption framework and then details the two prominent frameworks such as TOE and HOT-fit. The research questions and the research framework are presented at the end of this section.

Cloud Computing Adoption Models

Various theories have been proposed by the scholars in the IS research domain. However, the most notable theories in cloud computing adoption studies in organisations are the Technology-Organisation-Environment (TOE) and Human-Organisation-Technology (HOT) frameworks. Several studies point out the benefits associated with cloud computing adoption, however, it is also important for organisations to consider cloud computing adoption as an organisational issue. Scholars have proposed various theories to explain the organisational context and the fit between the proposed technology innovation and the organisation fit itself (Oliveira et al. 2014). Although, there are other theories such as the Theory of Reasoned Action, the Theory of Planned Behaviour and the Technology Acceptance Model (Awa et al. 2016), these are not taken into account as they are limited to an individual's choice (Oliveira et al. 2014).

Technology-Organisation-Environment (TOE) Framework

The TOE model was proposed by Tornazky and Fleischer (1990) to provide a general framework for assessing the possibilities of adopting new technologies or innovations into an organisation. It considers three important contexts of an organisation that influence adoption of new technologies or innovation. The three contexts are technology, organisation and environment (Alshamaila and Papagiannidis 2013; Priyadarshinee et al. 2017). The technology aspect looks at both internal and external technologies as well as the technologies available for possible adoption. The organisational context captures the characteristics of an organisation. These characteristics include firm size, business scope, structure, resources, employees, top management support and culture. Meanwhile, the environment frame consists of market elements including competitors and competitive pressures, trading partners and their readiness, government support, support from the technology providers and sociocultural issues (Awa et al. 2016).

Human-Organisation-Technology (HOT-Fit) Framework

The HOT framework was built on the basis of existing information system evaluation studies. It provides a generic framework to thoroughly assess the quality of a system (Yusof et al. 2008) through three important contexts, namely human, organisation and technological. Willcocks (1994) explains that a successful implementation of technologies require a proper alignment between human, organisation and technologies factors. In fact, various studies point out the importance of human factors in the adoption of new technologies (Alharbi et al. 2016; Lian et al. 2014). Although the human factors in the organisation and the technology contexts can be complex and idiosyncratic in nature, it can offer great support in evaluating the effectiveness and efficiency. Yusof and Arifin (2016) explain that HOT-fit can be used as a comprehensive tool for evaluating organisational systems. Table 1 below provides a summary of previous studies on cloud computing adoption in relation to the two frameworks discussed above.

Table 1 Summary of Previous Research Results on Cloud Computing Adoption in Relation to TOE and HOT Frameworks

Framework used	Research method	Sample	Outcome	Reference
TOE	Qualitative	15 Semi-structured interviews in UK	TOE contexts are connected to each other	Alshamaila and Papagiannidis 2013
Sec-TOE	Quantitative	Online survey of 25 responses from NZ information security forum	Security and privacy regulatory concerns were inconclusive	Saleh and Janczewski 2016
TOE	Quantitative	A questionnaire survey of 110 Indian SMEs	Security and privacy and sharing and collaboration are the top priorities for cloud computing adoption	Priyadarshinee et al. 2017
TOE	Mixed method	Online survey of 136 Australian SMEs	A tested model for cloud computing adoption	Prasad et al. 2014
TOE and HOT	Quantitative	A questionnaire survey of 106 hospitals in Taiwan	Security and technical competence are among the top 5 most critical factors in cloud computing adoption	Lian, Yen and Wang 2014
TOE, HOT and IS strategy triangle	Quantitative	Online survey of 201 healthcare organisations in Saudi Arabia	Financial factors are among the top critical factors in cloud computing adoption	Alharbi, Atkins and Stanier 2016

The TOE framework was developed by Tornatzky and Fleischer (1990) with the intention to describe the innovation mechanism at the organisational level. On the other hand, the HOT-fit framework considers the human factor in the adoption of new technology. Both TOE and the HOT-fit frameworks both consider organisation and technology aspects in relation to the adoption of new technologies including cloud computing. These frameworks, however, ignore one of the key aspects in human and environment. Yusof et al. (2008) reiterate the need to consider human aspect as technical issues related to the effectiveness of proposed technology. At the same time, the HOT-fit framework considers the human side of issues in relation to the new technology adoption. However, it does not capture the issues associated with the environment. This is important as the consideration of both human and environmental factors can allow a comprehensive evaluation of new technologies. As there is an overall similarity between the two frameworks (Lian et al. 2014), combining both the TOE framework with the HOT-fit framework can support a comprehensive evaluation of various factors for supporting the organisations intention to adopt cloud computing technology. Recent studies conducted by Alharbi et al. (2016) and Lian et al. (2013) which combined the TOE and HOT-fit frameworks for evaluating the cloud computing technology adoption intention revealed the critical success factors in cloud computing adoption. Considering the benefits of TOE and HOT-fit frameworks, this study adopts the combined framework to assess the key security determinants in cloud computing adoption. Based on the literature review, the following research framework has been developed to assess the security determinants in cloud computing adoption. Figure 1 presented below illustrates the proposed research framework.

