International Transaction of Electrical and Computer Engineers System, 2019, Vol. 6, No. 1, 1-7
Available online at http://pubs.sciepub.com/iteces/6/1/1
Published by Science and Education Publishing
DOI:10.12691/iteces-6-1-1

Internal Threats from CSPs and the Continuance Intention to Use Cloud Computing

Kunle Elebute[*]

Department of Computer Science, University of Maryland University College, Largo, Maryland, USA
*Corresponding author: princekay123@gmail.com

Received October 11, 2018; Revised January 02, 2019; Accepted January 10, 2019

Abstract There is a growing concern among organizations using cloud computing about the alarming rate of internal attacks on private cloud-stored data such as unauthorized exposure, disclosure, and sale of customer's confidential information by employees or associates of a cloud service provider (CSP). These unprofessional practices conducted accidentally or intentionally within the infrastructure of a service provider are internal threats. While studies have shown consistently that these unauthorized practices constitute an internal threat to data confidentiality and privacy, researchers are yet to empirically substantiate how these breaches by insiders of CSPs affect an organization's continuance intention to use cloud computing. Furthermore, available studies on data security have not fully explored the perception of IT managers about how internal threats affect their strategy while making the decision to continue using cloud computing. Using a multinomial logistic regression, this study analyzed data collected from IT managers with cloud experience. Findings of this study indicated that internal threats such as unauthorized exposure, disclosure, and sale of customer's data to third-party firms by employees of CSPs significantly influence the continuance intention to use cloud computing. This study benefits IT stakeholders by exploring the impacts of internal security lapses from the CSP on the decision of organizations to continue using cloud computing.

Keywords: *internal threat, insider, cloud computing, data breach, intrusion, malware*

Cite This Article: Kunle Elebute, "Internal Threats from CSPs and the Continuance Intention to Use Cloud Computing." *International Transaction of Electrical and Computer Engineers System*, vol. 6, no. 1 (2019): 1-7. doi: 10.12691/iteces-6-1-1.

1. Introduction

Security is one of the highly discussed topics in information technology. In the cloud environment, security is even a higher concern because cloud users are not physically responsible for managing their cloud-stored data. The increasing rate of data theft and security breaches on the cloud infrastructure is alarming. When there is an attack on any IT infrastructure, cloud users are the worst hit because cloud users rely ultimately on the tools made available by the cloud service provider (CSP) to safeguard their cloud-stored data [1]. Therefore, cloud users must trust the service providers to effectively manage, monitor, and secure the cloud infrastructure hosting their sensitive data [2].

Research has shown that cloud users typically face both external and internal threats [3]. External threats are possible attacks from an unknown hacker or cyber-criminal who intrudes into the cloud infrastructure directly or indirectly (through malicious programs). Hackers are often motivated by commercial, activism, or personal reasons. On the opposite, internal threats are potential attacks from inside an organization that are carried out by either a disgruntled employee of an organization or a malicious staff of the CSPs [4]. Studies have shown that most internal attackers are motivated by grievances, retaliation, or act of sabotage. Aside from accidental deletion of information, there have been reported cases of unauthorized exposure, disclosure, or sharing of customer's data by employees of CSP. There are also cases of deliberate and unauthorized sale of customer's sensitive data to third-party firms by CSPs for client profiling and targeted advertisement.

Statistically, external attacks from hackers are the most common forms of a data breach, but internal breaches on the cloud infrastructure are typically more severe and could potentially result in a far greater breach of data privacy and theft of sensitive personal or corporate data [5]. What is more worrisome to cloud users is that attacks from an insider may occur without any trace if the internal staff wipes the audit logs that could implicate them. Given the dangerous nature of an internal threat, organizations using cloud computing must be aware of the security risks involved in storing data in the cloud and take proactive steps to mitigate internal threats.

Although previous studies have investigated the impact of security threats on cloud adoption, majority of these studies focused on external threats. Furthermore, existing studies that explored internal threats did not investigate the impact of internal threats on the continuance intention to use cloud computing. Therefore, in spite of the achievements of recent researches, there is still a gap in knowledge about internal threats for this study to fill.

Therefore, the purpose of this study was to investigate the impact of internal threats from CSPs on an organization's continuance intention to use cloud computing. Additionally, this study explored how internal threats from employees of CSPs affect IT managers' decision-making strategies regarding the continuance intention to use cloud computing.

