Winter 12-13-2014

Security and Privacy Concerns for Australian SMEs Cloud Adoption

Ishan Senarathna
Deakin University

Matthew Warren
Deakin University

Williay Yeoh
Deakin University

Scott Salzman
Deakin University

Security and Privacy Concerns for Australian SMEs Cloud Adoption

Ishan Senarathna
Deakin University, Australia

Matthew Warren
Deakin University, Australia

Williay Yeoh
Deakin University, Australia

Scott Salzman
Deakin University, Australia

Abstract

Cloud Computing has become increasingly important for Small and Medium-sized Enterprises because of its cost-effective benefits. However, the adoption of Cloud Computing over the recent years raised challenging issues with regard to privacy and security. In this study, we explored and presented the findings of the influence of privacy and security on Cloud adoption by SMEs. Based on a survey of SMEs across Australia, we analysed the data using structural equation modelling. We found that Cloud privacy and Cloud security are major concerns for SMEs to adopt Cloud computing. The study findings are useful for IT practitioners and regulatory bodies to understand how SMEs consider privacy and security issues for Cloud adoption.

Keywords: Cloud Computing, Privacy, Security, SMEs, Australia.

INTRODUCTION

Cloud Computing is an increasingly important area in the development of business services. Gartner Consulting defines Cloud Computing as "a style of computing in which scalable and elastic IT-enabled capabilities are delivered as a service using Internet technologies" (Plummer, Smith, Bittman, Cearley, Cappuccio, Scott, Kumar and Robertson, 2009). Cloud Computing provides different types of services delivered under different deployment models on demand, and uses a pay-as-you-go method.

Cloud Computing is a cost-effective IT solution which can benefit small, medium, and larger organisations as well as governments and public services.

Cloud Computing will potentially revolutionise the entire Information Communication Technology (ICT) industry (Tuncay, 2010). The Australian Cloud Computing market is forecasted to reach US$3. 33 billion in 2016 (Philsandberg, 2012). Further, the KPMG estimates that the increased adoption of cloud services in Australian firms could boost the Australian economy by US$3.32 billion a year (Bold, 2014).

Cloud Computing is a new business model in terms of economy and flexibility, which is particularly valuable for Small and Medium-sized Enterprises (SMEs), as Cloud Computing can be adopted with limited investment in infrastructure (Mudge, 2010). Cloud Computing is commercially viable for many SMEs due to its flexibility and pay-as-you-go cost structure (Sultan, 2011), however, within the SME sector and despite the potential benefits, the adoption rate of Cloud Computing is still relatively low in Australia compared to other countries in the Asian region (ACCA, 2012). This study investigates security and privacy concerns when adopting Cloud Computing by SMEs in Australia.

Cloud Computing Services

Three service models are extensively used by the Cloud Computing community to categorise Cloud Computing services (Ahuja and Rolli, 2011; Dillon, Wu and Chang, 2010; George and Shyam, 2010). Cloud Computing provides software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS) on demand and pay-as-you-go. SaaS in Cloud Computing eliminates the need to install and run an application on the client's computer (Marston, Bandyopadhyay, Zhang and Ghalsasi, 2011). In addition, it is not necessary to worry about software licensing nor upgrading to the latest versions. According to Sullivan (2010), there are various types of services that come under Software as a Service (SaaS), namely, Customer Relationship Management (CRM), video conferencing, IT service management, accounting, web analytics, and web content management etc. Similarly, application design, development, testing, deployment, hosting are services provided by Platform as a Service (PaaS). The development and deployment of applications without the cost and complexity of buying and managing the underlying hardware and software layers are facilitated by PaaS (Marston *et al*., 2011). Further, Sullivan (2010) explains that Infrastructure as a Service (IaaS) provides services such as server space, networking (N/W) equipment, memory, storage space and computing capabilities.

Cloud Computing Deployment Models

In reviewing the literature, services provided by Cloud Computing can be categorised according to the level of service and the way they are provided. Deployment models are recorded based on these characteristics. More recently, four Cloud Computing deployment models have been defined in the Cloud Computing community (Dillon, *et al*., 2010; Sasikala, 2011).