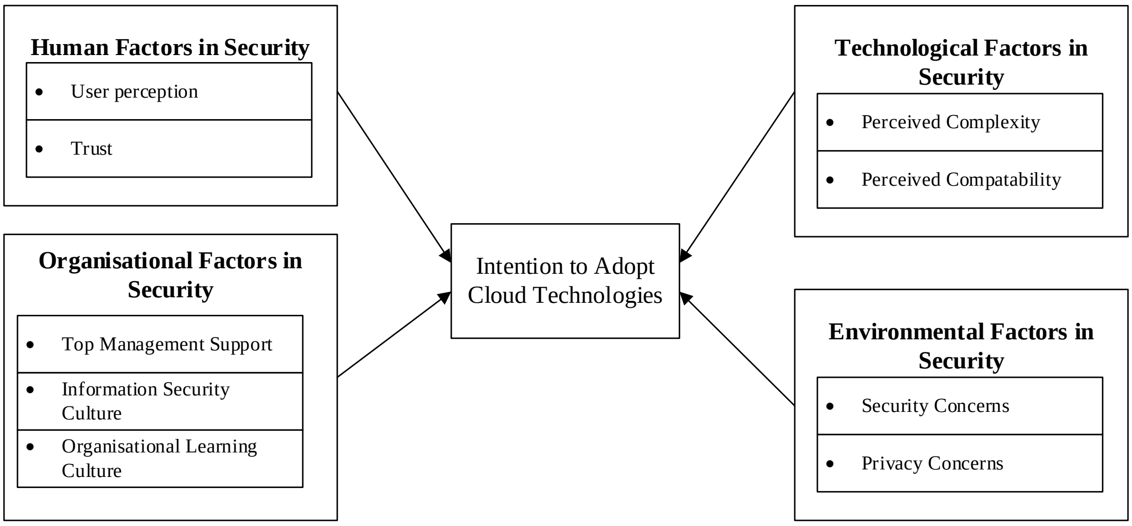

Figure 1. Sec-HOTE-Fit Framework

Research Questions

This research attempts to provide answers for the following research questions:

1. How do human, technology, organisation and environmental factors in relation to security encourage/discourage organisations' Cloud computing adoption?

2. How does information security shape organisational decision to adopt Cloud computing?

3. What recommendations on security management aspects could be introduced for organisations adopting Cloud computing?

Research Hypotheses

This section presents the research hypotheses and a framework that is structured according to TOE and HOT-fit frameworks. The dependent variable for this study is based on the adoption of Cloud computing.

Human Factors

The importance of human, organisational and environmental factors in the adoption of new technologies has been supported in the information systems domain. The user perception refers to individuals understanding of new technology. Both user's understanding of the potential benefits of the proposed technology and their understanding on how the new technology would be free of effort will have impact on new technology adoption (Davis 1989). Cloud computing is perceived as a platform to support business growth. The usefulness aspect may impact the organisations and the way their business is conducted. Willcocks (1994) explains that a deeper understanding of user perceptions and opinions about cloud computing are necessary prior to IT implementation, which can be done through the alignment of human, organisation and technology factors. Alharbi et al. (2016) and Lian et al. (2014) have included the human factors in their studies to understand the importance of user perception in cloud computing adoption. They found that human resources are a crucial consideration to take into account. In fact, the user perception of cloud computing technologies helps to increase the chance of adopting new technologies, however, trust is one of the important aspects in new technology adoption as cloud computing platform is meant for accessing virtualised resources, which involves off-site data storage, accessing applications and sharing of resources online (Motiwalla and Thompson 2012). The lack of trust can impede the new technology adoption (Balasooriya et al. 2017). Although, the technology aspect can address the trust issue to some extent, it is important to explore the relationship between trust and the user's perception of risk in using Cloud services. Considering the influence of perceived use and trust in cloud computing adoption, we propose the following hypotheses:

H1: The user perception will significantly impact the organisation's intention to adopt Cloud computing.
H2: Users' trust on Cloud computing technologies will significantly impact the organisation's intention to adopt Cloud computing.

