


# Towards an Understanding of Cloud Computing Adoption in SMEs: The Role of Security and Privacy Factors


Ruwan Nagahawatta, RMIT University, Australia\*

 <https://orcid.org/0000-0002-5358-9184>

Matthew Warren, RMIT University, Australia

Scott Salzman, Deakin University, Australia

Sachithra Lokuge, University of Southern Queensland, Australia

 <https://orcid.org/0000-0003-4558-687X>

## ABSTRACT

The advent of digital technologies such as cloud computing has provided enormous opportunities for small and medium-sized enterprises (SMEs) to digitalise their businesses. However, with increasing cloud computing adoption, the security and privacy threats to the SMEs are on the rise. By conducting an extensive review of literature, this paper examines and identifies the security factors that influence cloud computing adoption specifically by SMEs. The literature review focused on papers published in ten years related to the security requirements and associated cloud computing adoption factors by SMEs. The framework focused on understanding socio-technical factors that influence the intent to adopt cloud computing by SMEs. The findings attest to the impacts of key security and privacy-related factors (including cloud security standard, data privacy concerns, data security concerns, skilled personnel, technology readiness, perceived cloud security benefits, legal compliance and trust in cloud service providers) on SMEs' intent to adopt cloud computing.

## KEYWORDS

Cloud Computing, Small and Medium-Sized Enterprises, Socio-Technical Security and Privacy

## 1. INTRODUCTION

Cloud computing is considered a cost-effective, on-demand system that provides access to a shared pool of configurable computing resources. Nowadays, cloud-enabled solutions are widely used in various areas such as businesses, governmental offices, medical, education, and entertainment industry (Bhuiyan et al., 2019). Adoption of cloud services provides various benefits to the adopting organizations, such as resource efficiency (Khayer et al., 2020; Marston et al., 2011; Skafi et al., 2020), cost efficiency (Carroll et al., 2011) and productivity gains for all organizations (Skafi et al.,

DOI: 10.4018/IJCWT.343315

\*Corresponding Author

This article published as an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

2020). Cloud service providers (CSPs) are key in delivering computing services and can achieve computing-related tasks effectively and economically (Asiaei & Rahim, 2019). Cloud computing is more applicable for small and medium-sized enterprises (SMEs). They could take advantage of cloud computing services, which will enrich technology-enabled business and significantly reduce cost impacts on their business (Khayer et al., 2020). Businesses can derive several advantages from cloud computing (Asiaei & Rahim, 2019, Gupta et al., 2013). However, SME organizations are slow in accepting cloud services due to security and associated privacy concerns (Arafat, 2018). While many SMEs are moving into the digital marketplace, there is a golden opportunity for SMEs to reduce costs and improve information technology (IT) efficiency if they were to adopt cloud computing. Despite these advantages, there is still resistance from some SMEs to adopt cloud computing services (Bhuiyan et al., 2019).

While analysing prior literature on cloud computing adoption, it was found that prior research has mainly considered cloud computing security as a technology-related adoption issue (Alharbi, 2017; Khayer et al., 2020). However, in order to understand adoption, it is necessary to consider technological, human, social issues relating to cloud adoption security issues. These security and privacy requirements can be achieved by taking a comprehensive approach to adopting cloud computing from the organizational perspective. Prior researchers have emphasised security issues as being significant obstacles to adopt cloud computing. Further, some scholars have suggested security issues are key determinant to cloud computing adoption by organizations (Ayong & Naidoo, 2019; Khayer et al., 2020; Nagahawatta et al., 2021). Even though security is the most critical factor to consider when deciding the adoption of SMEs' cloud computing (Nagahawatta, 2022; Senarathna et al., 2018), studies have not identified all security-related factors together or provided an in-depth analysis of cloud computing adoption among SMEs.

Besides, the cloud computing landscape has changed significantly over the past decade. Not only are more providers and service offerings crowding the space, but cloud infrastructure that traditionally was limited to single-vendor data centres is also evolving. (Suo et al., 2018). Further, the virtual machine, which has been used in cloud computing for years, has become outdated as the container in cloud computing is increasingly becoming popular with the introduction of virtualization at the operating system level. (Liu & Zhao, 2014). Although cloud container provides many benefits, they also have process-level isolation, which may sometimes create a less secure environment (Suo et al., 2018). Therefore, it is essential to study security challenges in a new technological context. This study aims to investigate factors related to security that influence the intention to adopt cloud computing in SMEs. The research question being explored are:

What are the factors related to security and privacy that influence the intention to adopt cloud computing by SME's?

This study will contribute to the body of knowledge on security determinants to adopt cloud computing. Further, this research may provide policymakers with insights into adopting next-generation cloud computing effectively and enhancing cloud computing adoption among SMEs.

