# Cloud Computing- Architecture, Security Issues and Challenges

**Name of Author – Jay Prakash Soja**

Designation – Assistant Professor

Name of Department – Department of Computer Engineering /Applications
Name of organization – Ambedkar Institute of Technology, Shakarpur, Delhi (India)

**Abstract-** Cloud computing is a type of technology that provides remote services on the internet to manage, access, and store data rather than storing it on Servers or local drives. This technology is also known as server-less technology. Here the data can be anything like Image, Audio, video, documents, files, etc. Cloud computing is the delivery of computing services—including developing new applications and services, servers, databases, networking, hosting blogs and websites, delivery of software on demand, analysis of data, intelligence, streaming videos and audios over the internet.

**Keywords** – Cloud Computing ; DaaS, SaaS, IaaS, PaaS, DoS, Interoperability, Load Balancing, Rapid elasticity

## I. INTRODUCTION

Cloud Computing is defined as storing and accessing of data and computing services over the internet. It doesn't store any data on your personal computer. It is the on-demand availability of computer services like servers, data storage, networking, databases, etc. The main purpose of cloud computing is to give access to data centers to many users. Users can also access data from aremote server.

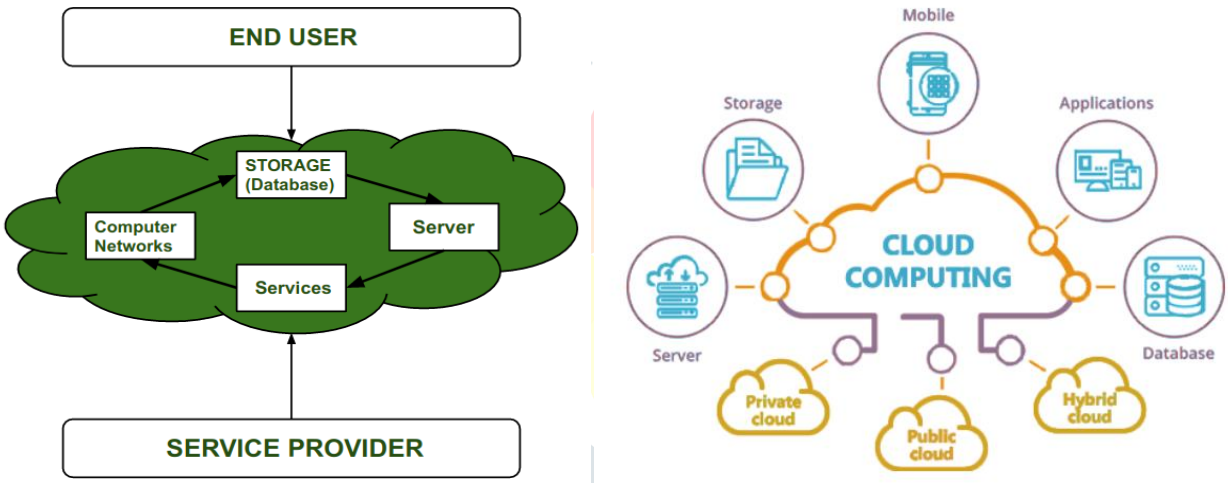


Fig-1 Cloud Computing (Application View)

**Need of Cloud Computing** -Before using Cloud Computing, most of the large as well as small IT companies use traditional methods i.e. they store data in Server, and they need a separate Server room for that. In that Server Room, there should be a database server, mail server, firewalls, routers, modems, high net speed devices, etc. For that IT compa nies have to spend lots of money. In order to reduce all the problems with cost, cloud computing come into existence and most companies shift to this technology. In 2009, Google Apps started to provide cloud computing enterprise applications.

**II. Cloud Computing Services -** Cloud computing is a general term for anything that involves delivering hosted services over the internet. These services are divided into four categories – Infrastructure as a Service (IaaS), Desktop as a Service (DaaS), Platform as a Service (PaaS) and Software as a Service (SaaS).

