Security architecture of cloud computing

Adesh Kumar
SLBSRSV, New Delh,i India

Abstract- Cloud computing has lots of benefits like cost saving and time reducing ability to perform new task. With all the benefits the cloud computing has a big concern about cloud security. Security architecture of cloud computing is main element which decides the level of security in cloud computing because exposure of cloud to the user depends on security architecture. Although there is no fixed security architecture standard defined yet for cloud computing but I will discuss some points that should be considered while designing cloud computing security architecture.

Keywords – security, architecture, cloud

I. INTRODUCTION

Implementation of Cloud computing efficiently is a big challenge. Proper security architecture should be designed to protect cloud and functioning of cloud properly. Cloud provides services like software as a service (SaaS), platform as a service (PaaS), Infrastructure as a service (IaaS), security as a service, communication as a service, database as a service etc. Cloud can be categories as three types as private cloud, public cloud, community cloud and hybrid cloud based on design and use of cloud.

A. Public Clouds-

A public cloud is a cloud computing deployment model that is open for use by the general public. The general public is defined in this case as either individual users or corporations. The public cloud infrastructure is owned by a cloud services vendor organization. The examples of public cloud are of Amazon Web Services, Google App Engine, Salesforce .com, and Microsoft Windows Azure.

B. Private Clouds

A private cloud is a cloud computing deployment model that is used by some organization. The private cloud computing environments intended to be used only by their employees or designated partners. It is also called as internal cloud. The private clouds can offer the benefits of public cloud computing, while still enabling the organization to retain greater control over the data and process.

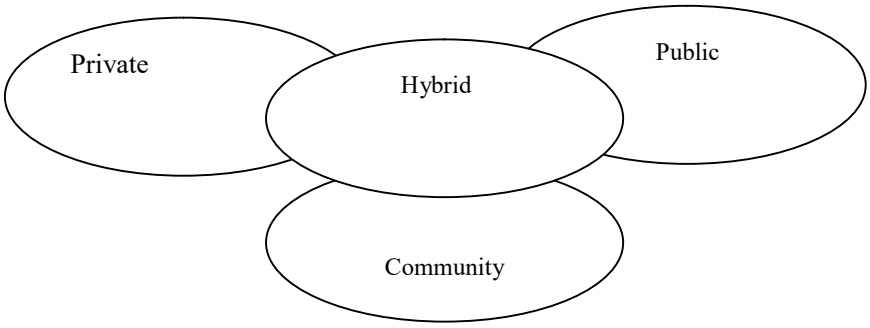

Figure 1. Cloud deployment models

C. Community Clouds

A cloud deployment model that is implemented for a community is called a community cloud. It may think as residing somewhere between a private cloud and a public cloud. The community cloud describes a shared infrastructure that is employed by and supported by multiple companies. This shared cloud resource may be utilized by groups that have overlapping considerations, such as joint compliance requirements, non-competitive business requirements.

D. Hybrid Clouds

A hybrid cloud is any combination of the previous three cloud deployment models. It is defined by NIST as "a composition of two or more clouds (private, community, or public). The clouds are bound together by standardized technology that enables data and application portability.

E. Cloud Software as a Service (SaaS)-

Software as a Service (SaaS) solutions deliver software applications over the Internet. A SaaS provider deploys software to the cloud user on demand, commonly through a licensing model. The provider may host the application on its own server infrastructure or use another vendor's hardware. The application may be licensed directly to an organization, a user or group of users, or through a third party that manages multiple licenses between user organizations, such as an ASP.

F. Platform as a Service-

PaaS is similar to SaaS, but the service is an entire application development environment, not just the use of an application. PaaS solutions differ from SaaS solutions in that they provide a cloud-hosted virtual development platform, accessible via a Web browser. PaaS solution providers deliver both the computing platform and the solution stack. This greatly accelerates development and deployment of software applications

G. Cloud Infrastructure as a Service (IaaS)-

In this type of services cloud infrastructure is provided to the cloud users as service. Infrastructure as a Service is the cloud service model that most clearly demonstrates the difference between traditional IT infrastructure and the cloud-based infrastructure service. IaaS describes the delivery of the computing infrastructure as a service.

