MODELLING THE INTENTION TO ADOPT CLOUD COMPUTING SERVICES: A TRANSACTION COST THEORY PERSPECTIVE

Ogan Yigitbasioglu
School of Accountancy
Queensland University of Technology
ogan.yigitbasioglu@qut.edu.au

ABSTRACT

This paper uses transaction cost theory to study cloud computing adoption. A model is developed and tested with data from an Australian survey. According to the results, perceived vendor opportunism and perceived legislative uncertainty around cloud computing were significantly associated with perceived cloud computing security risk. There was also a significant negative relationship between perceived cloud computing security risk and the intention to adopt cloud services. This study also reports on adoption rates of cloud computing in terms of applications, as well as the types of services used.

Keywords: Cloud computing, vendor trust, security, reliability, SAAS, IAAS, PAAS

INTRODUCTION

Despite the widely publicized benefits of cloud computing, the adoption of cloud-based solutions is not as high as one would expect according to evidence from studies in Germany (Benlian & Hess, 2011), Taiwan (Low, Chen, & Wu, 2011), India, and Southeast Asia (Gupta, Seetharaman, & Raj, 2013). Also, a report by the Australian Communications and Media Authority revealed that 66% of SMEs did not utilize cloud computing services, and those that did use it mainly for webmail (Australian, 2014).

Cloud computing has for many years attracted much attention from the business press, yet it is only more recently that empirical research has started to emerge in this field. Research to date has focussed on the factors that affect the intention to adopt cloud computing services in terms of expected benefits such as cost advantages and strategic flexibility, and its risks which, among others, relate to security, performance, and the hidden costs (Alshamaila, Papagiannidis, & Li, 2013; Benlian & Hess, 2011; Lee, Chae, & Cho, 2013). Other research has looked at a number of organizational factors that engender its adoption such as business process characteristics and top management support (Low, et al., 2011; Wu, Cegielski, Hazen, & Hall, 2013).

Although, a body of knowledge on the factors that drive the intention to adopt cloud computing services is forming, evidence is scarce and is restricted to a handful of geographic regions. Furthermore, a number of other factors remain relatively unexplored such as vendor trust, the uncertainty around cloud computing legislation, and the security and reliability of the service. Also, there is little knowledge of the types of cloud computing solutions used in terms of applications and services outsourced. This study aims to address this gap using transaction cost theory (TCE) (Williamson, 1985). TCE emphasizes the lack of trust in exchange relationships, as well as the various uncertainties that surround transactions, including technological uncertainty (Sutcliffe & Zaheer, 1998). These concepts may be of relevance in explaining organisations' intention to adopt cloud computing services. The purpose of this paper is to extend our understanding of the factors that drive cloud computing adoption, as well as to provide some evidence on adoption rates from a new region, which is Australia.

From a TCE point of view, I expect to find a relation between perceived uncertainty around the legislation of cloud computing and the perceived reliability and security of the service. Also, vendor opportunism is predicted to determine the perceived reliability and security of the service. Finally, I

expect to find an association between the perceived reliability and security of the service and the intention to adopt cloud computing.

The study makes a number of contributions to the cloud computing literature. First, I examine the impact of legislative uncertainty on the perceived security and reliability of the service, whereas most studies do not focus on legislation. Second, I test for the relationship between vendor opportunism and the perceived reliability and security of the service, which has received little attention in the cloud computing literature. Third, a methodological contribution is made by developing a more comprehensive construct for cloud computing security that captures confidentiality, integrity, and availability of information.

The structure of the paper is as follows. First, cloud computing is defined, which is followed by a review of the literature, particularly empirical papers on cloud computing from business and legal perspectives. Next, hypotheses are developed and the methodology is presented. This is followed with the analysis of the data and the results. Finally, the paper is concluded with a discussion of the results, as well as the implications for research and practice.

Literature review and hypotheses development

Cloud computing is a form of IT outsourcing (ITO) where IT resources are purchased over the Internet on a pay-per-use basis (Marston, Li, Bandyopadhyay, Zhang, & Ghalsasi, 2011; Ross & Blumenstein, 2013). Cloud computing services can be classified into three distinct groups: Software as a Service (SAAS), Platform as a Service (PAAS), and Infrastructure as a Service (IAAS) (Marston, et al., 2011). Whereas SAAS enables the access to software, PAAS allows the remote development and deployment of applications. Organizations also have the option to lease computer infrastructure without receiving any vendor support which is known as IAAS (Youseff, Butrico, & Da Silva, 2008). Two types of cloud computing configurations exist: private and public clouds (Marston, et al., 2011). Private clouds are similar to the traditional in-house IT delivery model, whereby computing resources are either kept within the boundaries of the firm or alternatively, dedicated hardware are leased from a provider. In contrast, public cloud computing services use virtualization to host multiple organisations' data on a common server and the data may be moved across different countries depending on the load and traffic (Marston, et al., 2011).

Cloud computing adoption has been studied using a number of theories including the Theory, Organization, Environment Framework (TOE) (Depietro, Wiarda, & Fleischer, 1990), the Theory of Reasoned Action (TRA) (Fishbein & Ajzen, 1975), and the Diffusion of Innovation Theory (DOI) (Rogers, 2010). Drawing from the TRA framework, a study by Benlian and Hess (2011) suggested that an organisations' intention to adopt cloud computing services was associated with the perceived opportunities and risks of using the technology. Opportunities of cloud computing included cost advantages, IT quality improvements, and strategic flexibility (Benlian & Hess, 2011). On the other hand, perceived risks of cloud computing related to security, performance, loss of strategic capabilities, and the potential hidden costs of the service (Benlian & Hess, 2011). Hidden costs can arise at any stage in the outsourcing life cycle, i.e. during contracting, transition, and, managing the effort. These unexpected costs can diminish the benefit of outsourcing or, in some cases, may make it more costly to outsource (Barthelemy, 2001). Low, et al. (2011) and Alshamaila, et al. (2013) adopted the TOE framework to study cloud computing adoption and found that, among others, relative advantage, top management support, competitive pressures and innovativeness were factors that encouraged the use of cloud computing. Wu, et al. (2013) combined the DOI theory with the information processing theory (March & Simon, 1958) and reported that business process complexity and information system compatibility were negatively associated with the intention to adopt cloud services. On the other hand, entrepreneurial culture and application functionality were positively associated with cloud adoption, which also confirmed Alshamaila, et al. (2013). Other studies used PEST analysis (Lee, et al., 2013) or

no particular theory (Gupta, et al., 2013) to study cloud computing adoption. These studies confirmed Benlian and Hess (2011) but also found that legal issues around cloud computing and the lack of understanding inhibited adoption.