A public Cloud Computing service model is available from a third-party service provider via the Internet. It is a cost-effective way to deploy IT solutions and provides many benefits such

as being elastic and service-based. Public cloud is the commonly used model and is suitable especially for SMEs because it provides almost immediate access to hardware resources, with no upfront capital investments for users, leading to a faster time to market in many businesses. This treats IT as an operational expense rather than a capital expense ('Opex' as opposed to a 'Capex' model) (Marston *et al*., 2011). Private Cloud Computing provides greater control over the Cloud Computing infrastructure and can be managed within the organisation. Therefore, it is often suitable for large organisations as they are using larger installations (Marston *et al*., 2011). Hybrid Cloud Computing is a combination of public and private Cloud Computing models which try to address the limitations of each (Zhang, Cheng and Boutaba, 2010). The community Cloud Computing infrastructure is controlled and shared by a group of organisations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations) (Sasikala, 2011). According to Lawrence *et al*., (2010) the different business models are used in each deployment model differently.

Privacy and security issues in the Cloud

There are a number of privacy, security, and trust issues associated with the cloud including lack of user control, potential unauthorised secondary usage, data proliferation, cross border data flow and dynamic provisioning, access, availability, backup, multi-tendency, and lack of standardisation (Pearson and Benameur, 2010). This is because cloud computing providers have multiple data centres at different geographical locations in order to optimally serve consumers' needs around the world and the jurisdictions involved can be quite difficult. Moreover, transferring data stored in the cloud to other jurisdictions may violate local laws, because of in most cloud service scenarios, consumers have no idea of where there data is stored, due to the dynamic nature of the cloud (Pearson and Benameur, 2010). Therefore, legal and regulatory issues arise which require careful consideration because the physical

location of data centres determines the set of laws that can govern the management of data (Sahandi, Alkhalil and Justice, 2012). However, for SMEs in particular, greater security can actually be achieved via the use of cloud services than they have the expertise or budget to provide in-house (Pearson, 2012).

Small and Medium-Sized Enterprises (SMEs)

A number of definitions for SMEs exist, many coming from various governmental and official sources such as SME agencies, ministries, governmental institutions, and national statistical institutions or bureaus around the world. The Australian Bureau of Statistics (ABS) defines a small business as having fewer than 19 employees, whereas micro businesses have fewer than 4 employees. Medium-sized enterprises are defined as businesses with 20 to 199 employees (DIISR, 2011).

CLOUD COMPUTING ADOPTION IN SMES

Carr (2005) suggests that, in many instances, using Cloud Computing might provide the first opportunity for SMEs to try new software approaches in a cost effective manner. Often SMEs are unable to afford their own dedicated IT but have a sufficient IT budget to buy the bandwidth and pay according to their need and usage (Monika, Ashwani, Haresh, Anand, Madhvendra and Vijayshri, 2010). In a Cloud Computing environment, SMEs can reduce their capital expenditure for IT infrastructure and, instead, utilise and pay for the resources and services provided by Cloud Computing (Rittinghouse and Ransome, 2009).

As previously explained, there are various types of business models related to Cloud Computing adoption, and their application depends on the nature and size of an enterprise (Handler, Barbier and Schottmiller, 2012; Rahimli 2013). Chang *et al*., in 2013 mentioned that

a number of SMEs has followed the classification of the appropriate business models and even adopted a combination of different business models to improve performance of their businesses. According to Lawrence *et al*., (2010), all direct and indirect go-to-market models in Cloud Computing are able to cater for SMEs needs, however, they are not necessarily suitable for large enterprises because of their scale and complexity. It has been found that the current charging pattern and other aspects of Cloud Computing make it more suitable for SMEs than for larger organisations (Misra and Mondal, 2010). Further, the public Cloud service provides a more valuable service to Micro-Small Businesses (non-employer business and with 1-4 employees) as they require many of the same business services provided to large organisations even though they may have only a PC and an Internet connection (Handler et al, 2012).

In addition, the findings of Sultan (2011) and Bharadwaj & Lal (2012) suggest that Cloud Computing is likely to be a more attractive option for most SMEs because of flexible cost structures and scalability. The Cloud services are more acceptable by SMEs because of relative advantage, flexibility, and scalability features (Salleh. Teoh and Chan, 2012).

REASEARCH MODEL

Cloud Computing provides different services which are delivered under various deployment models on demand, and uses a pay-as-you-go method. In this context, Cloud security and Cloud privacy are major concerns for SMEs adopting Cloud Computing.