2. Literature Review

2.1. Nature of Cloud Services

Cloud computing is a technology that provides a flexible infrastructural platform consisting of shared virtual servers [6]. One of the benefits of cloud computing is that it provides better performance and is cost effective for users [7,8]. Studies have shown that businesses benefit more from cloud computing because of the little or no setup and maintenance costs required to run a highly scalable hardware, software, and network resources in a cloud platform [9]. It is also believed that cloud computing shifts the responsibilities of managing IT facilities from the cloud users to the CSP, thus providing room for organizations to focus more on their business models [10].

Three different categories of cloud computing have been identified by various studies – public, private, hybrid, and community cloud [11]. While public cloud is an open and accessible to various users who are interested in sharing IT resources, private cloud is a customized infrastructure for dedicated use by individuals and organizations. Hybrid cloud is a combination of both public and private cloud whereas community cloud is a facility available for multiple organizations willing to pool resources together due to their similar target.

There are three popular cloud service models, namely: software-as-a-service (SaaS), platform-as-a-service (PaaS), and Infrastructure-as-a-service (IaaS) [11]. The SaaS model allows users to remotely run applications from cloud servers without procuring any hardware and software license. Some examples of this are Dropbox, Microsoft OneBox, and GoogleMail. A PaaS cloud platform allows users to procure dedicated servers to run custom-built applications, but the underlying hardware layer will be controlled by the CSP. Examples of PaaS are Amazon RDS. The IaaS is a platform that allows cloud users to procure their storage, network, and hardware infrastructure and can control the resources as provided by the CSP [9].

2.2. Internal Threats in the Cloud

As stated earlier, internal threats are possible hazards from an insider of an organization. In the context of this study, internal threat implies danger from the employees or associates of a CSP that constitute a vulnerability to organizations using cloud computing.

Recent studies have identified three crucial features of internal threats:

- They are malicious;
- They are intentional;
- They are carried out by an insider, mostly a former or current employee of an organization [12].

Internal threats are malicious and intentional since the attackers always aim to compromise the infrastructure from inside the organization [3]. Statistically, studies have shown that cloud-stored data can be exposed to a much higher integrity or privacy breach if there is an internal attack from a "rogue administrator" [5].

In a study on cyber insider threat, [13] identified three types of internal attackers - a traitor, masquerader, and unintentional perpetrator. The traitor is an insider from within an organization who gives access to external intruders. A masquerader is an external attacker who collaborates with the traitor to attack the IT infrastructure of an organization. Finally, an unintentional perpetrator is a user inside the organization who accidentally creates a vulnerability within the IT infrastructure of his or her organization and enables a cyber-attack. All these three insiders are catalysts aiding internal threats.

Studies indicate that most organizations using cloud computing collaborate with their service providers to deploy various multi-layer encryptions and security scanning tools that will easily detect intrusions and repress attacks as countermeasures to checkmate external attacks such as SQL injections, VM hijacking, and password break [3]. However, it is difficult to track internal attacks since members of the organization who are supposed to protect the infrastructure carry them out.

The deliberate or accidental exposure, disclosure, or sale of customer's sensitive information to third parties by insiders within a CSP's network is an internal threat that can expose organizations to attacks [14]. Thus, internal threats are malicious and can cause vulnerability, which is capable of undermining data privacy, confidentiality, and integrity. The malicious act of an insider causes a security gap that may likely cause a financial loss to the organization [4].

But why would employees desire to deliberately breach data of his organization or data of clients? Studies have shown that aggrieved employees or former employees could breach an organization's private data in retaliation of a perceived wrongdoing from the organization [3]. This, of course, is punishable legally. However, firms using cloud computing should be proactive in monitoring internal threat through constant auditing and proactive monitoring of employee's behaviors in order to avoid future calamities [15,16].

This study focused on the internal threats that could occur within the infrastructure of a CSP and will analyze three possible dimensions of internal threats within the CSP – unauthorized exposure, unauthorized disclosure, and unauthorized sale of data by employees of the CSPs.

The first dimension of internal threat within the CSPs is data exposure within the infrastructure of the provider. Data exposure is one of the security concerns of cloud users. Recent events have shown that organizations using cloud computing will likely face a security threat through unauthorized exposure of their private data to employees or staff of CSP.

