International Journal on Emerging Technologies (Special Issue on *RTIESTM-2016*) **7**(1): 68-71(2016)

ISSN No. (Print) : 0975-8364
ISSN No. (Online) : 2249-3255

Cloud Computing Services Model and Security Threats

Rajandeep Kaur [*] ***and Arshdeep Singh*** [**]
[*]*Research Scholar, AIET, Faridkot, (PB), INDIA*
[**]*Assistant Professor, AIET, Faridkot, (PB), INDIA*

(Corresponding author: Rajandeep Kaur)
(Received 04 October, 2015 Accepted 04 November, 2015)
(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: Cloud computing is an architecture for providing computing resources and services over internet on demand on the basis of as per use. Cloud computing provide various features, models and services. Due to reliability, scalability, high performance, low bandwidth, cost-effective many organizations are running their applications in cloud. Cloud computing services are provided by the third party provider who owns the infrastructure. Users have no any need to acquire infrastructure physically. It saves the cost and time of the organizations. Security is the main issue in cloud computing environment, because customer store confidential information with a cloud storage provided, which are not trusted. Cloud users have to face many problems to secure their data from attacks on cloud's datacenter. The aim of this paper to provide the clear idea about the cloud services, models and security threats.

Keywords: Cloud Computing, SaaS, PaaS, IaaS, Threats

I. INTRODUCTION

The term cloud refers to a Network of providing computing resource over the internet. These resources are present in the cloud and can be used by user whenever they needed. Cloud Computing is the delivery of computing services and applications through the Internet. Cloud Computing facilitates its customer by providing virtual resources via internet. According to U.S National Institute of Standards and Technology (NIST), "Cloud Computing is 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" [1]. According to Gartner," cloud computing can be defined as a style of computing that delivered IT capabilities 'as a service' to end users through internet" [2].

Cloud computing include various features such as on demand self service, pay as you go, broad network access, virtualization, scalability, low cost software. Cloud computing provide four type of deployment model to design or implement infrastructure. These are Private cloud, Public cloud, Hybrid cloud and community cloud. Cloud computing offer three type of services SAAS, PAAS and IAAS. The users of cloud computing have to face some security and privacy issues, due to attack on services and applications on the cloud they have to lost their important data. Some threats of cloud computing are discussed in this paper.

A. Characteristics of Cloud Computing

1. On-demand self service - Cloud Computing allows the users to use web services and resources on demand when they needed.

2. Resource Pooling - Consumers use a multi-tenant model to share a pool of resources.

3. Broad Network Access - Different platforms capabilities like mobile phones, laptops, computers, and personal digital assistants, are available through broad network access**.**

4. Rapid Elasticity- The ability to scale both up and down as needed.

5. Measured Services -Cloud systems automatically control and optimize resource use through a measured service capability that is appropriate for the type of service provided.

B. Deployment Model

1. Private Cloud- A private cloud is operated only within a single organization. In this cloud all the resources and applications are available only for the users of related organization and are managed by the organization itself or by third party. Private cloud have functionality similar to the Intranet in any organization. Private cloud is more expensive and secure as compared to the Public cloud. In private cloud there are no additional security regulations, legal requirements or bandwidth limitations that can be present in a public cloud environment, by using a private cloud, the cloud service providers and the clients have optimized control of the infrastructure and improved security, since user's access and the networks used are restricted [3]. One of the best example of a private cloud is Encalyptus System [4].

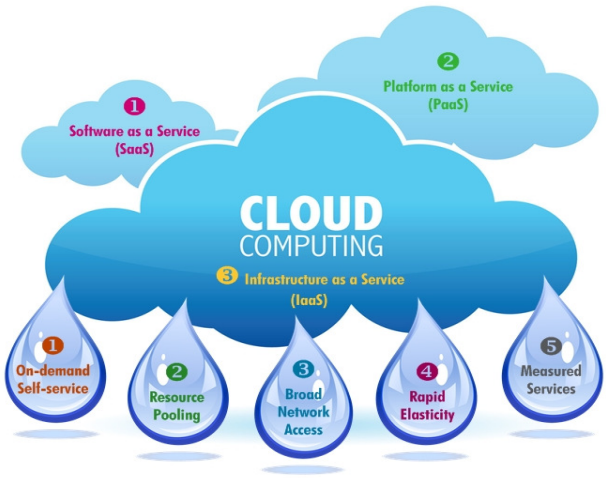

Fig. 1. Characteristics and services provided by cloud computing.