Cloud Privacy

At the broadest level, privacy is considered as a fundamental human right. The legislation supports the observation and enforcement of the protection of personal information as a

fundamental right (Pearson, 2012). However, privacy is not an absolute right. It always needs to be balanced against other rights and interests (Anthony, 2012). Privacy is an important issue in technological innovations, particularly when it has an online interaction. In the Cloud environment, privacy reflects a consumer's concerns about information being stored in the Cloud and accessed by other individuals anywhere in the world (Vanessa, 2014). In other words, input data for cloud services are uploaded by a user to the cloud. Typically the users' data are stored in a machine that the user does not own or control. As Abadi (2009 p.4) pointed out, "Compute power is elastic, but only if the workload is parallelizable, data is stored at an un-trusted host, data is replicated, often across large geographic distances, which are some of the cloud characteristics that make cloud fall into risks". According to a survey carried out among Chief Information Officers (CIOs) in Europe, approximately 70 per cent of CIOs were prevented from launching cloud computing solutions because of their privacy and security fears (Wijesiri, 2010). Since privacy is a leading cause of not adopting cloud solutions, the top six privacy practices required, as defined by Pearson (2009), are to: 1) minimize personal information sent to and stored in the cloud; 2) protect personal information in the cloud; 3) maximizes user control; 4) allow user choice; 5) specify and limit the purpose of data usage; and 6) provide feedback. Taking these requirements into consideration, it can be expressed that poor user control, loss of trustworthiness, and lack of transparency create most of the privacy issues.

Trust is a purely abstract and subjective term; therefore, it is ordinarily difficult to tangibly measure and effectively manage it (Sarwar and Khan, 2013). Trust arrangements between Cloud Computing service providers and users need to consider new and additional elements to cover all critical interactions (Mudge, 2010). Lack of transparency creates legal issues that are affected by the Cloud's physical location which creates difficulties in determining its jurisdiction. Because of this key issue, the Australian government is extremely concerned

about the location of outsourced personal data storage and there is a strong desire for cloud services to be only located within Australia's borders (Hutley, 2012). In other parts of the world, the European Union (EU) has privacy regulations that prohibit the transmission of some types of personal data outside the EU (Sultan, 2010).

Transferring personal data to a third party without accessing privacy issues creates huge risks of data loss, data theft, data damage, and data misuse. The Department of Finance and Deregulation in Australia has published a better practice guide to assist agencies to navigate typical legal issues in Cloud Computing agreements, with the intention of emphasizing the privacy concerns when adopting Cloud services (DFD, 2011). Later, Information Management Officer of the Australian Government has published a better practice guide "Privacy and Cloud Computing for Australian Government Agencies" to better understand how to comply with privacy laws and regulations when choosing cloud based services (IMO, 2013). This study will consider the legal issues related to Cloud services by considering the Australian privacy principles (APPs) in the privacy act reforms, published by the Victorian State Government (Anthony, 2012). This is another reason for emphasizing the importance of privacy in Cloud adoption in Australia. Therefore, this study hypothesizes that higher levels of privacy in the Cloud Computing environment, as perceived by organisation leaders, may motivate them to adopt Cloud Computing-based services.

Cloud Security

For the purpose of this paper, security means information security, maybe defined as "Preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved" (Pearson, 2012). The foundations of information security are based upon the confidentiality, integrity, availability, accountability, assurance, and resilience of information (Friedman and West, 2010). Security is defined as both the perception, or judgment, and fear

of safeguarding mechanisms for the movement and storage of information through electronic databases and transmission media (Lippert and Govindarajulu, 2006). Major issues pertaining to data security in the cloud computing environment are: data location and data transmission, data availability, data security (Mahmood, 2011), malicious insiders, outside attacks, and service disruptions (Behl, 2011). The biggest challenge with security of Cloud Computing is the delegation of confidentiality, availability, and integrity of data to a third party. The security of Cloud Computing is complicated because of the multi-tenancy of the virtualised resources (Opala, 2012). Cloud users may think that Cloud Computing simplifies security issues for users by outsourcing the responsibility to another party that is presumed to be highly skilled at dealing with them (Anthes, 2010). Industry practitioners (Chakraborty, Ramireddy, Raghu and Rao, 2010; McCabe and Hancook, 2009) have reported that security was a critical concern in the initial stages of Cloud Computing adoption. Bhayal (2011) states that Cloud security is the most important concern amongst cloud clients since the data owner does not know where the data is stored and data hosts cannot be considered as completely reliable.