The second dimension of internal threat is unauthorized data sharing or disclosure. Organizations using cloud services are also concerned those insiders within the CSPs could disclose or share their private information with other parties (individuals or organizations) without their consent. This disclosure or data sharing practice could be for client profiling or targeted advertisement. In order to mitigate against this practice, cloud users must work with their providers to ensure that employees of those providers do not have unrestricted access to all their sensitive data. It is pertinent that organizations apply additional encryption layers to corporate data at rest and in transit.

Furthermore, the third dimension of internal threat within the CSP is an unauthorized sale of customer's data. Organizations are also concerned that employees of CSPs could sell their corporate data to their competitors for profit. This practice of data auctioning is also known as "data brokering" and it occurs on both cloud and non-cloud environments [17].

2.3. Strategies to Mitigate Internal Threats

Several countermeasure plans have been proposed in recent researches to mitigate internal threats in the cloud environment. Some of the most effective strategies are decentralizing storage, auditing user activities, employee behavior monitoring programs, and training.

Decentralizing of storage and computing resources can assist organizations to check most internal threat issues [14]. Many organizations store sensitive data, encryption keys, wallet files, data files, and application configuration files in a single location for convenience. This practice is also preferred as a performance improvement strategy by many IT experts because it is believed that applications read data faster from files in a single location. Unfortunately, this practice is a security risk that can expose sensitive data to accidental or deliberate exposure.

Effective auditing of activities within the cloud environment can also guard against malicious insider attacks. In their study, [15] proposed a monitoring program involving log analysis and event correlation that can detect insider activities using processed log files. Findings from their research indicated that the log monitoring process will assist organizations to quickly detect threats on the servers and collect statistics useful for analyzing user behavioral pattern.

In another research, [16] advocated for a program that integrates employee behavioral model with an operational monitoring system to detect intent to attack from within an organization by current employees. Their study combined psychological variables such as behavior, action, and degree of displeasure with their organization as bases to predict the tendency of an employee to be malicious. In their research, [16] believed this behavioral monitoring program is an effective countermeasure plan to mitigate internal threats in any work environment.

Finally, training and employee orientation is a potent countermeasure to mitigate internal attacks. While investigating factors that can mitigate insider attacks, [1] recommended employee sensitization and trainings to reduce internal attacks and vulnerabilities. These trainings should be geared towards orientating employees and associates of CSPs about the negative impacts an insider threat can cause to CSPs and their clients. Adequate trainings will also assist organizations to develop a culture of professional integrity.

3. Methodology

3.1. Research Questions

There are three research questions for this study. The first research question and hypotheses captured the respondent's perception about unauthorized exposure of cloud user's private data.

RQ1: To what extent do concerns about an unauthorized exposure of customer's personal data to employees of a CSP influence an organization's continuance intention to use cloud computing?

$H_0$1: Concerns about an unauthorized exposure of customer's personal data to employees of a CSP does not significantly influence an organization's continuance intention to use cloud computing.

H_a1: Concerns about an unauthorized exposure of customer's personal data to employees of a CSP significantly influence an organization's continuance intention to use cloud computing.

The second research question investigated the degree of concern of cloud users regarding the unlawful disclosure or use of their private data by employees of their CSPs without their authorization.

RQ2: To what extent do concerns about an unauthorized disclosure of customer's data by employees of a CSP influence an organization's continuance intention to use cloud computing?

$H_0$2: Concerns about an unauthorized disclosure of customer's data by employees of a CSP does not significantly influence an organization's continuance intention to use cloud computing.

H_a2: Concerns about an unauthorized disclosure of customer's data by employees of a CSP significantly influence an organization's continuance intention to use cloud computing.

The third research question captured the concerns of cloud users regarding the sale of their data to other firms for profit motive by employees of their CSPs.

RQ3: To what extent do concerns about an unauthorized sale of customer data to a private party by employees of a CSP influence an organization's continuance intention to use cloud computing?

$H_0$3: Concerns about an unauthorized sale of customer's non-sensitive data to a private party by employees of a CSP does not significantly influence an organization's continuance intention to use cloud computing.

H_a3: Concerns about an unauthorized sale of customer's non-sensitive data to a private party by employees of a CSP significantly influence an organization's continuance intention to use cloud computing.

