Proc. of the Second Intl. Conf. on Advances in Electronics, Electrical and Computer Engineering -- EEC 2013

ISBN: 978-981-07-6935-2

Security: *Major Challenge for Acceptance of Cloud Technology*

[1Shubhi Jain]
Venkateshwara Institute of Technology
India

[2Gourav Singh]
Venkateshwara Institute of Technology
India

[3Rohit Kanauzia]
Uttrakhand Technical University
India

***Abstract*-In this paper, author discussed the driving forces that are posing hindrance in acceptance of cloud computing as the technology. The author laid stress on Security as a major factor of concern for the growth of cloud as a technology. They tried to provide a way to manage the issues of security and data management in a cloud efficiently and effectively so as to build a secure cloud system.**

***Keywords*-Authentication, Access Control, Security, Costing Model, Charging Model, SLA**

I. Introduction

According to NSIT cloud computing is defined as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." Cloud computing is also seen as a way to increase the capacity or to enhance the capabilities of the services provided dynamically without investing in new infrastructure, training new personnel or licensing new software. It extends the functionality of Information Technology's services.

Like any other evolving technology, Cloud computing is also endorsed with numerous challenges as the users are still modulating skeptical about its authenticity, since the user places their private data on to distinct distributed location where the data is managed by the third party service providers who owns the infrastructure. It is something like putting your data, running your software on someone else's hard disk using someone else's CPU and providing that person full access to your content without even doubting his authenticity.

II. Challenges faced by cloud computing

Based on the survey conducted by IDC in 2008, the major challenges that prevent cloud computing being adopted by organization are recognized as follows:

1. ***Security-*** The issue of security is considered major factor that hinders the acceptance of cloud computing. Some most common security issues which pose threat to organization's data and software are phishing, data loss, and

Proc. of the Second Intl. Conf. on Advances in Electronics, Electrical and Computer Engineering -- EEC 2013

ISBN: 978-981-07-6935-2

botnet (running remotely on a collection of machines). Also multi-tenancy model and pooled computing resources have also add much more to the problem of security in a cloud and it requires detailed study and new techniques to deal with such issues.

2. ***Costing Model***- The consumers of cloud services are required to understand the balancing among communication, computation and integration. While migrating to the cloud can reduce the cost of infrastructure, it significantly does raise the cost of data communication.

3. ***Charging Model-*** The cost analysis for the services provided to the consumers has become more complicated because of the elastic resource pool in a cloud against simple data centers where cost analysis is quite simple.

4. ***Service Level Agreement (SLA) -*** Although cloud consumers do not have control over the underlying computing resources, they do need to ensure the quality, availability, reliability, and performance of these resources when consumers have migrated their core business functions onto their entrusted cloud. In other words, it is vital for consumers to obtain guarantees from providers on service delivery. Typically, these are provided through Service Level Agreements (SLAs) negotiated between the providers and consumers. The first issue is the definition of SLA specification in such a way that has an appropriate level of granularity, namely the trade-offs between expensiveness and complicatedness, so that they can cover most of the consumer expectations and is relatively simple to be weighted, verified, evaluated and enforced by the resource allocation mechanism on the cloud. In addition, different cloud offerings (IaaS, PaaS, SaaS) will need to define different SLA metaspecifications. This also raises a number of implementation problems for the cloud providers. Furthermore, advanced SLA mechanism need to constantly incorporate user feedback and customization features into the SLA evaluation framework. [1]

5. ***What to migrate-*** Based on a survey (Sample size=244) conducted by IDC in 2008, the seven IT systems/applications being migrated to the cloud are: IT Management Applications(26.2%), Collaborative Applications(25.4%), Personal Applications(25%), Business Applications(23.4%), Applications development and deployment(16.8%), Server Capacity (15.6%), and Storage capacity(15.5%). This result reveals that organizations still have security/privacy concerns in moving their data onto the cloud. Currently, peripheral functions such as IT Management and personal applications are the easiest IT systems to move. The survey also shows that in three years time, 31.5% of the organization will move their Storage capacity to the cloud. However, this number is relatively low compared to Collaborative Applications (43.6%) at that time. [2]

6. ***Cloud Interoperability Issues-*** Each cloud offering has its

Proc. of the Second Intl. Conf. on Advances in Electronics, Electrical and Computer Engineering -- EEC 2013

ISBN: 978-981-07-6935-2

own way about how data/applications/users can interact with the cloud, which hinders the development of cloud system. The primary goal of interoperability is to allow flawless flow of data across the cloud and between cloud and local applications.

III. Security issues for clouds

Cloud comprises of many technologies like databases, operating systems, virtualization, resource scheduling, concurrency control, load balancing, and memory management. Therefore cloud handles the security issues for these technologies. To handle these security issues we aim at extending technologies so as to build a secure cloud system. More security can be achieved if the cloud can be divided into layers based on the functionality and security parameters are employed onto each layer.