## **2. RESEARCH BACKGROUND**

Cloud computing security and privacy is a complicated issue due to the multi-tenancy nature of virtual resources (Suo et al., 2018). Cloud users can perceive that security issues are reduced in cloud computing due to shared responsibility with a cloud service provider which is expected to be efficient in managing such issues (Alsafi & Fan, 2020). Among these security and privacy factors, lack of transparency, lack of trustworthiness and lower user control cause most issues. Suo et al., (2018) conducted a survey that found data privacy is the top concern when using cloud services. Bhuiyan et al., (2019) found 50% of businesses report privacy as their greatest concern when making decisions. Alsafi & Fan, (2020) report that privacy is a primary determinant for developing cloud infrastructure. Palos-Sánchez (2017) argues that privacy concerns need to be evaluated when adopting location-based

services. Suo et al., (2018) report that lack of control among users on cloud-based services gives rise to privacy being the primary concern. Tancock, et al., (2013) suggest security and privacy concerns are the factors most likely to discourage adoption of cloud computing services. Trusted relationships between service providers and users can be developed by considering new and additional elements at the time of interaction (Alsafi & Fan, 2020). Substantial risk of data theft, damage loss, and misuse can occur when data is being transferred to a third party. This risk cannot be mitigated completely even if policies are incorporated (Nagahawatta et al., 2019, Suo et al., 2018).

According to Heidt et al., (2019), SMEs are more risk adverse than large organizations. Further, SMEs perceive security and privacy features of the cloud to be more complicated and more difficult to identify compared to large organizations. In order to understand these complex security-related factors influencing SMEs' decision to adopt cloud computing, a structured literature review was conducted. A structured literature review is considered as the most suitable approach when several research publications on a given area of interest, or several disparate findings exist regarding a particular topic (Snyder, 2019). It ensures that the reviewed documents are towards the focus area's objectivity, providing transparency based on retrieval criteria (Senivongse et al., 2017).

### **3. LITERATURE EVALUATION**

In line with the identified research gaps, it is essential to understand how research has progressed regarding the phenomenon. Hence, a structured literature review was conducted by framing specific research questions followed by the articles' selection process within the domain using a quality assessment process (Senivongse et al., 2017). A structured literature review is the most suitable approach when several research publications on a given area of interest or several disparate findings (Snyder, 2019). It ensures that the reviewed documents are towards the focus area's objectivity, providing transparency based on retrieval criteria (Nagahawatta et al., 2020; Senivongse et al., 2017).

#### **3.1 Paper Selection Criteria**

Structured Literature Review. In the first process of the evaluation, 506 records were identified through searching the databases related to the adoption of cloud computing in general, which included published articles within ten years. After gathering the required articles, the SME related articles were selected. Also, the following articles were excluded from the selection: research-in progress articles, articles with a focus on individuals, articles that were not written in English, periodical articles published by news websites, trade journals, and magazines. This exclusion filtered unrelated articles and enabled the researcher to maintain the sample effectively (Snyder, 2019). These articles were carefully read and examined, and based on the examination, 398 articles were removed as their context was not discussed cloud security related factors. Furthermore, 87 articles were also excluded as they were conceptual studies, high technical focusing on algorithm development only, and focused on individual level papers. Ultimately, 21 articles were used to extract data for this study.

#### **3.2 Analysis of Cloud Security and Privacy-Related Concerns in SMEs**

The research was reviewed based upon the last ten years' literature related to cloud computing adoption among SMEs in different geographical backgrounds. They found that cloud security and privacy-related issues were the main concern for adopting cloud computing. Several researchers used the literature review to understand different factors connecting security and privacy issues in cloud computing. Analysis of cloud security and privacy-related issues in cloud computing related to SMEs is shown in Table 1. The findings from the reviewed articles indicate that most of the studies used survey methods to collect data.

As for the finding, most of the studies were conducted based on the developed countries (e.g., Ali & Soar, 2014; Dekker & Liveri, 2015; Marston et al., 2011), whereas some of them were based on developing countries (e.g., Amron et al., 2017; Bhuiyan et al., 2019; Wilson et al., 2015). When

Table 1. Analysis of Cloud Security and Privacy Related Concerns in the Use of Cloud Computing in SMEs

Security and privacy topics	Reference	Study context	Methods
Security compliances.	Marston et al., 2011	SMEs in the United States of America.	Survey
Security, privacy, and trust.	Sultan, 2011	SMEs in Britain.	Case study
Compliance, data privacy and cloud security.	Hinde, 2012	SMEs in South Africa.	Survey
Data security, human security, and privacy.	Gonzalez et al., 2012	SMEs in Brazil.	Survey
Compliance and regulatory and privacy.	Aleem, 2013	SMEs in Britain.	Survey
Cloud security, reliability, and privacy.	Gupta et al., 2013	SMEs in Asia-Pacific.	Survey
Data security, data privacy, and security compliance.	Carcary, 2014	SMEs in Ireland.	Survey
Cloud security and trust.	Yeboah-Boateng, 2014	SMEs in Ghana.	Survey
Cloud security and data protection.	Tehrani & Shirazi, 2014	SMEs in Canada.	Survey
Trust of the cloud provider and government regulations.	Jelonek et al., 2014	SMEs in Poland.	Survey
Cloud security, privacy, and trust.	Ali & Soar, 2014	SMEs in Australia.	Survey
Cloud security, security standards, and organizational readiness.	Oliveira et al., 2014	SMEs in Portugal.	Survey
Data security and cloud security benefits.	Dekker & Liveri, 2015	SMEs in the European Union.	Case study
Data privacy and security.	Wilson et al., 2015	SMEs in India.	Survey
Privacy, trust, and industry standards.	Doherty, 2015	SMEs in Ireland.	Survey
Human security, compliance, and top management support.	Gupta & Misra, 2016	SMEs in India.	Survey
Legal issues, service level agreement (SLA), data protection, and transparency.	Palos-Sánchez, 2017	SMEs in the European Union.	Literature review
Security, privacy, and human awareness.	Amron et al., 2017	SMEs in Malaysia.	Survey
Cloud security and privacy.	Senarathna et al., 2018	SMEs in Australia.	Survey
Security, privacy, trust, human security, and security standards.	Ayong & Naidoo, 2019	SMEs in South Africa.	Survey
Security, privacy, and organizational security.	Bhuiyan et al., 2019	SMEs in India.	Survey

