The Impact of Security Concerns on Personal Innovativeness, Behavioural and Adoption Intentions of Cloud Technology

Prasanna Balasooriya L. N., Santoso Wibowo,
Srimannarayana Grandhi, and Marilyn Wells

School of Engineering & Technology, Central Queensland University,
Melbourne, Australia
E-mail: p.balasooriya@cqu.edu.au

Received 16 August 2017; Accepted 22 October 2017;
Publication 27 November 2017

Abstract

Cloud services have gained popularity due to the number of advantages they provide to organizations and individuals such as reduced cost, better storage, and improved performance. However, a lot of organizations are still unwilling to shift their traditional in-house services to the Cloud due to the various security implications. Many Cloud service users are worried about the security of their data and privacy being violated. There are many reported cases of Cloud service providers illegally collecting personal data of their customers, which has led to service providers being viewed with greater suspicion than before. To overcome this, Cloud service providers must ensure that they inform the users exactly about which data is being used and how it is used. While it is the duty of the Cloud service provider to protect the data confidentiality and privacy of their customers, this should not be misunderstood or misused by customers to conduct illegal activities because Cloud service providers have to abide by the rules and regulations, including co-operating with law enforcement agencies if they need any particular customer's data. In this paper, we research the main security aspects for ensuring data confidentiality and privacy.

Journal of Software Networking, 265–290.
doi: 10.13052/jsn2445-9739.2017.013

Keywords: Cloud security, Data privacy, Confidentiality, Adoption, Challenges.

1 Introduction

Cloud computing is seen as one of the emerging technologies available in the information technology domain. The National Institute of Standard and Technology (NIST) defines Cloud computing as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources including networks, servers, storage, applications and services that can be rapidly provisioned and released with minimal management effort or service provider interaction [1, 2]. Cloud computing is found to be an important part of businesses and individuals as it helps organizations to reduce their operational costs by improving their services. In addition, the use of this technology increases the collaboration and scalability acceptance up to a non-comparable level [3].

Despite the numerous benefits of Cloud computing for businesses and individuals, there are some concerns such as security and privacy during its adoption [3]. Due to these concerns, organizations over the globe have been very slow in adopting Cloud services, with only 10% of US organizations and 19% of European organizations are using the Cloud computing [4]. It is also found that even organizations using Cloud services tend to limit their use. Giannakouris and Smihily [5] found that 49% of European organizations using Cloud services are only using the very basic services of email and data storage functionalities, and 57% of European organizations ranked the security breach as the main reason to prevent them from adopting Cloud services [5]. Singh et al. [6] believe that Cloud security, availability and performance are recognized as the biggest problems for Cloud adoption. Furthermore, Singh et al. [6] have further concern over the reporting structure of the incident of security and privacy violations in the Cloud computing. Therefore, ensuring data security and the privacy of the users' data on the Cloud is a critical factor that needs to be considered for the increasing use of the Cloud.

Nevertheless, providing secure and privacy protected Cloud services are highly challenging, as security and privacy problems could occur in different stages within the Cloud services context. Also, the success of the Cloud computing in the current information technology landscape has given a free pass for attackers to explore and target businesses and individuals [7]. These security and privacy issues which have occurred due to unethical and illegal use of the user's data, could hinder the acceptance of Cloud computing [8]. It is therefore critical for businesses and individuals to address data security, data integrity and privacy issues in the use of Cloud computing [9]. Thus, the main aim of this paper is to review the issues that are related to data security and privacy of Cloud computing.

2 Literature Review

2.1 Security

As per ISO 27001 standards, Cloud security has been described as the preservation of confidentiality, integrity and availability of information in the use of Cloud computing [10]. However, the use of Cloud computing may face many critical issues such as competitive pressure, vendor support and third party control, performance and availability. With its growing popularity, Cloud security has become a critical factor that needs to be considered during its adoption and use [11]. Research has shown that data security, availability and performance are some of the most important elements of the quality of the service that Cloud providers need to offer to their users [12, 13].

The Australian Bureau of Statistics (ABS) [14] has collected information on the factors that are limiting the use of Cloud services in Australia for the years 2015–2016 based on a sample size of 6750 businesses. Businesses with 0–4 employees are quite comfortable with the use of paid Cloud computing (61.3%) but their main problem for limiting the use of Cloud services is due to the insufficient knowledge of Cloud computing services (21.6%). This is also a similar issue for businesses with 5–9 employees (24.8%) and 20–199 employees (24.2%). On the other hand, the risk of a security breach (30.4%) is recorded as the main factor for limiting the use of Cloud services for businesses with 200 or more employees [14].

Table 1 presents a summary of factors that have limited the use of Cloud computing between 2015 and 2016 in Australia.

Xiang and Bo [11] indicated that more than 70% of its participants in their survey agreed that they do not intend to adopt or use Cloud services due to the fear of data security and privacy concerns. Furthermore, the number of major security breaches that occurred in the last few years has also contributed to the limited use of Cloud services by businesses and individuals. Cloud service providers have several security issues that they have to address, including (a) providing a secure connection for their users, (b) protecting data from hacker

Table 1 Factors that are limiting the use of Cloud services in Australia

Factors	0–4 Persons	5–9 Persons	20–199 Persons	200 or More Persons	Total
Risk of a security breach	14.0	18.2	23.6	30.4	16.2
Problems accessing data or software	6.2	8.7	8.4	15.9	7.2
Difficulties with unsubscribing or changing Cloud computing service provider	3.4	4.3	5.1	7.2	3.9
Uncertainty about the location of data	9.5	11.0	14.4	19.2	10.5
Uncertainty about legal, jurisdictional or dispute resolution mechanisms	6.9	8.4	9.6	12.8	7.6
High cost of Cloud computing services	10.1	12.0	12.2	19.8	10.9
Insufficient knowledge of Cloud computing services	21.6	24.8	24.2	22.1	22.8
Other factors	4.5	4.6	4.2	5.5	4.5
No factors limited or prevented the use of paid Cloud computing	61.3	55.8	51.0	43.6	58.7

Source: ABS, 2017.

attacks, (c) ensuring that data is accessible by the customers at all times, and (d) preventing data loss during transfer [12]. Mukherjee and Sahoo [13] point out that the adoption of Cloud computing lies with the security and privacy of the sensitive data of the organizations. If organizations are willing to keep their data in the Cloud, then organizations need to seek more clarification from the Cloud service provider on (a) how the Cloud provider encrypts organizational data and handle them, (b) how Cloud services providers handle the liabilities of data breaches and leakages, and (c) what is Cloud user substantiation.