Organisational Factors

Top management support is considered to be critical in the new technology adoption. Top management support includes the level of involvement, support and commitment by the senior management in adopting the Cloud computing technology (Alshamaila and Papagiannidis 2013). While there are many benefits of cloud computing, several literatures highlight the drawbacks associated with it. For example, when an organisation chooses to utilise a cloud computing platform to store its applications on a host server, this may lead to conflict of interest if the host organisation develops a similar application. With Cloud based technologies, quite often data is stored outside of the company which may raise the concern for data security and vulnerability (Motiwalla and Thompson 2012). To benefit from Cloud computing adoption, it is critical to have the support of the senior management in the organisation.

Previous studies elaborate the role of the top management support in promoting security culture and enforcing security policies (Priyadarshinee et al. 2017). In fact, their active participation may lead to development and enforcement of security policies. While Denworth (2015), Ray (2016) and Singh et al. (2015) have stated that security breaches and privacy concerns are the inhibitors in Cloud computing adoption, developing an inclusive culture where users are given the opportunity to raise their concerns on Cloud computing security and propose ideas to minimise the impact can help formulate policies that would have wider acceptance. Van Niekerk and Von Solms (2010) also explain that information security culture minimises the security risks and at the same time, promotes employee participation in enforcing security policies.

The organisation's culture is made up of beliefs, assumptions and values that are accepted by the employees (Balasooirya et al. 2016), whereas organisation learning culture refers to the orientation of an organisation in relation to their learning characteristics while adopting new technologies (Dhillon 1997). As the Cloud computing technology exposes organisations to security risks, it is important for organisations to identify the potential risks and develop a mechanism to address security issues. To successfully benefit from the Cloud adoption, organisations may need to support Cloud management team to research on the security risks associated with Cloud computing technologies (Fichman and Kemerer 1997). Based on the above arguments, we propose the following hypotheses:

H3: Top management support for information system security positively affect the adoption of Cloud computing.
H4: Information security culture within an organisation positively affects the adoption of Cloud computing.
H5: Strong organisational learning culture positively affects the adoption of Cloud computing.

Technological Factors

Previous studies conducted by Alshamaila and Papagiannidis (2013) and Alharbi et al. (2016) on Cloud computing adoption considered five perceptual characteristics including relative advantage, uncertainty, compatibility, complexity and triability as technology factors in security. The majority of these studies are based on the diffusion of innovation theory. Out of these five characteristics, perceived complexity and perceived compatibility standout. Perceived complexity refers to users' perception of new technologies as relatively difficult to understand and use (Rogers 2003). The complexity of new technologies determine the adoption rate. Rogers (2003) points out that organisations tend to ignore the new innovation if it is considered more challenging to use. Sahin (2006) explains that the user-friendliness of the new technologies is positively related to the acceptance rate. Hence, understanding the relative benefits of Cloud computing technology increases the chance of adopting it (Alharbi et al. 2016).

The perceived compatibility refers to users' awareness of new technologies as consistent with their values and needs (Rogers 2003). Compatibility is considered an important technological factor as the use of Cloud computing platform involves accessing an external system hosted by the other organisations. For this reason, there is an interest among Cloud service providers to increase compatibility with various technologies (Kamal 2006). Tornatzky and Fleischer (1990) also point out that compatibility is the important driver in adopting new technologies. Based on this, it can be argued that perceived complexity has a negative relationship with Cloud computing adoption whereas perceived compatibility positively affects Cloud computing adoption rate. Hence, we present the following hypotheses:

H6: Perceived complexity in ensuring the security of Cloud negatively affects the adoption of Cloud computing.
H7: Perceived compatibility of technology with security requirements of Cloud computing positively affects the adoption of Cloud computing.