comparing the contexts of developed and developing countries, it was found that in relation to the literature on developing countries, compliance and regulatory, security standards and government regulation issues were not considerably discussed.

### 3.3 Classification of Security and Privacy Related Factors

According to the literature review analysis, the most discussed security and privacy factors were classified into eight key security and privacy-related factors concerning the adoption of

**Table 2. Security and Privacy Related Factors in the Use of Cloud Computing**

Key Factors	Definition	Topics	Number of papers
Skilled personnel	The degree to which an organization possesses technology expertise in information security and behaviours of the IT personnel.	Awareness, professionalism, IT experts and top management support.	6 (9.7%)
Technology readiness	The degree to which an organization has the necessary technology infrastructure resources and security procedures to adopt cloud computing.	Technical competence, network security, infrastructure, Security policy.	8 (12.9%)
Perceived cloud security benefits	Expected benefits of cloud protection include access control and security awareness efforts, backup, and disaster recovery plans.	Cloud security auditing, physical security, data backup and data encryption.	4 (6.5%)
Data security	The degree to which cloud computing provides adequate security administration for the confidentiality, integrity and availability of data and applications in the cloud.	Vendor lock-in, data protection, confidentiality, data storage, data transmission and availability.	16 (25.8%)
Data privacy	The degree to which an organization's requirements of privacy concerns related to sensitive data or identity data in the cloud. (e.g., data location, governance of personal data, transparency, and data sharing control).	Data location, sensitive data protection, transparency, data sharing control, lack of data privacy and data oversight.	11 (17.7%)
Legal compliance	The degree to which an organization adheres to security and related privacy laws, regulations, acts, and compliance for legal requirements.	Forensic, legal compliance, SLA, accountability, and government regulation.	6 (9.7%)
Cloud security standards	The degree to CSPs and cloud service customers (CSCs) of an organization adhere to necessary guidelines and standards of cloud security.	ISO/IEC 27002 for cloud services, ISO 27001:2013 and COBIT5 and NIST security standard.	4 (6.5%)
Trust in CSPs	The degree to which an organization perceives their CSPs to be reliable, honest, and faithful concerning fulfilling the cloud security requirements.	Cloud environments openness, vendor reputation, vendor trustworthiness,	7 (11.3%)

cloud computing in SMEs, as shown in Table 2. The majority of the 25.8% of findings discussed data security issues, and 17.7% studies related to privacy. Technology readiness factors are discussed in 12.9% of studies, and 11.3% of findings discussed trust in CSPs factors. However, only 6.5% of the studies discussed the perceived benefits of cloud security. Security and privacy policies are an explicit statement of what is not and what is allowed to safeguard a system's security (Ayong & Naidoo, 2019). IT governance and policies are essential for safeguarding cloud security practices in an institution (Jelonek et al., 2014). Human security refers to appropriate and trustworthy information, security practices and behaviours by the end-users. The literature on information security has shown the humans are the weakest link in the fight against security breaches and can pose a challenge to cloud security (Gupta & Misra, 2016; Nagahawatta & Warren, 2020). Therefore, this research is vital for evaluating security and privacy determinants in the use of cloud computing. As a result, this research seeks to study cloud computing challenges and highlight the relationship between cloud security and privacy concerns among SMEs. This literature review has shown a knowledge gap in the relationship between security and privacy-related factors and the use of cloud computing from a social and technical perspective. Therefore, it is essential to study security and privacy concerns in the cloud context.

#### 4. THEORETICAL BACKGROUND

As per the structured literature review, various theories, frameworks, and models that scholars have proposed in the process of technology adoption were identified. Most adopted theories in this area are at the individual level rather than at the organizational level. The technology, organization, and environment framework (TOE) (Tornatzky & Fleischer, 1990), the diffusion of innovations (DOI) (Rogers, 1995), the institutional theory (DiMaggio & Powell, 1983) and human, organization and technology-fit (HOT-fit) framework (Yusof et al., 2008) are some of the theories that discuss computing adoption at organizational level. An intensive literature review on technology adoption in organizations indicated that most technology adoption studies are based on several theories for better understanding the technology adoption (Alsafi & Fan, 2020). Given the characteristics of unique technologies and the complex environment in which an organization functions, the integration of many theories into a unified model gives a greater theoretical basis for understanding technology adoption in organizations (Amron et al., 2017).