Figure 1 lists the most important factors that are limiting the adoption of Cloud computing services in the European Union. It is found that the risk of a security breach scored highest both for large organizations and SMEs, (57% and 38% respectively). Clearly, organizations attach importance to the protection of their IT systems, but the issue can be seen in the wider context of resilience to possible security breaches when using the Cloud.

Data plays a very important role in Cloud services with users submitting their personal information as well as storing and transferring sensitive and confidential information. Thus, Cloud data security challenges can be broadly classified into data confidentiality issues and data integrity issues. Both of these issues arise due to failed data security measures. Data confidentiality refers to protecting the customers' data from being disclosed to illegitimate

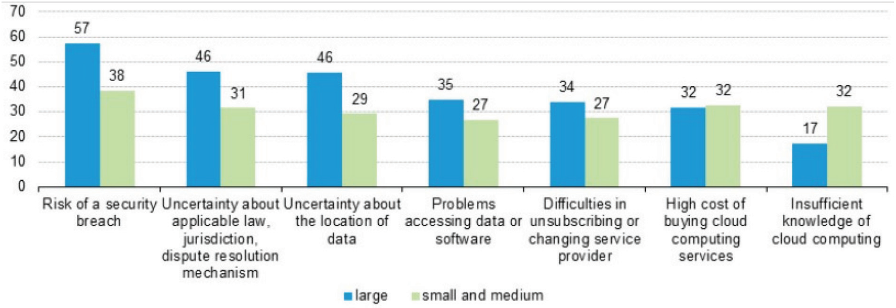


Figure 1 Factors Limiting Organizations from using Cloud Computing Services in the European Union.

Source: Giannakouris and Smihily, 2016.

Table 2 Main Challenges in Cloud Computing Adoption

Challenges	References
Data acquisition	[12, 15, 16, 17, 18]
Confidentiality	[3, 10, 15, 19, 20]
Integrity and authenticity	[6, 9, 15, 21, 22, 23]
Multi-tenancy	[10, 16, 17, 18]
Service level agreement (SLA's)	[12, 16, 24, 25, 26]
Insider attacks	[16, 27, 28, 29]

parties without their express approval while data integrity refers to protecting consumers' data from malicious modifications and ensuring the accuracy and consistency of data [2]. Table 2 presents the main challenges that need to be considered during the adoption and use of Cloud computing.

2.2 Confidentiality and Privacy

Data confidentiality entails preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information [30]. Cloud computing has been recognized as a next generation information technology model that could help businesses and individuals fulfil their requirements. However, the operational and administration model of Cloud computing differs from traditional information computing architecture. To provide a better and reliable service at low costs, Cloud service providers have to shift their applications to data centers where the management and administration of data and services are not trustworthy [31]. This feature could contribute to a new data security and privacy challenges in adopting and using the technology [32]. Therefore, it is important for Cloud service providers to address the issue of privacy that comes along with strong and extremely sensitive data stored in the Cloud environment so that users of Cloud computing will be able to enjoy the full benefits of the Cloud computing.

In Cloud services, there are many aspects of data confidentiality. The first issue is that of unauthorized data collection by the Cloud service providers themselves. Many Cloud services are free for the customers, whereby the business model is making revenue from advertising. In order to target their advertisements better and at the same time provide personalized ads, many Cloud service providers tend to violate the privacy of their customers by collecting unauthorized personal data of their customers [33]. One of the largest information technology organization, Google, which provides many Cloud services, including google drive, google play store, and Gmail, has been accused time and again of violating consumer privacy by collecting users' information surreptitiously [11, 34, 35]. In 2012, Google was fined $22.5 million by US authorities for violating privacy regulations by secretly collecting user data from the Safari browser [34]. In 2013, Google was again fined $17 million for a similar offence, and was also accused of collecting unauthorized data from every user of the google app play store and selling it to developers [34, 35]. Customers have a right to know exactly what data will be collected and how it will be used, which is why secretly collecting customer email addresses and selling it to developers without informing the users in advance, is a big violation of privacy [36].

The email Cloud service of Google, Gmail has also come under the scanner for privacy violations. In 2010, consumers filed a complaint against Google regarding the unauthorized scanning of private mails exchanged between consumers through Gmail, and using the data from the mails to target customers with personalized advertisements [37]. Google admitted to scanning emails and using the data for an advertisement generation, but stated that it had adequately informed its users of this in terms and conditions and therefore, there was no violation of privacy [37].

Encrypting user data is another key data security measure so that no one, not even employees have access to the data. [38]. A Cloud service provider, Skyhigh has conducted a survey amongst healthcare organizations regarding Cloud service usage and security risks. The research found that 33% of the organizations reported data leaks via employees in 2014, while 79% of the organizations stated data leaks as one of their topmost worries [39]. While all Cloud service providers need to ensure encryption and protection against misuse of data by employees, the healthcare industry is at the highest risk due to the high price that data mining organizations are willing to pay to obtain patient details for insurance and pharmaceutical organizations [39]. In fact, employees have resorted to selling their login credentials in order to make money, and 90% of the organizations surveyed had at least one employee credential on sale online [39]. Such data leaks by the employees constitute a violation of privacy as well as data confidentiality regulations, since the patient has no idea that his/her medical history is being sold by the Cloud service provider.

