Managing the Risks of Data Security and Privacy in the Cloud: A Shared Responsibility between the Cloud Service Provider and the Client Organisation

Michael Lane
University of Southern Queensland
Toowoomba, Queensland, Australia
Michael.Lane@usq.edu.au

Anup Shrestha
University of Southern Queensland
Toowoomba, Queensland, Australia
Anup.Shrestha@usq.edu.au

Omar Ali
University of Southern Queensland
Toowoomba, Queensland, Australia
Omar.Ali@usq.edu.au

Keywords

Cloud Computing, Challenges, Risks, Data Security, Data Privacy

Managing the Risks of Data Security and Privacy in the Cloud: A Shared Responsibility between the Cloud Service Provider and the Client Organisation

Introduction

Cloud computing has received much attention from both industry and academia in the last 10 years and is considered to be a major paradigm shift in Information Communications and Technology (ICT) (Ren et al. 2012; Cloud Security Alliance 2016, 2017) in terms of how ICT can be delivered and managed via the 'cloud'. However, while cloud computing presents many opportunities for organisations it also presents many challenges in terms of data security and privacy (Chen & Zhao 2012; Liu et al. 2015; Singh et al. 2016). We argue in this paper that the risks associated with ensuring appropriate levels of data security and privacy at the different layers in the cloud computing stack are particularly challenging for the client organisation. This is due to (1) increasing importance of data/information for organisations and (2) the different configurations of cloud computing services and deployment models that are possible. Cloud computing services can be delivered in terms of one or more services such as infrastructure, platform and software and in terms of one or more deployment models such as public, private, hybrid and community. These different configurations of one or more cloud computing services and cloud computing deployment models mean that not one party is totally responsible for data security and privacy in a cloud computing service. We also believe that it is highly likely that many client organisations are not fully aware and do not have appropriate risk management and mitigation strategies in place for data security and privacy risks that may exist in current cloud computing services that they are using. Hence data security and privacy in cloud computing services needs to be a shared responsibility between the client organisation and the cloud computing service provider (CSP). The client organisation needs to fully aware of what are the responsibilities of their CSP(s) and are they meeting these? What are the responsibilities of the client organisation and are they meeting these? And what are shared responsibilities between the CSP(s) and the client organisation in order to ensure that appropriate data security controls are in place for cloud computing services being used.

The structure of this paper is as follows. First we define and discuss cloud computing as a concept which is internet based and consists of different types of cloud computing services and different types of deployment models. Then, we argue why data security and privacy is a critical challenge for organisations who have or are considering adopting cloud computing services via one or more cloud computing deployment models. Furthermore, the associated risks to data security and privacy in the cloud need to be managed and mitigated with appropriate controls to an acceptable level. Next, we introduce the concept of shared responsibility between the cloud service provider and client organisations for managing risks associated with data security and privacy in the cloud. Then, we describe and justify the proposed methodology for this research in progress project. Finally, we conclude this paper by highlighting the planned contributions for research and practice by highlighting importance of a shared responsibility framework for the governance of data security and privacy in cloud computing services.

Cloud Computing – Definition, Services and Deployment Models

ISO/IEC (2014) provides the following definition: 'A Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand'. Similarly, Cloud computing is defined as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction (Mell & Grance, 2011). NIST provides a comprehensive conceptualisation of cloud computing as five essential characteristics, three cloud service models and four cloud deployment models (See Figure 1) (Cloud Security Alliance 2017).

