Issues in Information Systems
Volume 22, Issue 1, pp. 262-268, 2021

https://doi.org/10.48009/1_iis_2021_262-268

Research framework of human factors interactions with technical and security factors in cloud computing

Hongjiang Xu, *Butler University, hxu@butler.edu*
Sakthi Mahenthiran, *Butler University, smahenth@butler.edu*

Abstract

There are many advantages to adopt cloud computing, however, some important issues need to be addressed, such as cybersecurity, cost-saving, trust, implementation complexity, and cloud provider's reliability. This study developed a research framework to study the human factors that interact with technical and cybersecurity factors to affect the cloud-computing provider's performance from the user's perspective. Research hypotheses were developed and a survey was conducted to test the hypotheses and validate the research framework.

Keywords: Cybersecurity, Cloud computing, Trust, Providers' performance

Introduction

There are many cloud-computing providers including popular companies like Amazon, Google, and Microsoft that use cloud technology to provide a cloud environment for their customers. Although there are many advantages to adopt cloud computing, some important issues need to be addressed before organizations can trust third parties to deploy their systems (Radwan, Azer, & Abdelbaki, 2017), and store data in cloud computing. According to Radwan and Abdelbaki (Radwan et al., 2017), these issues include cybersecurity and integrity concerns, implementation complexity, and the cloud providers' capacity and reliability to provide uninterrupted services.

Drawing from the organizational change and IT performance literature, and by incorporating human factors such as trust in the supervisor, as well as IT complexity, cybersecurity, and reliability concerns of the users we hope to examine how human factors within a firm interacts with technical and security factors in cloud computing and study these issues in non-listed U.S. companies.

Literature review and hypotheses

Cloud Computing

Cloud computing is defined as applications delivered as services over the Internet, and data centers usually provide the services (Armbrust et al., 2010). There are a few ways to categorize different types of clouds, one way is to divide them into two types of cloud-based on the ownership of the cloud, one is public, and another is private. The public cloud refers to the cloud that is easily accessed by the public, and firms rent the cloud space from the provider and pay for the cloud services on a pay-as-you-go basis. Moreover, the private cloud refers to internal data centers of a business that is not accessible by the public, and all the costs are borne by the firm that is also the provider of the cloud services. Armbrust et al. (Armbrust et al., 2010) note that when businesses are large enough to benefit from the advantages

of cloud computing for reasons of security they tend to use their private clouds. Cloud computing providers make available a platform for users to share virtual machines to perform their daily activities, and this environment requires a level of trust and vigilance (Kaufman, 2009). Additionally, organizations using cloud computing can choose from a pool of software, hardware, and networking infrastructure managed independently within the organization or externally by the cloud computing vendors (Armbrust et al., 2010; Joint, Baker, & Eccles, 2009). Hence, the authors point out that the types of cloud ownership and the different ways to manage the software, hardware, and networking infrastructure can result in a myriad of combinations that add to the complexity of cloud computing.

A key barrier to the widespread adoption of cloud is the lack of trust in cloud providers by potential customers (Ko et al., 2011). In addition, according to Senyo et al. (Senyo, Addae, & Boateng, 2018), the literature tends to skew more towards the technological dimension neglecting the human and business conceptualization of cloud computing. Further, these authors argue that although there is a significant number of studies they have not been underpinned by sound theoretical frameworks. Borgman et al. (Borgman, Bahli, Heier, & Schewski, 2013) used the Technology-Organization-Environment framework to investigate the organizational factors inhibiting or supporting cloud-computing adoption. Their study finds that IT governance processes and organizational structures moderate the success of cloud computing adoption, but the study lacked specifics as to how human factors interact with technical factors to affect outcomes. Hence, we develop a research framework that specifically addresses how the human factors interact with technical and security factors to affect the organizational sustainability of cloud computing.

Cost Savings and Cybersecurity

Cloud computing can help organizations save costs in a few ways: from the scalability of resources to reduce physical hardware setups, to using digital files and documents that are delivered online, and to pay only for what is needed to reduce the upfront costs of various resources (Gupta, Seetharaman, & Raj, 2013). Moreover, cloud computing allows organizations to have immediate access to resources with little or no initial capital investments, which helps bring products and services to the market much faster (Karadsheh, 2012; Marston, Li, Bandyopadhyay, Zhang, & Ghalsasi, 2011). Additionally, the advancements in cloud computing technology have helped to make all kinds of systems more user-friendly. However, these cost savings and market factors have to be balanced with cybersecurity concerns and the costs of developing the technical capability to operate in the cloud.