Data confidentiality may be compromised due to malicious attacks by hackers or other outside threats. As the adoption of Cloud services is growing amongst individuals and businesses, the focus of hackers is also shifting from targeting private networks to targeting the Cloud [40]. AlertLogic conducted a research on the state of Cloud security from its 2,200 customers. Their research found that in 2014, 44% of the customers experienced a brute force attack compared to 30% of customers a year earlier [41]. There was an equal percentage of vulnerability scans (44%) which have also increased from 27% a year earlier [41]. Hackers mainly carry out these attacks with the intention of stealing personal data with the ultimate aim of financial fraud or identity theft. The vulnerability of Cloud services to hacker attacks became evident with the hacking of Apple's iCloud accounts in which the privacy of several celebrities was violated and personal data was stolen. This attack was caused due to weak data security measures and the absence of a two factor authentication system [42]. Retail giants Target and online retailer Zappos, both became victims of a data breach due to their private Cloud being hacked and credit card details, billing address and password of their clients being stolen [43]. Both attacks were caused due to loopholes in their data security such as weak data encryption systems that allowed hackers to read client data easily [43]. It can be seen that protecting data against misuse by parties with malicious intent is difficult due to the constant innovation by hackers in attacks including a new "man in the Cloud" method which hacks into the file synchronization software virtually undetected [44]. It is therefore critical for Cloud service providers to constantly evaluate their data security measures and implement the latest security measures to protect their user's data confidentiality and privacy.

2.3 Personal Innovativeness (PI)

Rogers [45] recognized that highly innovative individuals as an active information seekers who are willing to explore new ideas. Prasad [46] has explained that personal innovativeness as a tool where it helps to identify the personals who are willing to adopt new technologies than others in the industry. Furthermore, Rogers [31] has recognised early adopters as a key change agents and opinion leaders who will be supporting the decisions of modern technology adoptions. In addition to that, Lu et al. [47] described that the individuals who has higher personal innovativeness are expected to develop more positive belief about the target technology. Kuo and Yen [48] have identified personal innovativeness as an important factor affecting adoption behaviour of new technologies. Therefore, inclusion of personal innovativeness as a construct in this study will allow researcher to further understand the role of individuals in technology adoption.

2.4 Behavioural Intentions (BI)

Armitage and Conner [49] described behavioural intention (BI) as a person's perceived likelihood or subjective probability that he or she will engage in a given behaviour or in other words, intentions are assumed to capture the motivational factors that influence a behaviour and to indicate how hard people are willing try or how much effort they would expect to perform. Ajzen [50] pointed out that BI is an indicator of an individual's readiness to perform a behavioural task. Thus, this readiness can be captured by asking whether those individuals are intended, expect, or planning to engage a behavioural activity. Furthermore, Armitage and Conner [49] have also noted that BI has been found to have high predictive validity in relation to behaviour. Therefore, behavioural intention is a valuable construct in this study, and will be helpful to explore the user's intention of Cloud adoption.

2.5 Adoption Intentions (AI)

Sintonen and Immonen [51] have explained that consumers' willingness to adopt modern technology can be measured by analyzing the market due to individual's behavioural intention to adopt or start new services. Furthermore, Tsai and Hsu [52] believed that the organizational readiness to be used as an element to measure its capability of technology adoption. Thus, this construct has been used to explore the organizational readiness.

Table 3 shows the hypotheses used in this study. The proposed conceptual model used to test the hypotheses is shown in Figure 2. Table 4 lists 11 variables that are defined under these three constructs such as security (SEC), personal innovativeness (PI), behavioural intention (BI) to cover the key challenges that have been found in Table 2.

Table 3 Hypotheses used in the Study

Hypothesis ID	Hypothesis
H1	Security will positively impact the likelihood of personal innovativeness of the users
H2	Security will positively impact the likelihood of behavioural intention of the users
H3	Security will positively impact the likelihood of adoption intention of users
H4	Personal innovativeness positively relate to the likelihood of adoption intention
H5	Behavioural intention positively relate to the likelihood of adoption intention

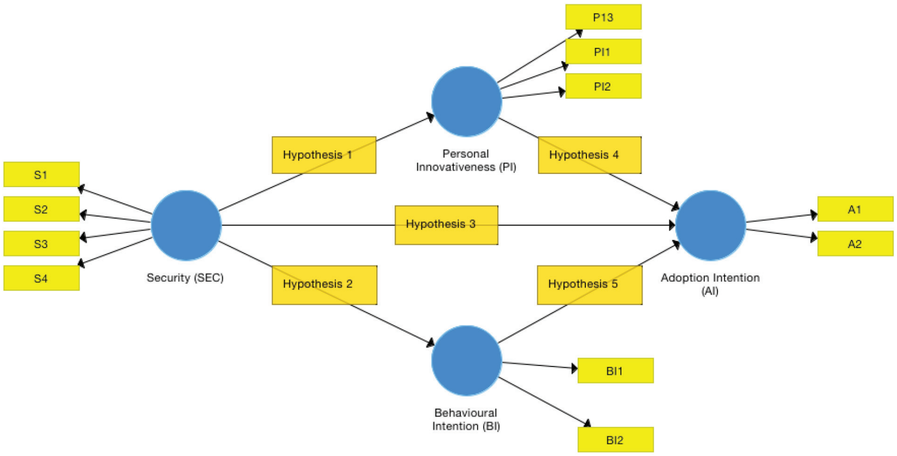


Figure 2 The Conceptual Model.

3 Research Methodology

3.1 Research Background

To evaluate the proposed conceptual model shown in Figure 2, the survey questionnaire was developed and distributed to IT professionals in Australia. The variables that have been used in this survey was chosen to gain better and deeper knowledge of how security and privacy concerns could affect personal innovativeness, behavioural intention and adoption intentions of Cloud computing adoption in Australia.

During the data collection, 200 statistically valid responses were collected from IT professionals who are actively involved in IT industry. To measure the

Table 4 List of Latent Variables and Factor Variables

Latent Variable	Factors	Factor Description	References
Security	S1	Users will be happy to send their information across Cloud	[3, 7]
	S2	Users are feeling safe to keep their information on the Cloud	[4, 9]
	S3	Users think that Cloud is more vulnerable to cyber crimes	[11, 12, 42]
	S4	Users think that in-house solutions are not better than Cloud	[5, 12, 13, 22, 26]
Personal Innovativeness	PI1	Users are interested on new technologies	[2, 3]
	PI2	Users are pleased to try new technologies	[12, 14]
	PI3	Users are happy to accept new tehnologies	[3, 14]
Behavioural Intention	BI1	Users will be using Cloud in the future	[3, 23]
	BI2	Like to use Cloud for work and personal	[2, 32]
Adoption Intention	AI1	Cloud is a promising technology	[4, 14]
	AI2	Like the Cloud concept	[4, 8, 13]

relationship between variables, 5-point Likert scale has been applied with two screening questions to capture the valid samples. In this survey, three major constructs such as security (SEC), personal innovativeness (PI), behavioural intention (BI) have been identified as influential factors that could affect the decision of Cloud adoption.