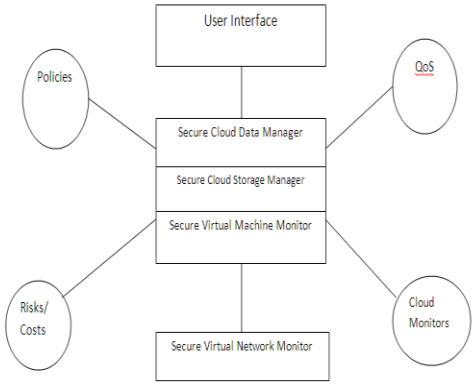

Figure:1 Layered framework for assured cloud

What we have tried to implement is to partition the cloud into segments such as secure data manager, secure storage manager, secure virtual machine monitor. Also we have separated the user interface and the network monitor. User interface is to provide consumers an interface to interact with the services provided via cloud technology. Virtual network monitor is used to create end-to-end virtual links with the requested bandwidth, as well as to monitor the computing resources. In Virtual machine monitor we are combining both hardware and software solutions. For secure cloud storage system we are employing techniques to integrate resources from multiple service providers to form a massive virtual storage system. When data is hosted from multiple domains to a storage host a Virtual machine will be created for each domain so as to separate the information and data processing. Now, we have to employ techniques for access management, resource pooling and authenticity. This can be done by utilizing Google's MapReduce technique. For secure cloud Data management, we are trying to devise algorithms which can help in efficient query optimization. In this paper we are focusing on how to efficiently and securely store data on to the cloud, provide authentic access to the data stored as well as we are trying to reduce the communication cost when the data is being transmitted on demand to the user. Like in OSI model of networks we have implemented security protocols at each layer separately similarly in this model we are trying to implement security protocols separately for each layer so as to reduce the complexity while handling the security issues.

Proc. of the Second Intl. Conf. on Advances in Electronics, Electrical and Computer Engineering -- EEC 2013

ISBN: 978-981-07-6935-2

IV. Conclusion

In this paper, we firstly discussed the definition of cloud according to NSIT. Then we focused on what challenges cloud computing is facing which is posing hindrance in acceptance of cloud technology widely and also withholding the consumers from investing in this technology. We then discussed security as a major challenge for cloud technology, since when the trusted data is placed on to a third party's infrastructure or when third party is provided the access to that data in that case lacking of security can pose potential threats to any organization which forces them not to adopt this technology. We are trying to implement security at levels which can help in managing the overall security on the cloud. Next we will come up with implementing these techniques and analyzing their results.

Refrences

[1] C.Weinhardt, A. Anandasivam, B. Blau, and J. Stosser. "Business models in the service world." IT Professional, vol. 11, pp. 28-33, 2009.

[2] F.Gens(2009, Feb.) "New IDC IT Cloud Services Survey: Top Benefits and Challenges", IDC eXchange, Available :http://blogs.idc.com/ie/?p=730 [Feb. 18,2010].

[3] K.Hemlen, M. Kantarcioglu, L.Khan, B.Thuraisingham "Security Issues for cloud computing", International Journal of Information Security and Privacy, 4(2), 39-51,April-June,2010.

[4] Kuyoro S.O., Ibikunle F, Awodele O. "Cloud Computing Security Issues and Challenges", IJCN, Vol(3): Issue(5): 2011

[5] Cloud Computing Use case discussion Group. Cloud Computing UseCases Version 3.0", 2010.

[6] R.K. Balachandra, P. V. Ramakrishna and A. Rakshit. "Cloud Security Issues." In PROC '09 IEEE International Conferences on Services Computing,2009, pp 517-520.

[7] P. Kresimir and H. Zeljko "Cloud computing security issues and challenges." In PROC Third International Conference on Advances in Human-oriented and Personalized Mechanisms, Technologies, and Services, 2010, pp 344-349.

[8] N. Leavitt. "Is Cloud Computing Really Ready for Prime Time?" Computer, vol. 42, pp. 15-20, 2009

[9] Bertino, E. (2002). Access Control for XML document, Data & Knowledge Engineering, 43 (3).

[10] W3c. (n.d.). SPARQL. Retrieved from http://www.w3.org/TR/rdf-sparql-query

[11] Mahout. (n.d.). Retrieved from http://lucene.apache.org/mahout/

[12] Lehigh University Benchmark (LUBM). (n.d.). Retrieved from http://swat.cse.lehigh.edu/projects/lubm

[13] Cloud Security Alliance (CSA). Available: http://www.cloudsecurityalliance.org [Mar. 19, 2010]

[14] B. Grobauer, T. Walloschek and E. Stocker, "Understanding Cloud Computing Vulnerablities," IEEE Security and Privacy, vol. 99,2010.