

# **A STUDY ON CLOUD COMPUTING & ITS SECURITY ISSUES**

Jaspreet kaur

Department of Computer Science Engineering, Sant Baba Bhag Singh University, Jalandhar, India

## **Abstract**

Cloud computing is one of the most widely used IT Technology. It plays a very important part in our daily life. Cloud delivered the online services to the users. Cloud computing gives services to clients according to their requirements. It provides data storage service to users which is one of the prominent service. An owner can put their data on cloud server and can access their data from anywhere whenever they want. As everyone putting their data on cloud, there is more concern about security of data. There are many security challenges present in cloud computing. In this paper, we will show some security issue related to cloud.

**Keywords-** Cloud computing, Models, Security Issues

## **1. Introduction**

Cloud Computing is internet based service which provide services to the customer according to their requirements. Cloud delivered services to the users on pay per use base. Clients can access their data from anywhere and anytime.

In traditional times, when there are no online services available, companies spent more money and cost to deal with resources and services. Cloud computing overcome the limitations of traditional system. Now, more and more individual and businesses are attracted towards cloud because of its increased reliability, greater scalability, flexibility and low cost.

There are two types of cloud computing models- Deployment models and Service models. The Deployment models are of four types. Private, Public, Hybrid and community cloud. The service models categorized as Infrastructure as a service (IAAS), Platform as a service (PAAS), Software as a service (SAAS). With the help of these models cloud computing work. As everyone shifting towards the cloud, so security of a data is big concern. There are many security challenges and threats present in cloud.

## **2. Cloud deployment models**

Cloud deployment models tell us about the nature of the cloud, where the servers is located and who control the servers. The cloud deployment models are of four types: - Public cloud, Private Cloud, Hybrid Cloud, Community Cloud.

### **2.1 Public Cloud**

Public Cloud delivered resources and services to everyone. This cloud is open for public. It provides services to clients according to their demand. There is no need to purchase the Infrastructure, instead of purchasing we can hire them. The users are unaware of where the Infrastructure are located. The cloud service provider handled all the services. Public cloud has many benefits like managing load, low operational cost etc.

### **2.2 Private Cloud**

Private cloud is more secure than Public cloud. Private cloud is suited for those which required more security. In public cloud only authorized users can access the services and resources. The organization has complete control over their data. This cloud hosted with two ways i.e. internally or externally. In internally hosted cloud the cloud is hosted within the organization and the organization has complete control over their information. In externally hosted cloud the organizations data is handled by third party. As compare to Public Cloud the Private cloud is costlier.

### **2.3 Hybrid cloud**

Hybrid cloud is mixture of Public Cloud and Private cloud. This cloud is suited for those organizations which want both the services of public and private cloud. This cloud also hosted the data externally or internally. According to the demand of clients this cloud exchanges the workload between Public cloud and Private cloud.

### **2.4 Community Cloud**

Community Cloud is shared among the several organizations which have the same motive. This cloud is also hosted by two ways i.e. internally or externally. Community cloud is cost efficient because the costs are shared by several organizations.

### **3. Cloud service models**

#### **3.1 Infrastructure as a service**

Infrastructure as a service is a type of cloud computing service. It is lower level of cloud service models. IaaS provides services like storage, virtual machines, network etc. IaaS provides these resources to users on pay per use basis and according to their requirements they can access the infrastructure resources. There is no need to install the infrastructure. This service models overcome the loads of buying the costly infrastructure and installing the infrastructure.

#### **3.2 Platform as a service**

Platform as a service is a service models that provide the platform to the customers. Users can develop, manage and run the applications through this service model. There is no need to worry about how to build and maintain the infrastructure, all these lower level resources are provided by the cloud service providers.

#### **3.3 Software as a service**

Software as a service is one of the fundamental service model. It is a complete service model. It provides software services to the end users. There is no need to download the software on own computer, the SaaS software can be accessible by user through web browser.

### **4. Security challenges in cloud computing**

#### **4.1 Malicious attacks**

Security issues can generated from within the enterprise and from outside world. Malicious attacker can access the sensitive data of users and lead to data breaches. In a cloud world, the insider can steal the data, change or destroy the data of users.

#### **4.2 Service hijacking**

In service hijacking the unauthorized users can gain access on authorized services. They can used different techniques to hijack the services like phishing, fraud etc.

#### **4.3 Browser security**

To send the data or information on network clients uses web browser. These web browser encrypt the clients credential and identity through SSL Technology. But the hackers can steal the information and credentials from middleware using sniffing packages.

#### **4.4 Denial of service**

Denial of service attack is a cyber-attack. In this attack, the system can overload and services are unavailable to the users or clients.

#### **4.5 Data backup and storage**

The regular backup and storage of data is very important to avoid the problem of data losses. But regular data backup also create security threats because the stored data is in unencrypted form and any unauthorized person can access those data and can misuse the data.

#### **5. Conclusion**

Cloud computing technology provides many advantages to clients. But this technology also provide many security issues. Due to these issues many enterprises are not want to shift into cloud technology. So in this paper we discussed the cloud deployment models i.e. private, public, hybrid and community cloud, cloud service models-IaaS, PaaS and SaaS and some security challenges.

#### **References**

- [1] R. Jathanna, , D. Jagli, “Cloud Computing and Security Issues”, Int. Journal of Engineering Research and Application, Vol. 7, Issue 6, ( Part -5) June 2017, pp.31-38
- [2] A Venkatesh, M. S. Eastaff,” A Study of Data Storage Security Issues in Cloud Computing”, International Journal of Scientific Research in Computer Science, Engineering and Information Technology, Volume 3,Issue 1, ISSN : 2456-3307
- [3] J. Alharthi, Dr. S. Alzahrani,” Security Issues in Cloud Computing”, Academic Journal of Research and Scientific Publishing , Vol 2 , Issue21, ISSN:2706-6495
- [4] C. Achebe, W. Travis,” Cloud Computing Overview and Application”, International Journal of Scientific Research and Engineering Development, Volume 2, Issue 6, Nov- Dec 2019
- [5] Mohamed Magdy Mosbah, “Current Services in Cloud Computing: A Survey ,” International Journal of Computer Science, Engineering and Information Technology (IJCEIT), Vol.3,No.5,October 2013
- [6] R. Choubey, R. Dubey, J. Bhattacharjee, “A Survey on Cloud Computing Security, Challenges and Threats”, International Journal on Computer Science and Engineering, ISSN: 0975-3397, Vol. 3 No. 3 March 2011, pp: 1227 – 1231.

Copyright protected @ ENGPAPER.COM and AUTHORS

[Engpaper Journal](#)



<https://www.engpaper.com>