Analysis On Security Of Cloud Computing

Muhammad Zunnurain Hussain, Muhammad Zulkifl Hasan

Abstract: In this paper, Author will be discussing the security issues and challenges faced by the industry in securing the cloud computing and how these problems can be tackled. Cloud computing is modern technique of sharing resources like data sharing, file sharing, basically sharing of resources without launching own infrastructure and using some third party resources to avoid huge investment . It is very challenging these days to secure the communication between two users although people use different encryption techniques [1].

Introduction:

Cloud Computing is basically the sharing of resources over communication media .Like internet as frequent user perform cloud computing and sharing their information over the internet using any cloud environment . It is the convenient way of sharing different resources without considering place and time for accessing that information and without investing in building huge infrastructure and then maintaining it. Examples of cloud computing is Google apps. User can access different services using browser and can install on different machines in different environment on web. In cloud computing, without investing any penny, we can use resources and it is the duty of the service provider to operate and maintain the services of cloud and ensure that the services provided to client are without any problem. It is the duty of cloud provider to properly manage and organize the resources and provide secure communication. The requirements may vary with time for creating a cloud [2].

Existing Cloud Computing Security Measures:-

Following methods need to be considered while keeping security of cloud in mind, which are as follows. **Mutual Audit ability**, Current systems mainly focus one way auditing, but now researchers have suggested that in order to achieve maximum output from cloud environment we have to consider two way auditing because it is beneficial for both i.e. service provider as well as user. for example: any important information can be shared on the mutual agreement of both the parties that will be highly secure as both of them will be taken in confidence before sharing such data across cloud. Modern researches have shown that detailed auditing implementation is not an easy task to do although we consider web services. Researchers suggested that we should undertake the auditing on regular basis involving some third party which will be safe, because then it will be third party duty to maintain and provide proper information regarding any mishap. By achieving mutual audit ability, researchers said we could get a secure environment [3].

- *Muhammad Zunnurain Hussain, Department of Computer Science, SCET Lahore, engrrhusain@gmail.com*
- *Muhammad Zulkifl Hasan, Computer Science Dept NUST, NIPCONS, engrrhasan@gmail.com*

Encrypt the data before transmission, Researchers have suggested that we can encrypt the data before sending it to the final destination to get a secure environment for cloud communication, as well as there must be some privilege users on both sides i.e. on the provider and end user according to which limited access should be allotted accordingly and we can save our communication from unauthorised access [4].**Open Security Architecture (OSA),** Researchers suggested that OSA is a framework that has no cost and can be efficiently combine inside the application software. It is a pictorial representation of flow of specific information and the policies, which can be implemented in securing the information at all level. The main components, which are engage in data flow, are as under: the end users, developers, system architect, third party auditors and cloud itself [5].

Conclusions:

Cloud computing is an emerging technology, which is providing users best facilities, according to their requirements without investing and building infrastructure. Researchers are working in this domain to improve the ways of securing cloud communication; some have tested trusted computing and some cryptographic techniques to secure the communication [6].

Reference:

[1] G. Kulkarni, J. Gambhir, T. Patil and A. Dongare, "A security aspects in cloud computing," in Software Engineering and Service Science (ICSESS), 2012 IEEE 3rd International Conference on, 2012, pp. 547-550.

[2] F. B. Shaikh and S. Haider, "Security threats in cloud computing," in Internet Technology and Secured Transactions (ICITST), 2011 International Conference for, 2011, pp. 214-219.

[3] Y. Chen, V. Paxson and R. H. Katz, "What's new about cloud computing security?" University of California, Berkeley Report no.UCB/EECS-2010-5 January, vol. 20, pp. 2010-2015, 2010.

[4] L. Arockiam, S. Monikandan and G. Parthasarathy, "Cloud computing: A survey," in Proceedings of International Conference on Computer Science and Engineering, Bangalore, India, 2011, pp. 67-74.

[5] T. Andrei and R. Jain, "Cloud computing challenges and related security issues," A Survey

Paper.DOI= Http://www.Cse.Wustl.Edu/~ jain/cse571-09/ftp/cloud.Pdf, 2009.

[6] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka and J. Molina, "Controlling data in the cloud: Outsourcing computation without outsourcing control," in Proceedings of the 2009 ACM Workshop on Cloud Computing Security, Chicago, Illinois, USA, 2009, pp. 85-90.