ISSN: 2455-1848
International Journal of Innovative Research & Growth
A Peer Reviewed & Referred International Journal
Volume-8 Issue-8 June-2019
Impact Factor-3.0
www.ijirg.com, editor@ijirg.com

Security Challenges & Solutions In Cloud Computing Environment

Prashant P. Pittalia
Department of Computer Science, Sardar Patel University, Gujarat, India
Email: - prashantppittalia@yahoo.com

Abstract
As the technology becomes an advance and transform business functions, more organizations are diverted from maintaining the data in traditional to transfer their data into the cloud. Cloud provider support for easy accessibility to servers, application services and databases that helps the organizations to make them free from storing, managing and sharing information. The cloud computing provides businesses flexibility and easy access to data anytime and anywhere. In such case the organizations are dependent on the cloud providers. Cloud providers like Amazon, Microsoft, and Google etc. have a strong security measures but it having some security breaches. Cloud based applications itself are very secure but when they are interact with each other in that case it may be possible user data to be exposed in the process. Day by day the complexity increase in the systems and threats are real on data. To maintain a high quality security standard the organization has to continuous at regular time interval the penetration testing and security testing should be performed. Organizations choose as per their need SaaS, IaaS and PaaS platforms for their corporate environment, due to the security and compliance with regulatory requirements at a cloud platform. This paper discusses various security aspects of cloud computing environment.
Keywords*: - Cloud computing, SaaS, private cloud.*

1- INTRODUCTION

Cloud computing is the on-demand availability of computer system resources, especially data storage and computing power, without direct active management by the user. The term is generally used to describe data canters available to many users over the Internet. Large clouds, predominant today, often have functions distributed over multiple locations from central servers[1].Cloud computing is an evolving term that describes the development of many existing technologies and approaches to computing into something different. Cloud separates application and information resources from the underlying infrastructure, and the mechanisms used to deliver those [2]. Cloud computing is defined as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or cloud provider interaction [3].

2- CHARACTERISTICS OF CLOUD COMPUTING

Cloud services have five essential characteristics those differences from, traditional computing environments:

2.1 On-demand self-service

As and when the people need the cloud resources they have to just demand for it and without human intervention it should be available to the users of cloud environments. Human intervention is totally removed.

2.2 Broad network access

Heterogeneous thin or thick client platforms like mobile phones, laptops, and PDAs can access resources as well as software services based on cloud.

2.3 Resource pooling

The provider‘s computing resources are pooled to serve multiple customers, clients

using a multitenant model, with different physical and virtual resources dynamically assigned and reassigned according to demand by the consumers. Examples of resources include storage, processing, memory, network bandwidth, and virtual machines. Also in private clouds resources are pooled between different parts of the same organization.

2.4 Rapid elasticity

Resources can be rapidly scale and it should be done automatically as per the customer requirements. Customers can purchase unlimited resources as per their capabilities. Customers can increase or decrease the quantity of resources at any time.

2.5 Measured service

According to the type of service (e.g., bandwidth, storage, processing, or active user accounts) customers used cloud systems automatically control and optimize resource usage. Resource usage can be controlled, monitored, and reported providing transparency for both the provider and consumer of the service.

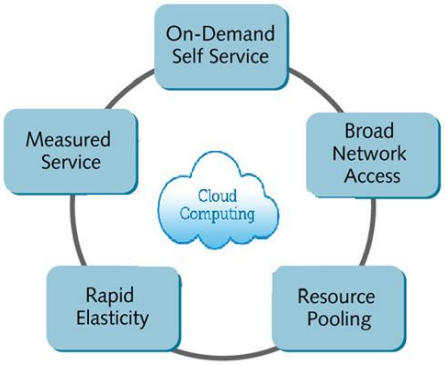

Fig. 1 Cloud Characteristics [4]

3- CLOUD SERVICE MODELS

Cloud computing basically provides three types of services which are classified in IaaS (Infrastructure as a Service) PaaS (Platform as a Service) and SaaS (Software as a Service) models.