The large amount of data stored in the cloud, including sensitive and critical information, attract highly skilled hackers who want to steal the information (Srinivasamurthy, Liu, Vasilakos, & Xiong, 2013). Hence, according to Badamas (Badamas, 2012), when organizations adopt cloud computing, one of the important challenges is cybersecurity. This concern is heightened when a business has sensitive information such as intellectual property, trade secrets, and personally identifiable information about their customers that make IT breaches a significant cost to the firms. Thus, cybersecurity, data confidentiality, data integrity, and the potential loss of data all become major issues with cloud computing. Thus, to be successful, organizations must learn to manage their human resources to deal with security and privacy risks associated with cloud computing adoption (Kamara & Lauter, 2010).

One of the major concerns to adopt cloud storage is the confidentiality and integrity of the data (Kamara & Lauter, 2010). According to Bisong & Rahman (Bisong & Rahman, 2011), the security threats are not unique to the cloud computing environment, and they exist in other computing platforms, networks, intranets, and Internet infrastructures because of users' interaction with these technologies. Nevertheless, there are additional challenges given the different platforms of the cloud computing users, and because the data is physically located in the 'cloud' which heightens the security concerns for organizations adopting cloud computing. For example, in cloud computing, data could be stored across wide geographical areas. And when the host of the cloud data is located in another country, where the laws and regulations of the host country are different from where the headquarters is located that can impact

the global cybersecurity concerns (Smith, 2009). Therefore, given fallibility human factors, ensuring cybersecurity in a cloud-computing environment can be technically challenging. According to Srinivasamurthy et al., (Srinivasamurthy et al., 2013), data protection techniques such as redaction, truncations, and obfuscation can be great concerns in cloud computing, and there are no accepted standards for how to address these concerns. Therefore, it is important for the cloud-computing providers to develop methods to deal with these technical challenges and to demonstrate their technical capacities of their users to ensure the provision of strong cybersecurity. Moreover, if the cloud providers fail to provide adequate cybersecurity they are not likely to gain the trust of the users.

Hypotheses

We develop and test five hypotheses, which are:

H1: The higher the level of users' trust (in his or her supervisor and the organization) the greater the performance of the cloud-computing provider.

H2: The greater the organizational cost-saving the greater the users' perception of the actual performance of the cloud-computing provider.

H3: The greater the users' perception of the adequacy of the cloud-computing provider's cybersecurity features the greater the users' perception of the actual performance of the cloud-computing provider.

H4: The greater the users' perception of the complexity of cloud computing the lower the perception of the actual performance of the cloud-computing provider.

H5: The higher the users' perception of the reliability of the cloud-computing provider the greater the perception of the actual performance of the cloud-computing provider.

Methodology

We designed an online survey, which was pilot-tested first using working graduate students, and local IT professionals. A two-step process helped us to come up with relevant items to develop the constructs from the users' perspective as affecting the actual performance of the cloud-computing provider. The live survey was conducted using the services of Qualtrics, which undertook a national U.S. online survey using the instrument we provided. The details of the items used in the survey instrument can be found in Xu and Mahenthrian's 2021 research paper (Xu & Mahenthiran, 2021). Qualtrics helped us obtain a sample of 158 participants from different states.

Data Analysis

This section discusses the results to test thehypotheses. First, we established the reliability and validity of our scales and the descriptive statistics are shown in Table 1. Second, we use ordinary least square (OLS) regression analysis to test hypotheses H1 to H5, which is reported in Table 2. Finally, Figure 1 shows the directional expectation for the hypothesized relationships and our findings.

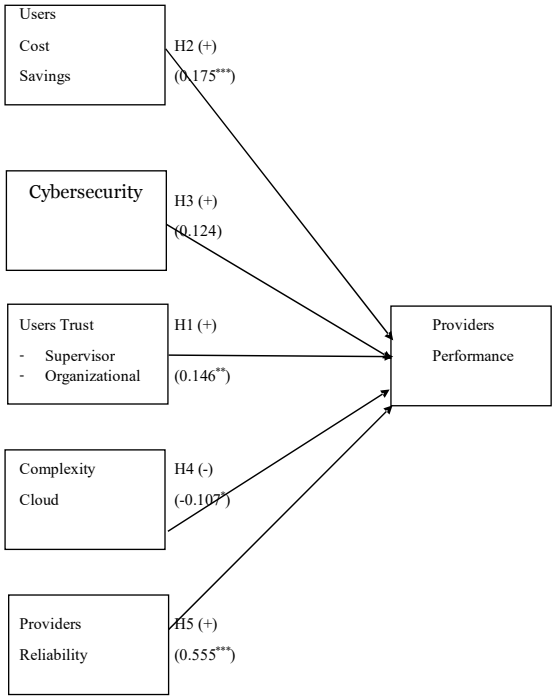

Figure 1. The Research Model for Human and Technical and Security Factors Impact Cloud-computing Provider's Performance

