International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 04 | Apr 2022 www.irjet.net p-ISSN: 2395-0072

How secured and safe is Cloud?

Menon Sanoop Govindankutty

Student, M. Sc IT, Keraleeya Samajam(Regd.) Dombivli's Model College, Maharashtra

---

Abstract – *Cloud Computing is the one of the hot and high value topic in the IT industry. Cloud computing provide a new method of delivering computing resources. Cloud computing resources includes data storage, processing to software, customer relationship management etc. The goal of cloud computing for private or public is to provide easy and scalable services to the IT industry. In simple words the delivery of software, storage, network, analytics and intelligence over the internet to provide faster, economic and flexible service to the client. Amazon rollout the first kind of cloud in 2006 after that many companies like Google, Oracle, Azure, IBM any many provide the cloud services. Services provided by cloud providers are Paas (Platform as a Service), Saas(Software as a Service), Iaas (Infrastructure as a Service). Virtualization is the one of the main keyword found in the cloud world. Virtualization is creation of virtual servers, infrastructure and computing. Virtualization is the one of the foundational element in the cloud computing. As all industries are moving into cloud the security is also as important and this research paper is going to check how safe is cloud?*

Key Words: Cloud computing, Virtualization, Security, AWS, AZURE, IAAS, PAAS, SAAS.

1.INTRODUCTION

Cloud computing is a general term for anything that involves providing the on demand services to end users over the internet. If a individual starts a business at early stage the resources used will be less as the number of employees are hand countable, but as the business grow the need of resources and count of employees increases. For that the system, network, data storage and servers will also be needed for the business. The resources to maintain, planning, security need to be paid so the expense of company will also increase as per growth. There will be many un wanted expenses due to resource wastages etc. To solve this problem cloud computing play a major role.

A cloud can be private or public. A public cloud sells services to anyone on the internet. A private cloud is a proprietary network or a data center that supplies hosted services to a limited number of people, with certain access and permissions settings. Private or public, the goal of cloud computing is to provide easy, scalable access to computing resources and IT services[1].

Cloud computing allows you to pay only for how much you use with much faster provision. Cloud Computing system are maintained by the cloud providers so the user doesn't have to worry about the maintenance

1.1 How Cloud Computing works?

Cloud computing works by enabling the services through a remote physical servers, database and computers to access data and cloud application over internet. An internet network connection provide the front end, which includes the accessing client device, browser, network and cloud software applications, with the back end, which consists of databases, servers and computers. The back end functions provide repository, storing data that is accessed by the front end.

Cloud computing heavily depends on Virtualization and automation. This helps users to utilize the services from any where in the world on their system over the internet. The users have to pay only to the services they are using instead of spending a large amount of money in the implementation and maintaining the setup by themselves. They can access the data, servers sitting anywhere in the world.

2. TYPES OF CLOUD COMPUTING SERVICES.

Cloud computing services are divided in to three categories Iaas- It stands for Infrastructure as a Service. Iaas provides computing architecture and infrastructure. Data storage, virtualization, servers and networking are taken care by the providers and is managed by the user application, middleware and data. Vendors manage above resources. Iaas is used by system administrators. Pros of Iaas is cloud provides the infrastructure, enhanced scalability and flexible. But the issue faced for the Iaas is service delays, network delays and security delays.

Paas- It stands for Platform as a service. In Pass the services provided are Programming language, Operating system, Server and Database. It provides with encapsulation. And the user can build, compile and run programs. This services are managed by the users they manage data and application resources. This service is used by the developers. Common PaaS products include Salesforce's Lightning Platform, AWS Elastic Beanstalk and Google App Engine. It is faster market for developers, easy deployment of web application. It is cost effective and scalable. The issues faced for these services are developers limited, migration issue and vendor lock-in.

Saas- Saas stands for Software as a service. In Saas cloud providers provide the software as a service to the end users. It is based on demand services, the service are provided to

customer on demand for the software. The user do not need to install the software on personal system. The user does not have to worry about the OS the user is using because it is universally accessible from any platform. Vendors Provide the modest and latest tools and allow multi-tenancy. The issue faced by user for this services can be portability, internet issue the size of software depends on its purpose so some heavy software need strong internet.

Deployment Model- There are 3 type of deployment model

1. Public cloud- In public model the providers provide the services like application, storage in general over the internet. It is easy and inexpensive to setup. No wasted resources as users have to pay as per the use only. But as this is public cloud security and privacy is a big concern if not managed properly.

2. Private cloud- In private cloud the resources are accessible for only limited number of public behind the firewall, so it minimizes the security concern. It is mainly used by organizations and it gives direct control over data.

