International Journal of Information Technology and Knowledge Management
December 2012, Volume 6, No. 1, pp. 65-67

SECURE AND SCALABLE OPERATIONAL MODEL IN REAL TIME BANKING USING CLOUD COMPUTING

Kamalpreet Singh*

Abstract: Cloud computing is an emerging computing paradigm in which resources of the computing infrastructure are provided as services of the internet. Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. Cloud computing is an emerging computing paradigm in which resources of the computing infrastructure are provided as services of the internet. Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. This paper explores various security methods such as Access Control, Telecommunications and Network Security, Information security governance and risk management, Application Security , Security Architecture and Design.

Keywords: Cloud Computing, Network Security, Convolution.

1. INTRODUCTION

Cloud computing provides a computer user access to Information Technology (IT) services *i.e.*, applications, servers, data storage, without requiring an understanding of the technology or even ownership of the infrastructure. To comprehend cloud computing, an analogy to an electricity computing grid is to be useful. A power company maintains and owns the infrastructure, a distribution company disseminates the electricity, and the consumer merely uses the resources without the ownership or operational responsibilities. Cloud computing is receiving a great deal of attention, both in publications and among users, from individuals at home to the U.S. government. Cloud computing is a subscription-based service where you can obtain networked storage space and computer resources. One way to think of cloud computing is to consider your experience with email. Your email client, if it is Yahoo!, Gmail, Hotmail, and so on, takes care of housing all of the hardware and software necessary to support your personal email account. When you want to access your email you open your web browser, go to the email client, and log in. The most important part of the equation is having internet access. Your email is not housed on your physical computer; you access it through an internet connection, and you can access it anywhere. If you are on a trip, at work, or down the street getting coffee, you can check your email as long as you have access to the internet. Your email is different than software installed on your computer, such as a word processing program. When you create a document using word processing software, that document stays on the device you used to make it unless you physically move it. An email client is similar to how cloud computing works. Except instead of accessing just your email, you can choose what information you have access to within the cloud. Similarly, a user's cloud computing access enables "shared resources, software, and information on-demand" on a fee-for-service basis. According to the National Institute of Standards and Technology (NIST), cloud computing exhibits several characteristics:

- Agility improves with users' ability to re-provision technological infrastructure resources.
- Application programming interface (API) accessibility to software that enables machines to interact with cloud software in the same way the user interface facilitates interaction between humans and computers. Cloud computing systems typically use REST-based APIs.
- Cost is claimed to be reduced and in a public cloud delivery model capital expenditure is converted to operational expenditure. This is purported to lower barrier to entry , as infrastructure is typically provided by a third-party and does not need to be purchased for one-time or infrequent intensive computing tasks. Pricing on a utility computing basis is fine-grained with usage-based options and fewer IT skills are required for implementation (in-house). The e-FISCAL project's state of the art repository contains several articles looking into cost aspects in more detail, most of them concluding that costs savings depend on the type of activities supported and the type of infrastructure available in-house.

2. SECURITY METHODS

The various security methods used in the are discussed below.

* *E-mail: kirandeep2226@gmail.com*

2.1 Access Control

Access controls are "security features that control how users and systems communicate and interact". When a user is prompted for a user ID and password, this is considered an access control. Threats to access control in cloud computing include frictionless registration processes, account hijacking, generic authentication attacks, and insecure identity and access management.

2.2 Telecommunications and Network Security

This domain discusses threats such as exploitation via cloud hacking, denial of service, and manipulation of vulnerabilities within a virtual machine, followed by countermeasures to mitigate these threats. Next, attacks and countermeasures on virtual machines vulnerabilities are discussed, followed by generic countermeasures to telecommunications and network security in the cloud.

2.3 Information Security Governance and Risk Management

The focus of analysis within this domain will center on information security policy as well as risk management/ assessment, both of which are administrative security controls. Fragmented and incomplete security guidance of cloud computing implementation might result in exploited vulnerabilities.

