SECURITY CONCERNS IN CLOUD COMPUTING: THE TRANSITION FROM A PRIVATE CLOUD TO A PUBLIC CLOUD

Prof.Rajesh Kumar Kashyap*

Dr.Sarika Sharma**

ABSTRACT

Cloud computing if not other reasons has been attributed for providing an opportunity and rather a level playing field where it makes small and medium enterprises acquire and operate the scale of IT technological advancements, which are normally found in large organizations alone. As long as the applications are run in an organization in a private cloud the issues and concerns with regards to the security are limited rather can be controlled by the internal systems. But when the applications or the IT environment is dynamically available over the internet, by the use of a third party provider it is a different ball game altogether. Organizations are always apprehensive about this move to a public cloud because it opens up a new array of security and privacy risks, which the applications were never accustomed to previously. This research paper tries to analyze the most vulnerable attribute of an organization's security concern which may derail the immense benefits which organizations gain by using a public cloud. The results reveal that data security is the highly potential component, which is prone to risk in the public cloud environment.

Keywords: cloud, security, data, private, public, hybrid, service model, Infrastructure-as-a-Service, Platform-as-a-Service, Software-as-a-Service

* M.C.A. Department, Z.E.S's ZIBACAR, Pune-41

** Director-MCA, JSPM's EICA, Wagholi, Pune

INTRODUCTION

The most important scalability aspect, which cloud computing offers to the previous shared resource technologies it is capability to provide services to organizations without any partiality, based upon the size of the organizations. Small entrepreneurs and enterprises have been fortunate to use technologies, which were literally unavailable to them previously because of which they had limited choices. Now cloud computing has offered them an opportunity where in they have to rent only the necessary infrastructure which includes computing power, storage space and web based applications which they can also use just as the big organizations do. Organizations, which have been using private clouds, which were not so dynamic have gradually, understood the immense benefits of doing their business over the internet by the use of a public cloud. According to concerns Yang & Chen (2010), Private cloud, public cloud, hybrid cloud and community cloud are the four ways in which a cloud can be deployed. The management of data and processes within the organization signifies what is called as a private cloud whereas the situation wherein the resources are dynamically provisioned over the Internet, via web applications/web services from an off-site third-party provider who shares resources denotes what is been called as a public cloud. When there is a mixture of multiple internal and/or external providers is called a hybrid cloud and a community cloud computing is said to be in action when many companies together construct and share infrastructure with the same policies and same concerns which will benefit all organizations jointly.

This paper specifically deals with public clouds and more specifically the new risk and challenges which organizations face when they encounter especially during a transition from private environment to a public environment. This paper is an endeavor to find the biggest vulnerabilities, which can be found in a public cloud environment and the extent of the risks it may possess to organizations and the impact on their business. This paper is an effort to examine the potential data security concerns, which hamper and overshadow the benefits provided by the transition to a public cloud environment. Also an attempt is made to list down the potential measures which could be employed in order to thwart the risks and more importantly increase the confidence levels of organizations whose apprehensions have been ever increasing as the transitions begin from a private to a public cloud.

LITERATURE REVIEW

It has been found that cloud computing is gaining momentum at an alarming rate (Rimal, Choi, & Lumb**,** 2009). Bisong & Rahman (2011) view that the concept of the cloud computing has been defined by multiple researchers in different ways. Out of them the most comprehensive and extensive definition is been given by Brandl, (2010) who states that "A Cloud is a collection of IT resources which includes servers, databases, and applications which are available on an on-demand basis, provided by a service providing company, which is available through the Internet, and provide resource pooling among multiple users." Jensen et.al (2009), classify cloud based upon different layers by the type of services they provide such as

- Infrastructure-as-a-service (IaaS)
- Platform-as-a-Service (PaaS)
- Software-as-a-Service (SaaS)

Infrastructure-as-a-service (IaaS) is at the lowest level of the service model which provides basic components such as Central Processing Units (CPU's), memory, and storage (Jensen, Schwenk, Gruschka and Iacono, 2009). Amazon's Elastic Compute is a classic example of this. The next level of service is Platform-as-a-Service (PaaS) which is providing the developers with a platform for carrying out their functions including the provision of systems and environments for developing, testing, deploying and hosting of web applications (Rimal et al., 2009). Google App Engine is an example of PaaS. Software-as-a-Service (SaaS) is at the top of the service model that provides the organizations with the basic "ready to use applications" (Jensen et al., 2009). It acts as an alternative to applications that are run locally in organizations (Vaquero, Rodero-Merino, Caceres, & Lindner, 2009). SaaS involves the distribution of application software to clients (Rimal et al., 2009). An example of SaaS is the online alternatives of typical office applications (Vaquero et al, 2009). According to Smith (2009), a public cloud enables organizations to spend money only on services that are actually receive and consume with the added flexibility of adjusting the amount of resources they need as their circumstance varies. Brandl,(2010) feel that the It heads of organizations have under intense pressure to scale back investments in capital assets, employees, and support costs thus enhancing the possibility of cloud adoption. The reduction in investments in capital assets, IT maintenance costs, and direct labor costs are being enhanced by the usage of cloud computing. When an organization goes in a