Transaction Cost Economics

Although, TCE has been the most frequently applied theory in the IT outsourcing (ITO) literature (Lacity, Khan, & Willcocks, 2009), only few papers have adopted it specifically to study cloud computing adoption (i.e. Benlian, 2009; Benlian, Hess, & Buxmann, 2009). TCE highlights the role of transaction costs and asset specific investments in market transactions. Transaction costs are associated with the time and effort to search, negotiate, contract, and maintain a relationship with vendors or customers (Williamson, 1985). When transaction costs become too high, TCE posits that organizations are better off to vertically integrate. One of the key issues in TCE is the distrust on the exchange partner. Trust is defined as the probability that the result of an outcome is positive for an individual/group even if no influence is exerted on the involved parties (Gamson, 1968). The problem of opportunism arises because of asset specific investments and the notion of incomplete contracts. Asset specific investments are investments by either of the parties that have little value outside the relationship. Contracts are incomplete because it is too expensive, if at all possible to specify all the possible contingencies in the contract, especially under high levels of uncertainty. Thus the concept of uncertainty is central to TCE. Williamson (1985) distinguishes between two types of uncertainties, namely primary and behavioural uncertainty. Behavioural uncertainty refers to opportunism, which is the result of incomplete contracts and the lack of trust. Primary uncertainty includes exogenous sources of uncertainty such as natural events, consumer preferences, technology, as well as regulations (Sutcliffe & Zaheer, 1998). Uncertainty according to the ITO literature is considered a deterrent to ITO (Aubert, Rivard, & Patry, 2004; Nam, Rajagopalan, Rao, & Chaudhury, 1996). Applying the TCE logic, Benlian, et al. (2009) found that application adoption uncertainty in terms of reliability, pricing and, contracting was negatively associated with the attitude toward SAAS adoption. In this study, I focus on both, behavioural uncertainty (opportunism) and a particular aspect of primary uncertainty: the uncertainty around the legislation of cloud computing; a concern that has been raised in the literature (Janssen & Joha, 2011; Lee, et al., 2013; Marston, et al., 2011). I do not focus on asset specificity in this study for several reasons. Asset specificity is not relevant for IAAS as there are low switching costs associated with switching providers (Clemons & Chen, 2011). With regard to SAAS, asset specificity has relevance in so far as customized software is concerned and this relationship has already been established (Benlian, et al., 2009).

Legal concerns regarding the cloud

Cloud computing presents unique challenges for its adopters from a legal point of view. Litigation may be problematic, potentially spanning multiple national borders, with the client in one nation, the vendor in another, the data centre in a third, and the Internet service provider spanning many others (Clemons and Chen, 2011). It is important that the legal system at the vendor's location is compatible with that of the client so that it meets local regulatory requirements (Marston et al., 2011). For example, the Australian Privacy Act limits the disclosure of customer data information to third parties, which might be difficult to enforce in foreign jurisdictions (APA, 2014). Clemons and Chen (2011) discuss a number of issues that makes cloud computing problematic from a legal point of view. Also, the contractual agreements governing the various parties from the cloud provider to subcontractors and to the cloud user may complicate matters (Martin, 2010). For example, it is not clear who would be liable when data is lost or compromised, especially when cross-border jurisdiction are involved (Jaeger et al., 2008; Egwutuoha et al., 2013). Reliance on the contract for managing risk is also problematic as it is unable to "completely cover and specify the complexity of an outsourcing project" owing to the IT subject matter of the contract being "a very volatile, fast-changing asset" (Leimeister et al. 2010, p. 6). In

addition, cloud providers could include clauses in its terms of use agreements granting the cloud provider a licence to use end-user data without charge or to insert jurisdiction and choice of law clauses (Svantesson and Clarke, 2010). Also, not all cloud providers permit clients to specify the location of the data (Clemons and Chen, 2011). Therefore, the cloud may lead an organisation from compliance to noncompliance without any notice (ISACA, 2012).

Security and reliability of cloud

The security and reliability of the cloud computing service is important as IT failure is often associated with significant impact on shareholder value as demonstrated by cases such as Sobeys Inc, Sydney Water, and TJX Companies (Parent and Reich, 2009). The relevant literature has expressed some concerns around cloud computing security (Grobauer, Walloschek, & Stocker, 2011; Gupta, et al., 2013; Marston, et al., 2011) which is known to affect its adoption (Benlian & Hess, 2011; Lee, et al., 2013). Security refers to the confidentiality, integrity, and availability of a system (Gordon & Loeb, 2002). There are advantages and disadvantages of cloud computing from a security point of view. Firstly, reputable and third party audited cloud computing providers such as Google and Amazon are likely to have better IT security than most other organisations. Large cloud computing vendors invest millions, if not billions of dollars into their IT architecture in terms of software and hardware to gain the trust of their clients. Cloud providers' data centres are also more likely to be better protected than an 'average' organisation's IT infrastructure. Furthermore, many large cloud vendors have data centres scattered around the world and mirror the data for additional backup (Egwutuoha, et al., 2013; Wu, 2011).

On the other hand, because of virtualization, when a virtual machine (VM) is compromised, access to other VMs on the same physical server is highly likely (Bizarro & Garcia, 2013). Also, from a confidentiality point of view, clients may be concerned that cloud computing vendors may be required to disclose information to their own governments as in the case of the Patriot Act (Zhou, Zhang, Xie, Qian, & Zhou, 2010). Thus, organisations may fail to comply with the Australian Privacy Act, which can result in large fines, as well as reputational drawbacks.

Concerns with respect to the reliability and bandwidth associated with the provision of applications was also raised in the literature (Benlian, et al., 2009; Smith & Kumar, 2004). Reliability of an information system refers to the availability of the system (Kim, Lee, & Ham, 2013). Availability is important because organizations have become increasingly dependent on their IT infrastructure. A temporary disruption to an organizations' IT infrastructure will in most cases result in financial loss, as well as damage to reputation. Also, because cloud computing relies on the Internet, connectivity problems could lead to service disruptions. This could be the Internet third party provider or the cloud service provider experiencing connectivity problems, rendering the service unavailable. For example, in 2009, Microsoft Azure, which is Microsoft's IAAS and PAAS service offering, went down for 22 hours. This happened again in 2013, when the services were unavailable for at least 8 hours (Parnell, 2013). Also, a large scale outage hit Amazon in 2011, affecting Amazon's Web Services' Elastic Compute Cloud. The outage took out popular social networking services such as Foursquare, FormSpring, Heroku, and Reddit (Winteford, 2011). Australia is especially vulnerable to power/Internet outages because of severe weather conditions.