A survey of CIOs and IT executives by the IDC (International Data Corporation) rated security as their main Cloud Computing concern, and almost 75 percent of respondents were worried about security (Sultan, 2010). Thus, security is one of the concerns about Cloud Computing that is delaying its adoption (Jamwal, Sambyal and Sambyal, 2011). Therefore, this study hypothesizes that higher levels of security in the Cloud Computing environment, as perceived by organisation leaders, may motivate them to adopt Cloud Computing based services.

The biggest challenge with the security of Cloud Computing is the delegation of the confidentiality, availability, and integrity of data to a third party. The security of Cloud Computing is complicated because of the multi-tenancy of the virtualised resources (Opala,

2012), and is one of the concerns about Cloud Computing that is delaying its adoption (Jamwal et al., 2011). Further, privacy is also a leading reason for not adopting cloud solutions (Pearson, 2009). According to Pearson (2009), poor user control, loss of trustworthiness, and lack of transparency creates most of the privacy issues. In addition, lack of transparency creates legal issues that are caused by the Cloud's physical location which creates difficulties in determining its jurisdiction. Because of this key issue, the Australian government is extremely concerned about the location of outsourced personal data storage and there is a strong desire for Cloud services to be only located within Australia's borders (Hutley, 2012). Frequently, SMEs are not able to invest large amounts in IT infrastructure (Foster *et al*., 2008) compared to larger organisations. However, a 2009 KPMG report on Australian lessons and experiences, shows that using Cloud Computing allows them to adopt innovative IT technologies quickly without paying upfront for capital investment (McCabe *et al.*, 2009). Cloud privacy, Cloud security and Cloud adoption and their measurement variables and relationships are shown in the research model (Figure 1). In this model, latent variables such as Cloud privacy (CP) and Cloud security (CS) are illustrated. These latent variables are measured by using three items each (e.g. CS1, CS2 etc…). Cloud adoption is the dependent variable and measured by four items. Measurement errors are denoted by e1, e2, etc.

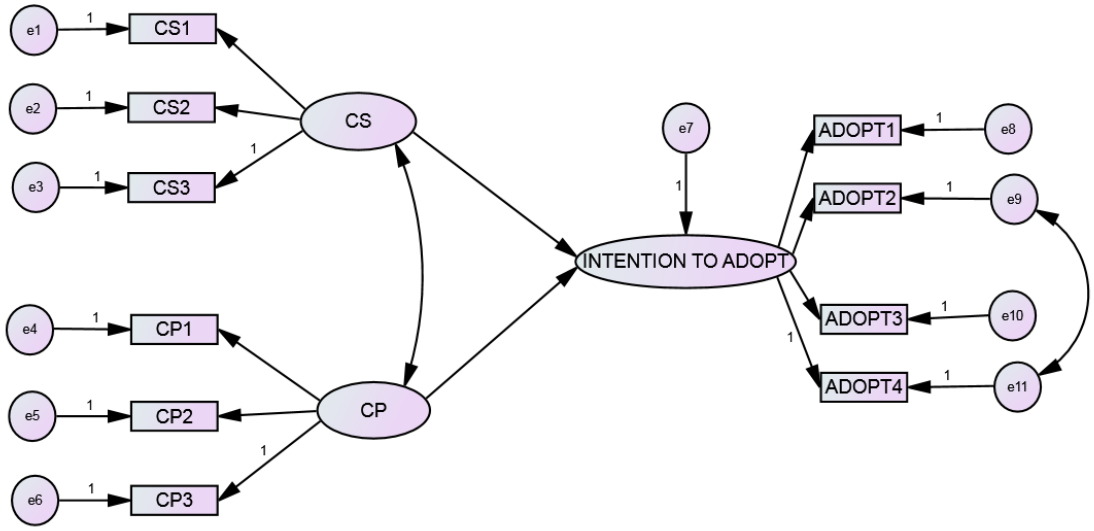

Figure 1. Research model of Cloud adoption

Based on the literature, two major adoption factors are identified for this study, namely: Cloud security and Cloud privacy. These constructs were analysed using theoretical, practitioner and government underpinnings.

