Security in Cloud Computing
Measures to Protect Sensitive Customer Data in the Cloud

Sunil K. Bedi
Whitireia Polytechnic
Wellington
sunil.bedi@whitireia.ac.nz

ABSTRACT

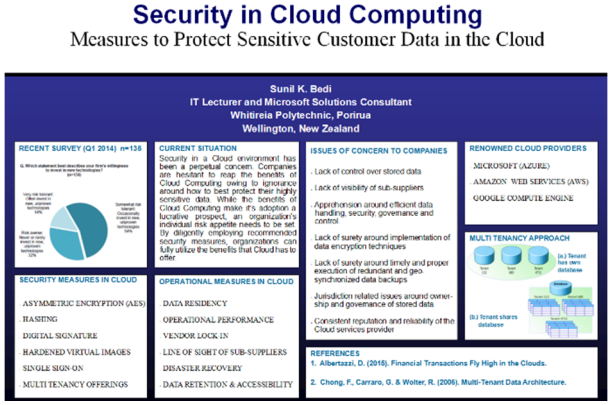
Cloud computing is a technology that provides users with a means of storing and retrieving data anytime and from any location. While a day to day user might be oblivious to the importance of security considerations in a Cloud environment, organizations involved in the management of sensitive data would consider it worthwhile to diligently implement provisions to ensure their sensitive data is not breached in any way either by the Cloud provider or while data is in transit. Financial organizations in particular seem to be paranoid by such security considerations and invest substantially to ensure the required Service Level Agreements (SLAs) along with proven security measures such as Asymmetric Encryption based on Advanced Encryption Standard (AES), Hashing, Digital Signature and Hardened Virtual Server Images etc. are in place before moving data to the Cloud provider.

Keywords: Cloud Computing, Security, Risk, Encryption, Vulnerabilities, Data Integrity, Issues, Jurisdiction, Threat, Hacking, Banks.

1. INTRODUCTION

Cloud Computing is the industry term for delivering hosted services over a network or the internet (ODCA, 2010). 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. Companies are starting to recognize and realize the benefits and advantages of Cloud computing. "Surprising enough, our risk and security gurus were comfortable with considering the Cloud for this application", Westpac's enterprise infrastructure architecture head Eugene Zaid stated (Tay, 2011). However, as with any emerging approach, there is some fear, uncertainty and concern about the technology's maturity (Leavitt, 2009).

Cloud computing has many security challenges that include network sniffing, port scanning, loss of governance whereby the service providers have more control over the data of their customers and client users, vendor lock-in risks, insecure or incomplete data deletion as well as the lack of a universal standard for data protection (Gold, 2012).



One of the predominant risks involved with Cloud computing is the data being uploaded to the service provider not being in control of the customer but being in the control of the service provider (Shrum, 2012). Such a risk can not only jeopardize an organization's invaluable data but also prove to be a huge privacy loophole. This makes Cloud service providers a high value cyber-attack target as multiple organizations can be using a single Cloud company as their primary data service (Horwath, 2012). Such issues can cause irreparable damage to an organization's reputation and financial standing should highly sensitive customer centric data is placed in possession of unauthorized users.

This poster appeared at the 6th annual conference of Computing and Information Technology Research and Education New Zealand (CITRENZ2015) and the 28th Annual Conference of the National Advisory Committee on Computing Qualifications, Queenstown, New Zealand, October 6-9, 2015. Michael Verhaart, Amit Sarkar, Rosemarie Tomlinson and Emre Erturk (Eds).

2. TECHNOLOGY MEASURES TO SAFE GUARD DATA IN THE CLOUD

The recommended technology measures to safeguard data in the Cloud are as follows: Asymmetric Encryption based on Advanced Encryption Standard (AES), Hashing, Digital Signature, Single Sign-On, Hardened Virtual Server Images and Multi Tenancy offerings by the Cloud provider. (i.) Asymmetric Encryption based on Advanced Encryption Standard (AES): In contrast to Symmetric Encryption, Asymmetric Encryption uses two separate keys – public key and private key to encrypt/decrypt the data whereas the latter uses just one shared key. As every asymmetrically encrypted message has its own private-public key pair, messages that were encrypted with a private key can be correctly decrypted by any party having the corresponding public key. Any message that has been encrypted with a public key can only be decrypted by the rightful private key owner thus providing confidentiality protection (Erl, 2013). (ii.) Hashing: The Hashing technique can be used when a one-way, non-reversible form of data protection is required such as in the case of password storage. Hashing technology can be used to derive a hashing code or message digest from a message which can be attached to the outgoing message. The recipient then applies the same hashing function to the incoming message to verify that the newly produced message digest is the same as the one attached to the message. Any alteration to the digest indicates that the message has been tampered with (Erl, 2013). (iii.) Digital Signature: The digital signature mechanism is a means of providing data authenticity and integrity through authentication and non-repudiation (Erl, 2013). In this technique, a message is a digital signature prior to transmission which is then rendered invalid if the message