The security of a system also affects its availability (Cooper, 2006; Hanmer, McBride, & Mendiratta, 2007; Kim, et al., 2013). Systems that are vulnerable to Distributed Denial of Service (DDoS) attacks or malicious software are unlikely to perform the required operations when compromised, which will therefore affect availability. For example, ConnectWise, Network Solutions, and Endnote experienced DDoS attacks in recent times that prevented access to the applications (Gurnee, 2013; Westervelt, 2013).

Given the lack of cloud client's understanding of the service (Lee, et al., 2013), as well as the perceived uncertainty or concerns around the legislation of cloud computing (Egwutuoha, et al., 2013; Marston, et al., 2011), I posit the following hypothesis.

> *H1: Perceived legal uncertainty is positively associated with perceived cloud computing security risk.*

Vendor opportunism in cloud

Opportunism has been studied for decades by economists concerned with the risks of contracting (Clemons & Chen, 2011). There are three types of risks associated with contracting: (i) shirking and deliberate under performance (Alchian & Demsetz, 1972; Aron, Clemons, & Reddi, 2005; Chen & Bharadwaj, 2009), (ii) poaching and the theft of intellectual property (Aron, et al., 2005; Chen & Bharadwaj, 2009; Clemons & Hitt, 2004), and (iii) opportunistic repricing, client lock-in, and vendor lock in (Aron, et al., 2005; Clemons & Row, 1992; Willcocks, Lacity, & Kern, 1999). All of these risk are relevant for the cloud computing service (Clemons & Chen, 2011). For example, a cloud vendor may shirk by deliberately under investing in server capability, creating slow-downs that can be blamed on the network (Clemons & Chen, 2011) There is also the view that cloud vendors might have an incentive to provide less processing power than specified in the SLA (Zhang, Ye, Shi, Du, & Guizani, 2013).

The role of trust has been extensively studied in the adoption of e-commerce (e.g. Gefen, Karahanna, & Straub, 2003; Hart & Saunders, 1997; Roca, García, & de la Vega, 2009; Teo & Liu, 2007) and is known to affect the success of ITO (Lee, Huynh, & Hirschheim, 2008). Trust is a critical aspect in many economic transactions and is considered a complexity reduction strategy (Luhmann, Davis, Raffan, & Rooney, 1979). The literature on trust posits that trust supports information sharing and adoption of e-commerce technologies (Hart & Saunders, 1997; Kim, Tao, Shin, & Kim, 2010; Suh & Han, 2003). Trusted vendors are not believed to act opportunistically even if contracts are considered incomplete. Research found a significant relationship between trust and security in e-commerce (Pavlou, 2003; Teo & Liu, 2007), mobile commerce (Siau & Shen, 2003), online trading systems (Roca, et al., 2009), and in e-payment systems (Kim, et al., 2010). Also Suh and Han (2003) suggests that website trust is positively associated with security. Therefore, a vendor that is likely to act opportunistically and not in the interest of the client, is likely to cause a security risk. Trust or the absence of trust does not only affect the purchase intentions directly (Gefen, 2000; Gefen, et al., 2003) but also through reduced risk (Jarvenpaa, Tractinsky, & Saarinen, 1999; Kollock, 1999). This leads to the following two hypotheses:

> *H2: Perceived vendor opportunism is positively associated with perceived cloud computing security risk.*

> *H3: Perceived vendor opportunism is negatively associated with the intention to increase the adoption of cloud computing services.*

As discussed previously, an important aspect of a system is its reliability and security irrespective of its features, look and feel. If the service is perceived to be unavailable or insecure, then users will be unable to perform their tasks. Security and reliability is therefore a determinant of the intention to use an online service (Greenberg, Li, & Wong-On-Wing, 2012; Gupta, et al., 2013; Luarn & Lin, 2005; Salisbury, Pearson, Pearson, & Miller, 2001).

> *H4: Perceived cloud computing security risk is negatively associated with the intention to increase cloud computing adoption.*

The proposed research model is shown below. In addition to the below paths, I control for size in terms of employees and turnover as size tends to affect technology adoption (Kimberly & Evanisko, 1981).

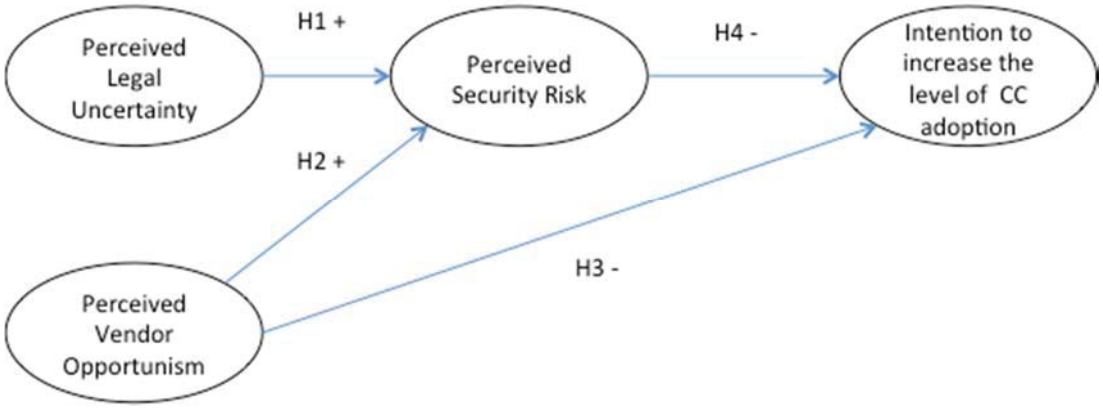

Figure 1: Research Model

METHOD

Data for this study was collected using an online survey. The questionnaire had two parts. The first part was applicable to both cloud computing users and non-users. The second part of the questionnaire was designed to capture the type of cloud computing services used. All the measures for testing the hypotheses of the study consisted of at least three indicators. The questions were answered using a 1-7 point Likert scale, where 1 represented "completely disagree" and 7 represented "completely agree".

The measure 'intention to increase the level of cloud computing adoption' was adopted from Benlian and Hess (2011). The measure 'perceived security risk' captured the availability, confidentiality and integrity of the system (Gordon & Loeb, 2002). This measure was modelled as a formative construct as it was considered to 'form' the construct and because the items were not expected to correlate highly (Bollen, 1998). For example, confidentiality of data was not expected to correlate with the uptime of the service or the Internet speed. All the other measures were modelled as reflective measures. The measures 'perceived legal uncertainty' and 'perceived vendor trust' had three indicators each and were based on previous studies (Bahli & Rivard, 2003; Benlian & Hess, 2011; Featherman & Pavlou, 2003).