The diagram below (Figure 1) displays the conceptual framework of the research, which shows all the four variables and their respective hypotheses for this study.

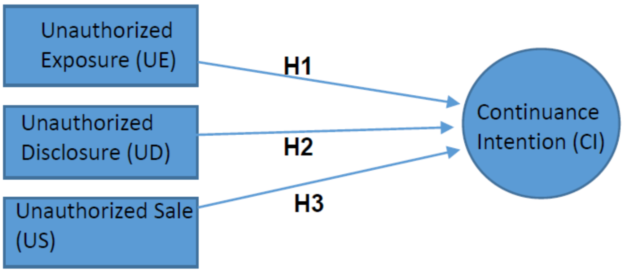
Unauthorized Exposure (UE)
Unauthorized Disclosure (UD)
Unauthorized Sale (US)
H1
H2
H3
Continuance Intention (CI)

Figure 1. The conceptual framework of research

3.2. Variables and Measurements

This study was a quantitative non-experimental correlational study and it investigated the possibility of a relationship between three independent variables and a dependent variable. The independent variables for this study were: (i) unauthorized exposure (UE); (ii) unauthorized disclosure (UD); and (iii) unauthorized sale (US). The only dependent variable was continuance intention (CI).

The UE variable measured the respondent's perception about user's concerns regarding unauthorized access to customer's sensitive data by employees of CSPs. The second variable, UD, referred to the respondent's perception regarding user's concerns about unauthorized disclosure or sharing of sensitive customer data by employees of CSPs. The third variable, US, captured respondent's perception about a practice where employees of CSP deliberately sell customer's sensitive data. A 5-point Likert-scale was used to collect responses for all the three independent variables. Respondents were asked to rate their concerns about data insecurity on a scale of 1 to 5 with 1 being "strongly disagree" and 5 being "strongly agree". Table 1 (below) displays the descriptions of all the variables.

Table 1. Variables and Definitions

Labels	Variables	Definition
UE	Unauthorized Exposure	A situation where employees of a CSP has unauthorized access to customer's sensitive data
UD	Unauthorized Disclosure	A situation where employees of a CSP disclose, use, or share customer's sensitive data without authorization
US	Unauthorized Sale	A practice where employees of a CSP sell customer's sensitive data
CI	Continuance Intention	The intention to continuously use cloud computing

The dependent variable (CI) measured the respondent's willingness to continue to use cloud computing in spite of the perceived insecurity caused by internal sabotages. There were three possible outcomes for the responses. Respondent's responses were coded as follows: "No"=1, "Undecided"=2, and "Yes"=3. Using IBM SPSS version 24 statistical software, data collected for the independent and dependent variables were coded as ordinal (ordered) and nominal (unordered or categorical) respectively [18,19].

3.3. Survey, Sampling, and Population

A web-based survey was employed to collect responses from 137 participants. The population for this study was IT managers with cloud experience. A simple random sampling was used to ensure that all qualified respondents were given an opportunity to participate in the study. For convenience and speed, a polling panelist service was employed to distribute the survey across multiple polling platforms. Two screening criteria were employed to determine eligibility to participate in the study. Respondents must be a decision-maker (management position) and a cloud user. The measurements from the survey were extracted from a previously validated survey instrument developed by [20]. The survey did not collect any data that could personally identify any of the respondents. All respondents in this study signed an electronic informed consent form to safeguard their privacy and confidentiality.

3.4. Data Collection and Analysis

The data collection was done entirely online and a web-based polling platform was used to host the survey and collected data. The data were then transferred directly into the SPSS application for processing and data analysis. In addition to descriptive statistics, a multinomial logistic regression analysis was conducted to test the hypotheses since the dependent variable had more than two possible outcomes [18]. Three factors mandated the use of multinomial logistic regression for this study: (i) the dependent variable had three possible outputs ("No", "Undecided", and "Yes") from responses collected; (ii) there was a perceived linear relationship between the two variables in the study; and (iii) there were no outliers in the data set [19].

4. Results

4.1. Profile of Respondents

Table 2 below captures the demographic distributions of the respondents for this study according to their gender, age, the highest level of education, job title, and size of their organization.