3.2 Methodology

Haenlein and Kaplan [53] explained that the use of first generation techniques could face three common limitations such as (a) the population of a simple model structure, (b) the assumption that all variables can be considered as observable and; and (c) the conjecture that all variables are measured without error, which could limit the applicability of those techniques. Therefore, as suggested by Hair et al. [54], the Partial Least Squares – Structural Equation Modelling (PLS-SEM) is a better statistical solution to be used in this study.

Isma'ili et al. [55] mentioned that PLS-SEM is a multivariate analysis technique that can be used identify the correlations between multiple variables.

Furthermore, Isma'ili et al. [55] believed that the PLS-SEM factor analysis technique can be used to measure the latent variables that are not directly measured, and PLS-SEM path analysis technique can be used to expose the relationships between each latent variable. Volckner et al. [56] have concluded that PLS-SEM is particularly appropriate when the model is complex, because it does not lead to estimation problems or improper or non-convergent results. Therefore, PLS-SEM has been chosen as an appropriate technique to be used in this study.

3.3 Results

As suggested by Anderson et al. [58], we have adopted a two-tier approach which include (a) confirmatory factor analysis and (b) analysis of structural equation model through discriminant validity in this study. If factor analysis is misinterpreted and discriminant validity is not established, then scales used and conclusion made will be incorrect in other approaches. However, use of two-tier approach could eliminate this discrepancy, and have benefits including (a) the number of comparative strengths that allow meaningful inferences to be made, (b) an assessment of whether any structural model would give acceptable fit, and (c) ability to make any asymptotically independent test of the substantive or theoretical model of interest [58]. Therefore, the use of Anderson et al. [58] approach is more appropriate for this study. Figure 3 illustrates the basic path model of the proposed model.

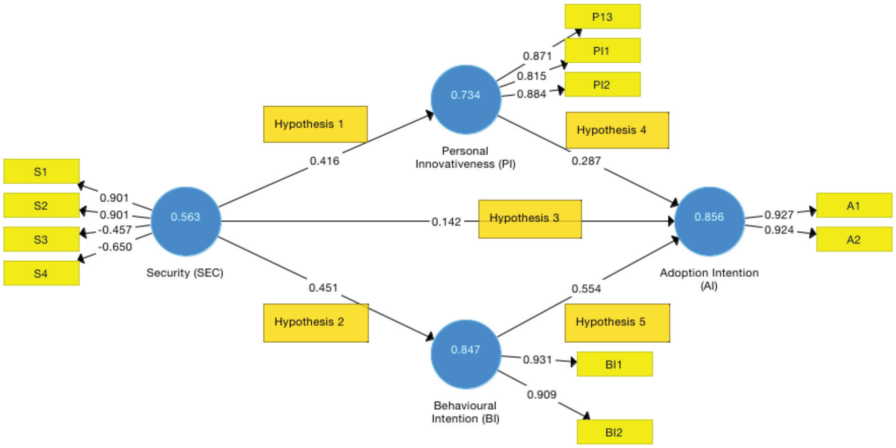


Figure 3 The Conceptual Model with Loadings.

3.3.1 Target endogenous variable variance

The coefficient of determination, R2, is 0.856 for the adoption intention latent variable. Thus, this explains that security (SEC), personal innovativeness (PI) and behavioural intentions (BI) substantially explain 86% of variance of adoption intention (AI).

3.3.2 Inner model path coefficient sizes and significance

The inner model suggests that behavioural intention has the strongest effect on adoption intention (0.554) followed by personal innovativeness (0.287) and security (0.142). Furthermore, security has more effect on behavioural intention (0.451) than its influence on personal innovativeness which is 0.416. In addition to this explanation, the hypothesised path relationship between (a) security and personal innovativeness (H1), (b) security and behavioural intention (H2), (c) personal innovativeness and adoption intention (H4), and (d) behavioural intention and adoption intentions (H5) are statistically significant. However, hypothesised path relationship between security and adoption intention (H3) is marginally significant, because its standardized path coefficient (0.142) is greater than 0.1.

3.3.3 Outer model loading

The correlations between latent variables and indicators are presented in Table 5. Thus, this will present the path coefficients in the proposed model.

The Smart-PLS software application that has been used in this study to find the path coefficient estimation in the outer model has been configured to stop

Table 5 Outer Loadings of the Proposed Model

	Latent Variables			
Indicators	Adoption Intention (AI)	Behavioural Intention (BI)	Personal Innovativeness (PI)	Security) (SEC)
A1	0.927			
A2	0.924			
BI1		0.931		
BI2		0.909		
PI1			0.815	
PI2			0.884	
PI3			0.871	
S1				0.901
S2				0.901
S3				–0.457
S4				–0.650

Table 6 Number of iterations carried out

	Al	A2	BI1	BI2	PI3	PIl	PI2	S1	S2	S3	S4
Iteration 0	0.540	0.540	0.543	0.543	0.389	0.389	0.389	0.508	0.508	0.508	0.508
Iteration 1	0.544	0.537	0.569	0.517	0.387	0.401	0.380	0.420	0.431	−0.063	−0.315
Iteration 2	0.546	0.534	0.578	0.508	0.401	0.372	0.393	0.415	0.431	−0.070	−0.318
Iteration 3	0.546	0.535	0.579	0.507	0.401	0.372	0.393	0.414	0.432	0.071	−0.317
Iteration 4	0.546	0.535	0.579	0.507	0.401	0.372	0.393	0.414	0.432	−0.071	−0.317
Iteration 5	0.546	0.535	0.579	0.507	0.401	0.372	0.393	0.414	0.432	−0.071	−0.317
Iteration 6	0.546	0.535	0.579	0.507	0.401	0.372	0.393	0.414	0.432	−0.071	−0.317
Iteration 7	0.546	0.535	0.579	0.507	0.401	0.372	0.393	0.414	0.432	−0.071	−0.317

the estimation when (a) the stop criterion of the algorithm was reached 300 iterations, or (b) the maximum number of iterations has reached, whichever comes first. The iteration process is adopted to make the model acceptable [59]. Based on the above presented criteria, the measurement model is assessed.