2. Public Cloud- A cloud infrastructure is provided to many customers and is managed by a third party and exist beyond the company firewall. Multiple enterprises can work on the infrastructure provided, at the same time and users can dynamically provision resources [3]. These clouds are fully hosted and managed by the cloud provider. Public clouds offer rapid elasticity and scalability. It is typically based on **pay-per use** model. There is less visibility and control in a public cloud than a private cloud because the underlying infrastructure is owned by the service provider. Public cloud does not ensure higher level security. Public cloud examples include- Microsoft Azure. Google App Engine.

3. Hybrid Cloud- Hybrid cloud is an intermixture of two or more cloud deployment models. In this, a private cloud linked to one or more external cloud services, centrally managed, provisioned as single unit. These deployment models are connected such a way that they able to transfer data without affecting each other. Hybrid cloud provides more secure control of the data and application all allows various parties to access the information over the internet. A well-constructed hybrid cloud can be useful for providing secure services such as receiving customer payments and employee payroll processing. Hybrid cloud offers both features of public and private cloud scalability. An example of hybrid cloud is Amazon Web Services (AWS).

4. Community Cloud- Community cloud allows system and services to be accessible by group of organizations. The infrastructure is shared between several organizations from specific community which has common things such as mission, security requirements and policy. These clouds are normally based on an agreement between related business organizations such as banking or educational. The community cloud environment may be operate locally or remotely.

II. LITERATURE SURVEY

In cloud computing, the users access computing resources through internet on demand. The cloud provide SaaS, PaaS and IaaS services with own features. But the users have to face various security challenges to protect their data from cloud threats. Kamara and Lauter, put more emphasis on two type of cloud i.e. Public and Private cloud. The infrastructure are owned and managed by the trusted users. But in public cloud it is controlled by the cloud providers, which is not safe because the data shared with untrusted servers [6]. As Per Tababi et al, In cloud computing, the responsibility for privacy and security lies between users and cloud service provider, but in delivery model the responsibility is differ. As in SaaS, cloud providers are considered more accountable for securing application services rather than users. In PaaS, users provide more responsibility towards application services while cloud providers are accountable for securing user's applications from others users. In Iaas, the users protect the operating system and applications and providers are responsible for protecting user's data[7]. As per IDC survey, the major challenges related to cloud computing is security. They find, it is very important to protect confidential and vital information of the users. Such as credit card detail, and patient's medical report from wicked users [8]. As Rabi Prasad Padhy, All the security issues of cloud computing are highlighted in this paper. It will be difficult to achieve end-to-end security due to complexity of the cloud. New security techniques need to be developed and improved [3].

III. SERVICE MODEL

Cloud Computing provides three type of services:

1. SssS- *Software as a Service.*
2. PaaS- *Platform as a Service.*
3. IaaS- *Infrastructure as a Service.*

1. Software as a Service (SaaS):

SaaS can be described as a process by which Application Service Provider (ASP) provide different software application over the internet. This makes the customer to get rid of installing and operating the application on own computer and also eliminates the tremendous load of software maintenance, continuing, safe guarding and support [5].

SaaS refers to a software that is deployed on a hosted service and is accessible via internet. In SaaS all users run on same version software. SaaS is typically end user applications delivered on demand over the network on the basis of pay-per-use. The users of SaaS do not need to managing infrastructure, which may include services, operating systems, storage, any individual application capabilities. The example of SaaS include Google Apps, Saleforce.com.

