Cloud computing adoption concerns within organizations

Sunil K. Bedi
IT Lecturer
Whitireia Polytechnic
45 Pharazyn Street
Lower Hutt 5010, Wellington
(+64) 21 2200772
sunil.bedi@whitireia.ac.nz

ABSTRACT

Cloud computing is a technology that provides users with a means of storing and retrieving data anytime and from any location. Many key providers like Amazon and Microsoft are offering cloud technology for both business and personal use. While personal and non-critical business users may not be too concerned with the security and various other risks associated with the cloud computing paradigm, it seems organizations involved in the handling and management of sensitive data would consider it worthwhile to diligently investigate such issues and invest time and money to ensure any such provision to store confidential data on the cloud has been thoroughly planned and executed. Financial establishments should carefully consider factors like Data and Transport Security, Data Residency, Operational Performance, Vendor Lock-In and Jurisdiction before adopting Cloud based services.

Categories and Subject Descriptors

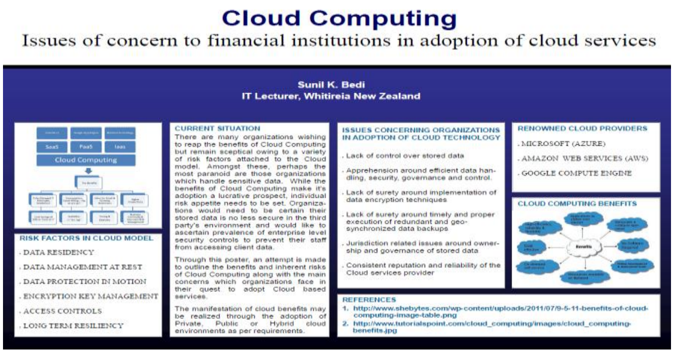
C.2.4 [**Cloud computing**]: Issues of concern to financial institutions in adoption of Cloud computing.

General Terms

Management, Measurement, Performance, Reliability, Security, Human Factors, Standardization, Legal Aspects, Verification.

Keywords

Cloud computing, risk, vulnerabilities, data integrity, issues, jurisdiction, threat, hacking, banks.



This poster paper appeared at ITX 2014, incorporating the 5th annual conference of Computing and Information Technology Research and Education New Zealand (CITRENZ2014) and the 27th Annual Conference of the National Advisory Committee on Computing Qualifications, Auckland, New Zealand, October 8-10, 2014. Mike Lopez and Michael Verhaart, (Eds).

1. INTRODUCTION

Cloud computing is 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, 2011). Cloud Computing is the industry term for delivering hosted services over a network or the internet (ODCA, 2010). It treats computing as a service rather than a product, enabling users to access and share a wide variety of applications, data and resources through an interface such as their web browser. The key features of a cloud computing entity are massive scalability to meet user needs, the existence as an abstract entity to deliver multiple service levels to outside users, economy of scale, and dynamic configuration of services on demand, often by virtualization (Foster, 2008). As a new paradigm, cloud computing is considered as a significant improvement over other computing models like the client-server of the 1990's and the older time-sharing model of the early 1970s. As an innovation, cloud computing has made possible the provision of contemporary and new computing services less expensively to a wider market (Reddy, 2011). However, Cloud based services do not come without potential risks and abuse which can become a major cause of concern, especially in case of financial organizations entrusted with the safe-keeping of confidential data.

2. BENEFITS OF CLOUD COMPUTING

The five main benefits of the cloud computing paradigm are as follows: On-demand self-service, broad network access, resource pooling, rapid elasticity and measured service. (i.) On-demand self-service: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider (Chabrow, 2011). This allows unrestricted accessibility to modify the contents of one's cloud storage space anytime and anywhere. (ii.) Broad network access: Cloud Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms such as mobile phones, laptops and PDAs (Isaca.org, 2011). This characteristic enables a user to use nearly any internet connected device to access their data from anywhere and from any time. (iii.) Resource pooling: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth (Mell & Grance, 2011). (iv.) Rapid elasticity: Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time (Chabrow, 2011). The elasticity characteristic can provide more storage space or more computing power to a user at any given time and can also reduce said space or power to accommodate for their needs. (v.) Measured service: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth and active user accounts). Resource usage can be monitored, controlled and reported, providing transparency for the provider and consumer (Chabrow, 2011). As with utilities like gas, water, or electricity, the measured service provides the user with set pricing on data usage, storage space, processing power, and other cloud uses (Isaca.org, 2011). This is the pricing characteristic of cloud computing which enables a user to accurately determine the cost of the services they are utilizing.

3. RISKS IN CLOUD COMPUTING

There are numerous risks and challenges associated with the adoption of Cloud Computing which requires serious contemplation such as network sniffing, port scanning, loss of governance over stored data, vendor lock-in risks, insecure or incomplete data deletion, as well as the lack of a universal standard for data protection along with geo-synchronized redundant backups (Gold, 2012). Ashford (2013) identified six main areas that need to be addressed are: data residency, data management at rest, data protection in motion, encryption key management, access controls, and long-term resiliency of the encryption system. These are briefly highlighted in the table below:

Table 1. Six main areas for risk mitigation in cloud computing

No.	Risk Heading	Elaboration
1	Data residency	Different host country laws can lead to data control inadequacies.
2	Data management at rest	Geo-synced redundant backups, data integrity and quality, IP protection, Data recovery.
3	Data protection in motion	Secure data transportation
4	Encryption key mgmt.	Secure and stringent encryption key management mechanism in place
5	Access controls	Service disruption, accessibility issues, high latency and load balancing issues resulting in increased response times.
6	Long-term resiliency of the encryption system	Using different encryption keys for different data sets, use of improvised algorithms and use of DES (data encryption standard).

4. CONCLUSION

Although perfect and 100% secure cloud based systems remain yet to be implemented, the above factors can contribute towards establishing a reduced risk cloud computing framework for organizations such as banks and other financial institutions whose primary concern is to safeguard sensitive data. As the cloud model evolves, it is imperative to constantly review, monitor and implement timely enhancements to the above factors. In doing so, organizations can safely and productively rely on adopting the cloud model while minimizing risk.

5. REFERENCES

[1] Mell, P., Grance, T. (2011). The NIST Definition of Cloud Computing. Retrieved from: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[2] ODCA (2010). Open Data Center Alliance. Retrieved from: http://www.opendatacenteralliance.org/ourwork/cloudcomputing

[3] Foster, I., Zhao, Y., Raicu, I., & Lu, S. (2008). Cloud computing and Grid computing 360-degree compared. Proceedings of the 2008 Grid Computing Environments Workshop, 1-10.

[4] Reddy, V. K., Reddy, L. S. S. (2011). Security architecture of cloud computing. International Journal of Engineering Science & Technology, 3(9), 7149-7155.

[5] Chabrow, Eric (2011) 5 Essential Characteristics of Cloud Computing. Retrieved from: http://www.inforisktoday.com/5-essential-characteristics-cloud-computing-a-4189

[6] Isaca.org (2011) Essential characteristics of cloud computing. Retrieved from: http://www.isaca.org/Groups/Professional-English/cloud-computing/GroupDocuments/Essential%20characteristics%20of%20Cloud%20Computing.pdf

[7] Gold, J. (2012). Protection in the cloud: Risk management and insurance for cloud computing. Journal of Internet Law, 15(12), 1-28.

[8] Ashford, W. (2013). Six security issues to tackle before encrypting cloud data. Retrieved from: http://www.computerweekly.com/news/2240180087/Six-security-issues-to-tackle-before-encrypting-cloud-data