Table 2. Demographics of Respondents

Profile	Sample	Frequency	Ratio (%)
Gender	Male	81	59.12
	Female	56	40.88
Age	18-29 years	31	22.63
	30-39 years	72	52.55
	40-49 years	24	17.52
	50-59 years	6	4.38
	60 years and above	4	2.92
Education	High School	20	14.60
	Bachelor Degree	77	56.20
	Graduate School or Higher	40	29.20
Job Title	IT Manager	61	44.85
	Senior Manager	26	19.12
	IT Executive (CIO, CTO, etc)	17	12.50
	IT Director	25	18.38
	Other	7	5.15
Size of Firm	Less than 250 Employees	44	25.43
	250 – 499 employees	35	20.23
	500 – 749 employees	31	17.92
	750 – 999 employees	19	10.98
	1,000 employees and above	44	25.43

Statistics from Table 2 indicate that there were more male respondents than female respondents that participated in the study. The percentage of male respondents was 59.12% (n=81) compared to the percentage of female respondents, which was 40.88% (n=56). Furthermore, the highest age of the respondents that participated in this study was 30-39 years with 52.55% (n=72) of the total population of the study. Thus, the demographics of the respondents reflected a higher population of young IT managers and cloud users. The demographic statistics also indicated that the population had Bachelor degree as the highest educational level for the majority of the respondents. The sample's statistics displayed in Table 2 also show that the surveyed companies were composed of both large and small scale enterprises. There were 44 (25.43%) organizations with less than 250 employees and 44 (25.43%) organizations with more than 1,000 employees.

4.2. Descriptive Statistics

The descriptive statistics conducted for this study are shown in Table 3. The mean (M) and standard deviation (SD) for the variables have positive values. This shows a normal distribution of the data set [19]. However, the skewness and kurtosis values for the variables are mixed with both negative and positive values.

Table 3. Descriptive Statistics

Variables	M	SE	SD	Skewness	Skewness *SE*	Kurtosis	Kurtosis *SE*
UE	3.76	.09	1.06	-.719	.208	-.125	.413
UD	3.66	.10	1.21	-.553	.207	-.833	.411
US	3.62	.09	1.11	-.569	.207	-.535	.411
CI	2.93	.02	.29	-4.216	.207	18.978	.411

4.3. Hypothesis Testing

Three hypotheses were tested in this study using multinomial logistic regression analysis. The results of each of the hypothesis are presented below:

$H_0$1 Concerns about an unauthorized exposure of customer's personal data to employees of a CSP does not significantly influence an organization's continuance intention to use cloud computing

This hypothesis stated that concerns about unauthorized exposure of customer's private data to employees of CSPs do not significantly impact the decision of organizations to continuously use cloud computing. Respondents were asked if they would stop using cloud computing if their organization's personal data were exposed to employees of their CSPs.

A multinomial logistic regression analysis was conducted between the independent variable, unauthorized exposure (UE), and the dependent variable, continuance intention (CI). Results of the analysis are presented in the table below:

Table 4. Likelihood Ratio Tests

Model	Model fitting criteria	Likelihood ratio tests		
	-2 log likelihood	Chi-square	df	Sig.
Intercept	10.716	.000	0	
UE	45.487	34.770	4	.000

The data from Table 4 shows a Pearson's chi-square of 34.770, *df* of 4, and Sig. of .00. The data analysis for the hypothesis also produced a Pseudo R-Square value of .226 (Cox and Snell), .327 (Nagelkerke) and .218 (McFadden). Therefore, the results of the multinomial logistic regression tests for the first hypothesis was $\chi2 = 34.770$, (4), p = .000. This result is statistically significant since the p-value was lower than the .05 threshold. Therefore, the null hypothesis is rejected.

$H_0$2 Concerns about an unauthorized disclosure of customer's data by employees of a CSP does not significantly influence an organization's continuance intention to use cloud computing.

The second hypothesis was regarding the concerns about unauthorized disclosure of customer's data for commercial profiling by CSPs and if that has a significant influence on an organization's continuance intention to use cloud computing. Respondents were asked if they would discontinue using cloud computing because of unauthorized disclosure of their organization's private data by employees of the cloud providers. A multinomial logistic regression analysis conducted between the independent variable, unauthorized disclosure (UD), and the dependent variable, continuance intention (CI), indicated the results below:

Table 5. Likelihood Ratio Tests

Model	Model fitting criteria	Likelihood ratio tests		
	-2 log likelihood	Chi-square	df	Sig.
Intercept	11.183	.000	0	
UD	39.060	27.878	4	.000

As shown in Table 5, the Pearson's chi-square was 27.878, *df* was 4, and Sig. was .000. Results from the data analysis for the second hypothesis also produced a Pseudo R-Square value of .184 (Cox and Snell), .267 (Nagelkerke) and .174 (McFadden). Therefore, the results of the multinomial logistic regression analysis were $\chi2 = 27.878$, (4), p = .000, which implies that the result was statistically significant since the value of p was less than the .05 threshold. Therefore, the null hypothesis is rejected.

