International Journal of Information Technology and Management

Vol. VI, Issue No. I, February-2014, ISSN 2249-4510

STUDY OF CLOUD COMPUTING - SECURITY ISSUES AND CHALLENGES

AN INTERNATIONALLY INDEXED PEER REVIEWED & REFEREED JOURNAL

www.ignited.in

International Journal of Information Technology and Management
Vol. VI, Issue No. I, February-2014, ISSN 2249-4510

Study of Cloud Computing - Security Issues and Challenges

Meena Mehta

Assistant Professor, Maharaja Agarsen College

Abstract – This paper is based on the cloud computing security issues. Cloud computing as a new type of highly developed technology accelerates the novelty for the computer industry. Cloud computing is a computing model based on networks, particularly based on the Internet, whose task is to make sure that users can simply use the computing resources on insist and pay money according to their usage by a metering pattern similar to water and electricity use. However security issues in cloud computing is a major concern. Security is one of the foremost challenges that hamper the growth of cloud computing. Together, service providers struggle to decrease the risks over the clouds and augment their dependability in order to build mutual trust between them and the cloud customers.

Keywords:- Cloud computing, security issues, challenges

----------♦----------

INTRODUCTION

Cloud computing is highly scalable and creates virtualized resources that can be made available to users. Users do not require any special knowledge about the concept of Cloud computing to connect their computers to the server where applications have been installed and use them. Users can communicate through Internet with remote servers.

Cloud computing has grown from being a promising business concept to one of the fastest growing segments of the IT industry. Now, recession-hit companies are increasingly realizing that simply by tapping into the cloud they can gain fast access to best-of-breed business applications or drastically boost their infrastructure resources, all at negligible cost. But as more and more information on individuals and companies is placed in the cloud, concerns are beginning to grow about just how safe an environment it is.

Cloud computing applied in the field of education, a lot of problems had been studied, such as the technology for future distance education cloud [1], teaching information system [2] [3] [4], the integration of teaching resources[5], teaching systems development[6].

CLOUD HOSTING COMPANIES HAVE APPROACHED SECURITY

As with most SaaS offerings, the applications forming Smart Clear's offering are constantly being tweaked and revised, a fact which raises more security issues for customers. Companies need to know, for instance, whether a software change might actually alter its security settings. One of the world's largest technology companies, Google, has invested a lot of money into the cloud space, where it recognizes that having a reputation for security is a key determinant of success. "Security is built into the DNA of our products," says a company spokesperson. "Google practices a defense-in-depth security strategy, by architecting security into our people, process and technologies".

BEST PRACTICE FOR COMPANIES IN THE CLOUD

- Inquire about exception monitoring systems
- Be vigilant around updates and making sure that staff doesn't suddenly gain access privileges they're not supposed to.
- Ask where the data is kept and inquire as to the details of data protection laws in the relevant jurisdictions.
- Seek an independent security audit of the host
- Find out which third parties the company deals with and whether they are able to access your data

- Be careful to develop good policies around passwords; how they are created, protected and changed.
- Look into availability guarantees and penalties.
- Find out whether the cloud provider will accommodate your own security policies.

CLOUD COMPUTING SECURITY ISSUES

As cloud computing is becoming increasingly more main stream, it becomes harder to distinguish between the generic securities issues that an IT manager needs to tackle, from those that are specific to cloud computing. Things like *roles and responsibilities*, *secure application development, least privilege* and many more apply equally well in traditional environments as they do in the cloud.

So what are the new cloud computing security issues?

