CC UNIT III

CLOUD ARCHITECTURE- LAYERS AND MODELS

CLOUD ARCHITECTURE

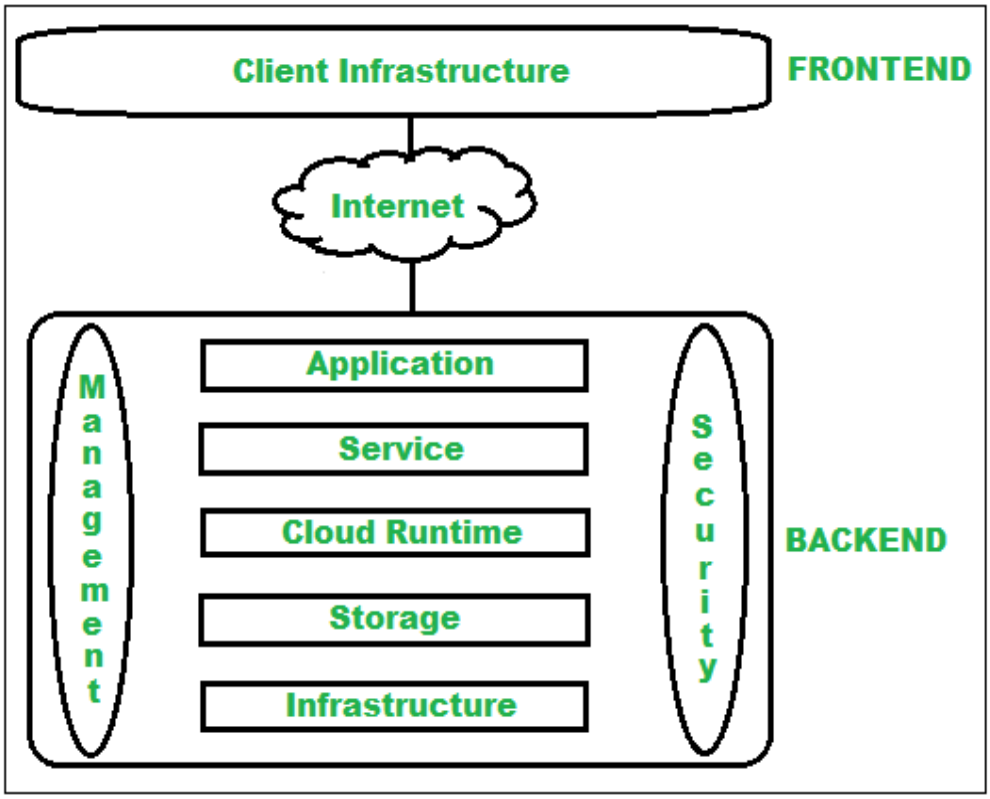


Figure 1: Cloud Architecture

Front End

- The front end is used by the client.
- It contains client-side interfaces and applications that are required to access the cloud computing platforms.
- The front end includes web servers (including Chrome, Firefox, internet explorer, etc.), thin & fat clients, tablets, and mobile devices.

Back End

- The back end is used by the service provider.
- It manages all the resources that are required to provide cloud computing services.
- It includes a huge amount of data storage, security mechanisms, virtual machines, deploying models, servers, traffic control mechanisms, etc.

Note: Both front end and back end are connected to others through a network, generally using the internet connection

Components of Cloud Computing Architecture

There are the following components of cloud computing architecture -

Client Infrastructure

- Client Infrastructure is a Front end component.
- It provides GUI (Graphical User Interface) to interact with the cloud.

Application

- The application may be any software or platform that a client wants to access.

Service

- A Cloud Service manages which type of service you access according to the client's requirement.

Runtime Cloud

- Runtime Cloud provides the execution and runtime environment to the virtual machines.

Storage

- Storage is one of the most important components of cloud computing.
- It provides a huge amount of storage capacity in the cloud to store and manage data.

Infrastructure

- It provides services on the host level**,** application level**,** and network level**.**
- Cloud infrastructure includes hardware and software components such as servers, storage, network devices, virtualization software, and other storage resources that are needed to support the cloud computing model.

Management

- Management is used to manage components such as application, service, runtime cloud, storage, infrastructure, and other security issues in the backend and establish coordination between them.

Security

- Security is an in-built back end component of cloud computing. It implements a security mechanism in the back end.

Internet

- The Internet is medium through which front end and back end can interact and communicate with each other.

LAYERS IN CLOUD ARCHITECTURE

- Cloud is the outcome of several layers of cloud architecture intelligently placed over one another.
- Cloud computing architecture is made of several layers for better operational efficiency.
- Below is a general picture of cloud layers.

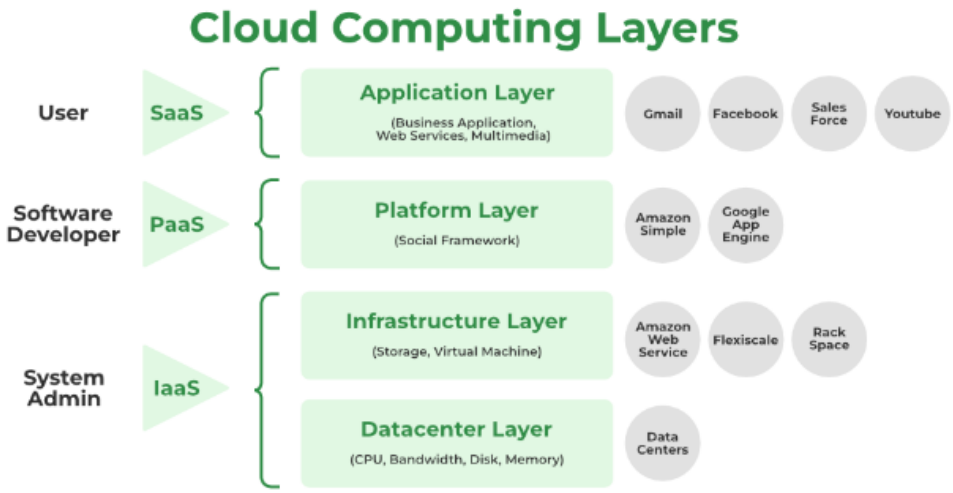


Figure 2: Cloud Computing Layers

Application Layer

- The application layer, which is at the top of the stack, is where the actual cloud apps are located.
- Cloud applications, as opposed to traditional applications, can take advantage of the automatic-scaling functionality to gain greater performance, availability, and lower operational costs.
- This layer consists of different Cloud Services which are used by cloud users.
- Users can access these applications according to their needs.