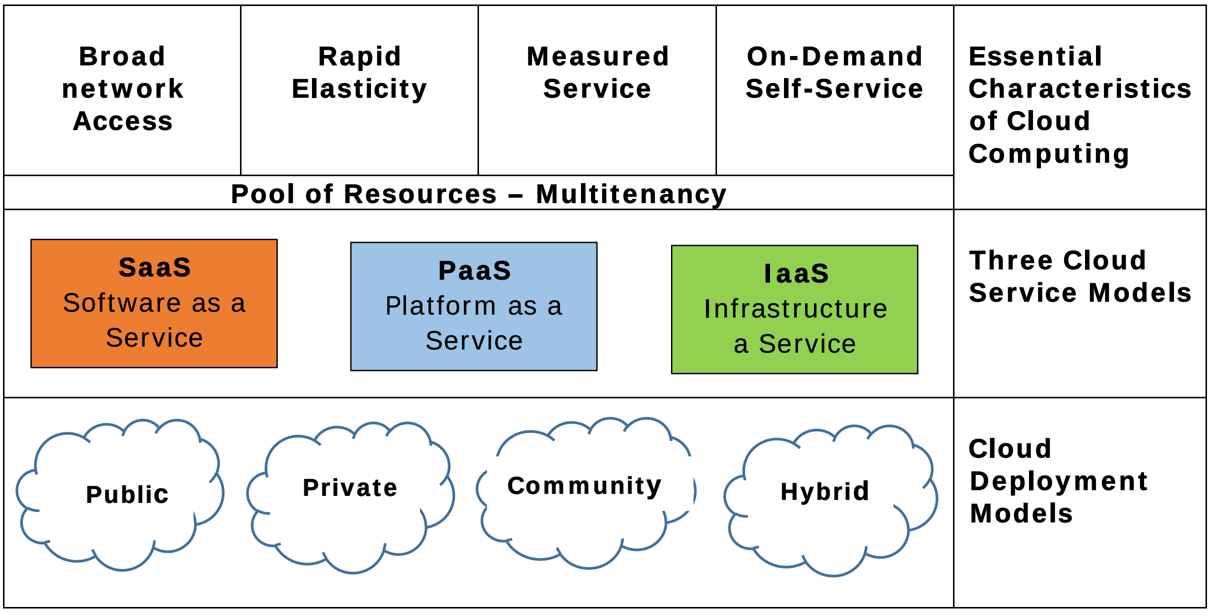

Broad network Access
Rapid Elasticity
Measured Service
On-Demand Self-Service
Essential Characteristics of Cloud Computing
Pool of Resources – Multitenancy
SaaS Software as a Service
PaaS Platform as a Service
IaaS Infrastructure a Service
Three Cloud Service Models
Public
Private
Community
Hybrid
Cloud Deployment Models

Figure 1: Cloud Computing: Essential Characteristics, Service Models and Deployment Models (Adapted from Cloud Security Alliance 2017)

Data security threats in cloud computing

Cloud Security Alliance (2013, 2016) identified a Top 9 coined as 'The Notorious Nine: Cloud Computing Top Threats in 2013' and a subsequent top 12 security threats coined as 'The Treacherous 12: Top Threats to Cloud Computing' in 2016. These are ranked in order of severity if the security threat is realised. (1) Data Breaches (2) Weak Identity, Credential and Access Management (3) Insecure APIs (4) System and Application Vulnerabilities (5) Account Hijacking (6) Malicious Insiders (7) Advanced Persistent Threats (APTs) (8) Data Loss (9) Insufficient Due Diligence (10) Abuse and Nefarious Use of Cloud Services (11) Denial of Service and (12) Shared Technology Vulnerabilities. Clearly it is evident from these cloud computing security threat rankings that data security is of paramount importance. Hussain et al. 2016 also noted that data security was a high priority particular in SaaS applications. Data Breaches are ranked number 1 in 2013 and 2016 and Data Loss is ranked 2 and 8 in both years while many of the other security threats are likely to impact on data security such as Account/Service Hijacking (may give unauthorised person access to sensitive data), Malicious Insiders (this is internal threat from CSP employees) and Misuse of Cloud Services (A CSP employees may access sensitive data of an organisation) and Shared Technology Vulnerabilities (Multi-Tenancy nature of cloud computing may exposure an organisation's data) etc. It should also be noted that Insufficient Due Diligence was ranked 8 and 9 in 2013 and 2016 and emphasises that ensuring that cloud computing is meeting an organisation's data security and privacy obligations is indeed a shared responsibility. Liu et al. 2015 and Singh et al. 2016 arrived at similar conclusion and categorised major security and privacy concerns with cloud services into loss of control, lack of transparency, virtualisation issues, multitenancy issues and management issues. They identified a number of technology and management security and privacy controls but noted that there are still many gaps in the identified areas of concern.