RESEARCH APPROACH

A considerable amount of literature has shown that the quantitative survey method can be used effectively to evaluate the acceptance of new technologies (Flick, 2009; Jahangir and Begum, 2007; Lease, 2005). A quantitative research method will therefore be applied in this study. The survey method is chosen as an efficient way to reach larger numbers of Australian SMEs quickly, while protecting their anonymity. An in-depth examination of previous

research found that quantitative survey methodology had been successfully applied within each research study (Vanessa, 2014; Oliveira, Thomas and Espadanal, 2014).

There are three phases in the study design. In phase one, academic and practitioner literature on technology adoption, Cloud Computing and SMEs will be studied to identify the key factors for successful Cloud Computing adoption by SMEs. In phase two, a structured questionnaire will be used to collect the quantitative data from Australian SMEs. A questionnaire is the major instrument to be designed for a survey to collect data from SMEs (Tancock, Pearson and Charlesworth, 2013). Data analysis, model verification, and modifications will be conducted in phase three.

DATA COLLECTION AND ANALYSIS

Most of the cloud business models and frameworks proposed by leading researchers are quantitative (Armbrust et al., 2010 and Buyya et al., 2009). Therefore, the best method adopted in this investigation included surveys. This study will be performed using a survey data collection method and data will be collected by IT managers or decision-makers in the IT sections of selected SMEs.

Online surveys can use larger samples. The Australian Communications and Media Authority reported that 94 percent of SMEs are estimated to be connected to some form of internet service (ACMA, 2010). With this high level of internet usage by SMEs, an online survey tool is considered to be the best choice to collect data for this study, especially in Australia. The population for this study will be SMEs in Australia. The questionnaire was divided into two parts. The first part of the survey captured the demographic details of the responding organisations and the second part of the survey captured perception of the security and privacy

of Cloud Computing. For each construct, three to four questions were formulated capturing the perception and adoption of Cloud Computing by SMEs. All of the reflective indicators of a construct were measured on a 7-point Likert scale using scales from "strongly disagree" to "strongly agree". Table 1 summarises the demographic characteristics of responding organisations. The results show that 61.8% of organisations that responded were micro, 21.1% small, and 17.1% medium. Not surprisingly, states with larger populations provided higher response rates. Of the 152 organisations that responded, only 33% indicated that they were using some form of Cloud Computing.

Table 1. Demographic characteristics of responding Australian organisations

Survey participant organisations (n=152)		
No. of employees		
0 to 4 (micro)	94	61.8%
5 to 19 (small)	32	21.1%
20 to 199 (medium)	26	17.1%
State / Territory		
VIC	30	19.7%
NSW	30	19.7%
QLD	42	27.6%
WA	19	12.5%
SA	47	11.2%
TAS	11	7.2%
NT	3	2.0%

Descriptive statistics are used to summarise the basic features of data. These summary measures included measurements expressing location and dispersion. With descriptive analysis, the raw data is transformed into a form that will make it easy to understand and interpret (Zikmund 1994).

The reliability of the measurements has been verified using the cronbach's alpha coefficient. The constructs are considered adequate when the cronbach's alpha values are above the recommended value of 0.7 (Hair, Black, Babin and Anderson, 2010; Malhotra, 2010). Cronbach's alpha values exceed 0.7 for all constructs in this study (Security – 0.703, Privacy – 0.750, and Adoption – 0.993).

The hypothesis proposed in the study were tested using a structural equation modelling approach using Analysis of Moment Structures (AMOS). The model fit was evaluated with comparative fit index (CFI), root mean square error of approximation (RMSEA) and relative chi-square (CMIN/DF). These figures in the data analysis had a good model fit as the CFI was 0.985, the RMSEA was 0.073, and the CMIN/DF was 1.803 i.e. less than 3. The Figure 2 shows that Cloud security and Cloud privacy are positively related to the Cloud adoption (Path coefficient = .11 and .10 for security and privacy respectively).

