Cloud Computing: Cloud Delivery Models, Cloud Deployment Models and Basic Security Challenges

Jayasudha Govindasamy
Asst. Professor, Department of Computer Science
Kailash Women's College
Salem, India
jayasudha.phd.2019@gmail.com

Parimala Rathakrishnan
Asst. Professor, Department of Computer Science
AVS College of Arts & Science
Salem, India
malapari1982@gmail.com

***Abstract* – Cloud Computing is a model that gives the access throughout the world to shared pools of customizable resources over the Internet. That is, it can execute several applications at the same time on more than one system. It allows user to get unlimited storage capacity for storing information. With the advantages of High Scalability, Flexibility, Disaster Recovery, Cost Efficient, etc.. Even though lot of advantages, it can have some security issues in development of Cloud. The Cloud Models are used as Private Cloud, Community Cloud, Public Cloud & Hybrid Cloud. Its also provide some services, they are, Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), & Infrastructure-as-a-Service (IaaS). This paper is aimed at Covering Basics of Cloud Computing, Cloud Delivery Models, Comparing Cloud Delivery Model, Deployment of Cloud Models, Security Issues and Solution.**

Keywords- Cloud Computing; Software-as-a-Service (SaaS), Platfoem-as-a-Service (PaaS), Infrastructure-as-a-Service (IaaS), Security Issues, Solution.

I. INTRODUCTION

Cloud Computing is the usage of Hardware and Software to provide a service through the Internet. The Cloud Computing users can access the large number of files and applications from one device to another device along with Internet. The symbol of a Cloud is now used to specifically represent the boundary of Cloud environment.

Fig.1. Symbol of Cloud

Cloud Computing provide many services, it includes Servers, Storage, Databases, Software, Network, Analytics and Intelligence over the Internet. This Cloud Model is made of three Delivery Models and four Deployment Models.

II. CLOUD DELIVERY MODELS

A Cloud delivery model specifies the capabilities offered to the Users and the Applications supported in Cloud Computing. Three Common Cloud delivery Models are available.

- Infrastructure-as-a-Service(IaaS)
- Platform-as-a-Service(PaaS)
- Software-as-a-Service(SaaS)

A. Infrastructure-as-a-Service(IaaS)

Infrastructure-as-a-Service (IaaS) is a form of Cloud Computing, which can provide virtual Computing Resources such as Servers, Storage, Hardware, Connectivity, Networking, Operating System, and other "raw" IT resources, through the Internet. Some organizations use their own platforms and applications with in their Service Provider's infrastructure. It is mainly used to provide Cloud consumers with a High level of Control and responsibility.

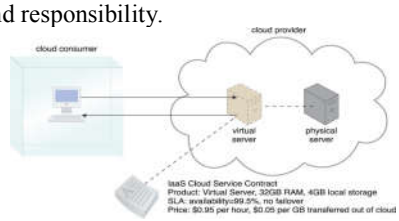

Fig. 2. IaaS Delivery Model

B. Platform-as-a-Service(PaaS)

The Platform-as-a-Service (PaaS) delivery model provides us computing platforms which typically includes the Programming Language execution environment, Database, Web Server, Operating System etc.. The Paas model is offering in which a service provider delivers a platform to clients, enabling them to develop, run, and manage their business application, instead of develop any new application and maintain that infrastructure.

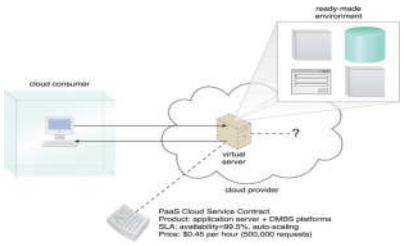

Fig. 3. PaaS Delivery Model

C. Software-as-a-Service(PaaS)

The Software-as-a-Service (SaaS) is one of the software that is deployed through the Internet rather than installed on our computer. It eliminates the spending large amount of money for Hardware Installations and maintenance. The SasS model is highly used as E-Mail services, cloud-based file management services, etc.

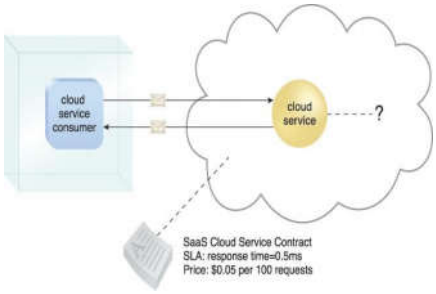

Fig. 4. SaaS Delivery Model

III. COMPARING CLOUD DELIVERY MODELS

We can compare these Cloud delivery models based on Data, Applications, Runtime, Middleware, Operating System, Virtualization, Servers, Storage and Networking.

- IaaS: In this model, we can manage Data, Applications, Runtime, Middleware and Operating System. And Virtualization, Servers, Storage & Networking can manage by Providers.
- PaaS: In PaaS model, Data & Applications only managed by users, remaining are managed by Providers.
- SaaS: In SaaS model, everything is managed by providers only.

IV. CLOUD DEPLOYMENT MODELS

There are four types of Cloud Deployment Models available, they are,

- Public Cloud
- Private Cloud
- Community Cloud
- Hybrid Cloud

A. Public Cloud

The Public Cloud has a huge amount of virtual resources, which may include Storage capabilities, Applications or Virtual machines; user can access these over the Internet. The main advantage of this Public cloud is Cyber Security.