Google Infrastructure - Security Design Overview (2017) provides a good overview of how a cloud service provider such as Google can provide security for the different layers and service models in the cloud computing stack. Google emphasise that the security of their cloud infrastructure takes a holistic approach from physical security of data centres, to the security of cloud computing hardware and software that underpinning their cloud computing infrastructure to the physical technical and administrative security controls that are put in place to achieve preventive, detective and corrective security functionality in a cloud service (Liu et al. 2015). A detailed analysis on the data security and privacy controls provided in the cloud by prominent CSPs reveals the following matrix of different types of security controls that would need to be put in place in the different cloud services models (www.amazon.com; www.microsoft.com; www.ibm.com; www.techtalk.com).

Table 2 Mapping responsibility for data Security & privacy requirements to cloud service models: (developed from Microsoft, Techtalk, IBM, and Amazon)
C= Client; CSP = Cloud Service Provider

Responsibility	On-premise	SaaS		PaaS		IaaS	
Data Governance	C		C		C		C
Endpoints Protection	C		C		C		C
User Access Management	C		C		C		C
Identity Infrastructure	C	CSP	C	CSP	C		C
Application	C	CSP		CSP	C		C
Network Control	C	CSP		CSP	C		C
OS Security	C	CSP		CSP			C
Host	C	CSP		CSP		CSP	
Network	C	CSP		CSP		CSP	
Data Centre	C	CSP		CSP		CSP	

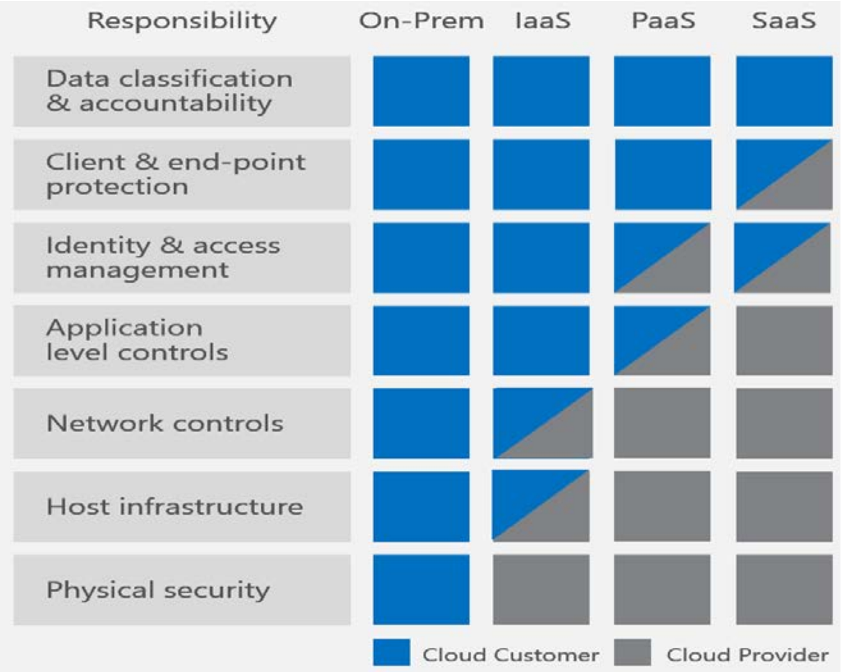
Clearly again the mapping of cloud security responsibilities between the CSP and client organisation in Table 2 demonstrates that there is an overlapping of responsibility for some of the security controls that need to be put in place. However data security and more broadly data governance is primarily the responsibility of the client organisation, although poor security or security vulnerabilities in lower levels of the cloud computing stack can obviously impact on data security and privacy. Furthermore given that data breaches, data loss and data deletion are major concerns, data classification will play increasingly important role, in determining what is the appropriate level of security and privacy for different types of data that is stored and processed in the cloud.