Partial Least Squares Analysis (PLS) was used to test the hypothesized relationships using the SmartPLS software (Ringle, Wende, & Will, 2005). PLS is a structural equation modelling technique that has a number of advantages over covariance-based techniques such as LISREL and AMOS. PLS has fewer restrictions on the data in terms of sample size and normality (Chin, 1998). Generally, a sample size that is equal or larger than 10 times the number of indicators for the scale with the largest number of formative constructs (Chin & Newsted, 1999) is considered adequate, although smaller sizes are also acceptable (Nicolaou & Masoner, 2013; Tabachnick & Fidell, 2001).

The sample consisted of 1,170 Australian firms. The survey targeted IT decision makers. Contact details were purchased from a local e-mail list broker. A cover letter with the link to the online survey was e-mailed to the respondents in April 2014. To encourage participation, a one hundred dollar gift voucher was offered as a prize in a draw. Two weeks after the delivery of the survey, a reminder was sent to the participants. In total, 125 questionnaires were completed. Due to missing data, 5 responses were deleted resulting in 120 usable responses. The sample size was adequate based on the established rule of thumb (Chin and Newsted, 1999). The data was checked for the possibility of a response bias. The results indicated that there was not a significant difference between the early and late responders. I also tested for common method bias, which is a potential problem when the same person provides all the answers. Harman's single-factor test was carried out by entering all the measures into a factor analysis. Common method bias is present when a single factor emerges from the factor analysis or when the majority of

covariance is explained by one factor. The test revealed that this was not the case as four factors emerged that explained most of the variance (Podsakoff and Organ, 1986).

RESULTS

The majority of the respondents were senior IT managers with more than 10 years of experience in their current positions. More than 78% of the respondents' age fell between 41 and 60 years old, indicating that they were highly experienced. Many industries were represented in the final sample as evident from the distribution in Table 1. The majority of the companies had a turnover of over 100 million AUD. Also, most companies had employees above 100.

Demographic Characteristics of Respondents (n=120)	Count
Respondents Position	
CIO (CTO)	28
IT Manager	46
IT Decision Maker	17
Other	29
Sector	
Manufacturing	20
Retail	13
Financial and Insurance Services	11
Construction	11
Wholesale	10
Information, media, and telecommunications	9
Utilities	7
Other Services (real estate, professional, food etc.)	39
Turnover	
Less than 1 M	4
1 – 10 M	9
11 – 50 M	28
51 – 100 M	17
More than 100 M	62
Number of employees	
Less than 50	12
51-100	13
101-500	41
501-1000	11
More than 1,000	43

Table 1: Demographic Characteristics of Respondents

Mean values, standard deviation and Cronbach's alpha values are shown in Table 2. Higher values than 0.7 for Cronbach's alpha confirmed that the scales were reliable (Fornell and Larcker, 1981). Scale reliability is only applicable to reflective measures and therefore was not relevant to the measure 'perceived security risks', which was modelled as a formative construct (Diamantopoulos and Winklhofer, 2001). Mean values for items measuring the intention to increase the level of cloud computing adoption were fairly high in relation to other measures suggesting that organizations viewed cloud computing services as a viable alternative to in-house IT capabilities. Furthermore, relative high mean scores on the legal measures indicated that the uncertainty around the legal issues of using cloud computing was a concern for some. Internet reliability had the largest standard deviation indicating that Internet speed or connectivity varied significantly from region to region. Based on the qualitative

feedback, some of the respondents mentioned Internet connectivity as the main impediment to the adoption of cloud services. Also, one respondent mentioned that job security was a main concern if the organisation migrated to the cloud.

Measure	Item Mean 1 -7	σ	Cronbach's alpha
Intention to Increase the Level of Cloud Computing Adoption			0.929
If there are superior offers, cloud computing providers should be used for computing resources	4.97	1.48	
Our company should increase the use of cloud computing services	4.82	1.57	
I support the further adoption of cloud computing	5.27	1.48	
Perceived Vendor Opportunism			0.855
We trust cloud computing providers*	4.39	1.23	
Cloud computing providers are unlikely to act opportunistically*	3.83	1.43	
Cloud computing providers will exploit contractual loopholes to the detriment of your company	4.04	1.22	
IT contracts with cloud providers are risky	4.05	1.34	
Perceived Legal Uncertainty			0.854
In case of damage, present liability law is unclear about who will bear the damage	4.63	1.05	
The legal framework for the cloud in Australia does not sufficiently safeguard the consumer	4.69	1.13	
We are unsure of how well we would be protected in the rule of law from cloud computing failure	4.93	1.27	
Perceived Security Risks			NA
The confidentiality and security of your business data are not guaranteed when adopting cloud computing solutions	4.41	1.70	
Cloud computing is more vulnerable to information system attacks	3.73	1.45	
Our company's IT resources are more secure when compared to the cloud	4.14	1.64	
Cloud computing services aren't as reliable as in house computing resources	3.46	1.48	
Cloud computing services are unlikely to have the same uptime as local computing resources	3.32	1.51	
The Internet is not as reliable or fast enough to support our computing needs	4.09	1.83	

1 – highly disagree, 7 – highly agree
NA: Not Applicable
*Scale reverse coded

Table 2: Measures and Mean Values

I also asked adopters of cloud computing the extent of their satisfaction with the services so far. The adopters indicated that cloud services met their expectations (mean: 5.34) and that they were satisfied as evident from the high mean value (mean: 5.32).

Cloud computing in one form or another was adopted by 85 organizations, compromising about 71% of the sample. The adoption rate was significantly higher than the German study of Benlian and Hess (2011), which was 40% for SAAS. Furthermore, Gupta, et al. (2013) reported in a predominantly Asia pacific survey that only about a quarter of its respondents used IAAS or SAAS. Only three out of the 85 users used exclusively e-mail such as G-mail, suggesting that many adopters used a mixture of cloud services. Figure 2 shows the types of applications used by respondents.