**Infrastructure as a Service (IaaS) -** IaaS is also known as Hardware as a Service (HaaS). It is one of the layers of the cloud computing platform. It allows customers to outsource their IT infrastructures such as servers, networking, processing, storage, virtual machines, and other resources. Customers access these resources on the Internet using a pay-as-per use model. In traditional hosting services, IT infrastructure was rented out for a specific period of time, with pre-determined hardware configuration.The client paid for the configuration and time, regardless of the actual use. With the help of the IaaS, clients can dynamically scale the configuration to meet changing requirements and are billed only for the services actually used. IaaS cloud computing platform layer eliminates the need for every organization to maintain the IT infrastructure. IaaS provides Computing as a Service (CaaS) includes virtual central processing units and virtual main memory for the Virtual machine that is provisioned to the end users. IaaS provider provides back-end storage for storing files. IaaS also works as Network as a Service (NaaS) that provides networking components such as routers, switches, and bridges for the Virtual machines.

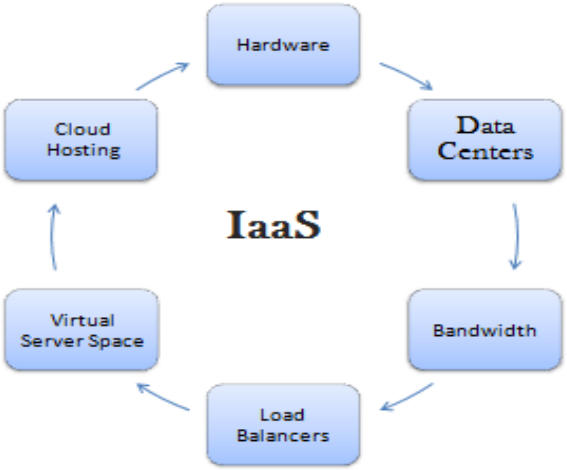


Fig-2 Infrastructure as a Service (IaaS)

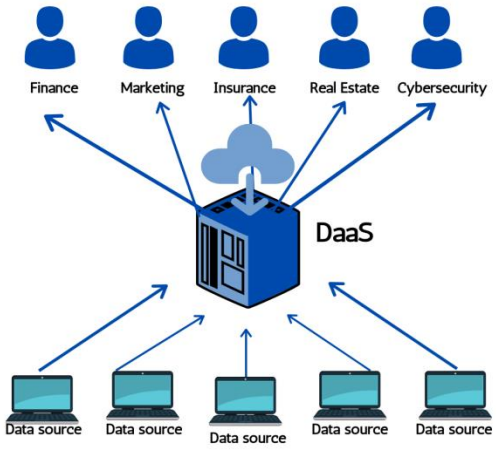


Fig-3 Desktop as a Service (DaaS)

**Desktop as a Service (DaaS) -** Desktop as a Service (DaaS) is a cloud computing offering where a service provider delivers virtual desktops to end users over the Internet, licensed with a per-user subscription. The provider takes care of backend management for small businesses that find creating their own virtual desktop infrastructure to be too expensive or resource-consuming. This management typically includes maintenance, back-up, updates, and data storage. Cloud service providers may also handle security and applications for the desktop, or users may manage these service aspects individually. With Desktop as a Service (DaaS), the cloud services provider hosts the infrastructure, network resources, and storage in the cloud and streams a virtual desktop to the user's device, where the user can access the desktop's data and applications through a web browser or other software. Organizations may purchase as many virtual desktops as they need through a subscription model.

**Software as a Service (SaaS) -** SaaS is also known as "on-demand software". It is a software in which the applications are hosted by a cloud service provider. Users can access these applications with the help of internet connection and web browser. SaaS is managed from a central location hosted on a remote server accessible over the internet. Users are not responsible for hardware and software updates. Updates are applied automatically. The services are purchased on the pay-as-per-use basis. Big Commerce, Google Apps, Salesforce, Dropbox, ZenDesk, Cisco WebEx, and GoToMeeting are the examples of SaaS.