Platform Layer

- The operating system and application software make up this layer.
- Users should be able to rely on the platform to provide them with Scalability, Dependability, and Security Protection which gives users a space to create their apps, test operational processes, and keep track of execution outcomes and performance.

Infrastructure Layer

- It is a layer of virtualization where physical resources are divided into a collection of virtual resources using virtualization technologies like Xen, KVM, and VMware.
- This layer serves as the Central Hub of the Cloud Environment, where resources are constantly added utilizing a variety of virtualization techniques.
- The infrastructure layer is crucial to cloud computing since virtualization technologies are the only ones that can provide many vital capabilities, like dynamic resource assignment.

Datacenter Layer

- This layer is also known as Hardware Layer.
- This bottom most layer of cloud architecture, the hardware layer, primarily deals with all the hardware powering clouds.
- The hardware includes but is not restricted to routers, servers, switches, power and cooling systems.
- In a cloud environment, this layer is responsible for Managing Physical Resources such as servers, switches, routers, power supplies, and cooling systems.
- Providing end users with services requires all resources to be available and managed in data centers.
- Physical servers connect through high-speed devices such as routers and switches to the data center.

Service Layer

- The Service Layer is spread across all the layers of cloud computing.
- Each Cloud Computing Layer deploys a service model/ Deployment Model or Service Layer.
- They are also known as actual layers of Cloud Computing. They are:
    - Infrastructure as a Service(IaaS)
    - Platform as a Service(PaaS)
    - Software as a service. (SaaS)
- Each service or the layer has its own characteristic advantage.
- The IaaS is the most suitable for organizations who covet the ultimate control of their cloud platform.
- PaaS is more apt for users who want an Operating System or any other software pre-installed in the cloud.
- Even if these users were to opt for IaaS, they would reap no added benefits because their requirements are different altogether.
- Similarly, software as a service is meant for less proficient users, who only need an application to perform specific functions.
- SaaS clients only concern themselves with the applications and not the cloud architecture.
- Some users might not even have an idea that their service is running with cloud computing underlying it.

INFRASTRUCTURE AS A SERVICE (IaaS)

- IaaS is also known as **Hardware as a Service (HaaS)**.
- IaaS is the basic layer of the cloud that comprises hardware and network.
- IaaS is used by Network Architects.
- It gives access to the resources like virtual machines and virtual storage.
- 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.
- IaaS is offered in three models: public, private, and hybrid cloud.
- The private cloud implies that the infrastructure resides at the customer-premise.
- In the case of public cloud, it is located at the cloud computing platform vendor's data center, and the hybrid cloud is a combination of the two in which the customer selects the best of both public cloud and private cloud.
- IaaS provider provides the following services -
    - **Compute:** Computing as a Service includes virtual central processing units and virtual main memory for the Vms that is provisioned to the end- users.
    - **Storage:** IaaS provider provides back-end storage for storing files.
    - **Network:** Network as a Service (NaaS) provides networking components such as routers, switches, and bridges for the Vms.
    - **Load balancers:** It provides load balancing capability at the infrastructure layer.

Figure 3: Services provided by IaaS Providers

- **Example:** DigitalOcean, Linode, Amazon Web Services (AWS), Microsoft Azure, Google Compute Engine (GCE), Rackspace, and Cisco Metacloud.

FEATURES OF IaaS

Following are the features of IaaS -

- **Resources are available as a service:** IaaS cloud computing platform layer eliminates the need for every organization to maintain the IT infrastructure.
- **Services are highly scalable:** With the help of the IaaS cloud computing platform layer, clients can dynamically scale the configuration to meet changing requirements and are billed only for the services actually used.
- **Dynamic and flexible:** IaaS offers a flexible and dynamic solution for IT organizations or software developers that wish to address their IT infrastructure needs with a cloud-based outsourcing model.
- **GUI and API-based access:** Customers can provision, configure and operate the servers and infrastructure resources via a graphical dashboard, or programmatically through application programming interfaces (APIs).
- **Automated administrative tasks**
    - IT organizations that manage data centers and hardware infrastructure in the on premise model are responsible for routine updates, patches, and maintenance activities that can affect the availability of hardware resources and the software applications that depend on them.
    - In contrast, IaaS service providers handle upgrades and maintenance to their servers without compromising infrastructure availability for customers.

ADVANTAGES OF IaaS

- **Shared infrastructure**: IaaS allows multiple users to share the same physical infrastructure.
- **Web access to the resources**: Iaas allows IT users to access resources over the internet.
- **Pay-as-per-use model**: IaaS providers provide services based on the pay-as-per-use basis. The users are required to pay for what they have used.

- **Focus on the core business**: IaaS providers focus on the organization's core business rather than on IT infrastructure.
- **On-demand scalability**: On-demand scalability is one of the biggest advantages of IaaS. Using IaaS, users do not worry about to upgrade software and troubleshoot the issues related to hardware components.

DISADVANTAGES OF IaaS

- **Security**: Security is one of the biggest issues in IaaS. Most of the IaaS providers are not able to provide 100% security.
- **Maintenance & Upgrade**: Although IaaS service providers maintain the software, but they do not upgrade the software for some organizations.
- **Interoperability issues**: It is difficult to migrate VM from one IaaS provider to the other, so the customers might face problem related to vendor lock-in.