Thus, the results presented in Table 6 determine the number of iterations that have been carried out during the execution of procedure. If the algorithm cannot converge the data that has been used in the analysis in less than 300 iterations as configured, it indicates that the data that has been used has abnormality such as small sample size, too many identical values in indictors or existence of outliers. However, the results presented in Table 6 indicate that the algorithm converged only after 8 iterations instead of reaching 300 iterations. Therefore, it confirms the there is no abnormality in the data, and estimation in this study was good.

3.3.4 Indicator reliability

Isma'ili et al. [55] pointed out that it is an essential procedure to determine the reliability and validity of the latent variables to complete the examination of the model. Thus, Table 7 presents the results of indicator loadings, indicator reliability, composite reliability, and AVE values. As seen in the Table 7, all the indicators have individual reliability values that are much greater than the minimum acceptable level of 0.4 and close to the preferred level of 0.7 except SEC 3 and SEC 4. The indicator variable SEC 3 and SEC 4 indicate that it has negative effects on Security construct. Thus, these values can be removed from the proposed model.

3.3.5 Internal consistency reliability

As suggested by Hair et al. [54], composite reliability has been used to find the internal consistency reliability of the model. As seen in Table 7, the values presented are greater than 0.6 except for security variable. Thus, composite

Table 7 Summary of Outer Model

Latent Variable	Indicator id	Loading	Indicator Reliability	Composite Reliability	AVE
Security	S1	0.901	0.812	0.217	0.563
	S2	0.901	0.812		
	S3	−0.457	−0.209		
	S4	−0.650	−0.423		
Personal Innovativeness	PI1	0.815	0.665	0.892	0.734
	PI2	0.884	0.782		
	PI3	0.871	0.756		
Behavioural intention	BI1	0.931	0.867	0.917	0.847
	BI2	0.909	0.826		
Adoption Intention	AI1	0.927	0.853	0.922	0.856
	AI2	0.924	0.854		

values that are above its threshold have demonstrated high level of internal consistency.

3.3.6 Convergent validity

To explore convergent validity of the mode, average variance extracted (AVE) are examined. It has been found that all the AVE values that are presented in Table 7, are greater than its threshold value of 0.5. Therefore, this result has confirmed that convergent validity of the proposed model.

3.3.7 Discriminant validity

Fornell and Larcker [60] stated that the square root of AVE in each latent variable can be used to establish discriminant validity, if this value is larger than other correlation values among the latent variables. Therefore, the results of the Fornell and Lacker's analysis that have been presented diagonally in Table 8 have exceeded its standard threshold value of 0.50, which confirms the discriminant is well established in the model.

Table 8 Discriminant Validity through Fornell & Lacker's Analysis

Latent Variable	AI	BI	PI	SEC
AI	0.925			
BI	0.748	0.920		
PI	0.597	0.452	0.857	
SEC	0.511	0.451	0.416	0.751

Table 9 T-value Significance

Latent Variable	Original Sample	Sample Mean	Standard Error	T-statistics	P-value
BI -> AI	0.554	0.551	0.064	8.668	0.000
PI -> AI	0.287	0.288	0.058	4.980	0.000
SEC -> AI	0.142	0.143	0.057	2.498	0.013
SEC -> BI	0.451	0.452	0.051	8.824	0.000
SEC -> PI	0.416	0.422	0.053	7.856	0.000

3.3.8 Structural path significance

To investigate the significance of inner and outer models, T-statistic values are generated through bootstrap procedure in SmartPLS. During the execution of bootstrap procedure, 5000 samples were taken from the original samples for the purpose of this study. Thereafter, bootstrap procedure has generated an approximate T-statistics values that to be used in this study.

It can be seen from Table 9 that all the T-statistic values have exceeded the standard threshold value of 1.96. This result confirms the outer loading of the proposed model are highly significant, and the validity of the hypotheses. Therefore, we can confirm that the hypotheses that have been developed are true and they can be adopted.

4 Discussion

Cloud security is a vast topic with different types of threats that have to be dealt with by having several security measures put in place. The Cloud is generally used by customers to transmit and store data, and therefore data security is one of the biggest issues in the use of Cloud, specifically data confidentiality and privacy. Customers fear losing their data, or having sensitive data leaked, which may lead to serious issues like identity theft. Data security involves protecting the customers' data all across the data life cycle starting from data input to data transfer and data destruction, with each phase requiring unique security measures. Table 10 presents the key findings of this review that can be derived in this study in relation to the protection of data confidentiality and customer privacy.

The Cloud service providers are legally bound to inform their customers about exactly which data they are collecting and how that data will be used. This helps put customers at ease since they have a clear understanding of how their personal data will be used. The major threat to data confidentiality and privacy is from the employees of the Cloud service providers who have

Table 10 Key Findings

Key Findings	References
Cloud service providers face a plethora of security issues and need to implement various security measures	[12, 13, 41]
Different data security measures need to be put in place for the various phases of the data life cycle, specially to ensure data confidentiality and privacy	[36, 57]
Cloud service providers should disclose exactly what personal data will be collected and what that data will be used for, thereby maintaining privacy and confidentiality	[36]
Data should be properly encrypted so that it cannot be accessed or misused by the employees of service provider	[38, 39]
Malicious attacks from hackers need to be prevented at every stage of the data life cycle so that there is no breach of data confidentiality	[40, 43]
Cloud services have to comply with the country's legal rules, which includes disclosing customer data to the law enforcement agencies if needed	[13, 37]

access to customer data. In order to protect the data from being misused by the employees, it is necessary to have a good data encryption, which makes it difficult for employees to access the data itself, thereby ensuring privacy and data confidentiality. The Cloud data is extremely vulnerable to threats from hackers and therefore adequate security measures need to be taken to protect Cloud services from malicious attacks. Despite the importance of data confidentiality and privacy, Cloud service providers can disclose sensitive personal data to law enforcement agencies if needed.

