AN OVERVIEW OF CLOUD COMPUTING AND ITS SECURITY THREATS

[1]Aditi Londhe, [2]Rahul Kumar Chawda

[1]MCA Student, [2]Assistant Professor
[1] Computer Science Department,
[1] Kalinga University, New Raipur, Chhattisgarh, India

Abstract: Cloud Computing is growing day by day and known to be very common on IT industry. Cloud Computing can be understand as a process of availing data center to multiple users over the internet. A central server distributes functions to multiple location and various users. Cloud Computing helps sharing resources from one system to other. Cloud Computing can be dedicated to single organization or can be available for many organizations. Cloud for single organization is called Enterprise or Private Cloud, cloud for many organizations is called Public Cloud and the combination of both is called as Hybrid Cloud. Security Risks in Private Cloud can be managed easily but when it comes to Public and Hybrid Cloud, preventing its data seems to be next to impossible. In this proposed paper, we will discuss about Cloud Computing, its security threats and how can it be prevented.

***IndexTerms*– Cloud Computing, SaaS, PaaS, IaaS, Public, Private, Hybrid.**

I. INTRODUCTION

Cloud Computing is a service provided for various users to store, manipulate and process the data. It acts as a data center over the internet. It is believed that Cloud Computing has been invented by Joseph Carl Robnett Licklider in the 1960's with the intention to connect people and data from anywhere and anytime. In 1983 CompuServe provided a small amount of disk space to users so that they could store any data files. In 1994, AT&T launched first all web-based, online platforms for personal and business communication and entrepreneurship. In 2000, Amazon Web Services launched their own Cloud Storage named as AWS S3. AWS is one of the Largest Cloud Computing in the world. It provides Public Cloud shared by the whole wide world. When people share a Public Cloud, there is always concern for security. What if hackers and phishers found their way in the Cloud Computing? Private Cloud is said to be more secure than the Public and Hybrid Cloud but it does not mean it can never experience Cyber Attacks. To know some measure to prevent the security risks of Cloud Computing, we first have to learn in detail about the Cloud Computing.

Cloud Computing is categorized in Cloud Models. Basically Cloud Models are divided in two types: Service Model and Deployment Model. The next section describe about the service models of Cloud Computing.

II. SERVICE MODELS

When we talk about service models, it means services that are provided by the Cloud Computing itself. If we learn deeply about the service models of Cloud Computing, there will be a lot of them as the Cloud Computing is expanding rapidly. But the following three are most common and known by every IT industries. They are:-

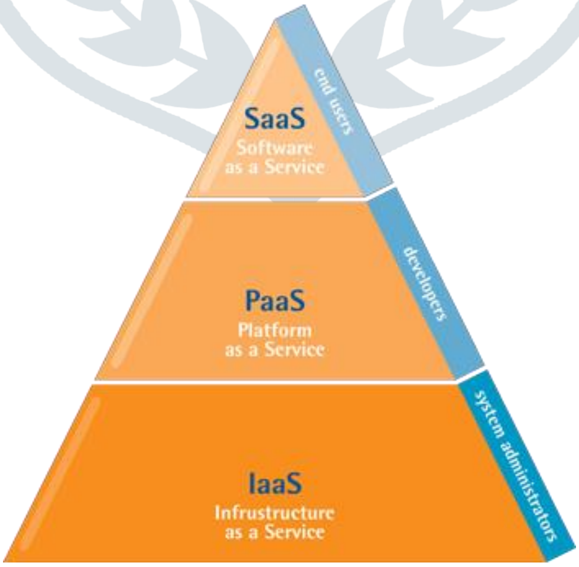

Figure 1.1 A graphical representation of SaaS, PaaS and IaaS (Cloud Computing Service Model).
(Image Credits: Google)

a. IaaS (Infrastructure as a Service):

IaaS or Infrastructure as a Service is a service of providing Infrastructure on the Cloud to the multiple users. It provides servers, networking storage space and data-center space. It runs on pay-as-you-go basis. The user does not need to invest in hardware. IaaS is more flexible service and is available on demand. It is an innovative service and it also reduces the workloads of the user. The service will be available as you continue to pay. Users mostly prefer IaaS as it provide every facility and user does not need to worry about anything.