PLATFORM AS A SERVICE (PAAS)

- It is used by Developers.
- Platform as a Service (PaaS) provides a runtime environment.
- It allows programmers to easily create, test, run, and deploy web applications
- One can purchase these applications from a cloud service provider on a pay-as-per use basis and access them using the Internet connection.
- A PaaS provider hosts the hardware and software on its own infrastructure.
- As a result, PaaS frees users from having to install in-house hardware and software to develop or run a new application.
- Thus, the development and deployment of the application take place independent of the hardware**.**
- PaaS includes infrastructure (servers, storage, and networking) and platform (middleware, development tools, database management systems, business intelligence, and more) to support the web application life cycle.
- PaaS providers provide the Programming languages, Application frameworks, Databases, and Other tools:
    - **Programming languages:** PaaS providers provide various programming languages for the developers to develop the applications. Some popular programming languages provided by PaaS providers are Java, PHP, Ruby, Perl, and Go.
    - **Application frameworks:** PaaS providers provide application frameworks to easily understand the application development. Some popular application frameworks provided by PaaS providers are Node.js, Drupal, Joomla, WordPress, Spring, Play, Rack, and Zend.
    - **Databases:** PaaS providers provide various databases such as Clear DB, PostgreSQL, MongoDB, and Redis to communicate with the applications.
    - **Other tools:** PaaS providers provide various other tools that are required to develop, test, and deploy the applications.

Figure 4: Services provided by PaaS Providers

Example: Google App Engine, Force.com, Joyent, Azure.

FEATURES OF PAAS

There are the following characteristics of PaaS -

- **Development Environment**: PaaS provides a development environment for building and testing applications, with tools for code development, version control, and collaboration.
- **Multi-tenancy:** PaaS is designed to support multi-tenancy, allowing multiple customers to share the same infrastructure and resources while keeping their applications and data isolated.
- **Integration:** PaaS provides integrated tools and services for application development, such as databases, messaging systems, and caching, that can be easily integrated into applications.
- **Infrastructure Management:** PaaS abstracts the underlying infrastructure, allowing developers to focus on building and deploying applications without worrying about hardware and network infrastructure
- **Scalability:** PaaS provides the ability to automatically scale applications and services as demand changes, without manual intervention.

ADVANTAGES OF PaaS

- **Simplified Development**: PaaS allows developers to focus on development and innovation without worrying about infrastructure management.
- **Lower risk**: No need for up-front investment in hardware and software. Developers only need a PC and an internet connection to start building applications.
- **Prebuilt business functionality**: Some PaaS vendors also provide already defined business functionality so that users can avoid building everything from very scratch and hence can directly start the projects only.
- **Instant community**: PaaS vendors frequently provide online communities where the developer can get the ideas to share experiences and seek advice from others.

- **Scalability**: Applications deployed can scale from one to thousands of users without any changes to the applications.

DISADVANTAGES OF PaaS

- **Vendor lock-in**: One has to write the applications according to the platform provided by the PaaS vendor, so the migration of an application to another PaaS vendor would be a problem.
- **Data Privacy**: Corporate data, whether it can be critical or not, will be private, so if it is not located within the walls of the company, there can be a risk in terms of privacy of data.
- **Integration with the rest of the systems applications**: It may happen that some applications are local, and some are in the cloud. So there will be chances of increased complexity when we want to use data which in the cloud with the local data.

SOFTWARE AS A SERVICE (SAAS)

- SaaS is also known as "**on-demand software**".
- SAAS is used by the end user.
- It is highly scalable to suit the small, mid and enterprise level business.
- Users can access these applications with the help of internet connection and web browser.
- It is a software distribution model in which services are hosted by a cloud service provider.
- These services are available to end-users over the internet so, the end-users do not need to install any software on their devices to access these services.
- There are the following services provided by SaaS providers -
    - **Business Services** - SaaS Provider provides various business services to start-up the business. The SaaS business services include **ERP** (Enterprise Resource Planning), **CRM** (Customer Relationship Management), **billing**, and **sales**.
    - **Document Management** - SaaS document management is a software application offered by a third party (SaaS providers) to create, manage, and track electronic documents.
    - **Example:** Slack, Samepage, Box, and Zoho Forms.
    - **Social Networks** - As we all know, social networking sites are used by the general public, so social networking service providers use SaaS for their convenience and handle the general public's information.
    - **Mail Services** - To handle the unpredictable number of users and load on e-mail services, many e-mail providers offering their services using SaaS.

Figure 5: Services provided by SaaS Providers

FEATURES OF SAAS

Following are the features of SaaS –

- **Multitenant Architecture**:
  - Multitenant architecture is one in which all users and apps share a single, centrally maintained infrastructure and codebase.
  - Because all SaaS vendor clients share the same cloud infrastructure and code base, vendors can innovate faster and save on development.
- **Easy Customization**:
  - Each user has capacity to readily customize programs to meet their business operations without compromising the shared cloud infrastructure.
  - These customizations are unique to each firm or user, and they are always kept during upgrades, according to the way SaaS is designed.
  - As a result, SaaS companies can upgrade their software frequently, with minimal risk to their customers and a reduced cost of adoption.
- **Subscription based billing:** Software as a Service applications are subscription based, and this enables customers to buy the SaaS applications whenever they require them and discontinue whenever the enterprise decides that they are not needed any more.
- **Improved Access:** SaaS architecture offers better access to data than any other network so that all users have secured access to the same information, making it easier for them to collaborate
- **Security:** SaaS offers encrypted storage that limits access to sensitive information. You can also integrate the SaaS application with external Key Management Frameworks to ensure extra protection.
- **Collaboration:** SaaS applications facilitate multiple users to collaborate. It allows users to comment, assign and share tasks on the application to work together.