Institutional theory can help describe why organizations are hesitant to adopt technology practices from the standpoint of technology adoption. Institutional theory is well established in extant literature and is valuable for understanding the acceptance of specific technical advancements (Alkalbani et al., 2017; Cavusoglu et al., 2015). Furthermore, institutional theory, specifically in the technology sector, gives a thorough knowledge regarding the organizational, environmental, and societal pressures at the macro-level of factor analysis (Almudawi et al., 2019). When the focus is on technology adoption as a social phenomenon, this theory is useful (Almudawi et al., 2019; Cavusoglu et al., 2015). When mimetic, coercive, and normative institutional pressures exist, isomorphism can arise at the organizational level (Cavusoglu et al., 2015). It has been suggested that these pressures affect the integration of innovations with a firm's existing system (Alkalbani et al., 2017). Therefore, institutional theory is appropriate for explaining the influence of institutional pressures on cloud computing adoption at the macro-level. Given it depends on these three institutional forces, institutional theory has been emphasized as relevant in the context of SMEs. Therefore, institutional theory can be used for cloud computing adoption as it considers the socio-technological context. Further, the socio-technological can optimize the security and privacy factors that impact the decision to adopt cloud computing.

According to the TOE framework, the decision to adopt cloud computing at the organizational level is influenced by technological, organizational, and environmental aspects (Senarathna et al., 2018). The literature noted that most authors combined the TOE framework with other theories to better understand several factors, including security and privacy related issues about cloud adoption (Amron et al., 2017; Asiaei & Rahim, 2019; Senarathna et al., 2018). However, TOE does not consider the human aspects of the cloud computing adoption context; therefore, there is a need to use another theory that considers the human aspects.

The HOT-fit, defines three characteristics: technological, human, and organizational, which have been integrated to assess technology (Yusof et al., 2008). In the acceptance of any new technology breakthrough, human aspects are also crucial. For example, when considering whether to use cloud computing in a healthcare setting, the human component should be considered (Alharbi et al., 2016; Lian, 2017). The HOT fit has significant overlap with the TOE framework, except that it does not consider the environmental context. Hence, the HOT fit model has deemed a supplement model for the TOE dimensional framework to study SMEs' cloud computing adoption. In fact, various studies point out the importance of human factors in adopting new technologies in SMEs (Amron et al., 2017). For example, some authors combined the TOE framework with other theories to better understand several factors, including security related issues about cloud adoption (Senarathna et al., 2018; Amron et al., 2017; Asiaei & Rahim, 2019).

## 5. DERIVING THE CONCEPTUAL MODEL

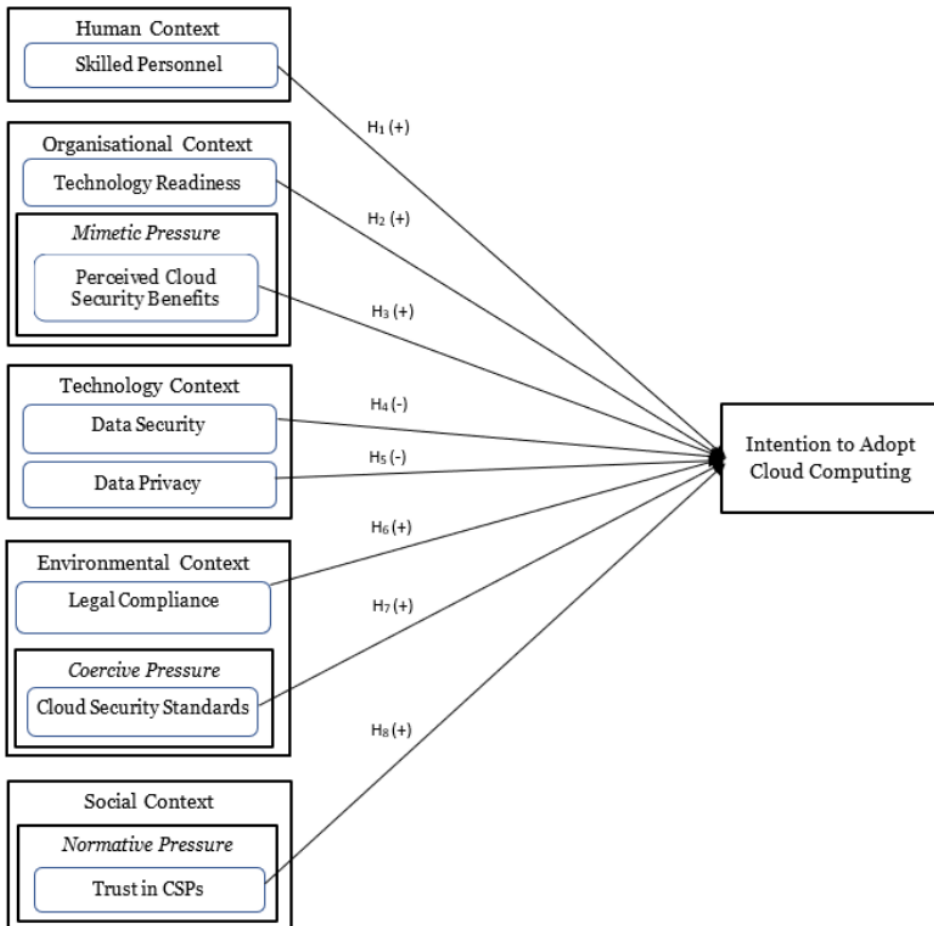
By utilizing the fundamentals of theoretical models such as TOE, HOT fit framework and institutional theory, this research attempted to understand security and privacy-related factors that influence intention to adopt cloud computing in Australian SMEs. The conceptual model developed in this study integrated technological, organizational, environmental, human, and social contexts. Figure 1 depicts the conceptual research model proposed in this research. A review of the literature identified eight key, independent factors affecting the intention of SMEs to adopt cloud computing: skilled personnel, technology readiness, perceived security benefits, data security concerns, data privacy concerns, legal compliance, cloud security standards, and trust in CSPs.