Fig-4 Software as a Service (SaaS)


Fig-5 Plateform as a Service (PaaS)

**Platform as a Service (PaaS)** – It provides a runtime environment. It allows programmers to easily create, test, run, and deploy web applications. User can purchase these applications from a cloud service provider on a pay-as-per use basis and access them using the Internet connection. In PaaS, back end scalability is managed by the cloud service provider,so end- users do not need to worry about managing the infrastructure. PaaS provides platform (middleware, development tools, database management systems, business intelligence, and more) to support the web application life cycle.PaaS includes infrastructure (servers, storage, and networking). PaaS providers provide the Programming languages, Application frameworks, Databases, and Other tools. Google App Engine is the example of PaaS.

**Load Balancing -**Cloud load balancing is defined as dividing workload and computing properties in cloud computing. Load balancing is the method that allows you to have a proper balance of the amount of work being done on different pieces of device or hardware equipment. Typically the load of the devices is balanced between different servers or between the CPU and hard drives in a single cloud server. It is used to improve the speed and performance of each single device, and protect individual devices from hitting their limits by reducing their performance. It enables enterprises to manage workload demands or application demands by distributing resources among multiple computers, networks or servers.

**On-Demand Self-Service** - On-demand self service allows customers to use cloud computing as required without human contact between consumers and service providers. Using the features of on-demand self-service, consumers can arrange various cloud resources as needed. In addition to being safe and attentive to the client, the self-service system must be user-friendly in order to access the various cloud resources and to track the service offerings effectively. The primary benefit of on-demand self-service generating efficiencies for both consumers and providers of cloud services

***Resource Pooling***- The service provider's or enterprise's computing resources are pooled to serve multiple users through a multi-tenant model (i.e., many users can access the same location's resources). These different physical and virtual resources are assigned dynamically according to demand.

**Rapid Elasticity** -Elasticity is a 'rename' of scalability This is the capabilities available to users can be provisioned elastically and released when no longer needed, in some cases automatically. This allows rapid scaling, up or down, according to current demand.

**Multi-Cloud Strategy** -Multi-Cloud strategy involves the implementation of several cloud computing solutions simultaneously. It permits sharing of web, software, mobile apps, and other client-facing or internal assets across several cloud services or environments. Multi-cloud environment is used by the organisations for reduction of dependence on a single cloud service provider and improving fault tolerance.

**(III) Types of Cloud - Public Cloud**

Public Cloud provides a shared platform that is accessible to the general public through an Internet connection. Public cloud operated on the pay-as-per-use model and administrated by the third party viz Cloud service provider. In the Public cloud, the same storage is being used by multiple users at the same time. Public cloud is owned, managed, and operated by businesses, universities, government organizations, or a combination of them. Amazon Elastic Compute Cloud (EC2), Microsoft Azure, IBM's Blue Cloud, Sun Cloud, and Google Cloud are examples of the public cloud. Public Cloud is less secure because resources are shared publicly. Performance depends upon the high-speed internet network link to the cloud provider. The potential for cost saving is the major reason of cloud services adoption by many organizations. Cloud computing gives the freedom to use services as per the requirement and pay only for what you use.