Shared Responsibility Framework - Managing Data Security in the Cloud

Key CSPs, such as Amazon, Google and Microsoft have already highlighted that security is a ***shared responsibility*** where they have the responsibility "of" the cloud, however users are largely responsible for security "in" the cloud (see, Amazon Shared Responsibility Model: https://aws.amazon.com/compliance/shared-responsibility-model/, Google Cloud Platform – customer responsibility matrix: https://cloud.google.com/security/ or Microsoft Azure Shared Responsibilities: https://gallery.technet.microsoft.com/Shared-Responsibilities-81d0ff91). Considerations for shared responsibilities are also provided in the US National Institute of Science and Technology (NIST) standards and PCI DSS Cloud Computing Guidelines (Grance & Jansen 2011; PCI DSS 2013).

Clearly when we examine the AWS Shared Responsibility Model (AWS 2017), their focus of responsibility is largely in IaaS. It is apparent that there is a significant onus on the customer or consumer of AWS cloud services to do their due diligence and ensure that the appropriate controls are in place to ensure appropriate level of data security and privacy particularly in PaaS and more so in SaaS and depending on the type of cloud deployment model(s) being used, this complicates matters even further.

Microsoft also view cloud services security as a shared responsibility between the CSP and the client organisation (see Figure 2) (Simorjay 2017) drawing heavily on PCI DSS 3.2 standard (PCI DSS 2017). Interestingly they see data classification and accountability as solely, the responsibility of client organisation across all three cloud services models. It is only at the lower levels of network stack that physical security, host infrastructure and network controls are primarily the responsibility of cloud service provider. While client and endpoint protection, identity and access management and application level controls are a shared responsibility the responsibility resides largely with the client organisation. Moreover with the SaaS, a larger level of responsibility is shared by the client organisation provider and progressively the CSP needs to assume great responsibility for security with PaaS and IaaS. However, clearly this shared responsibility model indicates that the responsibility for data security largely resides with the client organisation.



Responsibility	On-Prem	IaaS	PaaS	SaaS
Data classification & accountability	🟦	🟦	🟦	🟦
Client & end-point protection	🟦	🟦	🟦	◩
Identity & access management	🟦	🟦	◩	◩
Application level controls	🟦	🟦	◩	⬛
Network controls	🟦	◩	⬛	⬛
Host infrastructure	🟦	◩	⬛	⬛
Physical security	🟦	⬛	⬛	⬛

🟦 Cloud Customer ⬛ Cloud Provider

Figure 2: Shared Responsibility for Three Cloud Services Models (adopted from Simorjay 2017)

The Google Cloud Platform: Customer Responsibility Matrix (Google 2017) also emphasises that security including data security in their Google Cloud Platform is indeed a shared responsibility. Using the Payment Card Industry Data Security Standard (PCI DSS 2017) Google outline in a detailed document what are responsibilities of the GCP as a cloud service provider and the client organisation drawing on a PCI-DSS Responsibility Matrix. Google adheres to the PCI-DSS requirements set forth for a level 1 Service provider, in other words Google Cloud Platform (GCP) is required to be compliant with PCI DSS and all requirements that directly apply to a service provider. GCP is also very clear that with regard to GCP hosting of cloud services some of the PCI DSS requirements are the sole responsibility and need to be implemented by GCP, some of PCI DSS requirements are the sole responsibility and need to be implemented by the customer and whereas some are a shared responsibility and need to be implemented in part by both parties.

