Cloud Computing and Emerging Security Challenges

Devaang Soni
M.Tech Scholar
JECRC University

Vijay Prakash Sharma
Assistant Professor
JECRC University

Abstract: In recent years, various Cloud Computing technologies have gained rapid popularity and Cloud can be cited as most prominent or proficient technology today. While the economic case for cloud computing is compelling, the security challenges it poses are equally striking. Cloud provides many advantages like fast access, elasticity, cut costs but it is coupled with many security threats such as replay attack, eaves dropping, denial of services attack etc. In past three decades, the world of computation has changed from centralized to distributed systems and now we are using virtual centralization as cloud computing. Cloud computing is a standard in which information is placed over the internet on the virtual servers which is extracted by the users at the front end. It is an effective way of tumbling the cost of computer hardware and works in the direction of purveying a multiple access to an information resource on the same time by different users. This paper presents a various services provided by cloud and the challenges in that service.

***Keywords*: Cloud, Purveying, Virtualization, Cloud Security, Elasticity.**

I. INTRODUCTION

Cloud computing is a big development in this era of technology. It is a paradigm shift in which computing has moved away from personal computers and even the individual enterprise application server to a ‘cloud’ of computers i.e. computing is done in a remote location (out in the clouds), rather than on your desktop or portable device. When we provide some services to our client and we are hiding the idea behind it, we can say we are cloud. Cloud computing is one of the distributed system that offers the products and services globally. Scalability and dynamic infrastructure are the core features of Cloud computing. Cloud Computing offer its services for the public environment that is available to all the web users either publicly or privately. Main objective of cloud computing is to share the product and services with organization so that lot of economic benefits will be achieved by adopters. There are different kind of clouds exist respective the clients and the services such as public cloud, private cloud etc.

According to the type of resources, the complete cloud computing architecture is divided in number of layers. The bottom most layer of cloud computing defines the core components such as memory, CPU, storage etc. This layer is also called infrastructure layer of cloud computing and it is denoted by Infrastructure-as-a-Service (IaaS). The Second layer of cloud architecture provides the platform-as-a-service (PaaS). This layer of cloud deals with the hosting environment and the distribution of the services to different clients via this platform. The actual deployment and the execution of the service is done at this layer. The top layer of cloud is Software-as-a-service (SaaS) [1]. Web services are commonly used to provide the access to IaaS service and the web browsers are used to access the SaaS application.

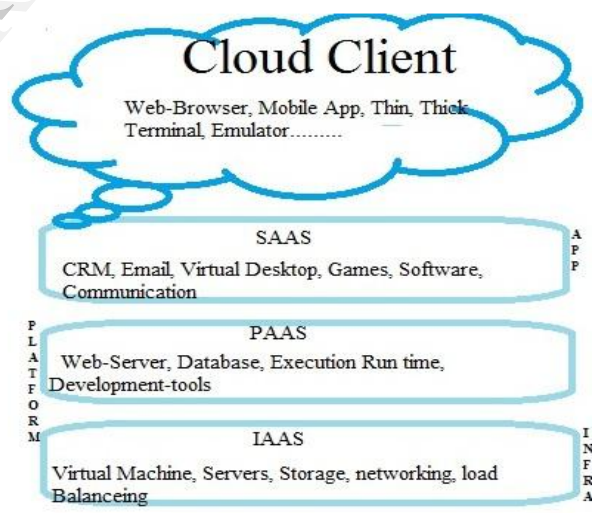
Cloud Client
Web-Browser, Mobile App, Thin, Thick Terminal, Emulator.........
SAAS
CRM, Email, Virtual Desktop, Games, Software, Communication
APP
PAAS
Web-Server, Database, Execution Run time, Development-tools
PLATFORM
IAAS
Virtual Machine, Servers, Storage, networking, load Balanceing
INFRA

Figure 1: Cloud Services

The platform based services are provided by both kind of services and both kind of environments. Cloud computing provides a service and the product over the web. As the cloud provides many services through internet.

II. DEPLOYMENT MODELS OF CLOUD COMPUTING

The cloud can be deployed in three models. They all are described in many ways but in general it is described as below:

A. *Private Cloud*

A private cloud is one in which the services are maintained on a private network, a company or a individuals. The whole infrastructure is also purchased by a company. In this cloud the highest security is provide by the cloud provider but it reduces the cost savings for a company because the company required to purchase and maintain all the software and infrastructure for this type of cloud. The figure:2 explain its structure [2].