Table 1 confirms that the scales have good reliability, with all the Cronbach alpha coefficients being greater than 0.70. Figure 1 shows only five factors affecting provider's performance, but Table 1 shows nine factors including provider's performance (Perf). This is because we controlled for the level of adoption of cloud-computing (Adopt) and the firm size (Size) in our OLS regression analyses. Additionally, the trust construct has two factors users' perception of their trust in-supervisor and organizational trust that have been combined in Figure 1.

Table 1. Descriptive Statistics

Variable	**Mean**	**Standard Deviation**	**Cronbach Alpha (number of items)**
Perf	5.79	1.00	0.93 (10)
Super_Trust	5.18	1.31	0.93 (4)
Org_Trust	5.21	1.22	0.91 (4)
Cost_Sav	5.48	1.04	0.77 (3)
Complex	5.18	1.29	0.90 (5)
Cybersecurity	5.54	1.07	0.83 (4)
Reli_Sha	5.58	0.96	0.90 (8)
Adopt	3.23	2.10	n/a
Size	4.80	1.78	n/a

Hypothesis H1 states that the higher the level of users' trust (in his or her supervisor and the organization) the greater the performance of the cloud-computing provider. Table 2 shows that supervisor trust (Super_Trust) is significantly and positively associated with the providers' performance at $p < 0.01$ level, but organizational trust is not significantly associated with providers' performance. Hence, we conclude that there is partial support for hypothesis H1. The results suggest that once the IT employees

trust their immediate supervisors' technical competency, the level of organizational trust does not affect the cloud-computing provider's performance.

Hypothesis H2 states that the greater the users' perception of the organizational cost-saving the greater the users' perception of the actual performance of the cloud-computing provider. Table 2 shows that cost saving (Cost_Sav) is positive and significantly associated with the providers' performance at $p < 0.01$ level, which provides support for hypothesis H2. Hence, we conclude that the greater the anticipated cost savings of using cloud computing the greater the perceived actual performance of the cloud-computing provider.

Hypothesis H3 states that, the greater the provider's cloud capability (measured in terms of providing cybersecurity) the greater the users' perception of the actual performance of the cloud-computing provider. Table 3 shows that providers' capability is positive but not significant. Hence, we conclude that there is no support for hypothesis H3. This result means that user's perception of the provider's provision of cybersecurity is not a key consideration affecting cloud-computing performance, and a possible rational for it is provided in the conclusion section. Hypothesis H4 states that, the greater the users' perception of the complexity of cloud computing the lower the perception of the actual performance of the cloud-computing provider. Table 2 shows that technological complexity (Complex) is significant and negatively associated with the performance of the cloud-computing provider at $p < 0.08$ level, which provides support for hypothesis H4.

Hypothesis H5 states that the higher the users' perception of the reliability of the cloud-computing provider the greater the perception of the actual performance of the cloud-computing provider. Table 2 shows that sharing and reliability (Reli_Sha) reasons as perceived by the users is positive and significantly associated with the performance of the cloud-computing provider at $p < 0.01$ level, which provides strong support for hypothesis H5.

Table 2. Regression of Cloud-Computing Performance on Trust, Cost-savings, Technological Complexity and cybersecurity, and Reliability

Variable	Standardized Coefficients – Beta	t – Stat	Sig.
Constant	0.694	2.222	0.028
Super_Trust***	0.243	2.728	**0.007**
Org_Trust	-0.114	-1.359	0.176
Cost_Sav***	0.164	2.496	**0.014**
Complex*	**-0.104**	-1.756	**0.081**
Cybersecurity	0.090	1.035	0.302
Reli_Shar***	0.588	7.740	**0.000**
Adopt	0.016	0.328	0.743
Size**	0.094	1.964	**0.051**

N = 158, Adj. R2 = 0.677, F = 39.048***, D-W Stat = 2.060

***, **, *, indicates significance levels of $p < 0.01$, $p < 0.05$, and $p < 0.10$ levels.

Conclusions

The study attempts to bridge the research gap in the literature that has down played human and organizational factors such as the users' trust, users' perceptions of reliability, and technical complexity that affect the users' perception of cloud-computing providers' performance. The findings are shown in Figure 1, and both OLS regression and SEM analyses indicate that supervisor trust, cost savings, and reliability and sharing reasons for adopting cloud computing significantly and positively affects users' perception of the cloud-computing provider's actual performance. The results provide support for hypotheses H1, H2, and H5.