$H_0$3 Concerns about an unauthorized sale of customer's non-sensitive data to a private party by employees of a CSP does not significantly influence an organization's continuance intention to use cloud computing

The third hypothesis was related to the concerns about the unauthorized sale of customer's non-sensitive data to other firms by employees of CSPs and how that could significantly affect an organization's continuance intention to use cloud computing. A multinomial logistic regression analysis was conducted between the independent variable, unauthorized sale (US), and the dependent variable, continuance intention (CI). Results of the analysis are presented in the table below:

Table 6. Likelihood Ratio Tests

Model	Model fitting criteria	Likelihood ratio tests		
	-2 log likelihood	Chi-square	df	Sig.
Intercept	11.381	.000	0	.
US	39.511	28.130	4	.000

In Table 6, the Pearson's chi-square was 28.130, *df* was 4, and Sig. was .000. Therefore, the results of the multinomial logistic regression to test the third hypothesis was $\chi 2$ = 28.130, (4), p = .000. The results also produced a pseudo r-square value of .186 (Cox and Snell), .270 (Nagelkerke) and .176 (McFadden). These result of the multinomial logistic regression for the third hypothesis was statistically significant since the value of *p* was lesser than the .05 threshold. Therefore, the null hypothesis is rejected.

5. Discussions

The results of the first hypotheses test was significant ($\chi 2$ = 34.770, (4), p = .000). This indicates that IT decision-makers consider an unauthorized exposure of customer's data to employees of CSP as a major threat, which has a significant influence on their decision to continuously use cloud computing. Therefore, exposure of sensitive data stored on the cloud to the staff of CSP will undermine the privacy and confidentiality of data stored on the cloud. It will also influence the decision-making of IT managers. Such exposure, as shown from the literature review earlier in this study, constitutes a security risk and will negatively impact the decision to deploy new technology. This finding also indicates that data exposure from CSPs will shape the strategy of the respondents when considering whether to continue using cloud computing.

Based on the results of the statistical analysis conducted for the second hypothesis ($\chi 2$=27.878, (4), p=.000), the second null hypothesis was rejected. This implies that concerns about an unauthorized disclosure of customer's data by employees of CSPs has a significant influence an organization's continuance intention to use cloud computing. Therefore, an IT manager considers the possibility of an unauthorized disclosure of a customer's personal data stored on the cloud platform by employees of CSPs when deciding whether to continue using cloud computing. The results show that the majority of the respondents in this study perceive unauthorized disclosure of customer's data by CSPs as a security concern that plays a key role during decision-making.

The third results indicate that there is a relationship between the independent variable (US) and the dependent variable (CI). The result ($\chi 2$=28.130, (4), p=.000) was significant and it shows that cconcerns about an unauthorized sale of customer's private data to a third party by employees of a CSP significantly influences the continuance intention to use cloud computing. Therefore, the respondents in this study (IT managers) were seriously concerned about the privacy and confidentiality of their cloud-stored data and considered an unauthorized sale of their data a security breach that will determine whether to continue using cloud computing.

6. Conclusion

Many organizations using cloud computing are in a dilemma; they are fascinated by the benefits of deploying cloud computing, yet they are concerned about the security risks of running cloud-based IT operations. As already suggested by previous studies, internal and external threats are obstacles to cloud adoption. This study explored this topic further by investigating the impact of internal threats on an organization's continuance intention to use cloud computing.

Findings of this study provided new empirical evidence showing that an organization's continuance intention to use cloud computing is significantly influenced by internal threats such as exposure of customer's data to employees of CSPs, an unauthorized disclosure of customer's data, and unauthorized sale of customer's data to third party by employees of CSPs. Therefore, this study concludes that internal threats from the employees of CSPs significantly influence an organization's continuance intention to use cloud computing. Internal threats will always influence the strategy and decisions of IT managers as long as organizations using cloud computing do not have full control of the physical infrastructure underlying their cloud workspace.