This study examines the research questions based on a group of hypothesised connections designed from the research model. As indicated in the literature, the proposed connections were analysed as follows when any organization process is moved into the cloud, security and privacy-related factors assume an essential part of the decision making.

### 5.1 Human Context

Skilled personnel refer to the degree to which an organization possesses technology expertise in information security and behaviours of the IT personnel. SMEs are unlikely to adopt sophisticated

Figure 1. The proposed Conceptual Model



technologies when they lack IT and security knowledge (Lian et al. 2014). Due to the obstacles in developing necessary skills and knowledge, SMEs are tempted to postpone adopting advanced technologies like cloud computing (Gupta et al. 2013). Accordingly, this study postulates the following hypothesis.

H1: Skilled personnel has a positive influence on the intent to adopt cloud computing in SMEs.

## **5.2 Organizational Context**

The organizational context includes technology readiness of the organization and perceived benefits of cloud computing. Perceived cloud security benefits refer to cloud security's anticipated advantages, including access control and a security awareness effort, backup, and disaster recovery plan. While organizations derive considerable benefits from using cloud services, taking advantage of these benefits depends on their nature and size (Dekker & Liveri 2015; Oliveira et al., 2014). Technology readiness refers to the degree to which an organization possess necessary technology infrastructure resources and security procedures to adopt cloud computing. Technology readiness is one of the critical factors that influence cloud computing adoption in SMEs (Oliveira et al., 2014). In an organization, technological readiness is related to organizations' accessibility to IT resources to adopt technologies. Technology readiness has a significant impact on leadership when deciding on adopting an innovation. Accordingly, this study postulates the following hypotheses:

H2: Technology readiness has a positive influence on the intent to adopt cloud computing in SMEs.

H3: Perceived cloud security benefits have a positive influence on the intent to adopt cloud computing in SMEs.

## **5.3 Technological Context**

Data security concerns refer to the degree to which cloud computing provide adequate security administration for the confidentiality, integrity and availability of data and applications in the cloud. Data security is a crucial concern for cloud customers. According to Bhuiyan et al., (2019), improved data security standards play a critical role in institutions in the cloud computing adoption decision process (Doherty et al. 2015). Data privacy concerns refer to the degree to which organization requirements of protect privacy related to sensitive data or identity data in the cloud. Privacy is one of the core issues in cloud computing adoption, including the need to policy components during integration, protect identity information and transaction histories (Bhuiyan et al., 2019). Privacy issues corresponding with SMEs lack transparency, poor user control and trustworthiness (Senarathna et al. 2018). Accordingly, this study postulates the following hypothesis:

H4: Data security concerns have a negative influence on the intent to adopt cloud computing in SMEs.

H5: Data privacy concerns have a negative influence on the intent to adopt cloud computing in SMEs.

## **5.4 Environmental Context**

Environmental context refers to the external factors in which an organization conducts its business. Legal compliances refer to the degree to which an organization adheres to security and related privacy laws, regulations, acts, and compliance with legal requirements. Current regulations and laws impact organizational management's commitment to security compliance (Spanaki et al., 2019). Generally, organizations are accountable for ensuring that it complies with applicable laws and regulations for information security. Cloud security standards refer to the degree to which CSPs and cloud service customers (CSCs) of an organization adhere to necessary guidelines and standards of cloud security and privacy (Tehrani and Shirazi 2014). Coercive pressures force organizations to adopt specific



institutionalized rules. Practices and standards in the management of the organization for information security (Alkawsii et al. 2015) derive from cloud security standards. Cloud computing is a fast-moving technology, and the threat environment is developing substantially (Spanaki et al., 2019). Accordingly, this study postulates the following hypotheses:

H6: Legal compliance has a positive influence on the intent to adopt cloud computing in SMEs.

H7: Cloud security standards have a positive influence on the intent to adopt cloud computing in SMEs.