Environmental Factors

Environmental context refers to the external factors in which an organisation conducts its business (Balasooriya et al. 2017). The core idea behind Cloud computing is to allow organisations to access and utilise external resources (Motiwalla and Thompson 2012). The use of cloud computing services involves moving data across public networks on which organisations have little control over protecting it. Moreover, the lack of appropriate mechanism to protect the data while it is being transported across public networks and lack of necessary protocols to maintain customer privacy can raise data security and privacy concerns. In fact, security and privacy concerns are among the top reasons for not adopting cloud computing (Priyadarshinee et al. 2017). Motiwalla and Thompson (2012) explain that organisations have limited physical control over who accesses their data and how it is protected when the organisation's data is stored at Cloud service provider's location. Although there are traditional data protection regulations, these were developed on the basis of their use and the technologies available at that time. The new technologies pose new security challenges as these are not familiar and also not covered by the older data protection regulations. Ray (2016) and Singh et al (2015) also found that organisation's dependence to Cloud service providers come with security and privacy related risks. Therefore, we hypothesise the following:

H8: Security concerns negatively affect the adoption of Cloud computing.
H9: Privacy concerns negatively affect the adoption of Cloud computing.

Research Design

The aim of this research is to assess the security determinants in the adoption of Cloud computing by using a research framework developed on the basis of TOE and HOT-fit frameworks. Considering the nature of this study, a two-step mixed method is adopted as it helps researchers to offer solid inferences and provide divergent views (Venkatesh et al. 2013). In the initial step, a quantitative study 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 survey questionnaire are IT professionals of public listed organisations (PLO) in Australia, who are knowledgeable about their organisation's security and technology adoption processes. The PLOs are chosen for this study as they voluntarily comply with government regulations and are required by law to publish complete information about their organisations. Both IBM SPSS and AMOS 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 (Hair et al. 2010).

Conclusion

While several studies quoted security and privacy concerns as barriers in adopting Cloud computing, there is limited evidence to provide an in-depth understanding of the influence of security and privacy factors in its adoption. Hence, the overarching goal of this study is to assess security determinants in Cloud computing adoption. Findings of this study are expected to have both theoretical and practical implications. The results of this study will contribute to the body of knowledge on security determinants, technology adoption and Cloud computing. The results can be used by the researchers, senior management, IT managers and Cloud computing service providers to develop appropriate strategies for addressing security and privacy concerns and make a sensible decision for Cloud computing adoption.

References

Alharbi, F., Atkins, A., and Stanier, C. 2016. "Understanding the Determinants of Cloud Computing Adoption in Saudi Healthcare Organisations," *Complex Intelligent Systems* (2:1), pp. 155-171.

Al Ismaili, S., Li, M., He, Q., and Shen, J. "Cloud computing services adoption in Australian SMEs: a firm-level investigation," *PACIS 2016 Proceedings*, pp. 1-11.

Alshamaila, Y., and Papagiannidis, S. 2013. "Cloud computing adoption by SMEs in the north east of England," *Journal of Enterprise Information Management* (26:3), pp. 250-275.

Awa, H. O., Ukoha, O., and Emecheta, B. C. 2016. "Using T-O-E theoretical framework to study the adoption of ERP solution," *Cogent Business & Management* (3:1), pp. 1-23.

Balasooriya, P., Wibowo, S., and Wells, M. 2016. "Green Cloud Computing and Economics of the Cloud: Moving Towards Sustainable Future," *GSTF Journal on Computing* (5:1), pp. 15-20.

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.

Davis, F. 1989. "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology," *MIS Quarterly* (13:1), pp. 319-340.

Denworth, J. 2015. "Adoption of Cloud Computing in the Enterprise: The Progress in 2015," http://betanews.com/2015/12/29/adoption-of-cloud-computing-in-the-enterprise-the-progress-in-2015.

Dhillon, A. S. 1997. "An Interactive System for Learning Rotational Dynamics," *Journal of Computer Assisted Learning* (13), pp. 59-67.

Fichman, R. G., and Kemerer, C. F. 1997. "The Assimilation of Software Process Innovations: An Organizational Learning Perspective," *Management Science* (43:10), pp. 1345-1363.

Grandhi, S., and Wibowo, S. 2015. "Performance Evaluation of Cloud Computing Providers using Fuzzy Multiattribute Group Decision Making Model," in *Proceedings of the 12th International Conference on Fuzzy Systems and Knowledge Discovery*, Zhangjiajie, China.

Habjan, K. B., and Pucihar, A. 2017. "The Importance of Business Model Factors for Cloud Computing Adoption: Roe of Previous Experiences," *Organizacija* (50:3), pp. 255-272.

Hair, J. F., Black, W. C., Babin, B. J., and Anderson, R. E. 2010. *Multivariate Data Analysis*, NJ: Pearson Education.

Hashemi, S. 2013. "Cloud Computing Technology: Security and Trust Challenges," *International Journal of Security, Privacy and Trust Management* (2:5), pp. 1-7.