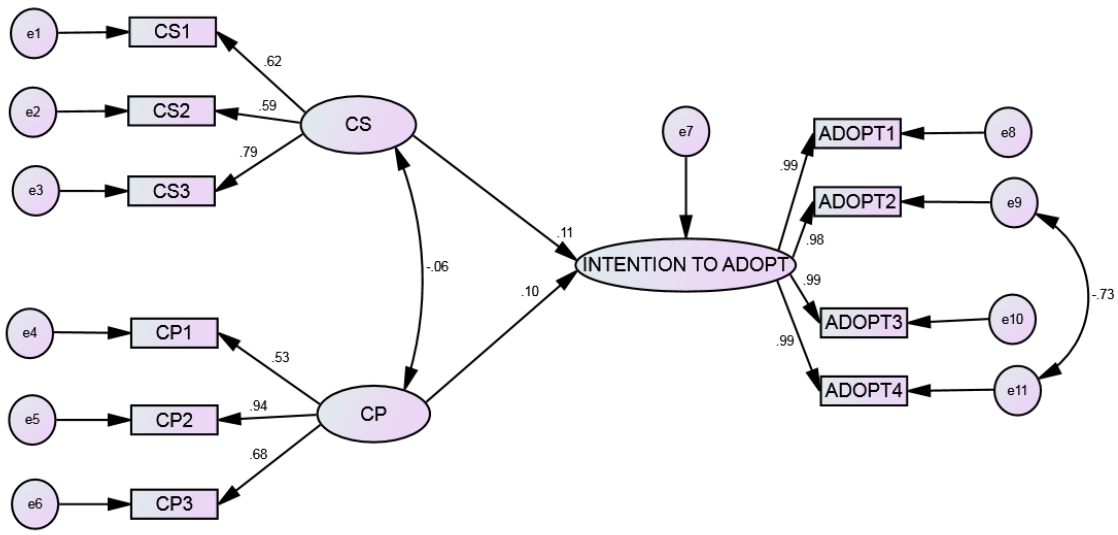

Figure 2. Results of AMOS structural model analysis

CONCLUSION

The literature indicates that the main inhibiting factor for Australian Cloud Computing adoption is the fear of dispatching organisational data to a third party. It also indicates that

public Cloud Computing is more economical when compared to private Cloud Computing, and that all business models can be used in Public Clouds. In general, therefore, it appears to be more beneficial for SMEs compared to larger organisations to adopt a Public Cloud Computing model, as it can provide them with a relatively better economic solution. Further, previous findings suggest that Cloud Computing adoption is more than just technology adoption. It includes a number of important changes such as cross-border data transfer, keeping data with a third party, remotely accessing resources and applications through the Internet and so on, which will need to be made when considering Cloud Computing adoption, but they do not necessarily apply to IT adoption. Furthermore, it is interesting to note that IT adoption mainly refers to in-house IT infrastructure, however, Cloud Computing adoption includes accessing resources outside the organisation through the Internet as a service. The study targets a specific Cloud Computing deployment method known as public Cloud Computing. It is essential for the adoption of public cloud systems that consumers and citizens are reassured that privacy and security is not compromised. This study extends the current understanding of Cloud Computing adoption by Australian SMEs (micro, small and medium enterprises) using a technology-based service adoption framework. The study suggests that security and privacy concerns influence adoption decisions in SMEs. This has implications for practitioners by indicating how consumers adopt technological innovative services. Further, it will be beneficial for consulting companies that are assisting SMEs with Cloud Computing implementation. In addition, the government could use the Cloud Computing model to assist with developing support programs and policies for Australian SMEs. It will be necessary to address the problems of privacy and security in order to provide and support trustworthy and innovative Cloud computing services. This study limited to research on public Cloud adoption. This can be extended for other deployment methods in future research. Further, the future research could build on this study by examining security

and privacy concerns for cloud adoption in different countries in both a qualitative and quantitative way as a mixed method.

REFERENCES

Abadi, D. J. 2009. "Data management in the cloud: Limitations and opportunities," *IEEE Data Engineering Bulletin* (32:1), pp 3-12.

ACCA. 2012. "Cloud Readiness Index 2012," Asia cloud computing association.

ACMA 2010. "Australia in the digital economy: The shift to the online environment."

Ahuja, S. P., and Rolli, A. C. 2011. "Survey of the State-of-the-Art of Cloud Computing," *International Journal of Cloud Applications and Computing* (1:4), pp 34-43.

Anthes, G. 2010. "Security in the cloud," *Communications of the ACM* (53:11), pp 16-18.

Anthony, B. 2012. "Forecast: Cloudy but fine," Victoria Privacy Commissioner.

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I. O. N., and Zaharia, M. 2010. "A View of Cloud Computing," Communications of the ACM (53:4), pp 50-58.

Behl, A. 2011. "Emerging Security Challenges in Cloud Computing," *IEEE international Conference Information and Communication Technologies (WICT)*).