It was surprising that we failed to find support for hypothesis H3 that stated the greater the users' perception of the adequacy of the cybersecurity features, the greater the users' perception of the provider's actual performance. Our analysis of the responses and the debriefing of participants indicate that the adequacy of cybersecurity provision by the cloud providers is verified before choosing the service provider. Hence, it may not have registered as a significant consideration affecting the provider's actual performance after the service provider was chosen. Not properly explaining to our responders the timing of the factors in evaluating the provider's performance may be a limitation of our study. Additionally, the OLS and the SEM analyses indicate that technological complexity negatively and significantly affects users' perception of the cloud-computing providers' performance that provides support for hypothesis H4. Hence, most of the study's hypotheses are supported, and the study contributes to developing a framework to use to understand human and organizational factors affecting users' perception of the cloud-computing providers' actual performance. Further, the tests show that all the scales have acceptable levels of convergent and discriminant validity and can be used to study the interaction of human factors with technical factors including users' perception of the cybersecurity features offered by the cloud computing providers in other contexts. We refer the readers to the recently published study by Xu and Mahenthiran (Xu & Mahenthiran, 2021) to obtain further details of items used in the survey instrument and about the methodology and the SEM analysis.

References

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., . . . Zaharia, M. (2010). A view of cloud computing. *Communications of the ACM, 53*(4).

Badamas, M. A. (2012). Cyber security considerations when moving to public cloud computing. *Communications of the IIMA, 12*(3), 1-18.

Bisong, A., & Rahman, S. M. (2011). An overview of the security concerns in enterprise cloud computing. *International Journal of Network Security and Its Applications, 3*(1), 30-45.

Borgman, H. P., Bahli, B., Heier, H., & Schewski, F. (2013). *Cloudrise: exploring cloud computing adoption and governance with the TOE framework.* Paper presented at the 2013 46th Hawaii international conference on system sciences.

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:https://doi.org/10.1016/j.ijinfomgt.2013.07.001

Joint, A., Baker, E., & Eccles, E. (2009). Hey, you, get off of that Cloud? *Computer Law & Security Review, 25*(3), 270-274.

Kamara, S., & Lauter, K. (2010). *Cryptographic cloud storage*. Paper presented at the Proceedings of Financial Cryptography:Workshop on Real-Life Cryptographic Protocols and Standardization.

Karadsheh, L. (2012). Applying security policies and service level agreement to IaaS service model to enhance security and transition. *Computers & Security, 31*(3), 315-326.

Kaufman, L. M. (2009). Data Security in the World of Cloud Computing. *IEEE Security and Privacy, 7*(4), 61-64. doi:10.1109/msp.2009.87

Ko, R. K., Jagadpramana, P., Mowbray, M., Pearson, S., Kirchberg, M., Liang, Q., & Lee, B. S. (2011). *TrustCloud: A framework for accountability and trust in cloud computing.* Paper presented at the 2011 IEEE World Congress on Services.

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing - The business perspective. *Decision Support Systems, 51*(1), 176-189.

Radwan, T., Azer, M. A., & Abdelbaki, N. (2017). Cloud computing security: challenges and future trends. *International Journal of Computer Applications in Technology, 55*(2), 158-172.

Senyo, P. K., Addae, E., & Boateng, R. (2018). Cloud computing research: A review of research themes, frameworks, methods and future research directions. *International Journal of Information Management, 38*(1), 128-139.

Smith, R. (2009). Computing in the cloud. *Research Technology Management, 52*(5), 65-68.

Srinivasamurthy, S., Liu, D. Q., Vasilakos, A. V., & Xiong, N. (2013). Security and privacy in cloud computing: A survey. *Parallel & Cloud Computing, 2*(4), 126-149.

Xu, H., & Mahenthiran, S. (2021). Users' Perception of Cybersecurity, Trust, and Cloud Computing Providers' Performance. *Information and Computer Security*.