b. PaaS (Platform as a Service):

PaaS or Platform as a Service is a service to provide a platform or environment to user. It provides every services and facilities required by the user to help in building and delivering a web application. It reduces the cost of hardware, software, hosting and managing all of the above. It helps the user to develop application and get to market faster, and it also reduces the complexity of the middleware. PaaS only provide an environment for the software to run and not software itself, people often get confused.

c. SaaS (Software as a Service):

SaaS or Software as a Service is a service to provide software on the cloud to the users worldwide. User can sign up and start using the software. User can access the data or the software from any computer that is connected to the cloud. Software as a Service is most commonly understood as Web Application. This software run on a server computer and anyone can have the access to it via the internet and a web browser.

III. DEPLOYMENT MODELS

Deployment Models are the model which describes how the cloud services will be accessible to users. Mainly these models are classified in three types:

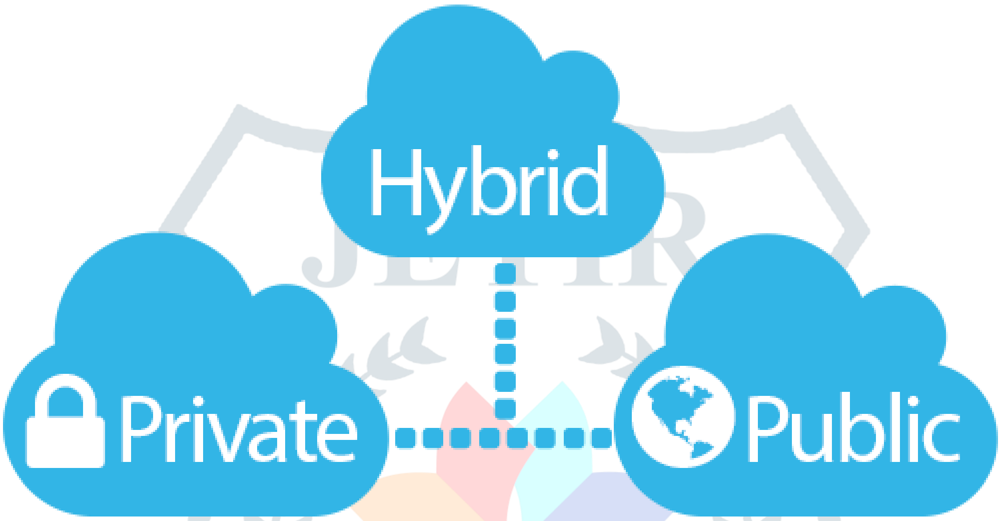

Figure1.2 A graphical representation of Private, Public and Hybrid Cloud Deployment Model.
(Image Credits: Google)

1. Private Cloud:-

Private Cloud means that the services will be accessible to only one organization that means only the people of the organization has access to the cloud. Other organizations are not allowed to use the cloud or have an access to it. The Private Cloud can be managed, owned and operated by a single organization. It is the more secure model than the rest, as no one else from outside the organization has access to it. In simple words, we can say that Private Cloud is considered as a data center that exists on a private network. It is also more costly than the rest. Below is the graphical representation of Private Cloud.

2. Public Cloud:-

Public Cloud models are just the opposite of Private Cloud. Where Private Cloud offers services to a single organization, Public Cloud offers service to more than one organization. Public Cloud can be understood as a service available for the public. Anyone can have the access authority in the Public Cloud. It is more flexible than private cloud but less secure. Private Cloud can be owned, managed and operated by several organization, business or government. It is less costly than Private Cloud. It can be considered as a datacenter that is available for public use. Below is the graphical representation of a Public Cloud.

3. Hybrid Cloud:-

As the name suggests Hybrid Cloud is a mixture of two or more cloud models. Mainly the Hybrid Cloud is a combination of Private and Public Cloud model. Users who choose Hybrid Cloud model can switch from Private to Public as per their convenience. It is highly cost effective, flexible than the rest. In Hybrid model there is always a risk of network issue and security. Amazon AWS is the largest Cloud and an example of Hybrid Cloud. Below is the graphical representation of Hybrid Cloud.