In this light, we propose that the principle of shared responsibility for data security and privacy in cloud computing (de Bruin & Floridi 2016) is an important perspective to be considered in applying the key principles of the Bright Internet Framework (Lee 2015, 2016). We believe that the use of cloud services by an organisation is a shared responsibility around storing potentially confidential data on a system that the organisation may not own or otherwise control (Sheppard 2014). While most cloud service providers promise that "reasonable" care is undertaken to minimize the risks to data security and privacy, the onus of doing due diligence of a cloud service provider's security practices is very much the responsibility of the organisation itself. As organisations increasingly move large parts of their enterprise ICT into the cloud it is essential that they understand the technology and security best practices that both the cloud provider and themselves can leverage to effectively minimize the risks ensuring appropriate level of security and privacy for their data. The Bright Internet initiative provides an excellent framework to lay out the principles of origin responsibility and deliverer responsibility of Internet traffic (Lee 2015, 2016). However, we believe the Bright Internet framework can be enhanced by including a shared responsibility that acknowledges the responsibility of the recipient/client organisation in the framework. A shared responsibility that includes clear expectations from the "user" side as well as the CSP will empower the Bright Internet initiative to fulfil its key goals of preventing anonymous malicious attacks from anonymous origins while maintaining freedom of expression and privacy protection in the cloud that adheres to the relevant legal jurisdictions and privacy laws.

Proposed Methodology

A Design science approach is appropriate for this research where the main aim is to design, implement and evaluate the principle of shared responsibility for the risks associated with data security and privacy in cloud computing environment. This Artefact, a shared responsibility framework for data security and privacy in cloud services will be designed from existing literature and current practice and implemented and evaluated as a comprehensive framework for solving a real world problem, proactively identifying and managing risks to data security and privacy in a range of cloud computing services (Hevner et al. 2004; Peffers et al. 2007). The Artefact will be evaluated across a range of client organisations using one or more cloud computing services via one or more cloud deployment models of one or more CSP(s).

Proposed contribution to theory and practice

Organisations will increasingly move large parts of their enterprise ICT to the cloud. However, currently many organisations do not fully understand how to ensure appropriate data governance – security and privacy in the cloud services being utilised. The problem is fundamentally shared between CSP and client organisation. The proposed shared responsibility model will provide guidance to organisations on the management and mitigation of the risks associated with ensuring an organisations' obligations to data security and privacy. This research seeks to provide organisations with an artefact - a framework for better understanding, implementing and evaluating appropriate data security and privacy controls in cloud services. This shared responsibility model will address the complexity of ensuring appropriate data security and privacy in cloud computing services which may be delivered by a range of different configurations of cloud service models and deployments. Depending the types of cloud service, the configuration of cloud service model and its deployment model, the responsibility for ensuring appropriate security and privacy of data will varying from solely the responsibility of the CSP or solely the responsibility of the client organisation to a shared responsibility of both the CSP and the client organisation.

References

Al Morsy, M., et al. (2010). An Analysis of the Cloud Computing Security Problem, pp. 1-6. APSEC 2010 Cloud Workshop, 30th Nov 2010. , Sydney, Australia.

AWS (2017). "https://aws.amazon.com/compliance/shared-responsibility-model/." Accessed on 20th September 2017, 2017, available from https://aws.amazon.com/compliance/shared-responsibility-model/.

Chen, D. and H. Zhao (2012). Data Security and Privacy Protection Issues in Cloud Computing. Proceedings of the 2012 International Conference on Computer Science and Electronics Engineering - Volume 01, IEEE Computer Society: 647-651.

Cloud Security Alliance (2017). "Security Guidance for Critical Areas of Focus in Cloud Computing." Accessed on 20th November, 2017, available from https://cloudsecurityalliance.org/download/security-guidance-v4/.

Cloud Security Alliance, C. S. (2016). "The Treacherous 12 - Top Threats to Cloud Computing." accessed on 20th October 2017, 2017, available from https://cloudsecurityalliance.org/group/top-threats/.