### **5.5 Social Context**

Trust in CSPs refers to the degree to which an organization perceives their CSPs to be reliable, honest, and faithful concerning fulfilling the cloud security and privacy requirements. Ayong & Naidoo (2019) emphasized the importance of layers of trust in cloud environments. Normative pressures come from the community's expectation that organizations are compelled to have the confidence of services as responsible customers (Skafi et al., 2020). This postulate that normative pressure (i.e., trust in CSPs) will enable the intention to adopt cloud computing in SMEs; this is shown in the following hypothesis:

H8: Trust in CSPs has a positive influence on adopting cloud computing in SMEs.

## **6. DISCUSSION**

This study provides an overview of the literature review on security and privacy-related factors that influence SMEs' cloud computing adoption in different countries. Through the prior studies, gaps in current security and privacy requirements related to cloud computing adoption in SMEs research have been identified as future work opportunities.

After an in-depth analysis of the existing literature, this study argued that many security and privacy-related factors and elements can influence the decision to adopt cloud computing. Further, these security and privacy factors depend on the countries' technical, human, organizational, social, and cultural environment. Also, studies provide inconclusive results regarding the relationship and interaction between cloud computing adoption and security and privacy factors.

Privacy-related issues corresponding with SMEs are lack of transparency, poor user control, and trustworthiness. Therefore, SMEs need to comply with legal requirements in their country. They need to protect customers' data as technological threats still influence all SMEs' cloud security and privacy aspects. Further studies highlight the importance of investigating the key security and privacy-related factors influencing the adoption of cloud computing in SMEs to achieve a high level of readiness and responsibility. Overall, security and privacy requirements related to cloud computing adoption lacked an overarching framework to guide future research and integrate findings.

The proposed integrated framework can provide an overarching theoretical framework for explaining the organizational security and privacy requirements that influence cloud computing adoption in SMEs. The conceptual model developed for integrating human, organizational, technological, environmental and social into a single framework offers a richer theoretical basis for explaining the organizational security and privacy requirements. This study's findings address the research gap in cloud computing adoption, especially related to security and privacy literature. Further, a unique research model can meet SMEs' complex security and privacy requirements that influence cloud computing adoption.

### **6.1 Practical and Theoretical Implications**

In practical terms, this study addresses the research gap by advancing the understanding of complex security and privacy-related factors influencing the adoption of cloud computing. The research findings provide important implications for technology consultants, cloud service providers, cloud

software vendors, SME owners and regulatory authorities. In particular, SMEs can benefit from understanding how security and privacy requirements affect cloud computing adoption. Additionally, an understanding of how the relationship between organization size and organization type affects cloud computing is crucial to SMEs making the right decision about the adoption of this technology. Additionally, the insights provided by this study could improve the SMEs' understanding of the security and privacy-related concerns of cloud computing, as well as the environment and social pressures. Most importantly, the ultimate beneficiaries would be SMEs as these insights could help to improve the cloud security environment in an SME.

This study examined security and privacy concerns related to cloud computing adoption of SMEs from a theoretical perspective. The main theoretical contribution is developing a unique research model to meet SMEs' complex security and privacy requirements that influence their adoption of cloud computing. Further, Integrating the factors of human, organizational, technological, environmental, and social into a single framework offers a richer theoretical basis for explaining the organizational security and privacy requirements. This study contributes to the value of future research for academics and derive essential implications for practitioners. Besides, this study's findings provide concrete theoretical support for further research in SME privacy and security domains. Further, this study's findings will contribute to the body of knowledge on security and privacy determinants in cloud computing.

## **6.2 Limitations and Future Research**

Since objective of this research was to identify security related factor influencing the cloud computing adoption of SMEs, the authors conducted a literature review to understand the current research landscape. There are several limitations of this study. First, this review focused only on investigating macro level security and privacy related factors. In addition, the sample only considered empirical research and no conceptual or research-in-progress papers were taken for the analysis. Second, specific security and privacy factors were identified and selected based on the literature and their relevance to theories that the study built upon.

The future direction of research can focus on case studies to explore SME security and privacy issues. This research examined macro-level security and privacy concerns related to cloud computing adoption by SMEs; however, future studies can examine security and privacy issues at the micro level. Further, future studies could contribute to what can be done to mitigate security and privacy problems by reducing these concerns and proposing the best approaches to protect SMEs.

## **PROCESS DATES**

Received: 7/4/2021, Revision: 9/12/2023, Accepted: 3/21/2024

## **FUNDING**

No funding was received for this work.

## **CONFLICTS OF INTEREST**

We wish to confirm that there are no known conflicts of interest associated with this publication and there has been no significant financial support for this work that could have influenced its outcome.