transition from a public to a private cloud the magnitude of risks and challenges that they face are going to be many fold which may include securing sensitive information such as intellectual property, and trade secrets. Risks such as confidentiality, Integrity, and availability issues, data loss, and system outages due to attacks from hackers will so be on the rise. Kamara and Lauter, (2010) are of the view that the risks and challenges sometime outweigh the benefits provided by a public cloud transition Across all the computer platforms, networks, intranets and internets these threat facing cloud computing do exist (Bisong & Rahman, 2011).

Several researchers have worked o the paradigm of cloud computing security and especially the importance of data security has been studied by many. Smith (2009), argues that physical location of data becomes a top security concern for enterprises especially if they are located in another country, where laws of the host country may affect the security of the data. The biggest hurdle to the adoption of cloud storage is the confidentiality and integrity of data and the extent of storing large amounts of data, including critical information, on the cloud also motivate highly skilled hackers (Srinivasamurthy & Liu, 2010).

There are seven major threats as explained by **Cloud Security Alliance (2010):**

- ***Abuse and Nefarious Use of Cloud Computing Services***
- ***Insecure Application Program Interfaces***
- ***Malicious Insiders***
- ***Shared Technology Issues***
- ***Data Loss/Leakage***
- ***Account Service and Traffic Hijacking***
- ***Unknown Risk Profile***

METHODOLOGY

A structured questionnaire was developed a focus group discussion of 25 IT experts was conducted to find out the security concerns and challenges in a public cloud based environment. The experts belong to a different array of industries, which included Manufacturing, direct marketing and services, IT Company and a web services company, which is a SME company. The four major areas of security concerns in a public cloud, which were discussed, are as follows:

1. General security concerns
2. Data security concerns
3. Network security concerns
4. Prevention and contingency planning concerns

RESULTS:

Manufacturing Domain:

The major security concerns of respondents who were from the manufacturing domain are as follows:

- Data security is the single greatest concern when considering moving into the public cloud
- Providers inability to protect the confidentiality of client data
- Lack of knowledge about the location of the organization's data
- Data Security is the Primary Concern
- Provider's turnaround time
- The provider's ability to enforce encryption, authentication, and the use of firewalls
- The ability of the provider to deal with packet sniffing
- Ability of provider to deal with malicious attacks such as viruses and worms and denial-of-service.
- The provider's physical security of the computer system as well as the risk of government intervention

Direct Marketing/ Service Domain:

The major security concerns of respondents who were from the direct marketing/service domain is as follows:

- The respondent ranked data security, network security, and general security concerns equally.
- The main concern is the turn-around time
- The main concern under network and security is the efficacy of provider's encryption, authentication, and firewall techniques
- In respect of general security concerns, malicious attacks from provider's employees and the protection of organizations trade secrets were the primary concerns.
- In terms of measures to enhance utilization and patronage of public cloud computing: service level agreements between provider and client, effective security measures such as encryption, authentication, and firewalls, regular audit of provider's network security, and regular audits of provider's general security.

INFORMATION TECHNOLOGY Domain:

The major security concerns of respondents who were from the IT domain are as follows:

- The respondent's most critical concern about public cloud computing is data security and consequently, provider's ability to protect the integrity, confidentiality, and location of data each received very high marks.
- The provider's turn-around time and ability to quickly deal with system outages.
- In respect of network and security concerns, the respondent's primary concern is the ability of provider to implement effective encryption, authentication, and firewall techniques.
- The provider's physical security, malicious activities of provider's employees, and security of organizations trade secrets
- Service level agreements between provider and clients, effective encryption, authentication, and firewall techniques, satisfaction with provider's preventive and contingency plan, regular audits of provider's data security by reputable audit company,

regular audits of provider's network security, regular audits of provider's general security, and satisfaction with provider's security architecture

WEB APPLICATIONS Company:

The major security concerns of respondents who were from the Web/ Internet based domain are as follows:

- The respondents were concerned for the ability of the cloud provider to protect the integrity and confidentiality of data
- The respondents gave maximum marks to concerns pertaining to distributed denial of service attacks and the provider's ability to deal malicious attacks from viruses and worms.
- In respect of general security concerns, the respondent's primary concern was the provider's ability to deal with physical security issues pertaining to the information technology infrastructure and the organization's trade secrets.