- First, there are definitely new threats relating to Cloud Computing Security Issues. There are whole new attack vectors that potentially give the attacker unlimited control over your IT infrastructure. If (as a moderately large enterprise) you have a group of 20 persons who have strong control ("power user") over your cloud computing account, or over your private cloud authentication framework, then you have a group of 20 people who have full, unmitigated control of your IT infrastructure's availability and the privacy of your business-critical data. And if one of these people is not careful, an attacker can get hold of the same powers.
- More than that, in a cloud computing (specifically public cloud) environment you also trust your critical data with the **cloud provider's personnel**. Most cloud providers are doing a very good job protecting customer data from outsiders. But are they equally diligent protecting the same data from their own technical people?
- Although the cloud computing infrastructure is generally very secure, it is also a **very tempting target** for the criminal underground. All public clouds have been engineered with cloud computing security as one of the top concerns. As a result, there have only been a small number of reported vulnerabilities. One example is reported here (PDF). Any such vulnerability reported or not, in your chosen cloud, might put your entire data at risk. In the "old world", infrastructural vulnerabilities sometimes actually pose a critical risk, but often are hidden behind multiple layers of security devices, both physical security and network/OS security.

Porticor mitigates most of the risk associated with cloud computing security issues. The Porticor Virtual Private Data System encrypts your business data and maintains the encryption keys secure but still under your control. You can rest assured that even if the cloud is somehow breached, **your data will remain secure and private.**

However, there are also some weak points that should be taken into account. Next, we present some of these issues:

- Security, privacy and confidence: Since the data can be distributed on different servers, and "out of the control" of the customer, there is a necessity of managing hardware for computation with encoding data by using robust and efficient methods. Also, in order to increase the confidence of the user, several audits and certifications of the security must be performed.
- Availability, fault tolerance and recovery are guaranteeing a permanent service with the use of redundant systems and to avoid net traffic overflow.
- Scalability: In order to adapt the necessary resources under changing demands of the user by providing an intelligent resource management, an effective motorization can be used by identifying a priori the usage patterns and to predict the load in order to optimize the scheduling.
- Energy efficiency: It is also important to reduce the electric charge by using microprocessors with a lower energy consumption and adaptable to their use.

CONCLUSION

In this paper we analyzed that Cloud computing security is a tractable problem, and many of the concerns that arise with cloud security stem from either a lack of knowledge or a lack of preparation. Cloud computing brings on a new set of challenges as more owners of data are introduced, more parties are included on contracts, and data is stored in offsite locations. Cloud computing has shown to be a very effective paradigm according to its features such as on-demand self-service since the customers are able to provision computing capabilities without requiring any human interaction; broad network access from heterogeneous client platforms; resource pooling to serve multiple consumers; rapid elasticity as the capabilities appear to be unlimited from the consumer's point of view; and a measured service allowing a pay-per-use business model.

REFERENCES:

[1] F. Jian, "Cloud computing based distance education outlook", China electronic education, 2009.10, Totally 273, pp.39-42.

[2] R. Hua, "Teaching Information System Based on Cloud Computing", Computer and Telecommunications, 2010.02, pp. 42-43.

[3] Y. Juan, S. Yi-xiang, "The Initial Idea of New Learning Society which Based on Cloud Computing", Modern Educational Technology, Vol.20, No.1, 2010, pp.14-17.

[4] T. Jian, F. Lijian, G. Tao, "Cloud computing-based Design of Network Teaching System", Journal of TaiYuan Urban Vocational college, Mar. 2010, pp.159-160.

[5] Y. Zhongze, "The basic principles of cloud computing and its impact on education", Satellite TV and Broadband Multimedia, 2010.6, pp.67-70.

[6] W. Xiaomei, J. Xiaoqiang, "Cloud computing on the Impact of Higher Education", Science & Technology Information, 2010.10, pp.397-398.

[7] A. Fernandez, D. Peralta, F. Herrera, and J.M. Benıtez "An Overview of E-Learning in Cloud Computing"

Web links -

[8] http://cloudcomputingtopics.com/2014/10/cloud-deployment-strategies-formulating-the-right-cloud-deployment-model/

[9] https://www.porticor.com/what-are-the-new-cloud-computing-security-issues/

[10] http://cloud.cio.gov/topics/advantages -and-challenges-cloud-computing-security