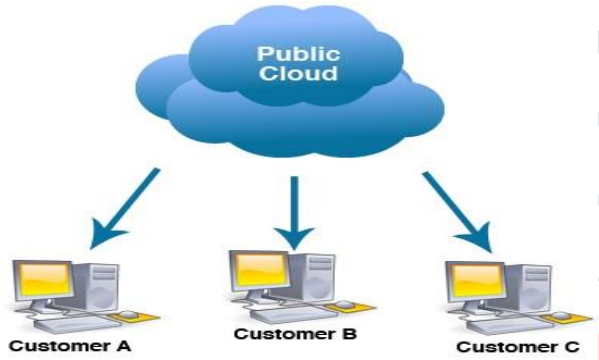


Fig-6 Public Cloud

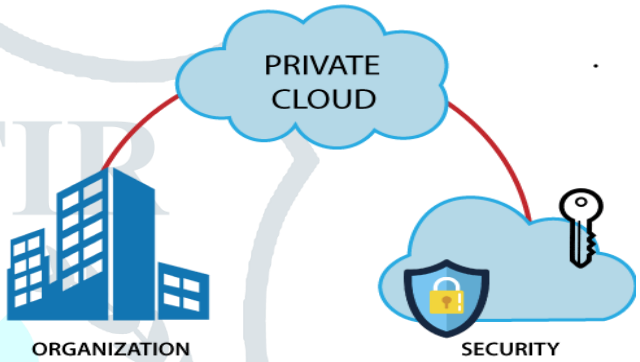


Fig-7 Private Cloud

**Private Cloud** – Private cloud is also known as an **internal cloud** or **corporate cloud.** It is used by organizations to build and manage their own data centers internally or by the third party. It can be deployed using Opensource tools such as Openstack and Eucalyptus. A private cloud provides IT services through the Internet or a private network to select users, rather than to the general public. All the data is protected behind a firewall. Private cloud provides a high level of security and privacy to the users. Private cloud offers better performance with improved speed and space capacity. It allows the IT team to quickly allocate and deliver on-demand IT resources. The organization has full control over the cloud because it is managed by the organization itself. So, there is no need for the organization to depends on anybody. It is suitable for organizations that require a separate cloud for their personal use and data security is the first priority. An organization properly architects and implements a private cloud, it can provide most of the same benefits found in public clouds, such as user self-service and scalability, as well as the ability to provision and configure virtual machines and optimize computing resources on demand. HP Data Centers, Microsoft, Elastra-private cloud, and Ubuntu are the example of a private cloud.

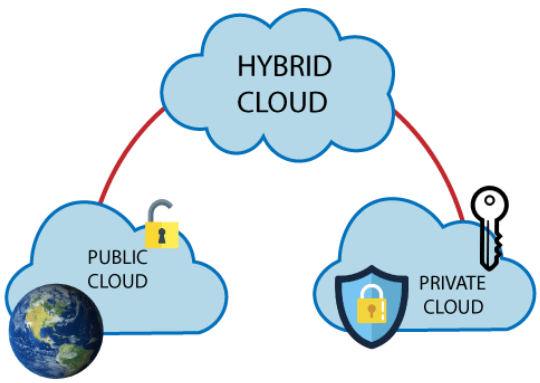


Fig-8 Hybrid Cloud

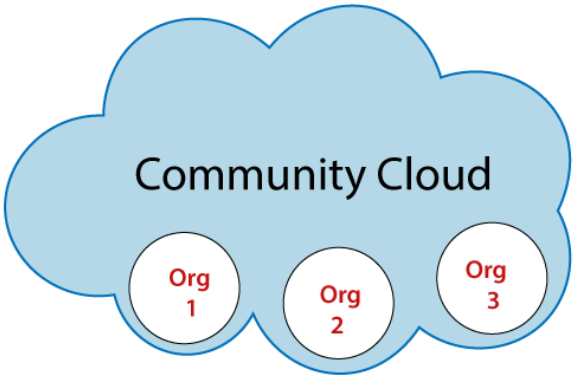


Fig-9 Community Cloud

**Hybrid Cloud**

Hybrid Cloud is a combination of the public cloud and the private cloud. Hybrid Cloud = Public Cloud + Private Cloud. Hybrid cloud is partially secure because the services which are running on the public cloud can be accessed by anyone, while the services which are running on a private cloud can be accessed only by the organization's users. Hybrid clouds are capable of crossing isolation and overcoming boundaries by the provider. Therefore, it cannot be simply categorized into public, private or community cloud. It allows the user to increase the capacity as well as the capability by assimilation, aggregation and customization with another cloud package / service. Hybrid cloud is suitable for organizations that require more security than the

public cloud. It helps you to deliver new products and services more quickly. Hybrid cloud provides an excellent way to reduce the risk. It offers flexible resources because of the public cloud and secure resources because of the private cloud. Google Application Suite (Gmail, Google Apps, and Google Drive), Office 365 (MS Office on the Web and One Drive), Amazon Web Services are examples of hybrid cloud.