This study has two limitations. The first limitation of this study is the small sample size and the profile of the respondents. Future study can increase sample size and include broad parameters to retrieve a more diverse distribution of respondents. Furthermore, the second limitation is that the scope of the study was limited to only security-specific threats to the continuance use of cloud computing. Future research can expand this scope to cover non-security related factors that may also constitute reasonable threats to an organization's continuance intention to use cloud computing.

References

[1] Kajiyama, T., Jennex, M., & Addo, T. (2017). To cloud or not to cloud: How risks and threats are affecting cloud adoption decisions. *Information and Computer Security, 25*(5), 634-659.

[2] Elebute, K. (2018). Trust and Continuous Deployment of Cloud Computing: A Quantitative Analysis. *Journal of Computer Sciences and Applications, 6*(2), 69-74.

[3] Yusop, Z. M., & Abawajy, J. (2014). Analysis of insiders attack mitigation strategies. *Procedia-Social and Behavioral Sciences, 129*, 581-591.

[4] Rao, R. V., & Selvamani, K. (2015). Data security challenges and its solutions in cloud computing. *Procedia Computer Science, 48*, 204-209.

[5] Babu, B. M., & Bhanu, M. S. (2015). Prevention of insider attacks by integrating behavior analysis with risk based access control model to protect cloud. *Procedia Computer Science, 54*, 157-166.

[6] Hawedi, M., Talhi, C., & Boucheneb, H. (2018). Security as a Service for Public Cloud Tenants (SaaS). *Procedia Computer Science, 130*, 1025-1030.

[7] Wu, K., Vassileva, J., & Zhao, Y. (2017). Understanding users' intention to switch personal cloud storage services: Evidence from the Chinese market. *Computers in Human Behavior, 68*, 300-314.

[8] Sadooghi et al. (2017). Understanding the performance and potential of cloud computing for scientific applications. *IEEE Transactions on Cloud Computing, 5*(2), 358-371.

[9] Phaphoom, N., Wang, X., Samuel, S., Helmer, S., & Abrahamsson, P. (2015). A survey study on major technical barriers affecting the decision to adopt cloud services. *Journal of Systems and Software, 103*, 167-181.

[10] Alsmadi, D., & Prybutok, V. (2018). Sharing and storage behavior via cloud computing: Security and privacy in research and practice. *Computers in Human Behavior, 85*, 218-226.

[11] Mell, P., & Grance, T. (2011). The NIST definition of cloud computing. *NIST Special Publication, 800*(145), 7.

[12] Mishra, P., Pilli, E. S., Varadharajan, V., & Tupakula, U. (2017). Intrusion Detection Techniques in Cloud Environment: A Survey. *Journal of Network and Computer Applications, 77*, 18-47.

[13] Liu, L., De Vel, O., Han, Q. L., Zhang, J., & Xiang, Y. (2018). Detecting and Preventing Cyber Insider Threats: A Survey. *IEEE Communications Surveys & Tutorials, 20*(2), 1397-1417.

[14] Callegati, F., Giallorenzo, S., Melis, A., & Prandini, M. (2018). Cloud-of-Things meets Mobility-as-a-Service: An insider threat perspective. *Computers & Security, 74*, 277-295.

[15] Ambre, A., & Shekokar, N. (2015). Insider threat detection using log analysis and event correlation. *Procedia Computer Science, 45,* 436-445.

[16] Sticha, P. J., & Axelrad, E. T. (2016). Using dynamic models to support inferences of insider threat risk. *Computational and Mathematical Organization Theory, 22*(3), 350-381.

[17] Kaptur, M. E., Fisher, S. D., Robinson, D., & Fisher, C. D. (2018). Big Data and the Bigger Picture. *European Journal of Economics, 2*(2).

[18] Creswell, J. W., & Creswell, J. D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches.* Sage publications.

[19] Field, A. (2013). *Discovering statistics using IBM SPSS Statistics* (4th ed.). Thousand Oaks, CA: Sage.

[20] Yang, H., & Lin, S. (2015). User continuance intention to use cloud storage service. *Computers in Human Behavior, 52*, 219-232.