ADVANTAGES OF SaaS

- **SaaS is easy to buy**: SaaS pricing is based on a monthly fee or annual fee subscription, so it allows organizations to access business functionality at a low cost, which is less than licensed applications.
- **One to Many**: SaaS services are offered as a one-to-many model i.e. a single instance of the application is shared by multiple users.
- **Less hardware required for SaaS**: The software is hosted remotely, so organizations do not need to invest in additional hardware.
- **Low maintenance required for SaaS**
  - Software as a service removes the need for installation, set-up, and daily maintenance for the organizations.
  - The initial set-up cost for SaaS is typically less than the enterprise software.
  - SaaS vendors are pricing their applications based on some usage parameters, such as a number of users using the application.
  - So SaaS is easy to monitor and does automatic updates.
- **No special software or hardware versions required**
  - All users will have the same version of the software and typically access it through the web browser.
  - SaaS reduces IT support costs by outsourcing hardware and software maintenance and support to the IaaS provider.

- **Multidevice support**: SaaS services can be accessed from any device such as desktops, laptops, tablets, phones, and thin clients.
- **API Integration**: SaaS services easily integrate with other software or services through standard APIs.
- **No client-side installation**: SaaS services are accessed directly from the service provider using the internet connection, so do not need to require any software installation.

DISADVANTAGES OF SaaS

- **Security**: Actually, data is stored in the cloud, so security may be an issue for some users. However, cloud computing is not more secure than in-house deployment.
- **Latency issue**
- Since data and applications are stored in the cloud at a variable distance from the end-user, there is a possibility that there may be greater latency when interacting with the application compared to local deployment.
- Therefore, the SaaS model is not suitable for applications whose demand response time is in milliseconds.
- **Total Dependency on Internet**: Without an internet connection, most SaaS applications are not usable.
- **Switching between SaaS vendors is difficult**: Switching SaaS vendors involves the difficult and slow task of transferring the very large data files over the internet and then converting and importing them into another SaaS also.

SERVICE PROVIDERS OF CLOUD COMPUTING

- A CSP (cloud service provider) is a third-party company that provides scalable computing resources that businesses can access on demand over a network, including cloud-based compute, storage, platform, and application services.
- Cloud Service providers (CSP) offers various services such as Software as a Service**,** Platform as a service and Infrastructure as a service**.**
- The cloud service providers host these services in a data center, and users can access these services through cloud provider companies using an Internet connection.

IaaS Providers

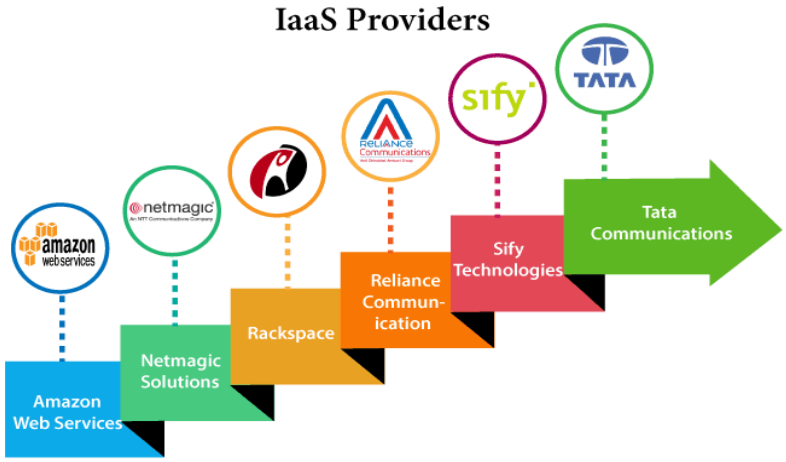


Figure 6: IaaS Providers

IaaS Vendor	Iaas Solution	Details
Amazon Web Services	Elastic, Elastic Compute Cloud (EC2) MapReduce, Route 53, Virtual Private Cloud, etc.	The cloud computing platform pioneer, Amazon offers auto scaling, cloud monitoring, and load balancing features as part of its portfolio.
Netmagic Solutions	Netmagic IaaS Cloud	Netmagic runs from data centers in Mumbai, Chennai, and Bangalore, and a virtual data center in the United States. Plans are underway to extend services to West Asia.
Rackspace	Cloud servers, cloud files, cloud sites, etc.	The cloud computing platform vendor focuses primarily on enterprise-level hosting services.
Reliance Communications	Reliance Internet Data Center	RIDC supports both traditional hosting and cloud services, with data centers in Mumbai, Bangalore, Hyderabad, and Chennai. The cloud services offered by RIDC include IaaS and SaaS.
Sify Technologies	Sify IaaS	Sify's cloud computing platform is powered by HP's converged infrastructure. The vendor offers all three types of cloud services: IaaS, PaaS, and SaaS.
Tata Communications	InstaCompute	InstaCompute is Tata Communications' IaaS offering. InstaCompute data centers are located in Hyderabad and Singapore, with operations in both countries.

PaaS Providers

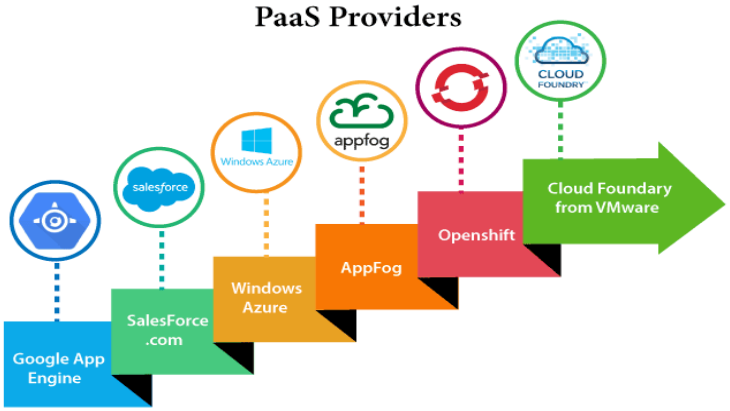


Figure 7: PaaS Providers

Providers	Services
Google App Engine (GAE)	App Identity, URL Fetch, Cloud storage client library, Log service
Salesforce.com	Faster implementation, Rapid scalability, CRM Services, Sales cloud, Mobile connectivity, Chatter.
Windows Azure	Compute, security, IoT, Data Storage.
AppFog	Justcloud.com, SkyDrive, GoogleDocs
Openshift	RedHat, Microsoft Azure.
Cloud Foundry from VMware	Data, Messaging, and other services.