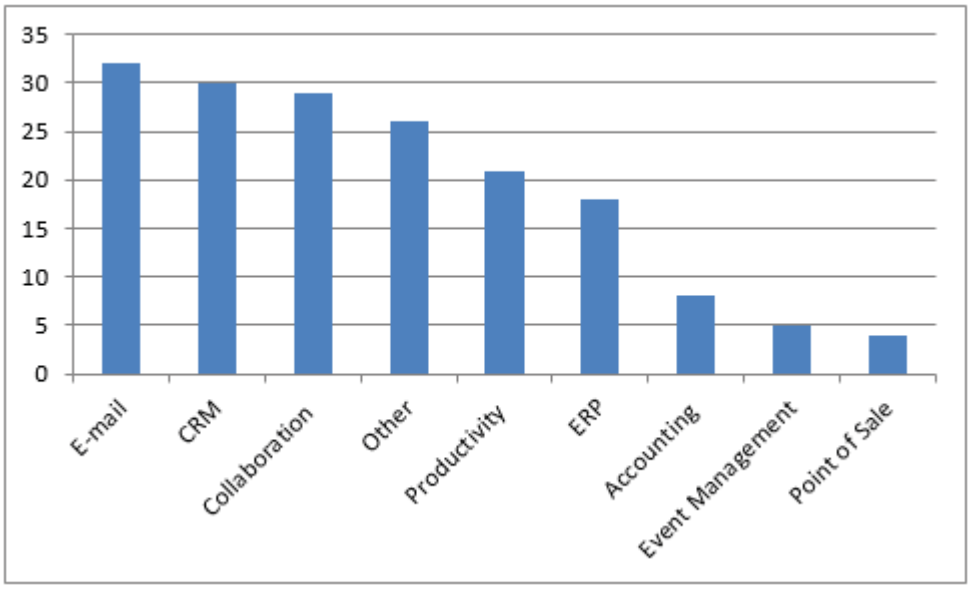

Figure 2: Types of Cloud Applications Used

Other applications included payroll, file share, various testing tools, e-mail filtering, travel management, content management, and human resource management systems. Out of the 85 cloud computing (SAAS) adopters, 24 (28%) indicated that they also used IAAS, whereas there were a total of 22 (26%) PAAS adopters. Furthermore, 54 (64%) firms indicated that their data was stored in Australia, although not exclusively. On the other hand 51 (60%) companies indicated that their data was stored abroad and only 12 (14%) had their data on premise. Figure 3 shows the adoption intentions of non-adopters. The majority had no intention of adopting cloud computing services at the time of the survey.

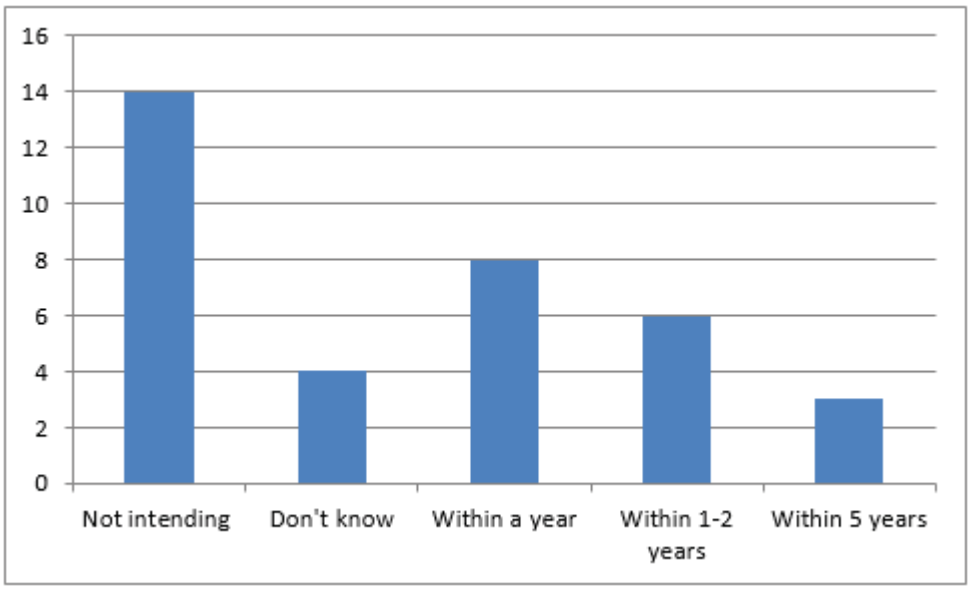

Figure 3: Non-adopters' Adoption Intention

Discriminant validity of the constructs was assessed by comparing the square root of variance (AVE) extracted with inter-construct correlations. As per Table 3, the square root of AVE values in diagonal were larger than correlations and therefore discriminate validity was met (Chin, 1998). There were weak to strong correlations, which indicated that at least some of the hypotheses were likely to be supported.

	Perc. Leg.	Perc. Oppor	Perc. Security	Intention
Perc. Leg.	0.918			
Perc. Oppor	-0.131	0.840		
Perc. Security	0.689	0.124	NA	
Intention	-0.225	-0.364	-0.489	0.938

Table 3: Construct Correlations and Square Root of AVE

Convergent validity was satisfactory as all the indicator loadings were higher than 0.7 (see Appendix 2) for reflective constructs (Fornell and Larcker, 1981). Also, according to the PLS analysis, all the hypothesized relationships were significant and the signs were as expected. R-squared for perceived security risk was 0.522, explaining more than half of the variance. Perceived security risk and perceived vendor opportunism explained more than 30% of the variance in the intention to adopt cloud services. This was considered high as the model did not include many of the perceived benefits of cloud computing that drive its adoption (Benlian and Hess, 2011; Lee et al., 2013; Gupta et al., 2013). I also found a direct relation between perceived vendor opportunism and the intention to adopt cloud computing that was highly significant. Therefore, all the hypotheses in the study were supported. In terms of the control variables, there was no significant relationship between the size of the firms and the intention to adopt cloud computing services.