Protecting data on the Cloud is one of the highest priorities for Cloud providers. Thus, Cloud providers must invest more time and take robust security measures such as encryption of data during transmission and storage, limiting access to the data, continues review of security threats and implementation of system audits and accountability checks to protect data on the Cloud.

Vulnerability in the Cloud network, software applications or environment are golden opportunities for hackers who wanted to gain access and control of someone else data for their personal gain. Thus, preventing vulnerabilities and protecting data from hackers is another priority for the Cloud service provider. Here, Cloud providers could consider using some of the best known vulnerability prevention strategies such as (a) separation of infrastructure and services, (b) use of data obfuscation techniques where data can be transformed to hide the real meaning of the data, and (c) hiding or separating owners' details from the data to protect the data confidentiality further.

Protecting customers' data while complying with respective laws are also challenging for every Cloud service provider. The legal and disclosure requirements vary from country to country. Thus, respective privacy and data protection laws could be used to protect data and the privacy of the Cloud users. Based on the data protection and privacy laws, it will cover only the personal data where that is locally located. However, the fundamental rule of law is conflicting with the way that Cloud architecture is designed and developed. Cloud based e-mail can be seen as a good example of this situation. Storage of personal e-mails can be stored and located anywhere in the world. If the data goes all around the world, then it will no longer be clear which data protection laws will apply to protect users' data. Regardless of current data and privacy protection provisions, some of the countries have responded proactively to protect their citizens' data in the Cloud. The Swiss government has implemented their data protection in line with European Union (EU) law, where they have identified three key components such as (a) transfer of personal data to third parties, (b) transfer personal data abroad, and (c) data security. Thus, as per Swiss data protection provision, transfer or exporting personal data is permitted where the legislation ensures that adequate data protection measures are taken to protect personal data in accordance with the Swiss legislative requirement in the country where the data is located. Most importantly, Swiss data protection provision covers the special circumstances such as where personal data need to be transferred or exported, but there is no adequate protection is provided by the country where that data going to be stored. Thus, that provision has a mandatory requirement to mention the collection of the data and the business use of collected data in a contractual agreement.

Transferring sensitive data to a third party raises more questions than any other time. However, as per EU data protection law, the service provider or data handler remains responsible for the data under their care. Furthermore, the service provider who will be looking after data is permitted to subcontract one or more third parties to process customer data on behalf of them under their instruction. However, this needs to be closely monitored, and the service provider needs to ensure that contracted third parties are processing the data as per the instructions provided by them.

Sending or storing customer data could be seen as a privacy violation. There is no evidence to argue that Cloud customers know where their data is located. Furthermore, there is less evidence to indicate that Cloud service providers are providing location specific information to their customers. Thus, this issue needs to be looked at government level, and adequate data protection provisions need to be implemented to protect personal data.

Irrespective of the location of the personal data stored, Cloud service providers are responsible to safeguard the customer personal data which they collect and store. Furthermore, Cloud service providers or data collectors are required to implement additional measures to protect data from unauthorized access, illegal data destruction, thefts or misuse of data.

5 Significance of the Study

Based on the analytical results of this study, and the path model illustrated in Figure 3, it has been revealed that some of the factors that are related to security in particular cyber-attack and reliability are insignificant, and will not be able to influence personal innovativeness, behavioural intentions or adoption intentions which were not found in previous literature. Furthermore, it has revealed that security has less strength to influence adoption intentions. However, security is highly significant and positively affects behavioural intention (0.451) than personal innovativeness (0.416). Furthermore, behavioural intention has higher effects (0.554) than personal innovativeness (0.287) which is comparatively weak towards to adoption intentions linkage. Therefore, we can conclude that security is moderately strong predictor of personal innovativeness and behavioural intention. Furthermore, behavioural intention is moderately strong predictor of adoption intentions followed by personal innovativeness. However, security has been found as a weak predictor of adoption intentions, which also not exposed in previous studies.

In addition to above findings, analysis of inner model demonstrated in Figure 3 expressed that security, personal innovativeness and behavioural intentions together can only explain 85% of the variance in adoption intention. Security can only explain 84% of variance in behavioural intention, and 73% variance of personal innovativeness. This is a significant discovery where it suggests that there are other factors (approximately 15% for adoption intentions, 26% for personal innovativeness and 85% for behavioural intention) that need to be considered during the adoption of the technology. However, despite uncaptured concerns in inner model, Figure 3 suggests that security and behavioural intentions together is more significant in influencing adoption intention of new technologies, which is also not found in previous studies.

6 Conclusion & Future Direction

With the increasing popularity of Cloud services, Cloud security and privacy issues are gaining their importance. While there are several Cloud security issues, the one that is most worrisome for customers is data security, which includes data confidentiality and privacy protection. Stringent security measures need to be used to protect the Cloud data from hacker attacks. Hackers target user data with the intention of identity theft or financial fraud, which are very serious problems. Furthermore, cloud service providers must consider using service level agreements to provide an assurance to their customers about data protection and privacy.

In this review, applicable data and privacy protection laws have been discussed briefly, which is a really important factor in the adoption or use of this Cloud computing technology. Thus, this area needs to be explored in detail in future studies.

References

[1] Mell, P., and Grance, T. (2011). The NIST definition of cloud computing: recommendations of the national institute of standards and technology. NIST Special Publication 800-145.

[2] Shayan, J., Azarnik, A., Chuprat, S., Karamizadeh, S., and Alizadeh, M. (2014). Identifying benefits and risks associated with utilizing cloud computing. *Int. J. Comput. Softw. Eng.* 3, 1–6.

[3] Hashemi, S. (2013). Cloud computing technology: security and trust challenges. *International Journal of Security, Privacy and Trust Management* 2, 1–7.

[4] Denworth, J. (2015). Adoption of cloud computing in the enterprise: The progress in 2015. Available at: http://betanews.com/2015/12/29/adoption-of-cloud-computing-in-the-enterprise-the- progress-in-2015 [Accessed on 2017/01/12].

[5] Giannakouris, K., and Smihily, M. (2016). Cloud computing – Statistics on the use by enterprises. Available at: http://ec.europa.eu/eurostat/statistics-explained/index.php/Cloud_computing_-_statistics_on_the_use_by_enterprises [Accessed 2016/12/18].