B. *Public Cloud*

The public cloud is a general cloud which is available over the internet. A third party who is provider of that service via web applications or web services and take charges on utility basis. In this type of cloud the security is general no extra high security needed in public cloud. Many web application based on the public cloud like google drive, dropbox, where the user have to pay only the internet charges.

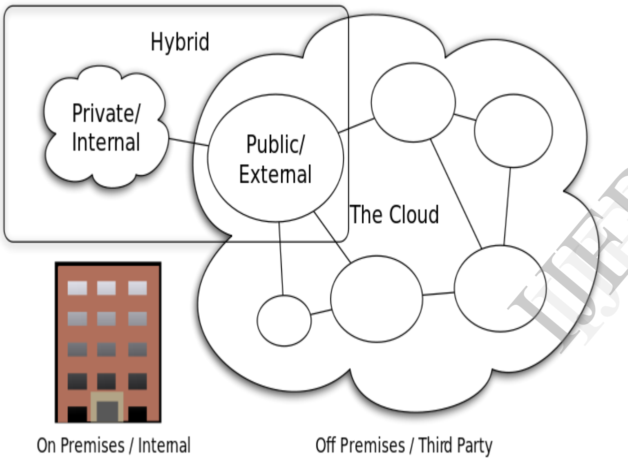

Figure 2: Cloud Deployment Models

C. *Hybrid Cloud*

The Hybrid cloud is a combination of a private cloud with the use of public cloud services. The main goal of hybrid cloud is to combine the service and data from various cloud models to make a automated environment. So the environment consists of various internal and external providers.

III. SERVICES PROVIDED BY CLOUD

Three types of services is provided by the cloud are SaaS, PaaS, IaaS.

A. *Software as a Service*

The cloud SaaS service also known as application service, and it is most popular service in cloud computing and very easy to use via web browsers over the internet. SaaS uses a web to deliver applications which are managed by a third-party whose interface is accessed on the client side. It is popular because everything is managed by the vendors like application, data, middleware, servers, virtualization, operating systems and networking. Many SaaS applications can be run directly through a web browser, it's a graphical representation so easy to learn and use for a new user.

B. *Platform as a Service*

Paas Provides the platform that are installed in top of the hardware, it makes computing infrastructure, the hardware access easy. It allows user to create application using software components that are restrained by the third party vendors. User don't have any problem like platform upgrade, scalability, maintenance etc. PaaS is scalable as much as it needed by the user, it gives better performance. This is the most complex in all three services of cloud. Cloud systems can offer an additional abstraction levels instead of supplying a virtualized infrastructure, they can provide the software platform where systems run on [2].

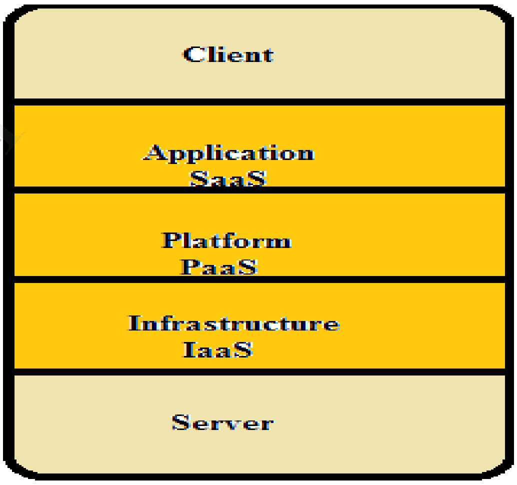

Figure 3: Cloud Services

C. Infrastructure as a Service

Instead of purchase servers, network equipment, a user can buy a fully service as a whole infrastructure as pay per use. In this whole process a third party allows user to install their server on their infrastructure and pay the billing amount to that third party, pay per use. In this type of service user just uses the distributed environment as his own infrastructure and it gives many cost benefits to the user. Through virtualization, they are able to split, assign, resize the resources to build an ad-hoc network as needed by the customers.

IV. CLOUD COMPUTING ATTACKS

Cloud Computing provides an efficient, prominent, flexible, cost-effective, shared environment to organizations, alternative to hosting their own computing resources. Cloud security is shared between cloud user and the cloud provider. The user and provider are the two entities that need to do trust on each other in the distributed share environment and whenever the need of enhancing the security both entities have to support each other.

