ISSN No. 0976-5697

Volume 5, No. 8, Nov-Dec 2014

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Bursting the Cloud: Security threats & Preventions

Jhankar Tyagi
Assistant Professor (Ad-hoc)
SRCASW, DU
Delhi, India

Ankita Tyagi
Centre for Development of Advanced Computing,
Department of Electronics and Information Technology
New Delhi, India

Abstract: This review paper attempts to address the security issues pertaining to cloud computing. The basic definition of a cloud and its components are also explained.

Keywords: Cloud computing, security, cloud model, components, threats

I. INTRODAUCTION

In the recent years, Cloud computing has become a household term. With the services like Google drive storage, cloud has become synonym to having a back up of your important information safely tucked away somewhere in the largest cloud i.e. Internet. It has lead to a paradigm shift which has created a more user centric environment where a user can access a service anytime anywhere. Even the corporate world has realized the convenience offered by cloud and is rapidly shifting its services on cloud based models.

Even though the picture looks very promising, there is the looming question of security in cloud computing which needs to be handled .The secure communication link becomes a necessity in cloud computing as here the user tends to upload his significant information on the cloud.
This paper makes an attempt to review the security threats & solutions pertaining to the same.

II. CLOUD COMPUTING

In words of Vaquero et al., (2009) cloud computing can be defined as “Clouds are a large pool of easily and accessible virtualized resources (such as hardware, development platforms and/or services).These resources can be dynamically re-configured to adjust to a variable load (scale), allowing also for an optimum resource utilization. This pool of resources is typically exploited by a pay-per-use model in which guarantees are offered by the infrastructure provider by means of customized service level Agreements.” [1]:

a. Components of cloud computing:

Technically, the Cloud System can be perceived as the composition of the following four layers:

a) The Resources & Network Layer which manages the physical and virtual resources.
b) 2.The Services Layer which includes the services, namely, Naas, IaaS, PaaS, SaaS/CaaS, the service orchestration function and the cloud operational function.
c) The Access Layer includes API termination function, and Inter-Cloud peering and federation function.
d) The User Layer includes End-user function, Partner function and Administration function.

Apart from these the Cross layer covers all the remaining functions. This system is quite flexible as it gives liberty to the cloud provider to implement all or a subset of these layers. However from the point of view of security it is recommended to properly modularize the cloud according to each layers responsibility [2].

III. CLOUD MODELS

There are four types of cloud computing models listed by NIST (2009):

a. Public Cloud which is for the general people where resources, web applications, web services are provided over the internet and any user can get the services from the cloud.
b. Private Cloud which is used by the organizations internally and is for a single organization, anyone within the organization can access the data, services and web applications but users outside the organizations cannot access the cloud.
c. Community Cloud: The cloud is basically the mixture of one or more public, private or hybrid clouds, which is shared by many organizations for a single cause (mostly security).
d. Hybrid Cloud: The Cloud is a combination of two or more clouds (public, private and community) [3].

IV. SECURITY PROBLEMS AND THEIR PRESCRIBED SOULTIONS

a. Hackers attacking the cloud itself: In this the most common strategy used is Denial of service (DOS) in which hacker floods the cloud with unnecessary requests. The cloud then exhausts it’s all resources in order to service them while the actual user requests get denied.

These types of attacks could be prevented if roles & responsibilities are properly demarcated among users. Managing the cloud access & privileges could also minimize the flooding attack risk [4].

b. Browser security: This can be easily bypassed if secure socket layer (SSL) is not configured properly.

a) Network sniffers could also be employed to hack browsers .Here hacker gets hold of data in middle of the communication and decrypts the information. This leads to hacker having access of user's credentials which again creates a big security risk.

b) ***Cross site scripting:*** Here browser's request is intercepted and it is redirected to hackers interface. The user enters his information thinking he is accessing the cloud.

c) ***SQL Injection Attack:*** SQL queries are targeted here which are frequently used in website development. The special characters are used by hackers to modify results from queries for their purpose.

A well configured SSL & use of strong encryption techniques can be a preventive measure against this threat [2, 4].

c. ***Inserting Malicious software in Cloud:*** This not only harms cloud service provider's authenticity & reliability among users but is also problematic for a user as spywares or malwares are installed on his system without his knowledge.

Restricting privileges & authentication could be a solution for this kind of attack [2, 4].

d. ***Lack of a single Authority:*** Leading to chaos which also creates confusion among users. The cloud should be managed in a hierarchical way so that each user can identify his responsibilities. Giving the user a simple ethical & cloud usage training could also resolve these issues [4,5].

e. ***Data loss & leakage:*** Conflicting interests and even a small unintentional deletion of data can render the cloud inactive. When a client request to remove a cloud resource then with most operating systems this will not remove accurately. Accurate data deletion is not possible because copies of data are stored in the nearest replica but are not available [6].

The countermeasure is the use of strong SQL queries which can delete replicas as well as the main server data so that consistency can be maintained.

f. ***Lock-in:*** It can be a supplier or customer centric. Supplier lock-in results in difficulty in migration from one platform to another as hardware/software is generally managed by different parties. Customer lock -in creates problem for user if he wants to shift from cloud to home IT location.

Use of portable API's could help to resolve this issue [2, 4].

g. ***Risk for cloud service providers:*** There are problems like law conflicts, ethical issue of data ownership and lack of a "Cloud governing body" which could create risk for service providers.

A well documented service agreement covering all possible details could be of help for both the parties [4, 7].

V. CONCLUSION

Though cloud computing has become the mantra nowadays and is no doubt a smooth & hassle free way of life, It certainly needs extra precautions. Apart from security there are also issues like that of data ownership (The actual data generating firm or the cloud service provider owns the data) which must be thoroughly documented before going for cloud service.

VI. REFERENCES

[1]. A Break in the Clouds: Towards a Cloud Definition by Luis M. Vaquero et al., Volume 39, Number 1, January 2009

[2]. Security Threats in Cloud Computing Environments by Kangchan Lee Electronics and Telecommunications Research Institute Department of Technology Management, Faculty of Management Sciences, International Islamic University, H-10,Islamabad, Pakistan, ".

[3]. The NIST Definition of Cloud Computing, Recommendations of the National Institute of Standards and Technology, Peter Mell, September 2011.

[4]. Sara Qaisar, Kausar Fiaz Khawaja "Cloud Computing: Network/Security Threats And Countermeausres", Interdisciplinary Journal Of Contemporary Research In Buisness jan 2012 vol 3, No 9, pp. 1326.

[5]. W. Li and L. Ping, "Trust Model to Enhance Security and Interoperability of Cloud Environment", Cloud Computing, Proceedings on First International Conference, CloudCom 2009, Beijing, China, December 1-4, 2009, Lecture Notes in Computer Science, vol. 5931, (2009), pp. 69-79.

[6]. Danish Jamil, Hassan Zaki "Security Issues In Cloud Computing and Countermeasures", International Journal of Engineering Science and Technology (IJEST).

[7]. Recommendation ITU-T E.409, "Incident organization and security incident handling: Guidelines for telecommunication organizations".