[6] Singh, I., Mishra, K. N., Alberti, A., Singh, D., and Jara, A. (2015). "A novel privacy and security framework for the cloud network services,". in *9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing,* pp. 301–305.

[7] Abuhussein, A., Bedi, H., and Shiva, S. (2012). "Evaluating security and privacy in cloud computing services: a stakeholder's perspective," in *International Conference on Internet Technology and Secured Transactions*, pp. 388–395.

[8] Tari, Z. (2014). Security and privacy in cloud computing. *IEEE Cloud Computing* 1, 54–57.

[9] Al-Jaberi, M. F., and Zainal, A. (2014). "Data integrity and privacy model in cloud computing," in *International Symposium on Biometrics and Security Technologies (ISBAST 2014)*, KL, Malaysia, pp. 280–284.

[10] Alouane, M.,and El Bakkali, H. (2015). "Security, privacy and trust in cloud computing: A comparative study," in *International Conference on Cloud Technologies and Applications*, Marrakech, Morocco, (IEEE), pp. 1–8.

[11] Xiang, T., and Bo, A. (2011). The issues of cloud computing security in high-speed railway. *Electronic and Mechanical Engineering and Information Technology* 8, 4358–4363.

[12] Subashini, S., and Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing, *Journal of Network and Computer Applications* 34, 1–11.

[13] Mukherjee, K., and Sahoo, G. (2012). A novel methodology for security and privacy of cloud computing and its use in e-Governance. In *2012 World Congress on Information and Communication Technologies*, Trivandram, India, pp. 561–566.

[14] Australian Bureau of Statistics (ABS). *Business Use of Information Technology*. Availabe at: http://www.abs.gov.au/ausstats/abs@.nsf/Primary MainFeatures/8129.0?OpenDocument [last accessed 2017/10/11].

[15] Ashktorab, V., and Taghizadeh, S. R. (2012). Security threats and countermeasures in cloud computing. *Int. J. Appl. Innov. Eng. & Manag.* 1, 234–245.

[16] Cahyani, N.D.W., Martini, B., Choo, K.K., and Al-azhar, A. (2017). Forensic data acquisition from cloud-of-things devices: windows smartphones as a case study. *Concurrency and Computation*, 29, pp. 1–16.

[17] Shahzad, A., Musa, S., Aborujilah, A., and Irfan, M.(2014). A new cloud based supervisory control and data acquisition implementation to enhance the level of security using testbed. *J. Comput. Sci.* 10, 652–659.

[18] Nguyen, N., and Khan, M. (2015). A closed-loop context aware data acquisition and resource allocation framework for dynamic data driven applications systems (DDDAS) on the cloud. *J. Syst. Softw*. 109, p. 88.

[19] Salazar, N.Y., and Jiming, H.(2012). Confidentiality and availability of data warehouses in the cloud computing system. *Indian Journal of Computer Science and Engineering*, 3, 720–730.

[20] Yau, S., An, H., and Buduru, A. (2012). An approach to data confidentiality protection in cloud environments. *International Journal of Web Services Research*, 9, 67–83.

[21] Saxena, R., and Dey, S. (2016). Cloud audit: A data integrity verification approach for cloud computing. *Procedia Computer Science*, 89, 142–151.

[22] Selvan, A., and Sujaritha, M. (2016). A survey on data security and integrity in cloud computing. *Int. J. Adv. Res. Comp. Sci.* 7, 26–30.

[23] Li, A., Tan, S., and Jia, Y. (2016). A method for achieving provable data integrity in cloud computing. *Journal of Supercomputing*, 1–8.

[24] Mohamadi, A., and Barani, S. (2015). "A review on approaches in service level agreement in cloud computing environment," in *Proceedings of the 4th Iranian Joint Congress on Fuzzy and Intelligent Systems*, Iran, (IEEE), pp. 1–4.

[25] Radha, K., Rao, T., Babu, S.M., Rao, T. and Reddy, V. (2015). Service level agreements in cloud computing and big data. *International Journal of Electrical and Computer Engineering*, 5, 158–165.

[26] Zhang, H., Ye, L., Shi, J., Du, X., and Guizani, M. (2014). Verifying cloud service-level agreement by a third-party auditor. *Security and Communication Networks*, 7, 492–502.

[27] Duncan, A.J., Creese, S., and Goldsmith, M. (2012). "Insider attacks in cloud computing. (TrustCom)," in *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, Liverpool, UK, pp. 857–862.

[28] Szefer, J., Jamkhedkar, P., Perez-Botero, D., and Lee, B. (2014). "Cyber defenses for physical attacks and insider threats in cloud computing," in *Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security*, pp. 519–524.

[29] Bleikertz, S., Kurmus, A., Nagy, Z., and Schunter, M. (2012). "Secure cloud maintenance: protecting workloads against insider attacks," in *Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security*, pp. 83–84.

[30] Pant, V. K., Prakash, J., and Asthana, A. (2015). Three step data security model for cloud computing based on RSA and steganography. *Green Computing and Internet of Things*, 490–494.

[31] Wibowo, S., Grandhi, S., Well, M., and Balasoriya, P. (2016). "A multi-criteria group decision making procedure for selecting cloud based ERP systems providers," in *The 12th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD)*, Changsha, China.

[32] Takabi, H., Joshi, J.B.D., and Gail-Joon, A. (2010). Security and privacy challenges in cloud computing environments. *IEEE Security & Privacy*, 8, 24–31.

[33] Balasooriya, P., Wibowo, S., and Wells, M. (2017). "Factors influencing Cloud technology adoption in Australian organizations," in *Proceedings of the 2nd International Conference on Information Technology*, Nakhonpathom, Thailand.

[34] Newman, N. (2014). Search, antitrust, and the economics of the control of user data. *Yale Journal on Regulation*, 31, 401–454.

[35] Scott, M. (2014). German regulator warns Google over collecting users' data. *The New York Times*, p. B2 (2014).

[36] Cox, J., and Cline, K. (2012). Parsing the demographic: the challenge of balancing online behavioral advertising and consumer privacy considerations. *Journal of Internet Law*, 15, 3–12.

[37] Chen, D., and Zhao, H. (2012). Data security and privacy protection issues in cloud computing. *Int. Conf. on Comput. Electr. Eng*. 1, 647–651.