However, hackers, attackers, and security researchers have shown that current model of cloud is not secure [3]. There are many loop holes in cloud which emerge inside or outside of cloud provider or consumer. As more companies interacts with cloud computing, look for hackers to follow. Some major attack vectors criminals may attempt include:

A. *Denial of Service Attacks*

This type of attack generally called DoS attack in market, where the attacker try to disturb the services provided by cloud. The cloud is distributed and shared over the internet so this makes DoS attacks much more harmful.

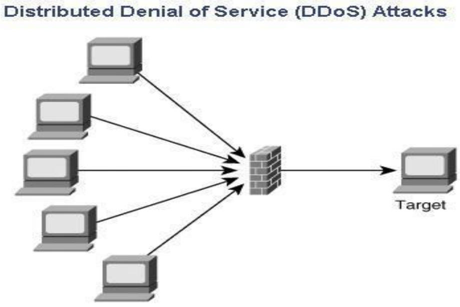

Figure 4: Dos Attacks

B. *Side Channel Attacks*

An attacker could attempt to compromise the cloud by placing a malicious virtual machine in close proximity to a target cloud server and then launching a side channel attack [4].

C. *Authentication Attacks*

This is the most week point for any service provider with hosting and virtual services. This is mostly target by hackers. There are many different ways to authenticate a fake user based on original user identity. The mechanism used to secure the authentication process and the methods used behind it are frequent target of hackers.

D. *Man in the Middle Attacks*

This is the common cryptographic attack used to know or modify the communication between end entities. A hacker placed himself between the both entities and try to do different techniques to alter the information called as packet capturing, packet crafting or using ARP poisoning.

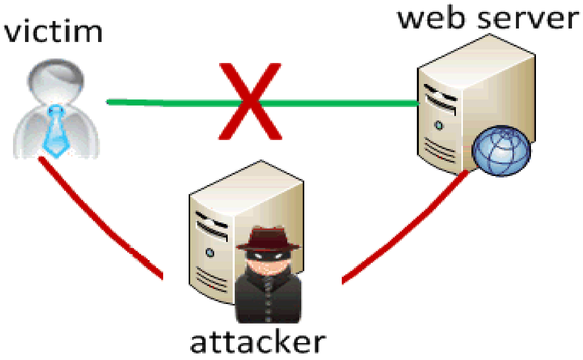

Figure 5: Man-in-Middle-attack

E. *Inside Job*

This type of attack is possible when a person, employee or a staff member who have the appropriate knowledge of system runs from client to server then he/she can root malicious codes to destroy everything in a distributed cloud systems.

IV. GENERAL REQUIREMENTS ON CLOUD SECURITY

Security is important aspects in cloud computing in distributed environment. There are many general requirements as below:

A. *Confidentiality*

It refers to only a authenticated and authorized user can access to protected data. Means only that person can use the protected data in cloud who is having the appropriate permission to access the data. Confidentiality refers that an unauthorized, unknown person, outsider, hacker cannot be able to access the protected data.

Cloud stores user data in various remote servers as a distributed environment, it can be access through a internet connection. The entire content of user data is stored with a single cloud provider or with multiple cloud provider. So the confidentiality compromise due to that numbers of cloud provider involved in storage of a single user.

Confidentiality can be achieved using proper cryptographic techniques, so taking the type of encryption into consideration, symmetric or asymmetric encryption algorithms, also key length and key management in case of symmetric cipher used [5]. Cloud provider should ensure proper deployment of encryption standards using NIST standards in it. User can also upload their data after encryption.

B. *Integrity*

Integrity means that the user data can be modified or alter only in authorize ways. Integrity may be associated with data, software and hardware [5]. Simply data integrity refers to protecting user data from modification, alteration, fabrication via unknown person.

Integrity can be achieved in cloud when cloud provider ensures the reliable and correct operation of cloud system in support of meeting its legal obligations. It can be done through service level agreement or any technical standard to which it has to confirm.

C. Availability

Availability refers to the property of a system being accessible and usable on demand by an authorize entity. In simple a organization that is providing cloud services has to open and usable their all resources all the time for users. The main cause for availability concern in cloud is DoS attack, where hacker can disturb the services.