experiences any subsequent unauthorized modifications. This technique uses both Hashing and Asymmetrical encryption. (iv.) Single Sign-On: This mechanism enables one Cloud service consumer to be authenticated by a security broker which establishes a security context that is persisted while the Cloud service consumer accesses other Cloud services or Cloud based IT resources thus eliminating the need to re-authenticate time and again with every subsequent request (Erl, 2013). (v.) Hardened Virtual Server Images: "Hardening" is the process of striping unnecessary software from a system to limit potential vulnerabilities that can be exploited by attackers (Erl, 2013). Default virtual machine images and software modules used by customers can be pre-hardened and updated with the latest patches and security settings according to fine-tuned processes (ENISA, 2012). (vi.) Multi Tenancy offerings by the Cloud provider: This approach warrants using a separate database for each tenant onboard with the Cloud provider. In contrast to using a shared database for multiple tenants, this approach ensures all data tables and schemas remain exclusive for each tenant thereby enhancing security from the Cloud provider.

3. LEGISLATIVE MEASURES TO SAFE GUARD DATA IN THE CLOUD

The recommended legislative measures for safe guarding data in the Cloud are as follows: (i.) Data Residency: Cloud computing arrangements may involve storing data in foreign jurisdictions and locations. When host country laws are different, or significantly less controlled than those of Australia or New Zealand, this can potentially lead to exposures or control inadequacies impacting data ownership, privacy, data return, service continuity etc. Irrespective of jurisdiction, data storage across multiple Cloud service providers could lead to data fragmentation, and issues with data ownership when terminating Cloud services (ODCA, 2014). (ii.) Operational Performance: Service Level Agreements (SLAs) in place to protect against issues like latency, workload management, limited line of sight of sub-suppliers, disaster recovery and round the clock access to data. (iii.) Vendor Lock-In: Vendor lock-in has been a perpetual challenge in IT, for example it becomes increasingly difficult to change a software product having implemented that software into a business process.

Table 1. Six Measures for Securing Data in Cloud

No.	Measure	Elaboration
1.	Asymmetric Encryption (AES)	Use of two separate keys – public key and private key to encrypt/decrypt the data.
2.	Hashing	Geo-synced redundant backups, data integrity and quality.
3.	Digital Signature	Data authenticity and integrity through authentication.
4.	Single Sign-On	Authenticating Cloud service consumers via security broker.
5.	Hardened Virtual Server Images	Striping unnecessary software to limit potential vulnerabilities.
6.	Multi Tenancy	Separate databases for tenants.

4. CONCLUSION

While Cloud computing has numerous advantages such as lower software and hardware costs, the ability to access data on the go and disaster recovery through the redundancy of data, each organization needs to carefully consider security and legislative/operational measures in order to fully realize a Cloud based working model to suit individual requirements. With key IT players like Microsoft, Amazon and Google offering Cloud based services to both business and consumers alike, Cloud computing is being adopted by more and more users.

However, organizations involved in handling sensitive data such as banks and other financial institutions must diligently prepare a customized plan to whole heartedly adopting the Cloud services model. In doing so, organizations can safely and productively rely on adopting the cloud model while mitigating risk.

5. REFERENCES

Tay, L. (2011). Westpac bursts risk analysis to Azure. Retrieved from: http://www.itnews.com.au/News/266585,westpac-bursts-risk-analysis-to-azure.aspx

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

Shrum, S. M., Paul. (2012). Common Risks of Using Business Apps in the Cloud. Retrieved from: http://www.us-cert.gov/sites/default/files/publications/using-cloud-apps-forbusiness.pdf

Horwath, C. (2012). Enterprise Risk Management for Cloud Computing. Retrieved from: http://www.coso.org/documents/Cloud%20Computing%20Thought%20Paper.pdf

Erl, T., Zaigham, M. & Ricardo, P. (2013). Cloud Computing Concepts, Technology & Architecture: Prentice Hall.

ENISA. (2012). Cloud computing benefits risks and recommendations for information security. Retrieved from: https://resilience.enisa.europa.eu/cloud-security-andresilience/publications/cloud-computing-benefits-risks-and-recommendations-forinformation-security

ODCA. (2014). Open Data Center Alliance. Retrieved from: http://www.opendatacenteralliance.org/docs/Data_Exchange_for_Software_as_a_Service_Rev1.0.pdf

Leavitt, N. (2009). Is cloud computing really ready for prime time. 42(1), 15-20.