Conclusion:

Based on the respondents as per the focus group discussion, it is revealed that indeed data security is a critical consideration when organizations make decisions regarding whether or not to adopt public cloud computing.

- The security concern is the single most important concern when moving into the cloud as the results depict. Enforceable service level agreements with clients and allow for the regular audits of data and network security by reputable audit companies is the key measure which can be used to boost confidence.
- Providers need to find ways of dealing with network security concerns as these concerns unanimously ranked second to data security concerns and was considered very important by all companies irrespective of size.

Thus it can be stated that a public cloud in spite of all the drawbacks and risks still have a lot of benefits associated which if focused properly on minimizing risks would enhance the usage of public clouds for betterment of business.

REFERENCES:

1. Bisong, A., & Rahman, S. M. (2011). An overview of the security concerns in enterprise cloud computing. *International Journal of Network Security & Its Applications (IJNSA), 3*(1), 30-45.

2. Brandl, D. (2010). Don't cloud your compliance data. *Control Engineering,* 57(1), 23.
3. Cloud Security Alliance. (2010). *Top threats to cloud computing: Survey results update 2012*. Retrieved from https://cloudsecurityalliance.org/research/top-threats/

4. Crnkovic, I., & Larsson, M. (Eds.) (2002), *Building reliable component-based software systems.* Norwood, MA: Artech House Publishers.

5. Jensen, M., Schwenk, J. O., Gruschka, N., & Iacono, L. L. (2009). On technical security issues in cloud computing. In *IEEE International Conference on Cloud Computing, 2009,* 109-116.

6. Kamara, S., & Lauter, K. (2010), Cryptographic cloud storage. *Proceedings of Financial Cryptography: Workshop on Real-Life Cryptographic Protocols and Standardization.* Retrieved from http://research.microsoft.com/pubs/112576/crypto-cloud.pdf

7. Ludäscher, B., Altintas, I. , Berkley, C., Higgins, D., Jaeger, E, Jones, M., . . . & Zhao, Y. (2006). Scientific workflow management and the Kepler system: Research articles. *Concurrency and Computation: Practice & Experience, 18*(10), 1039-1065. doi: 10.1002/cpe.v18:10

8. Orsillo, S. M., Roemer, L., & Barlow, D. H., (2003), Integrating acceptance and mindfulness into existing cognitive-behavioral treatment for GAD: A case study. *Cognitive and Behavioral Practice, 10*, 222-230. doi: 10.1016/S1077-7229(03)80034-2
9. Reese, G. (2009), *Cloud application architectures: Building applications and infrastructure in the cloud: Theory in practice*. Sebastopol, CA: O'Reilly Media.

10. Rimal, B. P., Choi, E., & Lumb, I. (2009). A taxonomy and survey of cloud computing systems. *Fifth International Joint Conference on INC, IMS and IDC*, 44-51.

11. Rittinghouse, J. W., & Ransome, J., F. (2009), *Cloud computing implementation, management, and security*. Boca Raton, FL: CRC. Press

12. Smith, R. (2009). Computing in the cloud. *Research Technology Management*, 52(5), pp.65-68.

13. Srinivasamurthy, S., & Liu, D. Q., (2010). *Survey on cloud computing security*. Retrieved from http://salsahpc.indiana.edu/CloudCom2010/Poster/cloudcom2010_submission_67.pdf

14. Stallings, W., (2006), *Network security essentials: Applications and standards* (3rd ed.). Upper Saddle River, NJ: Prentice Hall.

15. Vaquero, Luis., M, Rodero-Merino, L., Caceres, J., & Lindner, M. (2009), A break in the clouds: Towards a cloud definition, *ACM SIGCOMM Computer Communication Review, 39*, 50-55.

16. Vouk, M. A. (2008), Cloud computing: Issues, research and implementations. *Journal of Computing and Information Technology, 16*(4), 235-246.

17. Wang, L., von Laszewski, G., Kunze, M., & Tao, J. (2008), Cloud computing: A perspective study. *Proceedings of the Grid Computing Environments (GCE),* 1-11

18. Yang, J., & Chen, Z. (2010). Cloud computing research and security issues. *International Computational Intelligence and Software Engineering (CISE),* 1-3.

19. Zhang, L., & Zhou, Q. (2009). CCOA: Cloud computing open architecture, *IEEE International Conference on Web Services, 2009,* 607-616.