## REFERENCES

- Aleem, A., & Ryan Sprott, C. (2012). Let me in the cloud: Analysis of the benefit and risk assessment of cloud platform. *Journal of Financial Crime*, 20(1), 6–24. doi:10.1108/13590791311287337
- Alharbi, F. (2017). Holistic Approach Framework for Cloud Computing Strategic Decision-Making in the Healthcare Sector (HAF-CCS). (Doctoral dissertation, Staffordshire University, UK).
- Ali, O., & Soar, J. (2014). Challenges and issues within cloud computing technology. *Fifth international conference on cloud computing, GRIDs and virtualization*, 55-63.
- AlKalbani, A., Deng, H., Kam, B., & Zhang, X. (2017). Information Security compliance in organizations: An institutional perspective. *Data and Information Management*, 1(2), 104–114. doi:10.1515/dim-2017-0006
- Alkaws, G. A., Mahmood, A. K., & Baashar, Y. M. (2015). Factors influencing the adoption of cloud computing in SME: A systematic review. *2015 International Symposium on Mathematical Sciences and Computing Research (ISMSC)*. 220-225. IEEE. doi:10.1109/ISMSC.2015.7594056
- Almudawi, N., Beloff, N., & White, M. (2019). Cloud Computing in Government Organizations-Towards a New Comprehensive Model. Paper presented at the IEEE Smart World, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation.
- Alsafi, T., & Fan, I.-S. (2020). Cloud Computing Adoption Barriers Faced by Saudi Manufacturing SMEs. *IEEE*, 1–6. doi:10.23919/CISTI49556.2020.9140940
- Amron, M. T., Ibrahim, R., & Chuprat, S. (2017). A review on cloud computing acceptance factors. *Procedia Computer Science*, 124, 639–646. doi:10.1016/j.procs.2017.12.200
- Arafat, M. (2018). Information security management system challenges within a cloud computing environment. *Proceedings of the 2nd International Conference on Future Networks and Distributed Systems*. 60. ACM. doi:10.1145/3231053.3231127
- Asiaei, A., & Rahim, N. Z. A. (2019). A Multifaceted Framework for Adoption of Cloud Computing in Malaysian SMEs. *Journal of Science and Technology Policy Management.*, 10(3), 708–750. doi:10.1108/JSTPM-05-2018-0053
- Ayong, K., & Naidoo, R. (2019). Modelling the adoption of cloud computing to assess South African SMEs: An integrated perspective. *Proceedings of 4th International Conference on the Internet. Cyber Security and Information Systems*, 12, 43-56.
- Bhuiyan, M. Y., Othman, S. H., & Radzi, R. Z. R. M. (2019). An Enhancement of TOE Model by Investigating the Influential Factors of Cloud Adoption Security Objectives. *International Journal of Innovative Computing*, 9(1). Advance online publication. doi:10.11113/ijic.v9n1.192
- Carcary, M., Doherty, E., Conway, G., & McLaughlin, S. (2014). Cloud computing adoption readiness and benefit realisation in Irish SMEs, an exploratory study. *Information Systems Management*, 31(4), 313–327. doi:10.1080/10580530.2014.958028
- Carroll, M., Van Der Merwe, A., & Kotze, P. (2011). *Secure cloud computing: Benefits, risks and controls*. 2011 *Information Security for South Africa*. IEEE.
- Cavusoglu, H., Cavusoglu, H., Son, J. Y., & Benbasat, I. (2015). Institutional pressures in security management: Direct and indirect influences on organizational investment in information security control resources. *Information & Management*, 52(4), 385–400. doi:10.1016/j.im.2014.12.004
- Dekker, M., & Liveri, D. (2015). *Cloud security guide for SMEs*. European Union Agency for Network and Information Security. ENISA.
- DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review*, 48(2), 147–160. doi:10.2307/2095101
- Doherty, E., Carcary, M., & Conway, G. (2015). Migrating to the cloud: Examining the drivers and barriers to adoption of cloud computing by SMEs in Ireland: an exploratory study. *Journal of Small Business and Enterprise Development*, 22(3), 512–527. doi:10.1108/JSBED-05-2013-0069