Advantages of SaaS:

1. Easy to use- SaaS applications do not require more than a web browser.
2. Inexpensive- SaaS makes it affordable to small business and individuals for the pay as you go pricing model.
3. For better collaboration between teams since the data is stored in a central location.
4. software applications are ready to use once the user subscribes.
5. Scability.
6. Data managed by provider.

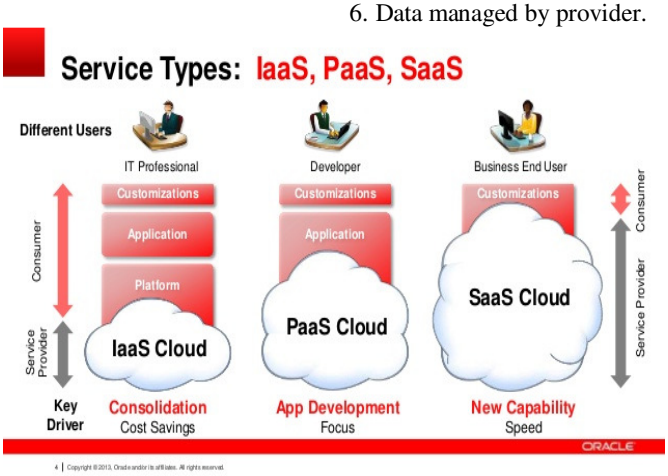

Fig. 2. Cloud Service Models (IaaS, PaaS,SaaS).

2. Platform as a Service (PaaS) :

PaaS is a development platform supporting the full ”Software Lifecycle” which allow cloud consumer to develop cloud services and applications directly on the PaaS cloud. Paas provide the user with the freedom of application design, application deployment, testing, deployment and hosting as well as application service such as team collaboration, web services integration and database integration, security. Scalability, storage. In Paas service the user has to pay for a subscription basis and charged only for what they used. It create web applications very easily and quickly on computing platform and it reduce the complexity, cost and maintenance of software. The well known PaaS providers are Cloud Foundry, Force.com, Orange Scope. Its different from SaaS because SaaS is deployed application and PaaS provide a platform to develop those applications.

Advantages of PaaS:

1. Scalable Solution.
2. Lower Total Cost of Ownership- Consumer need not purchase expensive hardware, server, power and data storage.
3. More Current System Software- It is the responsibility of the cloud provider to maintain software versions.
4. It enables non-developers to create web application through point and click tool.

3. Infrastructure as a Service (IaaS) :

IaaS refer to the sharing of hardware resources for executing service using virtualization technology. The uses does not manage the underlying hardware in the cloud infrastructure. Cloud consumer directly use IT infrastructure such as processing, storage, network and other computing resources. There are two type of resource provider processing power (network resources) and storage (memory resource). The provider offers virtual machine, physical server, storage, switching and connectivity resources to run enterprise applications on a pay-as-you-go basis. Virtualization is extensively used in IaaS cloud in order to integrate physical resources in an ad-hoc manner.

Advantages of IaaS:

1. Resources are available on demand so, the users have no any tension about the infrastructure to run application.
2. In the case of system failure, it is smoothly handled by the service provider.
3. IaaS allows the cloud provider to freely locate the infrastructure over the internet in a cost-effective manner.

IV. SECURITY THREATS IN CLOUD COMPUTING

Cloud computing has its advantages as long as certain risks associated with it. Like traditional PC system the cloud system have special and new security problems. Traditional security problems such as security vulnerabilities, virus and hack attack can also make threats to the cloud system. Hackers and malicious intruder may hack in to cloud accounts and steal sensitive data stored in cloud system. Some type of threats are discussed in following.

Malicious Insider: A malicious insider attacker may be a employee or a business partner who access the cloud network, applications, services or data, and misuse his or her authorized access to do unprivileged activities. Most of organizations hide their policies regarding employee's access level and their recruitment procedure. Due to lack of transparency in cloud provider's process and procedures, insider often have the privilege. These activities are bypass by a firewall or Intrusion Detection System (IDS) assuming it to be a legal activity [9]. There is the additional risk of remote "insider" threat in the public or hybrid cloud model i.e. an internal administrator at the cloud directly access the customer's data and steal or modify it [10].