3.1 IaaS (Infrastructure as a Service)

In this model cloud provider supports for storage space, computing, or network resources with which the customer can run and execute an operating system, applications, or any software that they choose. It provides the necessary hardware like, processor, RAM (Random Access Memory), web server, database server, networking devices, configuration and management of the various types of server etc. It is also referred to as Hardware as a Service (HaaS). The most commonly used example of IaaS is Amazon Elastic Cloud.

3.2 PaaS (Platform as a Service)

It provides the operating systems, programming languages, database servers, to build the software applications. People may compile and run their programs or software without knowing about the underlining hardware components at the cloud provider. The most common examples of PaaS are Google App Engine and Windows Azure Compute.

3.3 SaaS (Software as a Service)

The cloud providers make availability of application software to the customers. Customers have to just enter the data in the application software, manage users of applications and generate necessary reports. The most common example of SaaS is Microsoft office 365 and Google apps. Customer is an end-user of complete applications running on a cloud infrastructure and offered on a platform on-demand. All applications are accessible to the user only with the web browser; no need of any software installation is required on client device.

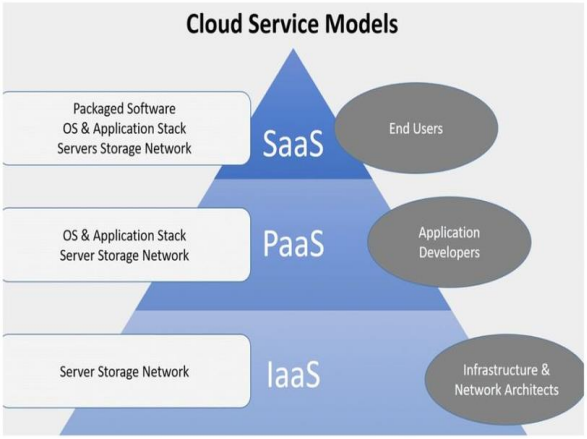

Fig. 2 Cloud Deployment Model [5]

4- DEPLOYMENT MODELS

According to the underlying infrastructure deployment model cloud is classified in Public, Private, Community, or Hybrid clouds.

4.1 Public Cloud

A public cloud's physical infrastructure is owned by a cloud service provider. Customers share this infrastructure and pay as per their resource utilization. Microsoft Windows Azure, Google App Engine, IBM Smart Cloud, Amazon EC2 are the public cloud.

4.2 Private Cloud

If any organization or customer wants to build a cloud only for itself and fully controls that cloud is known as private cloud.

4.3 Community Cloud

When customers with similar requirements get-together and wants to share an infrastructure and might share the configuration and management of the cloud is known as community cloud. This management might be done by themselves or by third parties.

4.4 Hybrid Cloud

Any combination of clouds (private or public could) form a hybrid cloud and be manage a single entity, provided that there is common aims between the standards used by the constituent clouds.

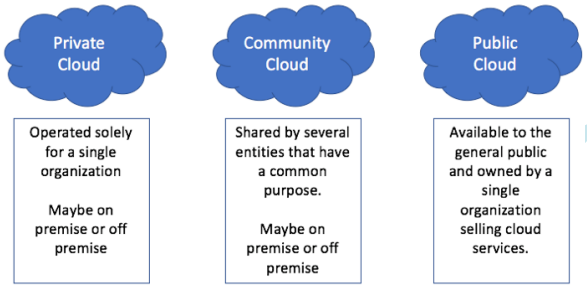

Fig. 3 Cloud Deployment Model [6]

5- SECURITY CHALLANGES FOR CLOUD

The issues related to the threats against the confidentiality, integrity, authentication, authorization and availability are resolved by making the cloud computing environment operationally very secure. Proper security architecture should be required to protect resources like infrastructure, networks, IT systems, information, and applications as well as to isolate the consumers. The following security issues are examined in secure architecture of cloud computing.

5.1 Data Centre Security

Data centres are the most important part of the cloud computing environment. It form technical basis for cloud computing. Every cloud service provider has to ensure that the all systems are secure with the current technology. Internet connection, power supply and air-conditioning should be designed to be redundant. Also permanent monitoring with video systems, movement sensors, trained employee and alarm systems. Data centre should be protect against the unauthorized entry and natural calamities. If customers need high level of availability for their services and safe data centre from any disaster it is required that data centre should be located far enough from each other geographically for reusability and backup purpose. Also the access the resources two factor authentication must be required.