The above table shows some popular PaaS providers and services that are provided by them -

SaaS Providers

Figure 8: SaaS Providers

The below table shows some popular SaaS providers and services that are provided by them -

Provider	Services
Salseforce.com	On-demand CRM solutions
Microsoft Office 365	Online office suite
Google Apps	Gmail, Google Calendar, Docs, and sites
NetSuite	ERP, accounting, order management, CRM, Professionals Services Automation (PSA), and e-commerce applications.
GoToMeeting	Online meeting and video-conferencing software
Constant Contact	Email marketing, online survey, and event marketing
Oracle CRM	CRM applications
Workday, Inc.	Human capital management, payroll, and financial management.

CHALLENGES AND RISKS IN CLOUD ADOPTION

Following are the challenges and risks in cloud adoption:

- Data Security and Privacy
- Compliance Risks
- Reduced Visibility and Control
- Cloud Migration
- Incompatibility
- Improper Access Controls and Management
- Lack of Expertise
- Downtime
- Insecure API

Data Security and Privacy

- The biggest concern with cloud computing is data security and privacy.
- As organizations adopt the cloud on a global scale, the risks have become more grave than ever, with lots of consumer and business data available for hackers to breach.
- The problem with cloud computing is that the user cannot view where their data is being processed or stored.
- And if it is not handled correctly during cloud management or implementation, risks can happen such as data theft, leaks, breaches, compromised credentials, hacked APIs, authentication breaches, account hijacking, etc.

Compliance Risks

- Compliance rules are getting more stringent due to the increased cyberattacks and data privacy issues.
- Regulatory bodies like HIPAA, GDPR, etc., ensure organizations comply with applicable state or federal rules and regulations to maintain data security and privacy for their business and customers.
- The issues arise for anyone using cloud storage or backup services.
- When organizations move their data from on-premises to the cloud, they must comply with the local laws. For example, every healthcare institution must comply with HIPAA in the US.
- And if they don't do it by any means, they could face penalties that can tarnish their reputation and cost them money and customer trust.

Reduced Visibility and Control

- Cloud computing offers the benefit of not having to manage the infrastructure and resources like servers to keep the systems working.
- Although it saves time, expenses, and effort, the users end up having reduced control and visibility into their software, systems, applications, and computing assets.
- As a result, organizations find it challenging to verify how efficient the security systems are due to no access to the data and security tools on the cloud platform.
- They also can't implement incident response because they don't have complete control over their cloud-based assets.
- In addition, organizations can't have complete insight into their services, data, and users to identify abnormal patterns that can lead to a breach.

Cloud Migration

- Cloud migration means moving your data, services, applications, systems, and other information or assets from on-premises (servers or desktops) to the cloud.
- This process enables computing capabilities to take place on the cloud infrastructure instead of on premise devices.
- When an organization wants to embrace the cloud, it can face many challenges while moving all its legacy or traditional systems to the cloud.
- The overall process can consume a lot of time, resources, and they have little idea how to deal with expert cloud providers already in business for years.
- Similarly, when they want to migrate from one cloud provider to another, they have to do it all over again, and they are not sure how the next provider will serve them.
- They face challenges like extensive troubleshooting, speed, security, application downtime, complexity, expenses, and more.
- All these are troublesome for organizations and also for their users.
- Ultimately, it can lead to poor user experience and thus, affect organizations in various directions.

Incompatibility

- While moving your workload to the cloud from on-premises, incompatibility issues may arise between the cloud services and on-premises infrastructure.
- This is a big challenge that may require the organizations to invest in making it compatible by any means or by creating a new service altogether.
- Either way, it invites troubles and expenditures for organizations.
- If most services of the chosen cloud are incompatible, you may move to the next service provider you have shortlisted and repeat the same process to find the best one suitable for your needs.

Improper Access Controls and Management

- Improper or inadequate cloud access controls and management can lead to various risks for an organization.
- Cybercriminals leverage web apps, steal credentials, perform data breaches, and whatnot. They may face access management issues if they have a large or distributed workforce.
- In addition, organizations can also face password fatigue and other issues such as inactive users signed for long terms, poorly protected credentials, weak passwords, multiple admin accounts, mismanagement of passwords, certificates, and keys, and more.
- As a result of poor access controls and management, organizations can be vulnerable to attacks.

Lack of Expertise

- Cloud technologies are rapidly advancing, and more and more services and applications are being released to cater to different needs.
- However, it's also becoming difficult for organizations to find skilled professionals to maintain the cloud systems.
- It's also costly for small and medium-sized businesses to hire expert cloud professionals.
- The reason is the cloud is a new concept for many, and it's still not mainstream. Not everyone in the team will be familiar with cloud technologies. And hence, the IT staff must also be trained how to use the cloud technologies efficiently by themselves.
- It again incurs a high cost, which is a burden for organizations with a limited budget.
- They will have to pay for the instructor and invest in recruiting and onboarding cloud professionals.

Downtime

- Another irritating thing about the cloud for many organizations can be downtime due to poor internet connection.
- If you have a consistent and high-speed internet connection, you can make the most of their cloud services.
- But if you don't, you may face repeated downtimes, lags, and errors.