Flooding Attack: Flooding attack is a Denial-of Service attack. The target of this attack to increase network conjunction by flooding it with huge amount of traffic. Flooding attack is occure in the PaaS and IaaS layer of cloud computing. In this, the attacker send a flood of packets one host machine to any other host machine. These packets have any type such as TCP, UDP, ICMP etc . It leads to fack use of cloud virtual machine.

Data Breach: Various authorized users and business organization's data are available together in the cloud environment, breaching to the cloud environment will potentially attack all the data of users. A data breach take place when a virtual machine access the other virtual machine on the same physical host. This type of attack may be done by the insider malicious to access the private data of other users in unauthorized way.

Denial of Service: A denial of service is an attack of IaaS layer. This attack make the network resources and virtually unavailable for the authorized users. An attacker can disrupt the services in a virtualized cloud environment by using all its CPU, RAM, disk space or network bandwidth. This cause a delay in cloud operations, and sometime cloud is unable to respond to others users and services. Denial of services attack is also common in business.

Sniffer Attack: Sniffer attacker attacks on the unencrypted data flowing in the network. The attacker capture these unencrypted packets and read the information. A network sniffer capture data as a third party when two communication parties communicate without using encryption techniques.

V. CONCLUSION

Cloud computing is an emerging technology which introduced itself as a service oriented technology. Cloud computing include on demand self services, rapid elasticity, reduce pooling, multi-tenancy, shared infrastructure. Cloud computing is a way to increase the capability and capacity without investing new infrastructure. Data security is the main issue in cloud's datacenter. Attack on datacenter, lost security of various user's confidential data. The future work is to provide safe cloud database and structure which helps to decrease the security risks faced by cloud computing.

REFERENCES

[1]. Peter Mell, Timothy Grance, "The NIST Definition of Cloud Computing‖", Jan, 2011. http://docs.ismgcorp.com/files/external/Draft-SP-800-145_cloud-definition.pdf.

[2]. Gartner, "What you need to know about cloud computing security andcompliance" (HeiserJ), [online] 2009, https://www.gartner.com/doc/1071415/need-know-cloud-computing-Security (Accessed 23 December 2013).

[3]. Rabi Prasad Padhy, Manas Ranjan Patra, Suresh Chandra Satapathy, " Cloud Computing: Security Issues and Research Challenges " *International Journal of Computer Science and Information Technology &Security (IJCSITS).* Vol. **1**, No. 2, December 2011, ISSN: 2249-9555.

[4]. B. R. Kandukuri, R. Paturi V. Rakshit, "Cloud Security Issues", *In proceeding of IEEE International Confrence on Service Computing,* pp. 517-520, 2009.

[5]. R.L Grossman, "The Case for Cloud Computing", IT Professional, vol. **11**(2), pp.23-27. 2009, ISSN: 1520-9202.

[6]. S. Kamara and K Lauter, "Cryptographic Cloud Storage"FC"10: *Proc. 14th Intl. Conf. on Financial cryptography and data security.* 2010, pp.136-149.

[7]. H. Takabi et al. "Security and Privacy Challenges in Cloud Computing Environment", *IEEE Security & Privacy,* Vol. **8**, no. 6, 2010,pp.24-31.

[8]. H. Mei, J. Dewei, L. Guoliang and Z. Yuan, " Supporting Database Applications as a Service". ICDE'09: *Proc. 25th Intl. Conf. on Data Engineering* 2009,pp.832-843.

[9]. Sellapan Palaniappan, "Secure Cloud Architecture", *Advanced Computing: An International Journal (ACIJ),* Vol. **4**, No.1, January 2013.

[10]. Candid Wueest, Mario Ballano Barcena, Laura O'Brien, "Mistake in the IaaS cloud could put your data at risk", Symantec, Version 1.01-May 1,2015.