IV. ADVANTAGES & DISADVANTAGES OF CLOUD COMPUTING

IoT provide many application and services to user but it also has some advantages and disadvantages. Firstly let’s talk about advantages of IoT.

A. Advantages:-

The advantages are given below:-

1. Cost Saving:-

People believe the rumor that Cloud Computing is really expensive but the fact is, it's really affordable for any type of business to get on the cloud. And it's also easy to use; there is no need to be an expert of Cloud Computing.

2. Recovery of Data:-

Every business or even individuals should have a backup of their important data. Cloud Computing provide you a facility to keep a backup of your data on the cloud. These files can be accessed through internet connection.

3. Accessibility:-

Accessibility is one of the main advantages of Cloud Computing. Due to which you can have access to your software or application of Cloud Computing from anywhere at any time.

4. Manageability:-

Managing or dealing with server issues almost does not exist in Cloud Computing. You just have to enjoy the simple web-based user interface to use your application or have access to it. You don't have to worry about technicalities; they are taken cared by the cloud providers.

5. Reliability:-

Cloud Computing is very reliable in nature. The cloud has to be very efficient as it is serving many clients at once and also has to maintain quality and consistency in its functionality and services. Even if a host server fails, you don't have to worry about server maintenance your data can be easily transferred to another server.

B. Disadvantages:-

The disadvantages are given below:-

1. Data Security:-

People using cloud are always concerned with the security issues. Private Clouds are considered to be much securing than Public Cloud. There is always a risk of hackers and phishers to attack the cloud and steal or misuse the data in it.

2. Downtime:-

As you know cloud provide services or applications on the cloud which means there is no software or application installed in your offline system. So once the internet is off or down due to some issues that means you can't access the data, software or application.

3. Limited Control:-

As we know cloud providers are the only ones to control the cloud which results in a limited access or control to the organization or an individual. Organization or any individual is not able to get any access to major administrative services they are only allowed to use the services and manipulate the data.

4. Software:-

If you want to manipulate the data locally through multiple devices, you have to download or install (as per need) the service in every devices through which you want to manipulate the files or data.

5. Vendor Lock-In:-

Organization or companies may find it difficult to change vendors. The applications which work in one platform will maybe not necessarily run in another platform. As we know some software or application run efficiently on one platform but are not supported by others. Same goes with cloud applications hence the organization is not allowed to change the vendors.

V. SECURITY THREATS

Everything has pros and cons so does Cloud Computing. In this section, we will talk about top three security threats of Cloud Computing and they are:-

5.1 Insecure Interfaces & APIs:-

Cloud providers help the user to use or manage the cloud service by providing them software interfaces and APIs. With the help of these user can monitor, manage all the actions. These APIs and interfaces are designed to secure the user experience and the data. But as the technology has advanced it has been used in both good and bad ways. We live in an age, where the risk of hackers and phishers has grown so much. Insecure interfaces and APIs can not only harm the user but also a whole organization. Hackers and phishers can use the data for wrong reasons and the credentials of the organization or the data can also be changed, which results in no-access to the organization to retrieve their data.

5.2 Data Loss and Leakage:-

The second top threat of cloud computing is Data Loss and Leakage. There are many ways in which the data can be lost. Sometimes the user deletes the data by him without having backups or when the data is stored in a device with viruses. The risk of data loss increases in Cloud Computing, sometimes because of the architecture of Cloud Computing or the operations of Cloud Computing. An organization can face a huge destruction if an encoded key is lost. Data Leakage and Data Loss is two different things. Data Loss can happen due to mistakes of an employee or the user but Data Leakage is done by an employee or user intentionally. Any culprit employee or user can make the data public for his/her own benefits. And mostly the risk of Data Loss and Data Leakage increases in Public Cloud Computing Model.

5.3 Hardware Failure:-

Another Security threat of Cloud Computing is hardware failure. As we know, Cloud Computing provides data center to users on cloud. That means it also have data servers which store the data for the users. These data servers need a lot of hardware architecture. And if any hardware fails to work it can result in effective destruction. A bulk quantity of data can be lost or even destroyed as the data storage hardware has failed to function. Hardware failure in large scale organization is a danger to an organization's existence. Unlike the two, this threat can be prevented and curable upto a certain level.