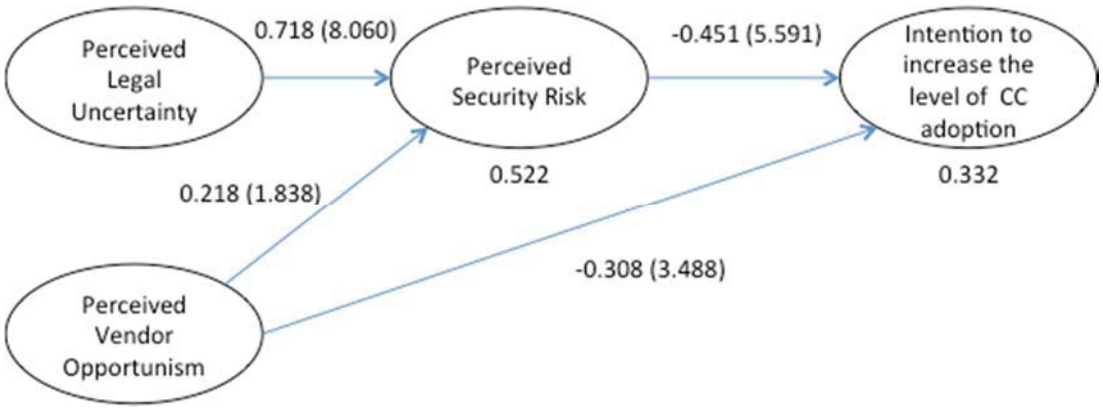

Figure 4: Path Coefficients, T-statistics, and R-squared

DISCUSSION AND CONCLUSIONS

This study applied TCE logic to the cloud computing adoption decision of organisations, a theoretical framework that has received little attention from the current cloud computing adoption literature. TCE highlights the adverse effects of uncertainty on transaction costs and differentiates between primary and behavioural uncertainty. In this study, I focused on a particular aspect of primary uncertainty, the perceived uncertainty around cloud computing legislation. Users are likely to have concerns with cloud computing legislation because liabilities may not be as clearly defined as in traditional outsourcing relationships. This is due to the nature of cloud, which involves many parties and foreign legislation (Egwutuoha, et al., 2013; Jaeger, et al., 2008; Marston, et al., 2011). The results of this study showed that the perceived legislative uncertainty around cloud computing was strongly associated with the perceived security risk of the cloud, confirming Hypothesis 1. Also, behavioural uncertainty in terms of perceived vendor opportunism was positively related to perceived security risk, although this relationship was not as significant as the direct relation to adoption. The highly significant and negative relation between perceived vendor opportunism and the intention to adopt cloud computing was consistent with previous studies (Gefen, 2000; Gefen, et al., 2003). Therefore, Hypothesis 2 and 3 were accepted, confirming a number of studies (Gefen, 2000; Gefen, et al., 2003; Jarvenpaa, et al., 1999; Knoll & Jarvenpaa, 1994). There was also a significant negative relationship between perceived security risk and the intention to adopt cloud computing services as suggested in the literature (Greenberg, et al., 2012; Gupta, et al., 2013). Therefore Hypotheses 4 was also supported.

This study makes a number of contributions. First, the results indicate that TCE logic is a powerful theoretical framework to explain an organisations intention to adopt cloud computing services just as other theoretical frameworks such as TOE, TRA, and DOI. The results also overall agree with the earlier ITO literature on the adverse effects of uncertainty on ITO (Aubert, Beaurivage, Croteau, & Rivard, 2008; Nam, et al., 1996). This study might also be of value to practitioners who are considering the adoption of cloud computing services. The results are likely to be generalizable to other geographical regions as the impact of cultural factors was considered to be low.

There are some implications of this study. Firstly, potential cloud computing adopters might be discouraged from adopting cloud services because of the associated security risk of cloud computing. While the legislation around cloud computing is still evolving, organizations might consider it more ‘safe’ to adopt services with local providers and data-centres that are subject to only local laws. Organisations may also want to consider hybrid solutions whereby only non-critical applications/data are outsourced (Goscinski & Brock, 2010; Marston, et al., 2011).

Contract negotiation and the SLA is vital and adequate diligence must be exercised to secure a favourable outcome. Clemons and Chen (2011) discuss the issues specifically around cloud computing contracts. Also, technology is improving that can automatically monitor compliance with SLAs (Zhang, et al., 2013) and check the integrity of the data on the cloud (Wang, Chow, Wang, Ren, & Lou, 2013). Furthermore, cloud vendors need to engage in trust building activities. It is commendable that some cloud service providers undergo third party assurance audits. Also, standards on cloud computing are being developed, although most of this effort does not address the problem of standardization and the vendor lock in problem (Clemons & Chen, 2011).

There are some limitations of the study. The response rate, although acceptable, was rather low. Hence, the results need to be interpreted with some caution despite the absence of a non-response bias. Also, it would be fruitful to use other theoretical frameworks and methods to study cloud computing adoption. For example, the institutional theory (DiMaggio & Powell, 1983) might present additional insight into other factors that affect adoption such as the role of fashion and fad (Abrahamson, 1991). Future research would also benefit from case studies or longitudinal studies that report on specific experiences of cloud computing migration/adoption.

REFERENCES

Abrahamson, E. (1991). Managerial fads and fashions: The diffusion and rejection of innovations. *Academy of management review*, 586-612.

Alchian, A. A., & Demsetz, H. (1972). Production, information costs, and economic organization. *The American economic review*, 777-795.

Alshamaila, Y., Papagiannidis, S., & Li, F. (2013). Cloud computing adoption by SMEs in the north east of England: A multi-perspective framework. *Journal of Enterprise Information Management, 26*(3), 250-275.

APA. (2014). Australian Privacy Act. Retrieved from Office of the Australian Information Commissioner, http://www.oaic.gov.au/privacy/privacy-resources/privacy-fact-sheets/other/privacy-fact-sheet-17-australian-privacy-principles

Aron, R., Clemons, E. K., & Reddi, S. (2005). Just right outsourcing: understanding and managing risk. *Journal of Management Information Systems, 22*(2), 37-55.

Aubert, B. A., Beaurivage, G., Croteau, A. M., & Rivard, S. (2008). Firm strategic profile and IT outsourcing. *Information Systems Frontiers, 10*(2), 129-143.

Aubert, B. A., Rivard, S., & Patry, M. (2004). A transaction cost model of IT outsourcing. *Information & Management, 41*(7), 921-932.

Australian. (2014). SMEs still scared of the cloud: ACMA. Retrieved from http://www.theaustralian.com.au/business/latest/eighty-per-cent-of-aussies-using-the-cloud-acma/story-e6frg90f-1226865028456

Bahli, B., & Rivard, S. (2003). The information technology outsourcing risk: a transaction cost and agency theory-based perspective. *Journal of Information Technology, 18*(3), 211-221.

Barthelemy, J. (2001). The hidden costs of IT outsourcing. *Mit Sloan Management Review, 42*(3), 60-+. Retrieved from <Go to ISI>://000168173400012.

Benlian, A. (2009). A transaction cost theoretical analysis of Software-as-a-Service (SaaS)-based sourcing in SMBs and enterprises.

Benlian, A., & Hess, T. (2011). Opportunities and risks of software-as-a-service: Findings from a survey of IT executives. *Decision Support Systems, 52*(1), 232-246.

Benlian, A., Hess, T., & Buxmann, P. (2009). Drivers of SaaS-adoption–an empirical study of different application types. *Business & Information Systems Engineering, 1*(5), 357-369.

