An Introduction of Cloud Computing Security and Privacy Issues in IT Industries

Varuna Upadhyay, Dr. Ashok Jain

Dept. of Computer Science and Engineering, Pacific (Pahar) University, Udaipur
email-varunaupadhyaya@gmail.com

Director, Aravali Institute of Technical Studies, Udaipur
email-drashokjain61@gmail.com

Abstract - Cloud Computing is a model that focuses on sharing data and computation over a scalable network. This technology has grown as promising business concept to one of the fastest growing segment of the IT industry. However, the fact that Cloud Computing offers huge opportunity to IT industry. Despite the potential gains achieved from the Cloud Computing in the organizations which are slow in accepting it due to security and privacy issues associated with it. The other aspect of Cloud Computing is that, the cost oriented IT companies are now realizing that simply by processing into the cloud they can gain fast access business applications and share their infrastructure resources at negligible cost. Regardless of the fact that cloud computing offers great advantages to the end users in which several issues that are mandatory to be addressed. It is one of the major issues which hinder the growth of cloud technology.

This paper introduces a full analysis of the Cloud Computing security issues focusing on the Cloud Computing types and the service delivery types
.

Keywords- Security, Privacy, Cloud Models, Issues.

1. Introduction

The advancement in Information Technology (IT) industry demand a new computing paradigm that supports delivery of computing services on minimal charges without installing them at local computers. Cloud Computing technology is a flexible on demand network provide services to users on pay as per use basis. Currently this technology has grown from being a promising business concept to one of the fast rising segments of the IT industry. Cloud models may be distributed in terms of Software-as-a-service (SaaS), Platform as-a-Service (PaaS) and Infrastructure-as a-Service (IaaS). These models may be further divided into public, private and hybrid clouds. On the basis of cloud requirement of users, the vendor can isolate the cloud infrastructure from rest of the platform using its models. This paper presents various issues related to the cloud and section 2 gives the related work.

Section 3 describes the security issues. Section 4 raises about privacy and the last section 5 gives the conclusion of this paper

2. Related Works

Development in the field of network base computing and applications on demand have lead to an explosive growth of application models such as Cloud Computing. This technology has generated a lot of attention and competition in the IT industry and it is recognized as one of and the top ten technologies [1]. In the year 2008 Gartner recognized seven security issues that need to be addressed before endeavor consider switching to the Cloud Computing model [2]. The paper presents various security issues in adopting Cloud Computing technology environment [3]. Gartner identified seven security issues that need to be addressed before enterprises consider switching to the Cloud Computing model [5]. In addition, the multi-tenancy model and the pooled computing resources in Cloud Computing have introduced new security challenges [6] that require novel techniques to tackle with.
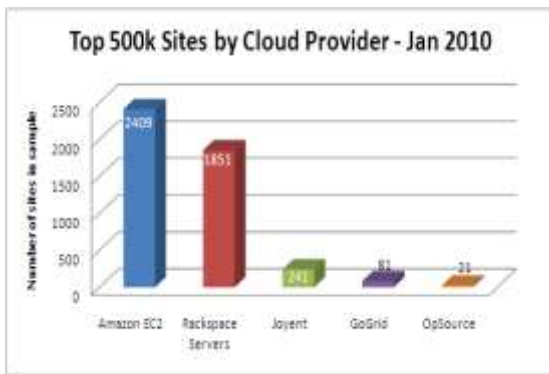
Figure 1. Cloud Providers. Top 500k sites by Cloud Provider.

According to [9] major cloud provider provide 500K site in the market because the IT industries are looking to move their internal company system to external cloud system because it reduces capital resources, IT maintenance costs and direct labor costs. The author pointed out the security vulnerabilities existing in the Cloud Computing model. They grouped the possible vulnerabilities into technology, cloud characteristics, security and control related [10]. The paper highlights high level security concerns in the Cloud Computing model such as payment, data reliability and privacy of important information [11]. The security challenges of the cloud service delivery model focusing on the software as a service model (SaaS) model [12]. The management of security in Cloud Computing focusing on Gartner's list on cloud security issues and the findings from the International Data Corporation enterprise [13]. Solution to various cloud security issues differ through cryptography, particularly public key infrastructure (PKI), use of multiple cloud providers, consistency of application program interface, improving virtual machines support and legal support[14]. The major issues exist in the technology mainly related to security, privacy and power efficiency [15].

The above literature review exposed that there are several papers discussing issues and challenges in Cloud Computing, but this paper addressing mainly security and privacy issues with IT industries focusing on cloud services.

3. Security Issues

According to the survey of International Data Corporation (IDC), security is the biggest issue of cloud adoption in IT industries. The security issues can be of two types internal and external. The exterior risk is posed by different persons and organizations that do not have direct access to the cloud. On the other side internal security risk is a well-known issue which can be posed by organizational affiliates, current or previous workers and other parties that have received access to an organization's servers, networks and data operations.

As per the IDC (International Data Corporation) survey on clouds in 2008 to rate the challenges and issues for the on-demand model of cloud, the surprising figures come as seen below figure 1.The graph simply states that security in cloud is the major challenge which causes both the architecture builder of cloud and its users to think over it before they go for real implementation.
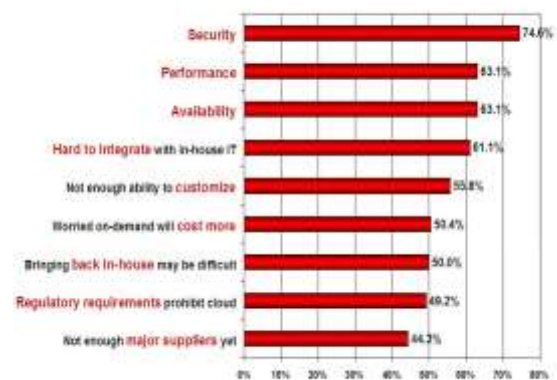

Figure2. Rating the issues for the on-demand model of cloud.