Kamal, M. 2006. "IT Innovation Adoption in the Government Sector: Identifying the Critical Success Factors," *Journal of Enterprise Information Management* (19:2), pp. 192-222.

KPMG Research. 2016. "Modelling the Economic Impact of Cloud Computing," pp. 1-52, https://www.kpmg.com/AU/en/IssuesAndInsights/ArticlesPublications/Documents/modelling-economic-impact-cloud-computing.pdf.

Lian, J., Yen, D. C., and Wang, Y. 2014. "An Exploratory Study to Understand the Critical Factors Affecting the Decision to Adopt Cloud Computing in Taiwan Hospital," *International Journal of Information Management* (34:1), pp. 28-36.

Mell, P., and Grance, T. 2011. "The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology," *NIST Special Publication*, pp. 800-145.

Motiwalla, L. F., and Thompson, J. 2012. *Enterprise Systems for Management*, Upper Saddle River, NJ: Pearson Education.

Oliveira, T., Thomas, M., and Espadanal, M. 2014. "Assessing the Determinants of Cloud Computing Adoption: An Analysis of the Manufacturing and Services Sectors," *Information & Management* (51:1), pp. 497-510.

Priyadarshinee, P., Raut, R. D., Jha, M. K., and Kamble, S. S. 2017, "A Cloud Computing Adoption in Indian SMEs: Scale Development and Validation Approach," *Journal of High Technology Management* (28:1), pp. 221-245.

Ray, D. 2016. "Cloud Adoption Decisions: Benefitting from an Integrated Perspective," *The Electronic Journal of Information Systems Evaluation* (19:1), pp. 3-21.

Rogers, E. 2003. *Diffusion of Innovations*, NY: Free Press.

Saedi, A. 2016. "Cloud Computing Adoption Framework: Innovation Translation Approach," in *Proceedings* of the *3rd International Conference On Computer And Information Sciences*, pp. 153-157.

Sahin, I. 2006. "Detailed Review Of Rogers' Diffusion of Innovations Theory and Educational Technology-Related Studies based on Rogers' Theory," *The Turkish Online Journal of Educational Technology* (5:2), pp. 14-23.

Salleh, K. A., and Janczewski, L. 2016. "Adoption of Big Data Solutions: A study on its security determinants using Sec-TOE Framework," in *Proceedings of the CONF-IRM 2016*, pp. 1-12.

Senarathna, I., Wilkin, C., Warren, M., Yeoh, W., and Salzman, S. 2018. "Factors That Influence Adoption of Cloud Comptuing: An Empirical Study of Australian SMEs," *Australasian Journal of Information Systems* (22), pp. 1-30.

Shayan, J., Azarnik, A., Chuprat, S., Karamizadeh, S., and Alizadeh, M. 2014. "Identifying Benefits and Risks Associated With Utilizing Cloud Computing," *International Journal of Computer & Software Engineering* (3:3), pp. 1-6.

Singh, I., Mishra, K.N., Alberti, A., Singh, D., and Jara, A. 2015. "A Novel Privacy and Security Framework for the Cloud Network Services," in *Proceedings* of the *9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, pp. 301-305.

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

Van Niekerk, J., and Von Solms, R. 2010. "Information Security Culture: A Management Perspective," *Computers & Security* (29:1), pp. 476-486.

Venkatesh, V., Brown, S. A., and Bala, H. 2013. "Bridging the Qualitative-Quantitative Divide: Guidelines for Conducting Mixed Methods Research in Information Systems," *MIS Quarterly* (37:1), pp. 21-54.

Wibowo, S., and Grandhi, S. 2019. "Performance Evaluation of Mobile Cloud Services: A Fuzzy Multicriteria Analysis Approach," in *Proceedings of the 14th IEEE Conference on Industrial Electronics and Applications*, Xi'an, China.

Willcocks, L. 1994. "Managing Technology Evaluation - Techniques and Processes," in *Strategic Information Management: Challenges and Strategies in Managing Information Systems*, R.D. Galliers and B.S.H. Baker (eds.), Oxford, pp. 365-381.

Yusof, M. M., and Arifin, A. 2016. "Towards an Evaluation Framework for Laboratory Information Systems," *Journal of Infection and Public Health* (9:6), pp. 766-773.

Yusof, M. M., Papazafeiropoulou, A., Paul, R. J., and Stergioulas, L. K. 2008. "Investigating Evaluation Frameworks for Health Information Systems," *International Journal of Medical Informatics* (77:6), pp. 377-385.