Bharadwaj, S. S., and Lal, P. 2012. "Exploring the impact of Cloud Computing adoption on organizational flexibility: A client perspective," Cloud Computing Technologies, Applications and Management (ICCCTAM), 2012 International Conference on, IEEE2012, pp. 121-131.

Bhayal, S. 2011. *A Study of Security in Cloud Computing*, Available from ProQuest Dissertations and Theses.

Bold, D. 2014. "New tools to help small businesses adopt cloud," (available at http://www.minister.communications.gov.au/malcolm_turnbull/news/new_tools_to_help_small_businesses_adopt_cloud#.VCy1FhZpXHR).

Buyya, R., Yeo, C. S., and Venugopal, S. 2009. "Market-oriented cloud computing: Vision, hype, and reality of delivering IT services as computing utilities," in 10th IEEE International Conference on High Performance Computing and Communications, pp. 5-13.

Carr, N. G. 2005. "The end of corporate computing," *MIT Sloan Management Review* (46:3), pp 67-73.

Chakraborty, R., Ramireddy, S., Raghu, T. S., and Rao, H. R. 2010. "The information assurance practices of cloud computing vendors," *IT professional* (12:4), pp 29-37.

Chang, V., Walters, R. J., and Wills, G. 2013. "The development that leads to the Cloud Computing Business Framework," International Journal of Information Management (33:3), pp 524-538.

DFD 2011. "Negotiating the cloud – legal issues in cloud computing agreements."

DIISR 2011. "key statistics: Australian small business," Australian government.

Dillon, T., Wu, C., and Chang, E. 2010. "Cloud Computing: Issues and Challenges,"), pp 27-33.

Foster, I., Zhao, Y., Raicu, I., and Lu, S. Year. "Cloud computing and grid computing 360-degree compared," Grid Computing Environments Workshop, 2008. GCE'08, Ieee2008, pp. 1-10.

Flick, U. 2009. An introduction to qualitative research, Sage: Los Angeles.

Friedman, A. A., and West, D. M. 2010. "Privacy and Security in Cloud Computing," Center for Technology Innovation at Brookings.

George, F., and Shyam, G. 2010. "Impact of Cloud Computing: Beyond a Technology Trend," *Systems Integration*), pp 262-269.

Hair, J. F., Black, W. C., Babin, B. J., and Anderson, R. E. 2010. Multivariate data analysis, (7 ed.) Englewood Cliffs: Prentice Hall.

Handler, D. P., Barbier, J., and Schottmiller 2012. "SMB Public Cloud Adoption: Opening a Hidden Market," Cisco Internet Business Solutions Group

Hutley, N. 2012. "Modelling the economic impact of cloud computing," KPMG, pp. 1-52.

IMO 2013. "Privacy and Cloud Computing for Australian Government Agencies. Version 1.1,") February 2013.

Jahangir, N., and Begum, N. 2007. "Effect of Perceived Usefulness, Ease of use, Security and Privacy on Customer Attitude and Adaptation in the Context of E-Banking," Journal of Management Research (7:3), pp 147-157.

Jamwal, D., Sambyal, A., and Sambyal, G. S. 2011. "Cloud Computing: Its security & Privacy Aspects," *International Journal of Latest Trends in Computing* (2:1), pp 25-28.

Lawrence, M. W. L., Brad, D. C. C., Chris, C., and Denna, M. 2010. "Cloud Computing Business Models for the Channel," pp. 1-12.

Lease, D. R. 2012. "Factors influencing the adoption of biometric security technologies by decision making information technology and security managers," *Retrieved from ProQuest Digital Dissertations. (AAT 3185680)*).

Lippert, S. K., and Govindarajulu, C. 2006. "Technological, Organizational, and Environmental Antecendents to Web Service Adoption," *Communication of the IIMA* (6:1), pp 146-158.

Mahmood, Z. 2011. "Data Location and Security Issues in Cloud Computing," *IEEE International Conference on Emerging intelligent Data and Web Technologies*).

Malhotra, N. K. 2010. Marketing research: An applied orientation, Pearson Upper Saddle River, NJ.

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

McCabe, B., and Hancook, I. 2009. "Cloud computing: Australian lessons and experiences," KPMG, pp. 1-20.