**Community Cloud**

Community cloud allows systems and services to be accessible by a group of several organizations to share the information between the organization and a specific community. It is owned, managed, and operated by one or more organizations in the community, a third party, or a combination of them. The cost is shared by specific organizations within the community. Therefore, community cloud has cost saving capacity. It is cost-effective because the whole cloud is being shared by several organizations or communities. It is suitable for organizations that want to have a collaborative cloud with more security features than the public cloud. It provides better security than the public cloud. It provides collaborative and distributive environment. Community cloud allows us to share cloud resources, infrastructure, and other capabilities among various organizations.

**(IV) SECURITY ISSUES**

Cloud service models not only provide different types of services to users but they also reveal information which adds to security issues and risks of cloud computing systems. IaaS which is located in the bottom layer, which directly provides the most powerful functionality of an entire cloud. IaaS also enables hackers to perform attacks, e.g. brute-forcing cracking, that need high computing power. Multiple virtual machines are supported by IaaS, gives an ideal platform for hackers to launch attacks that require a large number of attacking instances. Loss of data is another security risk of cloud models.

Data in cloud models can be easily accessed by unauthorized internal employees, as well as external hackers. The internal employees can easily access data intentionally or accidently. External hackers may gain access to databases in such environments using hacking techniques like session hijacking and network channel eavesdropping. Virus and Trojan can be uploaded to cloud systems and can cause damage. It is important to identify the possible cloud threats in order to implement a system which has better security mechanisms to protect cloud computing environments.

**Data Loss**

Data Loss is one of the issues faced in Cloud Computing. This is also known as Data Leakage. As we know that our sensitive data is in the hands of Somebody else, and we don't have full control over our database. So if the security of cloud service is to break by hackers then it may be possible that hackers will get access to our sensitive data or personal files

**Hacked interfaces and APIs**

Today every cloud service and application now offers APIs. IT teams use these interfaces and APIs to manage and interact with cloud services, including those that offer cloud provisioning, management and monitoring. The security and availability of cloud services depend on the security of the API. Risk is increased with third parties who rely on APIs and build on these interfaces, as organizations may need to expose more services and credentials. APIs and weak interfaces may expose organizations to security related issues such as confidentiality, accountability, availability APIs and interfaces are the very much exposed part of the system because they can be accessed from public networks.

**Account Hijacking**

Phishing, fraud, and software exploits are highly prevalent today, and cloud services add a new dimension to the threat because attackers can eavesdrop on activities, manipulate transactions, and modify data. Attackers may be able to use the cloud application to launch other attacks. Organizations must prohibit sharing of account credentials between users and services and must enable multifactor authentication schemes where available. Accounts, must be monitored so that every transaction should be traced to a human owner. The key is to protect account credentials from being stolen.

**Changing Service Provider**

Vendor lock In is also an important Security issue in Cloud Computing. Many organizations will face different problems while shifting from one vendor to another. For example, An Organization wants to shift from AWS Cloud to Google Cloud Services then they ace various problem's like shifting of all data, also both cloud services have different techniques and functions, so they also face problems regarding that. Also, it may be possible that the charges of AWS are different from Google Cloud etc.

**Denial of Service (DoS) attack**

This type of attack occurs when the system receives too much traffic. Mostly DoS attacks occur in large organizations such as the banking sector, government sector, etc. When a DoS attack occurs data is lost. So in order to recover data, it requires a great amount of money as well as time to handle it.

**Flooding Attacks**

In this type of attack the invader sends large number of requests for resources on the cloud rapidly so that the cloud gets flooded with the large number of requests. As per the study carried out by IBM cloud has a property to expand on the basis of amount of request. It will expand in so that it fulfills the requests of invader making the resources inaccessible for the normal users.

**(V) CHALLANGES**

Cloud computing, an emergent technology, has placed many challenges in different aspects of data and information handling.