5.2 Server Security

Most of the processes and computations are performed on the server. Due to this the operating system deployed on the server only necessary software packages should be added and any unnecessary programs and services should be disabled or uninstalled. To protect the server systems host firewalls or host-based intrusion detection systems should be implemented and regularly checking of important system files. Host-based intrusion detection systems are run on the IT system to detect attacks made at the operating system or application level. Examples of such attacks are failed login attempts, policy violations by users and malware such as Trojan horses. The hypervisor is the central component of server virtualisation controlling access to shared resources. The hypervisor can be attacked through intruders only by manipulating CPU registers that control the virtualisation functions. Also if there is any errors in the resources provided by the hypervisor to the virtual machines can compromised hypervisor. To this extent, CSPs who deploy server virtualisation should revert to certified, hardened hypervisors. PaaS or SaaS providers using server virtualisation, such as Windows Azure platform should guarantee the security of the guest operating systems.

5.3 Network Security

Cloud computing platforms have been misused either by placing malware or their processing power has been exploited to crack passwords using brute force attacks or to hide command and control servers used to control botnets. To prevent such attacks as well as the misuse of resources each cloud service provider should use Application Layer Gateway, anti-virus protection, Trojan detection, spam protection, firewalls and Intrusion detection and prevention systems with passing only encrypted data between two entities. Threat to public Cloud Computing platforms is the Distributed Denial of Service (DDoS) attack. Cloud service provider can protect themselves against DDoS attacks using high data rates services from larger Internet service providers (ISPs) and regulate their use in agreements. The incorrect configuring of different component with security measures in a system allow the successful attacks. Changing a configuration parameter for one component when interacting with other components lead to security vulnerabilities. For this reason, the components deployed need to be properly configured and securely. All it is needed that cloud service provider networks are suitably segmented, preventing any faults freely spreading in the network. For this reason different security zones are defined within the provider's network like security zone for the storage network, security zone for managing the cloud, security zone for the live migration. If the cloud services being administered remotely than it is must to use secure communication channel like SSH, TLS/SSL, IPsec, and VPN.

5.4 Encryption and Key Management

Cryptographic methods should be used to store, process and transport credential data securely over the cloud communication. The management of cryptographic keys in Cloud Computing environments is complex. Cloud service provider offerings the customer the option of encrypting their data themselves prior to storage on server. If the provider encrypts the data, security measures should be implemented to ensure that keys are generated, stored, used, shared, and destroyed on the basis of confidentiality, integrity and authenticity. The following key management practices should be implemented:

- Keys should be generated using key generators in a secure environment
- Cryptographic keys should be used only for one purpose.
- Keys should never be stored in the system always in encrypted form.
- Always backed up a key to protect against it lost from one of the system.
- The keys must be distributed securely
- The cloud's administrators should have no access to customers' keys.

6- CONCLUSIONS

Cloud computing is an emerging technology in today's information technology environment. It is necessary to understand the functionality of it and how it is works, what kind of cloud services, models and characteristics of its environment. The security issues related to the cloud computing environment like data centre security, server system security, network security and encryption with key management must be understand and corresponding solutions should be implemented before use of it.

7- REFERENCES

i. https://en.wikipedia.org/wiki/Cloud_computing

ii. Security Guidance for Critical Areas of Focus in Cloud Computing V2.1 available at: https://cloudsecurityalliance.org/csaguide.pdf

iii. Guidelines on Security and Privacy in Public Cloud Computing Wayne Jansen Timothy Grance Draft Special Publication 800-144 available at: http://csrc.nist.gov/publications/drafts/800-144/Draft-SP-800-144_cloud-computing.pdf

iv. https://www.linkedin.com/pulse/five-essential-characteristics-cloud-computing-sankar-somepalle
v. https://www.uniprint.net/en/7-types-cloud-computing-structures/
vi. https://chrislazari.com/what-is-cloud-computing/