Cloud Security Alliance (2013). "The Notorious Nine: Cloud Computing Top Threats in 2013." accessed on 8th September 2017, 2017, available from https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf.

de Bruin, B. and L. Floridi (2017). "The Ethics of Cloud Computing." Science and Engineering Ethics **23**(1): 21-39.

Google (2017). "Google Cloud Platform: Customer Responsibility Matrix." Accessed on 10th November 2017, 2017, accessible from https://cloud.google.com/files/PCI_DSS_Shared_Responsibility_GCP_v32.pdf.

Grance, T. and W. Jansen. "Guidelines on Security and Privacy in Public Cloud Computing ". Accessed on 10th September 2017, 2017, available from https://www.nist.gov/publications/guidelines-security-and-privacy-public-cloud-computing?pub_id=909494.

Hevner, A., et al. (2004). "Design science in information systems research." MIS Quarterly **28**(1): 75-105.

Hussain, S. A., Fatima, M., Saeed, A., Raza, I. and Shahzad, R. K. (2016). "Multilevel classification of security concerns in cloud computing." Applied Computing and Informatics **13**: 57-65.

ISO/IEC (2014). ISO/IEC 17789: Information technology — Cloud computing — Reference architecture, ISO/IEC.

Lee, J. K. (2015). "Research Framework for AIS Grand Vision of the Bright ICT Initiative." MIS Quarterly **39**(2): iii-xii.

Lee, J. K. (2016). "Invited Commentary - Reflection on ICT-enabled Bright Society Research." Information Systems Research **27**(1): 1-5.

Liu, Y., Sun, Y., Ryoo, J., Rizvi, S. and Vasilakos, A. V. (2015). "A Survey of Security and Privacy Challenges in Cloud Computing: Solutions and Future Directions." Journal of Computing Science and Engineering, 9(3): 119-133.

Luo, X., Yang, L., Hao, D., Liu, F. and Wang, D. (2014). "On Data and Virtualization Security Risks and Solutions of Cloud Computing " Journal of Networks 9(3).

Mell, P. and Grance, T. 2011. The NIST Definition of Cloud Computing, accessed on October 24, 2017, available at: http://csrc.nist.gov/publications/nistpubs/800- 145/SP800-145.pdf.

Microsoft (2017). "Azure PCI DSS 3.2 Responsibility Matrix 2017." Accessed on 20th October 20107, 2017, accessible from https://gallery.technet.microsoft.com/Azure-PCI-DSS-Responsibilit-02d4b4b2.

PCI DSS (2013). "PCI DSS Cloud Computing Guidelines." Accessed on 20th October 2017, 2017, available from https://www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_Cloud_Guidelines.pdf.

Payment Card Industry (PCI) Security Standards Council (SSC) (2017). "Payment Card Industry Data Security Standard: Requirements and Security Assessment Procedures."

Accessed on 10th September 2017, 2017, available from https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf?agreement=true&time=1511829927192.

Peffers, K., Tuunanen, T., Rothenberger, MA., and Chatterjee, S. (2007). "A Design Science Research Methodology for Information Systems Research." Journal of Management Information Systems **24**(3): 45-77.

Ren, K., Wang, C. and Wang, Q. (2013). " Security Challenges for the Public Cloud." IEEE Internet Computing **16**(1): 69-73.

Sheppard, D. 2014. Is Loss of Control the Biggest Hurdle to Cloud Computing?, accessed on October 24, 2017, available at: http://www.itworldcanada.com/blog/isloss-of-control-the-biggest-hurdle-to-cloud-computing/95131

Simorjay, F. (2017). "Shared Responsibilities for Cloud Computing." Accessed on 10th August 2017, 2017, available from https://gallery.technet.microsoft.com/Shared-Responsibilities-81d0ff91.

Singh, S., Jeong, Y. S. and Park, J. H. (2016). "A Survey on Cloud Computing Security: Issues, Threats, and Solutions." Journal of Network and Computer Applications **75**(November): 200-222.