VI. PREVENTION OF THESE SECURITY THREATS

As the Cloud Computing is expanding so is the threat for its security. Users have doubts about using Cloud Computing because of these threats. We are not claiming that we can stop these threats once and for all, but we can tell you several ways to prevent them. Below are the various things you can keep in mind the next time you are using Cloud Computing:-

- Check the security model of the Cloud Computing before using.
- Check if the Cloud Providers provides strong authentication and access controls.
- Ensure that the Cloud Provider have secured interfaces and APIs.
- Encrypt the important data.
- Ensure that the data protection is provided at both design and run time.
- Keep backups of your data and check backup strategies of your Cloud Provider.
- Check if the Cloud Provider maintain and manage the hardware regularly.
- Analyse who has the access to your data in cloud.
- Educate your employees about the proper defense techniques.
- Use strong authentication and validation techniques.

VII. CONCLUSION

Day by day, new technologies are emerging. They all come with their own pros and cons. Any technology that is handled right is a blessing otherwise it turns out to be a curse. In this paper we have described what is Cloud Computing? Its service models, deployment models, security threats and ways to manage and prevent those threats. Cloud Computing acts as a data center on cloud for the users to manage, access, manipulate and store the data. It provide data server on the internet to help the user maintain and manage the data easily. Cloud Computing has become famous in a short span of time due to its extra-ordinary features and regular updates. Cloud Providers are working day and night to make the cloud more secure for the user and will achieve that goal real soon.

VIII. ACKNOWLEDGEMENT

This research was supported / partially supported by Kalinga University, Raipur. I thank our assistant professor, Mr. Rahul Chawda, who provided insight and expertise that greatly assisted the research, although they may not agree with all of the interpretations/conclusions of this paper. I would like to show my gratitude to Mr. Rahul Chawda for sharing his pearls of wisdom with me during the course of this research. I am also immensely grateful for his comments on an earlier version of the manuscript, although any errors are my own and should not tarnish the reputations of these esteemed persons or organization.

REFERENCE

[1] Cloud Computing Review by Vivek Paul, Supriya Pandita and Prof. Meera Randiva.

[2] Introduction to Cloud Computing by Prof. Syed Neha Samreen, Prof. Neha Khatri-Valmik, Prof. Supriya Madhukar Salve, and Mr Pathan Nouman Khan.

[3] A Comparative Review on Data Security Challenges in Cloud Computing by Manpreet Kaur and Kiranbir Kaur.

[4] Security Related Issues in Cloud Computing: A Survey by Palkesh Soni, Ankit Upadhyay, Arvind Maheshwari and Prashant Lakkadwala.

[5] Solutions of Cloud Computing Security Issues by Jahangeer Qadiree and Mohd Ilyas Maqbool.

[6] Study on Cloud Computing by M. Aathishvar, N. Madhan Kumar and K. Ganesh.

[7] Data Security in Cloud Computing by Ch. Chakradhara Rao and A. V. Ramana.

[8] A Study on E-Learning and Cloud Computing by Dr. P. Neelakantan.

[9] Cloud Computing – An Overview by N. V. Muthu Lakshmi.

[10] Secure and Trusted Information Brokering in Cloud Computing by Jayalakshmi Kanagasabathy and C. Swaraj Paul.

[11] Overview of Cloud Computing, Benefits and Drawbacks by Nweso Emmanuel Nwogbaga and Ogbaga Ignatius Nwoyibe.

[12] Data Security and Integrity in Adoption of Cloud Computing by Ramesh Kumar Mojjada and Dr. (Prof.) Debnath Bhattacharyya.

[13] Cloud Computing – Wikipedia (https://en.wikipedia.org/wiki/Cloud_computing).

[14] Top cloud Security Threats (https://www.tripwire.com/state-of-security/security-data-protection/cloud/top-cloud-security-threats/).

[15] Advantages and Disadvantages of Cloud Computing (https://www.simplilearn.com/advantages-and-disadvantages-of-cloud-computing-article).

JETIR