II. SECURITY ARCHITECTURE ISSUES

There are many factors which affect the performance and implementation of cloud security architecture. There are many general issues in cloud security architecture such as security management, security compliance, controls, security awareness and cloud administrative issues. In addition to general issues there are more specific issues such as trusted hardware and software which provide secure environment for establish a secure connection and application execution platform.

A. Compliance-

The service provider in public cloud environment normally does not provide the information about the location of user's data stored to the user. The user of public cloud does not have knowledge of where its data is stored. So Cloud service provider must ensure the security of user data through some compliance certificate issued by cloud service provider.

B. Security Management-

Security management is the part of security architecture. Cloud service provider builds trust through security management. Security management is the tool to securely manage the data of cloud user in best possible way. Cloud security management should have the ability to identify and address the issues related to access control, vulnerability analysis, change control, incident response, fault tolerance, and disaster recovery and business continuity planning.

Trusted cloud computing- Trusted cloud computing is a type of computer security architecture. It is designed to protect cloud from attackers and hackers and ensure that cloud resources work properly when requested from customers. A trusted cloud computing system has the ability to protect data used by hypervisors and applications. It can also protect against unauthorized access to information and provide strong authentication, apply encryption to protect sensitive data that resides on stolen or lost devices. It also support compliance through hardware and software mechanisms.

C. Secure execution environment-

In a cloud computing environment, there are many applications which run on different servers in a distributed mode. These applications interact with the outside world and other applications and may contain sensitive information. The inappropriate access of this sensitive information would be harmful to a client. In addition, cloud computing is increasingly being used to manage and store large amounts of data in database centres located

at different places. Therefore, it is extremely important for the cloud vendor to provide a secure execution environment and secure communications for client applications and storage.

D. Identity management and access control-

Identification and authentication are the most important access control systems. Identification means provision to identify a valid user usually with help of a username or user logon ID to the system. For identity management following methods can be applied

a. Finger print scan
b. Retina Scan
c. Iris Scan
d. Hand Geometry
e. Voice
f. Handwritten signature dynamics

E. Secure Communications-

The application and data moves from from clout to outside in public cloud and within cloud in private cloud, therefore movement of data should be secured. Secure cloud communications involves the structures, transmission methods, transport formats, and security measures that provide confidentiality, integrity, availability, and authentication for transmissions over private and public communications networks.

F. API-

Common vulnerabilities such as weak antivirus software, unattended computing platforms, poor passwords, weak authentication mechanisms, and inadequate intrusion detection that can impact communications must be more stringently analyzed, and proper APIs must be used.

IV.CONCLUSION

It is the cloud security architecture which decides the security level of a particular cloud. The cloud security architecture decides how cloud users can interact with cloud. The cloud security architecture controls the exposure of cloud to the cloud users. In this paper I discussed about the security architecture of cloud.

REFERENCES

[1] R. L. Krutz and R. D. Vines, “Cloud Security: A Comprehensive Guide to Secure Cloud Computing”, Wiley Publishing, 2010
[2] J. W. Rittinghouse, and J. F. Ransome,” Cloud Computing: Implementation, management and Security”, CRC Press, 2010
[3] Cloud Computing Security: A Trend Micro White Paper, May 2010
[4] W. Juang and Y. Shue. “A Secure and Privacy Protection Digital Goods Trading Scheme in Cloud Computing”, 2010
[5] F. Douglis, “Staring at Clouds”, IEEE Internet Computing, June 2009
[6] W. Jansen,And T. Grance, DRAFT: Guidelines on Security and Privacy in Public Cloud Computing, NIST, U.S. Department of
[7] Commerce, Special Edition 800-144, January 2011