In cloud systems must have the ability to continue operation or provide full responses for the user request even in the possibility of a security breach. So the provider have to manages the backup of the servers for continue the services even there is a possibility of dos attack. DoS attack can down the server by sending many requests to server, a distributed environment is get together and sends the request to the cloud server as authenticate user and at last server down as a result.

To make services available provider must have proper backups, detection of DoS attack and recover from it is must.

D. Privacy

Privacy is a desire of a person to control the disclosure of personal, private data. In cloud data is stored in multiple location and location transparency for users so the privacy concern increases.

Cloud providers must assure their customers and provide a high degree of transparency into their operation and privacy assurance. On a related concern its important to know who has created the data, who has modified it, last access of data and so on. So cloud provider need to protect identity information.

E. Data Segregation

Multi-tenancy is one of the most challenge in the cloud computing, as multiple user can store their data using cloud application at a same place. In that situation where data of many users will located at the same location, so intrusion of data of one user by another user is possible. This could be done by a hacker, who gets initiated by vulnerability of cloud applications. It can be done through injecting any code to application of cloud and if the application executes this code without verification then there is high potential of intrusion into other data [6]. A malicious user can use application loopholes to bypass the security check and can access the protected data.

So cloud provider need to do below test on the application for vulnerability detection like SQL injection flaws, Data Validation, Insecure Storage. It can help to improve the application security in cloud.

F. Access Control

Access control is a key concern, because insider attacks are the huge risk in the cloud. A potential hacker is someone who has been entrusted with approved access to the cloud [4]. So everyone who uses the cloud services need to know that by whom the data is managed and what are the controls behind it. So solution is to this that at every user identity there is some attribute or identifier which defines the actual/valid user. So here cloud need to make the identity more reliable and able to got a authenticate user.

V. CONCLUSION AND FUTURE WORK

In present computing word cloud computing is the most usable and beneficial to user. Along with these all benefits, there are some security concern with cloud that need to be improve to provide quality assurance and satisfaction to the user. Cloud needs to address some potential security threats and for providing internet services. Although the cloud is one of the best way to use multiple server and the whole infrastructure with any investment, will affect the cost and scalable resources.

In this paper we discussed the cloud services, the deployment models, and the advantage using cloud services with a lower budget in the IT market. Alone with this the cloud has some potential security risk and some vulnerability issues that need to be addressed. Using some digitalization in identity proof for the employee that accessing cloud is the better way to minimize the unauthorized access, this will also address the integrity and non-repudiation issues in cloud.

REFERENCES

[1] Minqi Zhou, Rong Zhang, Wei Xie and Weining Qian, Aoying Zhou, “Security and Privacy in Cloud Computing: A Survey”, Sixth International Conference on Semantics, Knowledge and Grids, 2010.

[2] Anurag Porwal, Rohit Maheshwari, B.L.Pal, Gaurav Kakhani, “An Approach for Secure Data Transmission in Private Cloud”, International Journal of soft computing and engineering, volume-2, Issue-1, March 2012.

[3] Akhil Behl, “Emerging Security Challenges in Cloud Computing”, Center of Excellence, Advance Services, Cisco Systems.

[4] Young-Gi Min, Hyo-Jin Shin,Young-Hawn Bang, “Cloud Computing Security Issues and Access Control Solutions”, Journal of Security Engineering, February 2012.

[5] Huaglory Tianfield, “Security Issues In Cloud Computing”, IEEE International Conference on System, Man, and Cybernetics, October 2012

[6] S. Subashini, V. Kavitha, “A survey on security issues in service delivery models of cloud computing”, Journal of Network and Computer Applications, 2011.

[7] Shucheng Yu, Cong Wang, Kui Ren, Wenjinng Lou, “Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing”, IEEE Infocom, 2010.

[8] Anas Bouayad, Asmae Blilat, Nour el houda, Mohammmed El Ghazi, “Cloud Computing: Security Challenges”, LTTI laboratory, 2012

[9] Balachandra Reddy, Ramakrishna Paturi, Dr. Atanu Rakshit, “Cloud Security Issues”, IEEE International Conference on Service Computing, 2009.

[10] Wentao Lio, “Research on Cloud Computing Security Problems and Strategy”, IEEE, 2012.