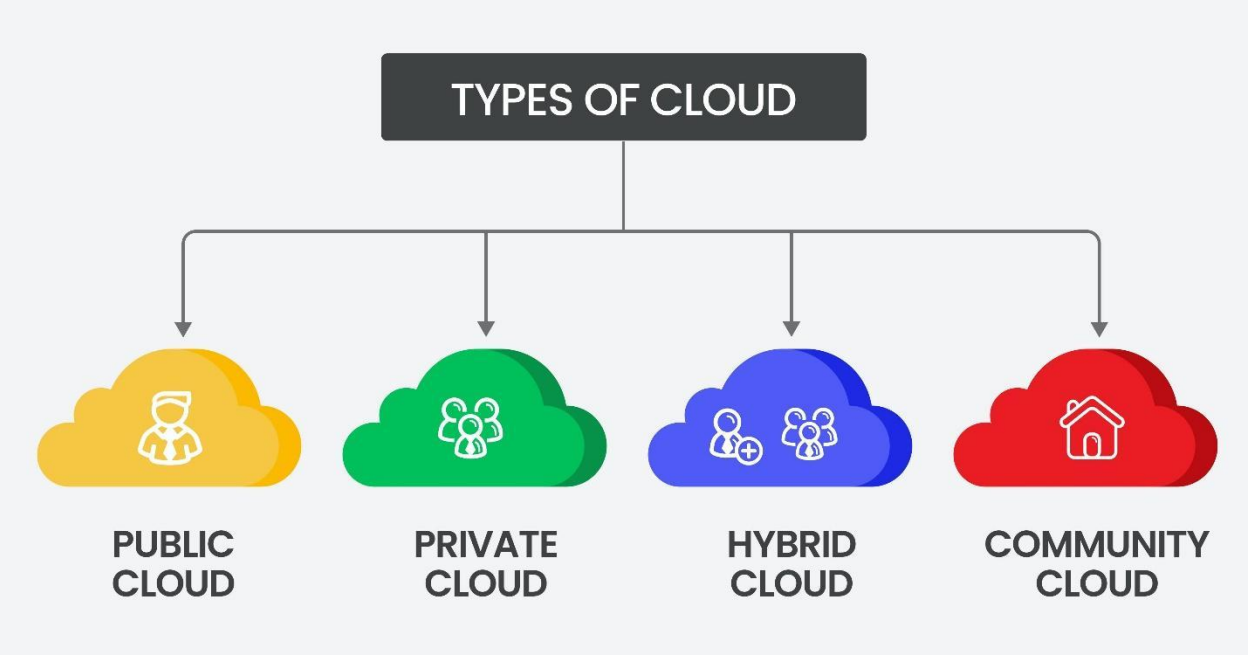
- It not only frustrates the users but also reduces their productivity.
- This way, organizations with poor internet connectivity are likely to face disruption in their business operations.
- They won't be able to access their data whenever they want. Hence, they can meet a lot of inefficiencies, missed deadlines etc.

Insecure APIs

- Using application interfaces APIs in cloud infrastructure enables you to implement better controls for your systems and applications.
- They are either in-built into the mobile apps or web to allow the employees and users to access the systems.
- However, if the external APIs you use are insecure, it can invite a lot of trouble for you in terms of security.
- These issues can provide an entry point for attackers to hack into your confidential data, manipulate services, and do other harm.
- Insecure APIs can cause broken authentication, security misconfigurations, break function-level authorization, expose data, and mismanagement of resources and assets.

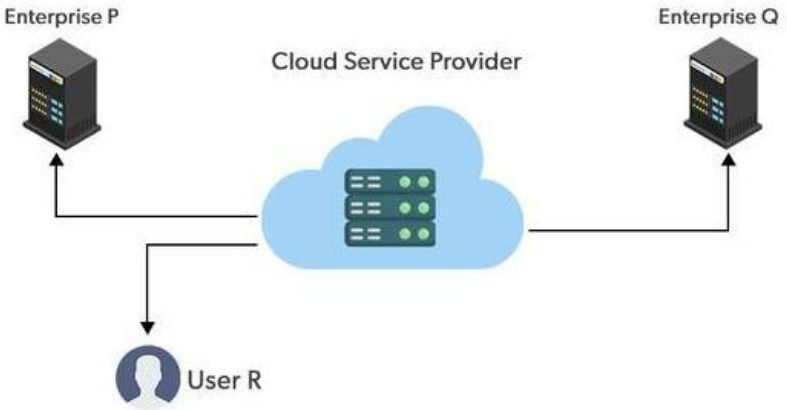
CLOUD DEPLOYMENT MODELS

- The cloud deployment model identifies the specific type of cloud environment based on ownership, scale, and access, as well as the cloud's nature and purpose.
- The location of the servers you're utilizing and who controls them are defined by a cloud deployment model.
- It specifies how your cloud infrastructure will look, what you can change, and whether you will be given services or will have to create everything yourself.
- Relationships between the infrastructure and the users are also defined by cloud deployment types.
- Different types of cloud computing deployment models are described below:
  - Public Cloud
  - Private Cloud
  - Hybrid Cloud
  - Community Cloud



PUBLIC CLOUD

- Public Cloud provides a shared platform that is accessible to the general public through an Internet connection.
- Public cloud is operated on the pay-as-per-use model and administered by the third party, i.e., Cloud service provider.
- In the Public cloud, the same storage is being used by multiple users at the same time.
- Public clouds are the go-to option for small enterprises, which can start their businesses without large upfront investments by completely relying on public infrastructure for their IT needs.
- 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.