[38] Wang, G., Liu, Q., Wu, J., and Guo, M. (2011). Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers. *Computers & Security*, 30, 320–331.

[39] Will, M., and Ko, R. (2015). A guide to homomorphic encryption. *The Cloud Security Ecosystem: Technical, Legal, Business and Management Issues*, pp. 1–34.

[40] Lanois, P. (2011). Privacy in the age of the cloud. *Journal of Internet Law*, 15, 3–17.

[41] Chou, T. S. (2013). Security threats on cloud computing vulnerabilities. *International Journal of Computer Science & Information Technology,* 5, 79.

[42] Elhai, J. D., and Hall, B. J. (2016). Anxiety about internet hacking: results from a community sample. *Computers in Human Behavior*, 54, 180–185.

[43] Huang, S.: Proposing a self-help privilege for victims of cyber attacks. *George Washington Law Review*, 82, 1229–1266.

[44] Liang, X., Shetty, S., Zhang, L., Kamhoua, C., and Kwiat, K. (2017). "Man in the cloud (MITC) Defender: SGX-Based user credential protection for synchronization applications in Cloud computing platform," in *IEEE 10th International Conference on Cloud Computing*, pp. 302–309.

[45] Rogers, E. M. (1995). *Diffusion of Innovations*, 4th ed. The Free Press, New York.

[46] Prasad, R.A.I. (1998). A conceptual and operational definition of personal innovativeness in the domain of personal innovativeness in the domain of information technology. *Information System Research*, 9, 204–215.

[47] Lu, J., Yao, J. E., and Yu, C. S. (2005). Personal innovativeness, social influences and adoption of wireless Internet services via mobile technology. *The Journal of Strategic Information Systems*, 14, 245–268.

[48] Kuo, Y. F., Yen, S. N. (2009). Towards an understanding of the behavioral intention to use 3G mobile value-added services. *Computers in Human Behavior*, 25, 103–110.

[49] Armitage, C. J. and Conner, M. (2001). Efficacy of the theory of planned behaviour: a meta-analytic review. *British Journal of Social Psychology*, 40, 471–499.

[50] Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50, 179–211.

[51] Sintonen, S., and Immonen, M. (2013). Telecare services for aging people: assessment of critical factors influencing the adoption intention. *Computers in Human Behavior*, 29, 1307–1317.

[52] Tsai, L., and Hsu, L. (2013). A study of the institutional forces influencing the adoption intention of RFID by suppliers. *Information and Management*, 50, 59–65.

[53] Haenlein, M., and Kaplan, A. M.(2004). A beginner's guide to partial least squares analysis. *Understanding Statistics*, 3, 283–297.

[54] Hair, J. F., Sarstedt, M., Hopkins, L., and Kuppelwieser, V. G. (2014). Partial least squares structural equation Modeling (PLS-SEM): An emerging tool in business research. *European Business Review*, 26, 106–121.

[55] Isma'ili, A., Li, M.J., Shen, J., and He, Q. (2016). Cloud computing adoption decision modelling for SMEs: a conjoint analysis, *International Journal of Web and Grid Services*, 12, 296–327.

[56] Völckner, F., Sattler, H., Hennig-Thurau, T., and Ringle, C. M. (2010). The role of parent brand quality for service brand extension success. *Journal of Services Research*, 13, 379–396.

[57] Rautela, S., Negi, A., and Chaudhary, P. (2015). Data security and updation of data lifecycle in cloud computing using key-exchange algorithm. *International Journal of Advanced Research in Computer and Communication Engineering,* 8, 380–386.

[58] Anderson, J. C., Gerbing, D. W., and Masters, J. C. (1998). Structural equation modeling in practice: A review and recommended two-step approach. *Psychological Bulletin*, 103, 411–423.

[59] Memon, A. F., and Rahman, I. A. (2014). SEM-PLS analysis of inhibiting factors of cost performance for large construction projects in Malaysia: perspective of clients and consultants. *The Scientific World Journal*, 1–9.

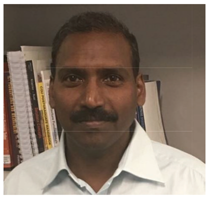
[60] Fornell, C., and Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, 39–50.

Biographies

Prasanna Balasooriya received the Masters of Information Technology (MIS) degree from Central Queensland University in Australia. His research interests include grid computing, information security, cloud computing, big data, digital transformation, and digital strategies. He has published several papers in reputed international journals. He is currently working on a project, assessing the suitability of cloud technology for local government organisations in Australia.

Santoso Wibowo is a Senior Lecturer at the School of Engineering & Technology and a member of Centre for Intelligent Systems. He holds a Master of Information Systems and a Master of Business from Central Queensland

University and RMIT University, Australia, respectively and a PhD in business information systems from RMIT University, Australia. His research interests include intelligent information systems, multi-criteria decision analysis, cloud technology and knowledge management with more than ninety refereed publications in international journals and conferences, including *Expert Systems with Applications, Computers & Industrial Engineering, Computers and Mathematics with Applications, Journal of Cleaner Production* and *Waste Management.*



S. Grandhi joined the School of Engineering & Technology as a Lecturer at Central Queensland University (CQU), Australia in 2001. Grandhi received his MBA and M.ERP degrees from Victoria University and MIS degree from Central Queensland University in Australia. His research interests include Open innovation, Clusters, Knowledge management and Enterprise systems. He received Vice Chancellor's award for Learning and Teaching for a commitment to being accessible and responsive to students' needs, enthusiasm about the area of teaching and high level of skills in practice. He also worked as a consultant for the world bank. He has published several papers in reputed international conferences, refereed journals and also participated in collaborative book chapters. He is currently working on a project, assessing technological spill-overs and open innovation in IT clusters.

Marilyn Wells is a Senior Lecturer and Head of Course for Postgraduate ICT within the School of Engineering and Technology. She holds a PhD in information systems implementation and a Masters of Information Systems, both from Western Sydney University. Her research interests are behavioural issues surrounding knowledge transfer in changing environments, particularly after implementing new organisational information systems, cloud technology implementation and ICT and strategic alignment. She currently supervises students researching in areas of cloud technology, social media forensics, ehealth, organisational learning management systems and integrating legacy systems into big data solutions.