- Gonzalez, N., Miers, C., Redigolo, F., & Simplicio, M., Carvalho, T., Na'slund, M., and Pourzandi, M. (2012). A quantitative analysis of current security concerns and solutions for cloud computing. *Journal of Cloud Computing: Advances, Systems and Applications*, 1(1), 11.
- Gupta, P., Seetharaman, A., & Raj, J. R. (2013). The usage and adoption of cloud computing by small and medium businesses. *International Journal of Information Management*, 33(5), 861–874. doi:10.1016/j.ijinfomgt.2013.07.001
- Gupta, S., & Misra, S. C. (2016). Compliance, network, security and the people related factors in cloud implementation. *International Journal of Communication Systems*, 29(8), 1395–1419. doi:10.1002/dac.3107
- Heidt, M., Gerlach, J. P., & Buxmann, P. (2019). Investigating the Security Divide between Sme and Large Companies: How Sme Characteristics Influence Organizational It Security Investments. *Information Systems Frontiers*, 21(6), 1285–1305. doi:10.1007/s10796-019-09959-1
- Jelonek, D., Stepniak, C., Turek, T., & Ziora, L. (2014). Identification of Mental Barriers in the Implementation of Cloud Computing in the SMEs in Poland. *IEEE*, 1251–1258.
- Khayer, A., Talukder, M. S., Bao, Y., & Hossain, M. N. (2020). Cloud computing adoption and its impact on SMEs' performance for cloud supported operations: A dual-stage analytical approach. *Technology in Society*, 60, 101225. doi:10.1016/j.techsoc.2019.101225
- Lian, J. W. (2017). Establishing a cloud computing success model for hospitals in Taiwan. *Inquiry*, 54, 0046958016685836. doi:10.1177/0046958016685836 PMID:28112020
- Lian, J. W., Yen, D. C., & Wang, Y. T. (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), 28–36. doi:10.1016/j.ijinfomgt.2013.09.004
- Liu, D., & Zhao, L. (2014). The research and implementation of Cloud computing platform based on docker. *2014 11th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP)*. 475-478, IEEE.
- Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing - the business perspective. *Decision Support Systems*, 51(1), 176–189. doi:10.1016/j.dss.2010.12.006
- Nagahawatta, R., & Warren, M. (2020). Key Security and Privacy Related Factors Influencing the Use of Cloud Computing in SMEs. In *proceedings of the ICIS 2020 SIGSEC: Workshop on Information Security & Privacy*.
- Nagahawatta, R., Warren, M., & Yeoh, W. (2020). A Study of Cybersecurity Issues in Sri Lanka' [IJCW]. *International Journal of Cyber Warfare & Terrorism*, 10(3), 59–72. doi:10.4018/IJCWT.2020070105
- Nagahawatta, R. T. S. (2022). Critical security and privacy related factors influencing the adoption of cloud computing in Australian small and medium-sized enterprises (Doctoral dissertation, RMIT University).
- Nagahawatta, R. T. S., Warren, M., Lokuge, S., & Salzman, S. (2021). Security Concerns Influencing the Adoption of Cloud Computing by SMEs: A Literature Review, in *27th Americas Conference on Information Systems*, Montreal, Canada.
- Nagahawatta, R. T. S., Warren, M., & Yeoh, W. (2019). Ethical Issues Relating to Cyber Security in Australian SMEs, in *8th Conference of the Australasian Institute of Computer Ethics (AiCE 2019)*, Deakin University, Australia
- Oliveira, T., Thomas, M., & Espadanal, M. (2014). Assessing the determinants of cloud computing adoption: An analysis of the manufacturing and services sectors. *Information & Management*, 51(5), 497–510. doi:10.1016/j.im.2014.03.006
- Palos-Sanchez, P. R. (2017). Drivers and Barriers of the Cloud Computing in SMEs: The Position of the European Union. *Harvard Deusto Business Research*, 6(2), 116–132. doi:10.3926/hdb.125
- Rogers, E. M. (1995). Diffusion of Innovations: modifications of a model for telecommunications. Die diffusion von innovationen in der telekommunikation. 25-38): Springer.

- Senarathna, I., Wilkin, C., Warren, M., Yeoh, W., & Salzman, S. (2018). Factors that influence adoption of cloud computing: An empirical study of Australian SMEs. *AJIS. Australasian Journal of Information Systems*, 22, 22. doi:10.3127/ajis.v22i0.1603
- Senivongse, C., Bennet, A., & Mariano, S. (2017). Utilizing a Systematic Literature Review to Develop an Integrated Framework for Information and Knowledge Management Systems. *VINE Journal of Information and Knowledge Management Systems*, 47(1), 250–264. doi:10.1108/VJIKMS-03-2017-0011
- Skafi, M., Yunis, M. M., & Zekri, A. (2020). Factors Influencing SMEs' Adoption of Cloud Computing Services in Lebanon: An Empirical Analysis Using TOE and Contextual Theory. *IEEE Access : Practical Innovations, Open Solutions*, 8, 79169–79181. doi:10.1109/ACCESS.2020.2987331
- Snyder, H. (2019). Literature Review as a Research Methodology: An Overview and Guidelines. *Journal of Business Research*, 104(1), 333–339. doi:10.1016/j.jbusres.2019.07.039
- Spanaki, K., Gürgüç, Z., Mulligan, C., & Lupu, E. (2019). Organizational cloud security and control: A proactive approach. *Information Technology & People*, 32(3), 516–537. doi:10.1108/ITP-04-2017-0131
- Sultan, N. A. (2011). Reaching for the 'cloud': How SMEs can manage. *International Journal of Information Management*, 31(3), 272–278. doi:10.1016/j.ijinfomgt.2010.08.001
- Suo, K., Zhao, Y., Chen, W., & Rao, J. (2018). An analysis and empirical study of container networks. *IEEE INFOCOM 2018-IEEE Conference on Computer Communications*, 189–197, IEEE.
- Tehrani, S. R., & Shirazi, F. (2014). Factors influencing the adoption of cloud computing by small and medium size enterprises. in *International Conference on Human Interface and the Management of Information*. 631–642. Springer.
- Tornatzky, L. G., Fleischer, M., & Chakrabarti, A. K. (1990). *Processes of Technological Innovation*. Lexington Books.
- Wilson, B. M. R., Khazaei, B., & Hirsch, L. (2015). Enablers and barriers of cloud adoption among small and medium enterprises in Tamil Nadu. *2015 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM)*, 140–145, IEEE. doi:10.1109/CCEM.2015.21
- Yusof, M. M., Papazafeiropoulou, A., Paul, R. J., & Stergioulas, L. K. (2008). Investigating Evaluation Frameworks for Health Information Systems. *International Journal of Medical Informatics*, 77(6), 377–385. doi:10.1016/j.ijmedinf.2007.08.004 PMID:17904898