Bizarro, P. A., & Garcia, A. (2013). VIRTUALIZATION: BENEFITS, RISKS, AND CONTROL. *Internal Auditing, 28*(4), 11-18.

Bollen, K. A. (1998). *Structural equation models*: Wiley Online Library.

Chen, Y., & Bharadwaj, A. (2009). An empirical analysis of contract structures in IT outsourcing. *Information Systems Research, 20*(4), 484-506.

Chin, W. W. (1998). The partial least squares approach for structural equation modeling.

Chin, W. W., & Newsted, P. R. (1999). Structural equation modeling analysis with small samples using partial least squares. *Statistical strategies for small sample research, 1*(1), 307-341.

Clemons, E. K., & Chen, Y. (2011). Making the decision to contract for cloud services: managing the risk of an extreme form of IT outsourcing. In *System Sciences (HICSS), 2011 44th Hawaii International Conference on* (pp. 1-10): IEEE.

Clemons, E. K., & Hitt, L. M. (2004). Poaching and the misappropriation of information: Transaction risks of information exchange. *Journal of Management Information Systems, 21*(2), 87-107.

Clemons, E. K., & Row, M. C. (1992). Information technology and industrial cooperation: the changing economics of coordination and ownership. *Journal of Management Information Systems, 9*(2), 9-28.

Cooper, C. (2006). The True Cost of Outsourcing. *Charter, 77*, 20-22.

Depietro, R., Wiarda, E., & Fleischer, M. (1990). The context for change: Organization, technology and environment. *The processes of technological innovation*, 151-175.

DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American sociological review*, 147-160.

Egwutuoha, I. P., Schragl, D., & Calvo, R. (2013). A Brief Review of Cloud Computing, Challenges and Potential Solutions. *Parallel & Cloud Computing, 2*(1).

Featherman, M. S., & Pavlou, P. A. (2003). Predicting e-services adoption: a perceived risk facets perspective. *International journal of human-computer studies, 59*(4), 451-474.

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention and behavior: An introduction to theory and research*.

Fornell, C., & Larcker, D. F. (1981). Structural equation models with unobservable variables and measurement error: Algebra and statistics. *Journal of marketing research*, 382-388.

Gamson, W. A. (1968). *Power and discontent* (Vol. 124): Dorsey Press Homewood, IL.

Gefen, D. (2000). E-commerce: the role of familiarity and trust. *Omega, 28*(6), 725-737.

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: an integrated model. *MIS quarterly, 27*(1), 51-90.

Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security (TISSEC), 5*(4), 438-457.

Goscinski, A., & Brock, M. (2010). Toward dynamic and attribute based publication, discovery and selection for cloud computing. *Future Generation Computer Systems, 26*(7), 947-970.

Greenberg, R., Li, W., & Wong-On-Wing, B. (2012). The effect of trust in system reliability on the intention to adopt online accounting systems. *International Journal of Accounting and Information Management, 20*(4), 363-376.

Grobauer, B., Walloschek, T., & Stocker, E. (2011). Understanding cloud computing vulnerabilities. *Security & privacy, IEEE, 9*(2), 50-57. Retrieved from http://ieeexplore.ieee.org/ielx5/8013/5739630/05487489.pdf?tp=&arnumber=5487489&isnumber=5739630.

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.

Gurnee, F. (2013). [Update] "Was not an Outage" ConnectWise Outage Denial of Service Attack to Blame? . Retrieved from http://www.lookscloudy.com/2013/03/connectwise-outage-denial-of-service-attack-to-blame/

Hanmer, R. S., McBride, D. T., & Mendiratta, V. B. (2007). Comparing reliability and security: Concepts, requirements, and techniques. *Bell Labs Technical Journal, 12*(3), 65-78.

Hart, P., & Saunders, C. (1997). Power and trust: Critical factors in the adoption and use of electronic data interchange. *Organization science, 8*(1), 23-42.

Jaeger, P. T., Lin, J., & Grimes, J. M. (2008). Cloud computing and information policy: Computing in a policy cloud? *Journal of Information Technology & Politics, 5*(3), 269-283.

Janssen, M., & Joha, A. (2011). Challenges for adopting cloud-based Software as a Service (SaaS) in the public sector.

Jarvenpaa, S. L., Tractinsky, N., & Saarinen, L. (1999). Consumer trust in an Internet store: A cross-cultural validation. *Journal of Computer-Mediated Communication, 5*(2), 0-0.

Kim, C., Tao, W., Shin, N., & Kim, K.-S. (2010). An empirical study of customers' perceptions of security and trust in e-payment systems. *Electronic Commerce Research and Applications, 9*(1), 84-95.

Kim, H.-b., Lee, D.-S., & Ham, S. (2013). Impact of hotel information security on system reliability. *International Journal of Hospitality Management, 35*, 369-379.

Kimberly, J. R., & Evanisko, M. J. (1981). Organizational innovation: The influence of individual, organizational, and contextual factors on hospital adoption of technological and administrative innovations. *Academy of management journal, 24*(4), 689-713.

Knoll, K., & Jarvenpaa, S. L. (1994). Information technology alignment or "fit" in highly turbulent environments: the concept of flexibility. In *Proceedings of the 1994 computer personnel research conference on Reinventing IS: managing information technology in changing organizations: managing information technology in changing organizations* (pp. 1-14): ACM.

Kollock, P. (1999). The production of trust in online markets. *Advances in group processes, 16*, 99-123.

Lacity, M. C., Khan, S. A., & Willcocks, L. P. (2009). A review of the IT outsourcing literature: Insights for practice. *Journal of Strategic Information Systems, 18*(3), 130-146. Retrieved from <Go to ISI>://000271333200003. doi:DOI 10.1016/j.jsis.2009.06.002

Lee, J.-N., Huynh, M. Q., & Hirschheim, R. (2008). An integrative model of trust on IT outsourcing: Examining a bilateral perspective. *Information Systems Frontiers, 10*(2), 145-163.

Lee, S.-G., Chae, S. H., & Cho, K. M. (2013). Drivers and inhibitors of SaaS adoption in Korea. *International Journal of Information Management, 33*(3), 429-440.

Low, C., Chen, Y., & Wu, M. (2011). Understanding the determinants of cloud computing adoption. *Industrial management & data systems, 111*(7), 1006-1023.

Luarn, P., & Lin, H.-H. (2005). Toward an understanding of the behavioral intention to use mobile banking. *Computers in human behavior, 21*(6), 873-891.

Luhmann, N., Davis, H., Raffan, J., & Rooney, K. (1979). *Trust; and, Power: two works by Niklas Luhmann*: Wiley Chichester.