Misra, S. C., and Mondal, A. 2010. "Identification of a company's suitability for the adoption of cloud computing and modelling its corresponding Return on Investment," *Mathematical and Computer Modelling* (53:3), pp 504-521.

Monika, S., Ashwani, M., Haresh, J., Anand, K., Madhvendra, M., and Vijayshri, T. 2010. "Scope of cloud computing for SMEs in India," Journal of Computing (2:5) MAY 2010, pp 144-149.

Mudge, J. C. 2010. "Cloud computing opportunities and challenges for Australia," ATSE, Melbourne, Victoria, pp. 1-34.

Oliveira, T., Thomas, M., and Espadanal, M. 2014. "Assessing the determinants of cloud computing adoption: An analysis of the manufacturing and services sectors," Information & Management (51:5), pp 497-510.

Opala, O. J. 2012. An Analysis of Security, Cost-Effectiveness, and IT Compliance Factors *Influencing Cloud Adotion by IT Managers*, Available from ProQuest Dissertations and Theses.

Pearson, S. 2009. "Taking account of privacy when designing cloud computing services," Software Engineering Challenges of Cloud Computing, 2009. CLOUD'09. ICSE Workshop on, IEEE2009, pp. 44-52.

Pearson, S. 2012. "Privacy, Security and Trust in Cloud Computing," pp. 1-57.

Pearson, S., Benameur, A. 2010. Privacy, security and trust issues arising from cloud computing. In: Cloud Computing Technology and Science (CloudCom), 2010 Second Annual International Conference, 30 Nov –3 Dec, pp. 693–702.

Philsandberg 2012. "Australia Leads Cloud Adoption in APAC," in Media in the Cloud, Frost & Sullivan

Plummer, D. C., Smith, D. M., Bittman, T. J., Cearley, D. W., Cappuccio, D. J., Scott, D., Kumar, R., and Robertson, B. 2009. ""Five refining attributes of public and private cloud computing"," *Gartner Research* (167182) 5 May 2009.

Rahimli, A. 2013. "Factors Influencing Organization Adoption Decision On Cloud Computing," *International Journal of Cloud Computing and Services Science (IJ-CLOSER)* (2:2), pp 141-147.

Rittinghouse, J. W., and Ransome, J. F. 2009. Cloud computing: implementation, management, and security, CRC Press: New York, London.

Sahandi, R., Alkhalil, A., and Justice, O. M. 2012. "SMEs' Perception of Cloud Computing: Potential and Security," in Collaborative Networks in the Internet of Services, Springer, pp. 186-195.

Salleh, S. M., Teoh, S. Y., and Chan, C. 2012. "Cloud Enterprise Systems: A Review Of Literature And Its Adoption," PASIS 2012 Proceedings2012.

Sarwar, A., and Khan, M. N. 2013. "A Review of Trust Aspects in Cloud Computing Security," *International Journal of Cloud Computing and Services Science (IJ-CLOSER)* (2:2), pp 116-122.

Sasikala, P. 2011. "Cloud Computing in Higher Education," *International Journal of Cloud Applications and Computing* (1:2), pp 1-13.

Sullivan, D. 2010. *The Definitive Guide to Cloud Computing*, (1 ed.) Realtime publishers, IBM.

Sultan, N. 2010. "Cloud computing for education: A new dawn?," *International Journal of Information Management* (30:2), pp 109-116.

Sultan, N. A. 2011. "Reaching for the "cloud": How SMEs can manage," International Journal of Information Management (31:3), pp 272-278.

Tancock, D., Pearson, S., and Charlesworth, A. 2013. "A privacy impact assessment tool for cloud computing," in Privacy and Security for Cloud Computing, Springer, pp. 73-123.

Tuncay, E. 2010. "Effective use of cloud computing in educational institutions," *Proscenia Social and Behavioral Sciences* (2), pp 938-942.

Vanessa, R. 2014. "A US-China comparative study of cloud computing adoption behavior: The role of consumer innovativeness, performance expectations and social influence," Journal of Entrepreneurship in Emerging Economies (6:1), pp 53-71.

Wijesiri, S. 2010. "Cloud computing - a new wave in IT," Daily News.

Zhang, Q., Cheng, L., and Boutaba, R. 2010. "Cloud computing: state-of-the-art and research challenges," *Journal of Internet Services and Applications* (1:1), pp 7-18.

Zikmund, W. G. 1994. *Exploring Market Research*, Dryden Press.