**Data Security and Privacy**

Data security is a major concern when switching to cloud computing. User or organizational data stored in the cloud is critical and private. Even if the cloud service provider assures data integrity, it is your responsibility to carry out user authentication and authorization, identity management, data encryption, and access control. Security issues on the cloud include identity theft, data breaches, malware infections, and a lot more which eventually decrease the trust amongst the users of your applications. This can in turn lead to potential loss in revenue alongside reputation and stature. Also, dealing with cloud computing requires sending and receiving huge amounts of data at high speed, and therefore is susceptible to data leaks.Security and Privacy of information is the biggest challenge to cloud computing. Security and privacy issues can be overcome by employing encryption, security hardware and security applications.

**Cost Management**

Even as almost all cloud service providers have a "Pay As You Go" model, which reduces the overall cost of the resources being used, there are times when there are huge costs incurred to the enterprise using cloud computing. When there is under

optimization of the resources, let's say that the servers are not being used to their full potential, add up to the hidden costs. If there is a degraded application performance or sudden spikes or overages in the usage, it adds up to the overall cost. Unused resources are one of the other main reasons why the costs go up. If you turn on the services or an instance of cloud and forget to turn it off during the weekend or when there is no current use of it, it will increase the cost without even using the resources.

**Multi-Cloud Environments**

Due to an increase in the options available to the companies, enterprises not only use a single cloud but depend on multiple cloud service providers. Most of these companies use hybrid cloud tactics and close to 84% are dependent on multiple clouds. This often ends up being hindered and difficult to manage for the infrastructure team. The process most of the time ends up being highly complex for the IT team due to the differences between multiple cloud providers.

**Performance Challenges**

Performance is an important factor while considering cloud-based solutions. If the performance of the cloud is not satisfactory, it can drive away users and decrease profits. Even a little latency while loading an app or a web page can result in a huge drop in the percentage of users. This latency can be a product of inefficient load balancing, which means that the server cannot efficiently split the incoming traffic so as to provide the best user experience. Challenges also arise in the case of fault tolerance, which means the operations continue as required even when one or more of the components fail.

**Portability-**This is another challenge to cloud computing that applications should easily be migrated from one cloud provider to another. There must not be vendor lock-in. However, it is not yet made possible because each of the cloud provider uses different standard languages for their platforms.

**Interoperability-** When an organization uses a specific cloud service provider and wants to switch to another cloud-based solution, it often turns up to be a tedious procedure since applications written for one cloud with the application stack are required to be re-written for the other cloud. There is a lack of flexibility from switching from one cloud to another due to the complexities involved. Handling data movement, setting up the security from scratch and network also add up to the issues encountered when changing cloud solutions, thereby reducing flexibility. Computing Performance- Data intensive applications on cloud requires high network bandwidth, which results in high cost. Low bandwidth does not meet the desired computing performance of cloud application.

**Reliability and Availability -** It is necessary for cloud systems to be reliable and robust because most of the businesses are now becoming dependent on services provided by third-party.

**Conclusion**

Cloud Computing is growing concept of availing software and hardware services from a cloud server through internet that leads to a number of benefits for its users. But it also raises some security problems which may affect its usage. Since Cloud Computing consists of connecting various cloud servers of different service providers, so data security and stealing important information is a big challenge. In various cloud service models like IaaS, PaaS, and SaaS, the performance depends on the network bandwith being provided by service providers . As described in this paper, storage and networks are the biggest security concerns in Cloud Computing. Virtualization that allows multiple users to share a physical server is a major concerns for cloud users. Virtual networks are target for some attacks.

**REFERENCES**

1. Cloud Computing Simplified' by Surbhi Rastogi
2. Fundamentals of Cloud Computing by Pattnaik P
3. Fundamentals of Cloud Computing by Prashant Kumar
4. MASTERING CLOUD COMPUTING BY BUYYA, VECCHIOLA AND SELVI
5. Cloud Computing Black Book by Kailash Jayaswal and John Wiley
6. The A To Z Of Cloud Computing by Swapnil Saurav.
7. Handbook of Cloud Computing by Dr. Anand Nayyar by BPB Publications
8. Cloud Computing by Dr Rajiv Chopra
9. Cloud Computing: A Hands-on Approach by Vijay K. Madisetti
10. Cloud Computing: Concepts, Technology & Architecture by Thomas Erl