March, J. G., & Simon, H. A. (1958). Organizations.

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing - The business perspective. *Decision Support Systems*, *51*(1), 176-189. Retrieved from <Go to ISI>://000288519200017. doi:DOI 10.1016/j.dss.2010.12.006

Nam, K., Rajagopalan, S., Rao, H. R., & Chaudhury, A. (1996). A two-level investigation of information systems outsourcing. *Communications of the ACM, 39*(7), 36-44.

Nicolaou, A. I., & Masoner, M. M. (2013). Sample size requirements in structural equation models under standard conditions. *International Journal of Accounting Information Systems*.

Parnell, B. A. (2013). Microsoft's Azure cloud down and out for 8 hours. Retrieved from http://www.theregister.co.uk/2012/02/29/windows_azure_outage/

Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: integrating trust and risk with the technology acceptance model. *International journal of electronic commerce, 7*(3), 101-134.

Podsakoff, P. M., & Organ, D. W. (1986). Self-reports in organizational research: Problems and prospects. *Journal of management, 12*(4), 531-544.

Ringle, C. M., Wende, S., & Will, S. (2005). SmartPLS 2.0 M3 Beta. *Hamburg, 2005*.

Roca, J. C., García, J. J., & de la Vega, J. J. (2009). The importance of perceived trust, security and privacy in online trading systems. *Information Management & Computer Security, 17*(2), 96-113.

Rogers, E. M. (2010). *Diffusion of innovations*: Simon and Schuster.

Ross, P., & Blumenstein, M. (2013). Cloud computing: the nexus of strategy and technology. *Journal of Business Strategy, 34*(4), 39-47.

Salisbury, W. D., Pearson, R. A., Pearson, A. W., & Miller, D. W. (2001). Perceived security and World Wide Web purchase intention. *Industrial Management & Data Systems, 101*(4), 165-177.

Siau, K., & Shen, Z. (2003). Building customer trust in mobile commerce. *Communications of the ACM, 46*(4), 91-94.

Smith, M. A., & Kumar, R. L. (2004). A theory of application service provider (ASP) use from a client perspective. *Information & management, 41*(8), 977-1002.

Suh, B., & Han, I. (2003). The impact of customer trust and perception of security control on the acceptance of electronic commerce. *International Journal of electronic commerce, 7*, 135-161.

Sutcliffe, K. M., & Zaheer, A. (1998). Uncertainty in the transaction environment: an empirical test. *Strategic Management Journal, 19*, 1-23.

Svantesson, D., & Clarke, R. (2010). Privacy and consumer risks in cloud computing. *Computer Law & Security Review, 26*(4), 391-397.

Tabachnick, B. G., & Fidell, L. S. (2001). Using multivariate statistics.

Teo, T. S., & Liu, J. (2007). Consumer trust in e-commerce in the United States, Singapore and China. *Omega, 35*(1), 22-38.

Wang, C., Chow, S. S., Wang, Q., Ren, K., & Lou, W. (2013). Privacy-preserving public auditing for secure cloud storage. *Computers, IEEE Transactions on, 62*(2), 362-375.

Westervelt, R. (2013). DDoS Attack Behind Latest Network Solutions Outage. Retrieved from http://www.crn.com/news/security/240158492/ddos-attack-behind-latest-network-solutions-outage.htm

Willcocks, L. P., Lacity, M. C., & Kern, T. (1999). Risk mitigation in IT outsourcing strategy revisited: longitudinal case research at LISA. *The Journal of Strategic Information Systems, 8*(3), 285-314.

Williamson, O. (1985). The economic institutions of capitalism. *Journal of Economic*.

Winteford, B. (2011). Growing pains: Amazon EC2 suffers huge outage. *itNews*. Retrieved from http://www.itnews.com.au/News/255549,growing-pains-amazon-ec2-suffers-huge-outage.aspx/1

Wu, W.-W. (2011). Mining significant factors affecting the adoption of SaaS using the rough set approach. *Journal of Systems and Software, 84*(3), 435-441.

Wu, Y., Cegielski, C. G., Hazen, B. T., & Hall, D. J. (2013). Cloud Computing in Support of Supply Chain Information System Infrastructure: Understanding When to go to the Cloud. *Journal of Supply Chain Management, 49*(3), 25-41.

Youseff, L., Butrico, M., & Da Silva, D. (2008). Toward a Unified Ontology of Cloud Computing. *Gce: 2008 Grid Computing Environments Workshop*, 42-51. Retrieved from <Go to ISI>://000265406000006.

Zhang, H., Ye, L., Shi, J., Du, X., & Guizani, M. (2013). Verifying cloud service-level agreement by a third-party auditor. *Security and Communication Networks*.

Zhou, M., Zhang, R., Xie, W., Qian, W., & Zhou, A. (2010). Security and privacy in cloud computing: A survey. In *Semantics Knowledge and Grid (SKG), 2010 Sixth International Conference on* (pp. 105-112): IEEE.

APPENDIX 1: LIST OF ABBREVIATIONS

AVE: Average Variance Extracted

CRM: Customer Relationship Management

DDoS: Distributed Denial of Service

DOI: Diffusion of Innovation Theory

ERP: Enterprise Resource Planning

IAAS: Infrastructure as a Service

ITO: Information Technology Outsourcing

NA: Not Applicable

PAAS: Platform as a Service

PLS: Partial Least Squares Analysis

SAAS: Software as a Service

SLA: Service Level Agreement

TCE: Transaction Cost Economics

TOE: Theory, Organization, Environment Framework

TRA: Theory of Reasoned Action

VM: Virtual Machine

APPENDIX 2: LOADINGS (WEIGHTS) AND COMPOSITE RELIABILITY

Indicator	Loadings (Weights)	Composite Reliability*
		0.942007
Perc. Leg. 1	0.905124	
Perc. Leg. 2	0.937834	
Perc. Leg. 3	0.913027	
		0.905261
Perc. Oppor. 1	0.934447	
Perc. Oppor. 2	0.903513	
Perc. Oppor. 3	0.789799	
Perc. Oppor. 4	0.717839	
		NA
Perc. Security 1	(0.514163)	
Perc. Security 2	(-0.018728)	
Perc. Security 3	(0.241093)	
Perc. Security 4	(0.319523)	
Perc. Security 5	(-0.176165)	
Perc. Security 6	(0.352393)	
		0.958477
Intention 1	0.935844	
Intention 2	0.944483	
Intention 3	0.941858	

NA: Not Applicable to formative constructs
*Threshold for Composite Reliability: 0.7