3. Hybrid cloud- In Hybrid cloud it is a mix of private as well as public. And It helps to get best of both private and public cloud.

3. SECURITY CONCERN IN CLOUD

- Virtualization is a technique in which a fully functional image of an operating system can be captured and run on the users physical machine. Hypervisor is required to run a virtual operating system in a virtual machine. And if the Hypervisor is vulnerable then the whole system can be compromised and hence the users data can be breached.

  Another risk involved with virtualization is with allocation and de-allocation of resources. If the memory is allocated to a user and after the use of that client and the same memory is allocated to another user without cleaning the memory then there is a possibility of the data exposure so the allocation and de-allocation is a big part of virtualization.

  So the proper planning of virtualization should be done. Resources should be properly verified and authenticated should be done before de-allocated to the users

- Storage in public cloud is another concern of security in cloud. In public cloud storage facilities are centralized and this attract hackers much often. This is a combination of hardware and software which make little complex design. A single loop hole can lead to compromise the public cloud. Suggestion for this issue is to use Private cloud if the data is highly sensitive.

- Multienancy is also considered as one the security concern by experts. The main advantage of cloud is that users can access or rent the resources when they need and only pay for that after that if any another user need the resource, then the infrastructure is used by another user. And this also led to a major security concern. The same storage, CPU, memory are shared to different users which make not only one but multiple users vulnerable.
  To avoid such issue a highly strong authentication should be done before sharing the resources to another users.

4. DATA SECURITY

There are two states where data is vulnerable in cloud. They are data at rest and data in transit. Data security is a big and major concern. Confidentiality and Integrity of data is based on mechanism such as encryption and decryption etc.

- **Data at rest**

  Data at rest means data present in cloud. Data present in cloud can be accessed through internet. This data can be backup or live data. If the functionality have any loop hole this data can be breached easily. The organization cannot control the data physically so this is a big concern. This can be counter by using private cloud with more controlled access.

- **Data in Transit**

  Data in transit means data travelling in and out of cloud. And it is more vulnerable than data at rest. Data in transit can be files, username, password etc. As the data is traveling from one place to other an intervention can cause major security concern. Data in transit can be secured through data encryption. So that if the data is eavesdropped still the data cannot be read by the intruder.

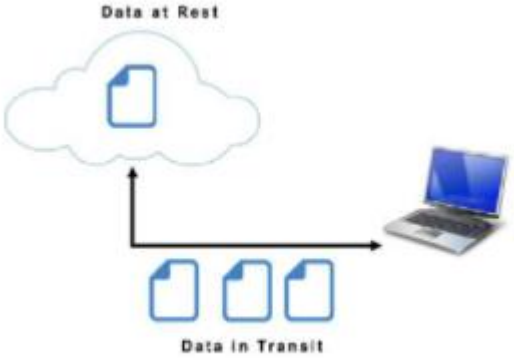

Fig 1: Data at Rest and in Transit.

5. SECURITY CHALLENGES

Securing cloud will be a big challenge for the organization. Hence it is very important to mimic the security vulnerability and create a good strong security model to establish in safe cloud environment. Major challenges involve:

- Lack of proper governance- Cloud providing organization have the complete control on resources but they have to provide the control to users once the resources is shared this can cause a big security gap. Google, Amazon and other cloud providers states that they don't take any responsibility, liability or authority for corruption, unauthorized etc. So this is a big major concern for the users.

- Malicious attack- Sometimes the architecture of cloud computing environments poses risks to the privacy and security of the customers [2]

- Insecure or incomplete data deletion- If client wants to delete the data will it delete the data accurately or it will just delete incompletely and which it will make a big data security concern due to multi-latency.

- Data interception- This treat poses more as more third part software and malicious codes are available for sniffing, spoofing etc.

6. CONCLUSION

Cloud computing are growing in faster rate. All type of industries are accepting the cloud computing technology. Data present in the cloud can be at high risk if the data is not protected properly. This paper discuss about data security, security concern and virtualization. This paper also discussed about the two states data at rest and data in transit.

REFERENCES

[1] https://www.techtarget.com/searchcloudcomputing/definition/cloudcomputing#:~:text=Cloud%20computing%20is%20a%20general,as%20a%20service%20(SaaS).

[2] Wang, Y., Chandrasekhar, S., Singhal, M., & Ma, J. (2016). A limited-trust capacity model for mitigating threats of internal malicious services in cloud computing. Cluster Computing,19(2), 647-662. doi:10.1007/s10586-016-0560-2