2.4 Application Security

When dealing with application security, the DoD must consider the three levels of cloud computing, PaaS, SaaS and IaaS. This chapter will delve into security issues with insecure interfaces, and then specific security issues within each of the three cloud levels, followed by countermeasures and recommendations. Exploitation of insecure interfaces and application programming interfaces (APIs). CSA lists insecure or weak interfaces and APIs as a top threat to cloud security. Interfaces for access control, encryption, and activity monitoring must encompass secure designs to prevent malicious and accidental circumventions of security policy.

2.5 Security Architecture and Design

In order to closely monitor resources for unauthorized activities or accesses, cloud customers should verify that proper security coding practices are utilized in cloud architecture designs. This chapter summarizes potential problem areas within cloud to include: shared technologies, failures in design, and authorization.

3. RESULT AND DISCUSSION

As a result, security is a high priority issue in clouds. The security and privacy violations of business data can be devastating. Several cloud security accidents had already happened. One of the notable security incidents occurred in March 2009 with Google Docs, when a system failure allowed the content of private documents to be exposed to everyone for a brief period of time. As a result of this security breakdown, The Electronic Privacy Information Center (EPIC), filed a detailed complaint with the Federal Trade Commission to request an injunction against Google offering their cloud service until "safeguards are verifiably established" claiming. Google's inadequate security is a deceptive business practice. Cloud security and vulnerability are similar to the traditional issues in networking and applications. In a cloud environment, security mostly depends on the security mechanisms supplied by cloud providers.

4. CONCLUSION

The telecommunication and network security domain addressed the relevant issues and countermeasures to cloud hacking and to DoS and VM attacks. Some of these measures include internal/external layered security controls such as IDS & IPS, as well as compartmentalization of virtual instances in order to protect dispersive system components. The security architecture and design domain dissected several important areas: establishing isolation management within shared technologies; designing architectures for meeting customer demands for service and availability; and certifying and accrediting systems before use, while leveraging federal solutions. The application security domain addressed exploitation and countermeasures to protect insecure interfaces. It provided methods on increasing security for PaaS, SaaS, and IaaS in the realm of message communication, information handling, key management, SDLC, tools and services, metrics, economics, and inter-host communication.

REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the Clouds : A Berkeley View of Cloud Computing", 2009.

[2] "Microsoft Windows Azure" http://www.microsoft.com/windowsazure/.

[3] "Google App Engine" http://code.google.com/appengine/.

[4] I. Foster and C. Kesselman, "The Grid: Blueprint for a New Computing Infrastructure", Oct. 1998.

[5] S. Clearwater, "Market-Based Control: A Paradigm for Distributed Resource Allocation", *World Scientific*, 1996.

[6] J. Shneidman, C. Ng, D.C. Parkes, A. AuYoung, A.C. Snoeren, A. Vahdat, and B. Chun, "Why Markets Could

(But Don't Currently) Solve Resource Allocation Problems in Systems", *Challenges*, 2005, p. 7.

[7] P. Cramton, Y. Shoham, and R. Steinberg, "Combinatorial Auctions", The MIT Press, 2005.

[8] A. Das and D. Grosu, "Combinatorial Auction-based Protocols for Resource Allocation in Grids", *Parallel and Distributed Processing Symposium*, 2005. *Proceedings. 19th IEEE International*, 2005.

[9] A. Marshall, "Principles of Economics (Great Minds Series)", Prometheus Books, 1997.

[10] "Market", From Wikipedia, the Free Encyclopedia http://en.wikipedia.org/wiki/Market.113 |

[11] D. Friedman, "The Double Auction Market Institution: A Survey", *The Double Auction Market: Institutions, Theories, And Evidence*, J. Rust, ed., Westview Press, 1993, pp. 3-26.

[12] R. Buyya, D. Abramson, J. Giddy, and H. Stockinger, "Economic Models for Resource Management and Scheduling in Grid Computing", *Concurrency and Computation: Practice and Experience*, **14**, 2002, pp. 1507-1542.