Confidentiality:
It refers to the prevention of unauthorized disclosure of information. In the cloud system it is related to the different areas like traffic analysis with some intellectual property rights and an encryption.

Integrity:
This required that data should not be modified by unauthorized modification of data should not be made by authorized persons. The integrity is provided by two techniques are RAID (redundant array of independent disks) and the other is digital signature.

Reliability and Availability
Any technology's strength is measured by its degree of reliability and availability. In this reliability denotes how often resources are available without disruption of data, and how often they fail. Availability can be understood as the possibility of obtaining the resources whenever they are needed with the consideration to the time it takes for these resources to be provisioned.

4. Privacy Issue

Cloud Computing poses privacy concerns because the service providers may access the data that is on the cloud that could accidentally be changed or even removed posing serious business trust and legal consequences [16]. Privacy is a core issue in many challenges in cloud computing including the need to protect identity in order, strategy components during integration and transaction history. A successful identity theft exploit can result in privacy loss that affects a company due to loss of credibility with confidence and negative publicity. Privacy protection mechanisms must be embedded in all cloud security solutions.

5. Conclusion

Cloud Computing can be considered as an integral component of almost all businesses in near future and it is expected to change the landscape of IT industry. There are some down sides as well to Cloud Computing. Out of those down falls one of the major factors is security issues. This paper present a better understanding of security and privacy issues of Cloud Computing in IT industries. This technology has the potential to become a leader in promoting a secure, effective and economically viable IT solution in the future.

Referances

[1] Tripathi A.,Mishra A. (2011). "Cloud Computing Research Challenges", IEEE 5th International conference on Biomedical Engineering and Informatics, pp- 1397-1401.
[2] Brodkin,(2010).5problemswithSaaSsecurity. Network World, 27(18), 1–27.
[3] Allen,J.M.(2011)."Cloudcomputing:heavenly solution or pie in the sky?Pennsylvania CPAJournal, 82(1), 1–4.
[4] S. Pearson,(2009) "Taking Account of Privacy when Designing Cloud Computing services", CLOUD¨09, Vancouver, Canada, pp. 2-6 .
[5] Lohr,S., (2007)"Google and IBM announced university initiative to address internet-scale computing challenges".
[6] Chen,Y., Paxson, V., and Katz, R., (2010)"What's New About Cloud Computing Security?", Electrical Engineering and Computer Sciences University of California at Berkeley
[7]Frank, G.,(Jul 2010) IDC Exchange homepage. [online].
[8] Brandl D. (2010, January). " Don't cloud your compliance data". Control Engineering, pp.23.
[9] Grobauer,B., Walloschek,T. and Stöcker, E."Understanding Cloud Computing Vulnerabilities," IEEE Security and Privacy, 2010 pp.2-6.
[10] Kresimir, P., andZeljko, H, "Cloud Computing security issues and challenges." Third International Conference on Advances in Human-oriented and Personalized Mechanisms, Technologies, and Services, 2010, pp. 344-349.
[11] Subashini,S. and Kavitha,V."A survey on security issues in service delivery models of Cloud Computing." J Network Computer Appl., 2010,pp.

[12] Ramgovind,S., Eloff,M. and Smith,E. "The Management of Security in Cloud Computing" IEEE International Conference on Cloud Computing, 2010 pp.
[13] Gunjan,K.., Tiwari,R. and Sahoo,G. "Towards Securing APIs in CloudComputing" IEEE publication 2010, pp 1-6.
[14] Dikaiakos,M. "Cloud Computing Distributed Internet computing for IT and Scientific Research", IEEE internet computing 2008 pp.10-13.
[15] European CIO Cloud Survey, Addressing security, risk and transition, May -2011.
[16] Ghanam,Y., Ferreira, J. and Maurer, F. "Emerging issues & challenges in Cloud- A hybrid approach", Journal of software engineering and applications 2011, pp. 923-937.

Websites

http://www.infoworld.com/d/security-central/gartner-seven-cloudcomputingsecurity-risks-853?page=0,1.

http://www.eecs.berkeley.edu/Pubs/TechRpts/2010/EECS-2010-5.html

http://blogs.idc.com/ie/..

Author

Varuna Upadhyay is a research scholar of Pacific Academy of Higher Education and Research University, Udaipur-Raj (India). After completing MCA from Rajasthan Vidhyapeeth University Udaipur she is persuing PhD on "Analysis the Impact of Cloud Computing in Indian Education System". She has relevant experience of teaching in the field of computer science in Nirmala College, Mumbai.

Dr. Ashok Jain

Author is a Director of Aravali Instittute of Technical Studies, Udaipur-Raj (India). After completing MTech (IT) and MBA, he did his PhD from Mohan Lal Sukhadia University on "A Critical Evaluation of e-Governance Implementation in Rajasthan State". He is having more than 32 years of experience in the field of information technology. He is the member of "Special Interest Group on e-Governance" of Computer Society of India. His area of interest is to study and provide consultancy for successful implementation of e-Governance and e-Learning implementation in India. The author received "Rashtriya Ratana Award" in 2002 for individual outstanding performance. He is the research guide and life member of CSI, IE (India), IIIE, IIMM, ISTD and many professional bodies. He is also the active member of Internet Governance Capacity Building Program (IGCBP) whose head office is in MALTA.