Advantages of Public Cloud

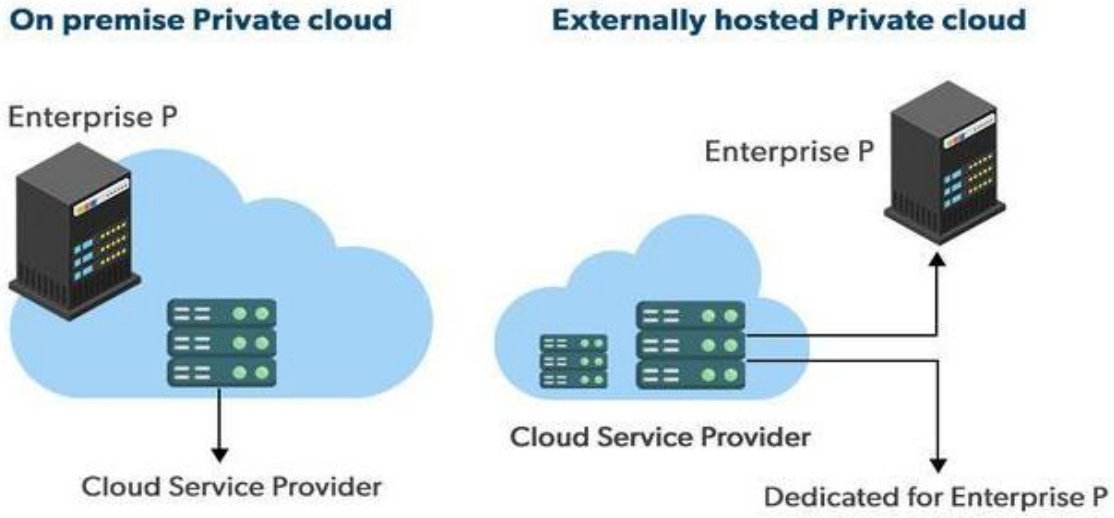
- Low Cost: Public cloud has a lower cost than private, or hybrid cloud, as it shares the same resources with a large number of consumers.
- Location Independent: Public cloud is location independent because its services are offered through the internet.
- Save Time: In Public cloud, the cloud service provider is responsible for the manage and maintain data centers in which data is stored, so the cloud user can save their time to establish connectivity, deploying new products, release product updates, configure, and assemble servers.
- Quickly and easily set up: Organizations can easily buy public cloud on the internet and deployed and configured it remotely through the cloud service provider within a few hours.
- Business Agility: Public cloud provides an ability to elastically re-size computer resources based on the organization's requirements.
- Scalability and reliability: Public cloud offers scalable (easy to add and remove) and reliable (24*7 available) services to the users at an affordable cost.

Disadvantages of Public Cloud

- Low Security: Public Cloud is less secure because resources are shared publicly.
- Performance: In the public cloud, performance depends upon the speed of internet connectivity.
- Less customizable: Public cloud is less customizable than the private cloud.

PRIVATE CLOUD

- The private cloud deployment model is the exact opposite of the public cloud deployment model.
- It’s a one-on-one environment for a single user (customer).
- There is no need to share your hardware with anyone else.
- The distinction between private and public clouds is in how you handle all of the hardware.
- It is also called the “internal cloud” & it refers to the ability to access systems and services within a given border or organization.
- The cloud platform is implemented in a cloud-based secure environment that is protected by powerful firewalls and under the supervision of an organization’s IT department.
- The private cloud gives greater flexibility of control over cloud resources.



Advantages of the Private Cloud Model

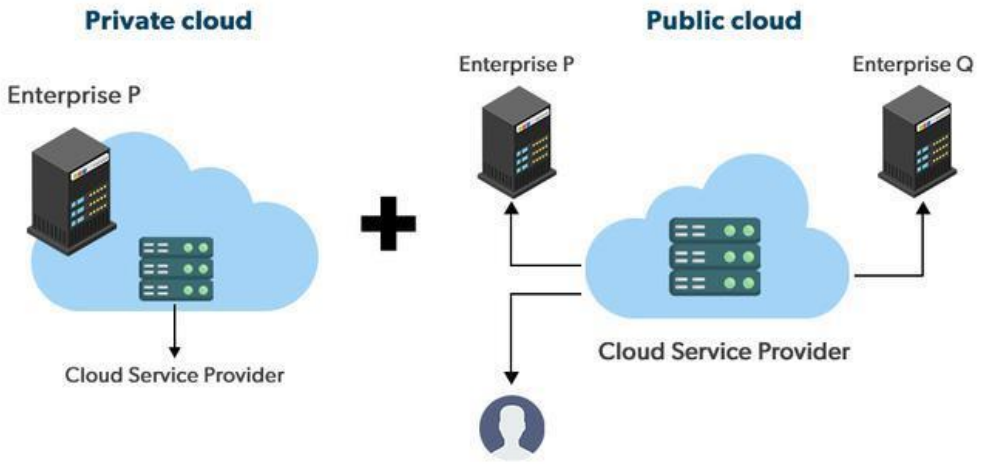
- **Better Control:** You are the sole owner of the property. You gain complete command over service integration, IT operations, policies, and user behavior.
- **Data Security and Privacy:** It's suitable for storing corporate information to which only authorized staff have access. By segmenting resources within the same infrastructure, improved access and security can be achieved.
- **Supports Legacy Systems:** This approach is designed to work with legacy systems that are unable to access the public cloud.
- **Customization:** Unlike a public cloud deployment, a private cloud allows a company to tailor its solution to meet its specific needs.

Disadvantages of the Private Cloud Model

- **Less scalable:** Private clouds are scaled within a certain range as there is less number of clients.
- **Costly:** Private clouds are costlier as they provide personalized facilities.

HYBRID CLOUD

- Hybrid cloud is a combination of public and private clouds.
  Hybrid cloud = public cloud + private cloud
- The main aim to combine these cloud (Public and Private) is to create a unified, automated, and well-managed computing environment.
- Organizations can move data and applications between different clouds using a combination of two or more cloud deployment methods, depending on their needs.
- In the Hybrid cloud, non-critical activities are performed by the public cloud and critical activities are performed by the private cloud.
- Mainly, a hybrid cloud is used in finance, healthcare, and Universities.
- The best hybrid cloud provider companies are Amazon, Microsoft, Google, Cisco, and NetApp.