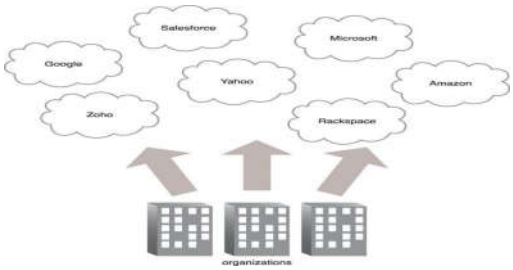

Fig. 5. Public Cloud

B. Private Cloud

Private Cloud has own Servers and infrastructure that has our data and applications, which is not shared by any other organization. In this type of cloud, the same organization is technically both the Cloud Consumer and Cloud Provider. The Private Cloud environment are flexibility, guaranteed resource availability, Security, Cost efficiently, etc..

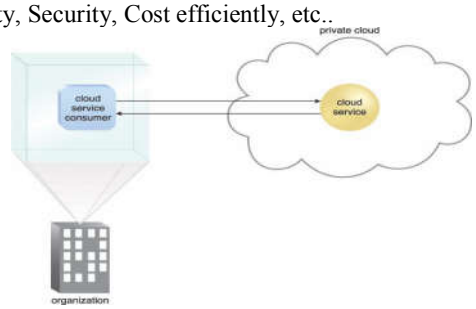

Fig. 6. Private Cloud

C. Community Cloud

Multiple organizations can share the same infrastructure for the common purpose is called Community Cloud. It is governed, managed, and secured commonly by all the multiple organizations.

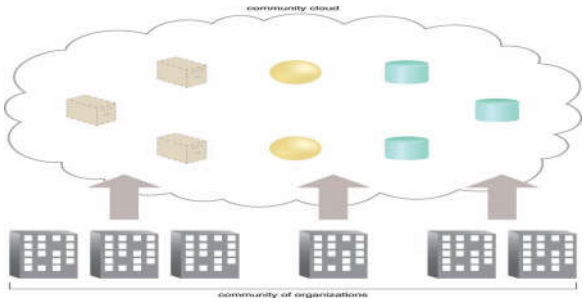

Fig. 7. Community Cloud

D. Hybrid Cloud

A combination of Public Cloud and Private Cloud is called as Hybrid Cloud. The benefits of this Cloud is, Control, Speed, Security, Cost efficiently and Scalability.

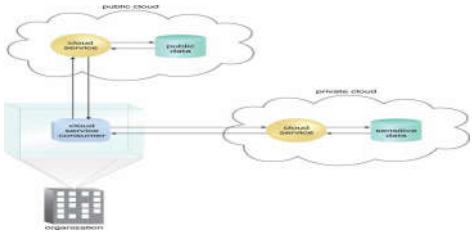

Fig. 8. Hybrid Cloud

V. CLOUD SECURITY ISSUES

In Cloud Computing, there are different types of Cloud security threats available. They are,

- Traffic Eavesdropping
- Denial of Service
- Insufficient Authorization
- Virtualization Attack
- Container Attack
- Overlapping Trust Boundaries

A. Traffic Eavesdropping

Eavesdropping is also called sniffing or snooping attack, which is attacker can theft information when it is transmitted over a network from computer, smartphone, or any other connected device.

B. Denial of Service

Denial of Service attack is also called Cyber Attack, which occurs when large amount of systems flood the resources of a targeted system, usually one or more webservers.

C. Insufficient Authorization

Insufficient Authorization attack occurs when the website permit the sensible content that should require many control restrictions.

D. Virtualization Attack

The attacker can attack the control of virtual machine is called virtualization attack.

E. Container Attack

Container attack is attack everything in container, which include the infrastructure, software supply chain, runtime and everything between them.

F. Overlapping Trust Boundaries

The attacker can exploit the cloud-based IT resources, which is shared by multiple cloud consumers is called Overlapping Trust Boundaries.

VI. SOLUTION

We can use encryption technique with Unique Identification Number (e.g. Aadhar Card Number) of Users, before upload our data to the cloud, and backup all details on our local system for further use.

CONCLUSION

Cloud computing is widely used by all. This paper is analyzed the full view of Cloud, Cloud Delivery Models & Comparison of all Models with diagrams. Types of Cloud deployment model are discussed. And finally, Security issues in the cloud computing are discussed

REFERENCES

[1] Top-Selling Author, Thomas Erl with Zaigham Mahmood and Ricardo Puttini, “Cloud Computing Concepts, Technology & Architecture”, Prentice Hall.

[2] Itisha Nowrin, Fahima Khannam, “Importance of Cloud Deployment Models and Security Issues of Software as a Service(SaaS) for Cloud Computing”, International Conference on Applied Machine Learning (ICAML), 2019.

[3] Syed Rizwan, Muhammad Zubir, “Basic Security Challenges in Cloud Computing”, 978-1-7281-5149-6/19/$31.00 © 2019 IEEE.

[4] Rajkumar Buyya, James Broberg, Andrzej Goscinski, “Cloud Computing : Principles and Paradigms”, Willey, 2011.

[5] Amit Gajbhiye, Krishna Mohan PD Shrivastva,”CCloud Computing: Need, Enabling Technology, Architecture, Advantages and Challenges”, 978-1-4799-4236-7/14/$31.00© 2014 IEEE.

[6] Amit Hendre, Karuna Pande Joshi, “A Semantic Approach to Cloud Security & Compliance”, IEEE 8th International Conference on Cloud Computing, 2015.

[7] Anagha Mukandley, Prajakta Dhamdhere, Yogesh Gajmal, “Data Access Security in Cloud Computing: A Preview”, International Conference on Computing, Power and Communication Technologies, 2018, IEEE.

.