Advantages of the Hybrid Cloud Model

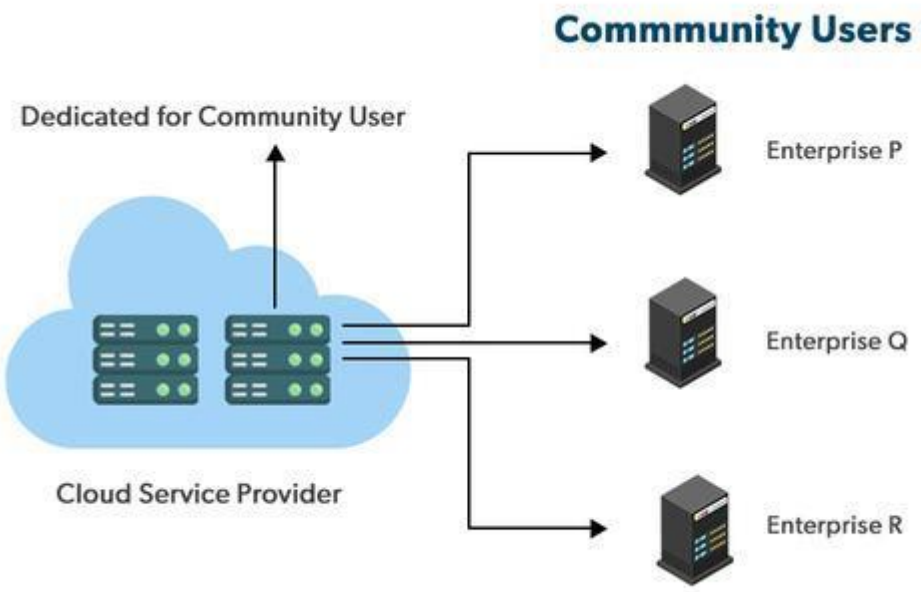
- **Flexibility and control:** Businesses with more flexibility can design personalized solutions that meet their particular needs.
- **Cost:** Because public clouds provide scalability, you'll only be responsible for paying for the extra capacity if you require it.
- **Security:** Because data is properly separated, the chances of data theft by attackers are considerably reduced.

Disadvantages of the Hybrid Cloud Model

- **Difficult to manage:** Hybrid clouds are difficult to manage as it is a combination of both public and private cloud. So, it is complex.
- **Slow data transmission:** Data transmission in the hybrid cloud takes place through the public cloud so latency occurs.

COMMUNITY CLOUD

- It allows systems and services to be accessible by a group of organizations.
- It is a distributed system that is created by integrating the services of different clouds to address the specific needs of a community, industry, or business.
- The infrastructure of the community could be shared between the organization which has shared concerns or tasks.
- It is generally managed by a third party or by the combination of one or more organizations in the community.



Advantages of the Community Cloud Model

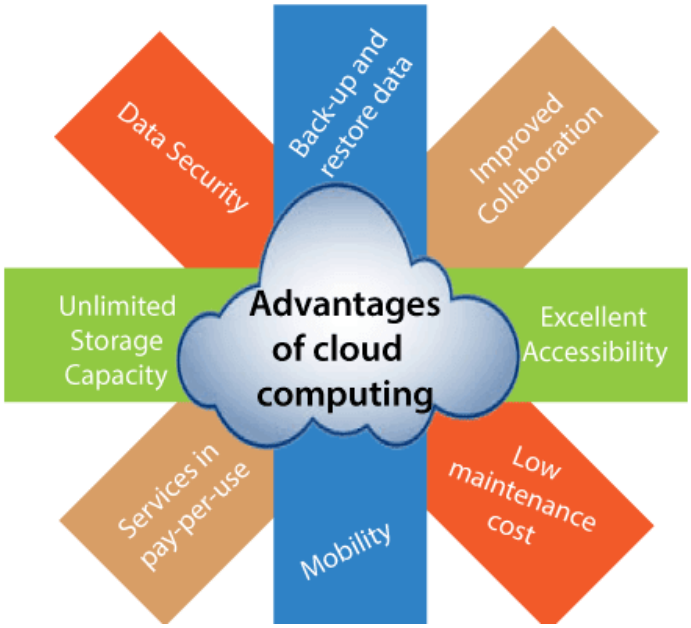
- **Cost Effective:** It is cost-effective because the cloud is shared by multiple organizations or communities.
- **Security:** Community cloud provides better security.
- **Shared resources:** It allows you to share resources, infrastructure, etc. with multiple organizations.
- **Collaboration and data sharing:** It is suitable for both collaboration and data sharing.

Disadvantages of the Community Cloud Model

- **Limited Scalability:** Community cloud is relatively less scalable as many organizations share the same resources according to their collaborative interests.
- **Rigid in customization:** As the data and resources are shared among different organizations according to their mutual interests if an organization wants some changes according to their needs they cannot do so because it will have an impact on other organizations.

ADVANTAGES OF CLOUD COMPUTING

- As we all know that Cloud computing is trending technology.
- Here, we are going to discuss some important advantages of Cloud Computing-



- **Back-up and restore data:** Once the data is stored in the cloud, it is easier to get back-up and restore that data using the cloud.
- **Improved collaboration:** Cloud applications improve collaboration by allowing groups of people to quickly and easily share information in the cloud via shared storage.
- **Excellent accessibility**
    - Cloud allows us to quickly and easily access store information anywhere, anytime in the whole world, using an internet connection.
    - An internet cloud infrastructure increases organization productivity and efficiency by ensuring that our data is always accessible.

- **Low maintenance cost:** Cloud computing reduces both hardware and software maintenance costs for organizations.
- **Mobility:** Cloud computing allows us to easily access all cloud data via mobile.
- Services in the pay-per-use model
- Cloud computing offers Application Programming Interfaces (APIs) to the users for access services on the cloud and pays the charges as per the usage of service.
- **Unlimited storage capacity:** Cloud offers us a huge amount of storing capacity for storing our important data such as documents, images, audio, video, etc. in one place.
- **Data security:** Data security is one of the biggest advantages of cloud computing. Cloud offers many advanced features related to security and ensures that data is securely stored and handled.