PRINCIPLES OF CLOUD COMPUTING-22ISE542

Module1:

1.Introduction,Cloud Infrastructure:

1.1:Cloud computing

1.2:Cloud computing delivery models and services

1.3: Ethical issues

1.4: Cloud vulnerabilities.

1.1:Cloud computing:

- Cloud computing is a technology that delivers various computing services over the internet. These services include storage, databases, servers, networking, software, and analytics. Instead of owning and maintaining physical hardware, businesses and individuals can use cloud services on a pay-as-you-go basis, which provides flexibility, scalability, and cost-efficiency.
- The main purpose of cloud computing is to give access to data centers to many users.
- Users can also access data from a remote server.

Why Cloud Computing?

- With increase in computer and Mobile user's, data storage has become a priority in all fields.
- Large and small scale businesses today thrive on their data & they spent a huge amount of money to maintain this data. It requires a strong IT support and a storage hub.

- For them Cloud Computing is a cheaper solution. Perhaps its efficiency in storing data, computation and less maintenance cost has succeeded to attract even bigger businesses as well.
- While accessing e-mail service our data is stored on cloud server and not on our computer. The technology and infrastructure behind the cloud is invisible

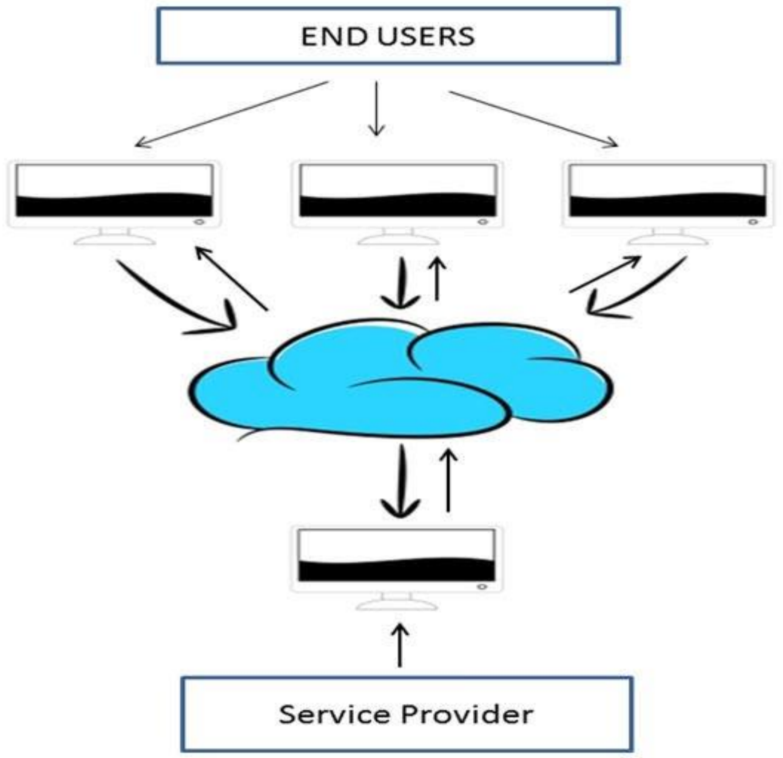
Key Features of Cloud Computing:

1. **On-Demand Service**: Resources are provided as needed, and users can scale services up or down based on their requirements.
2. **Broad Network Access**: Services can be accessed via the internet from a wide range of devices.
3. **Resource Pooling**: Multiple users share resources in a multi-tenant model, allowing for efficient use of computing power.
4. **Rapid Elasticity**: Resources can be scaled dynamically, enabling users to meet demand spikes or reduce costs when demand is low.
5. **Measured Service**: Cloud systems automatically control and optimize resource use by leveraging metering capabilities, providing transparency for both the provider and user.

Types of Cloud Computing:

1. **Infrastructure as a Service (IaaS)**: Provides virtualized computing resources over the internet (e.g., AWS, Microsoft Azure).
2. **Platform as a Service (PaaS)**: Offers platforms that allow developers to build applications without worrying about underlying infrastructure (e.g., Google App Engine).
3. **Software as a Service (SaaS)**: Delivers software applications over the internet, eliminating the need for installation (e.g., Google Workspace, Dropbox).

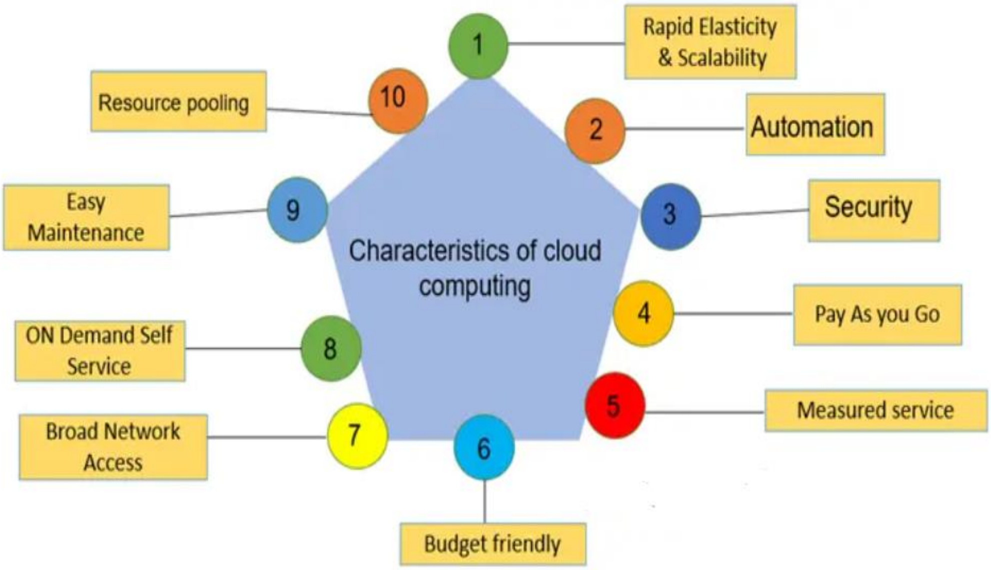
Cloud computing is widely adopted across industries for its ability to lower IT costs, improve performance, and enable remote access to applications and data.



The Essential Characteristics of Cloud Computing are:

- On-demand self service
- Multi-tenancy and resource pooling
- Broad network access
- Rapid elasticity and scalability
- Resource pooling
- Measured and reporting service
- Automation
- Resilience
- Large Network Access
- Work from any location
- Comfortable payment structure

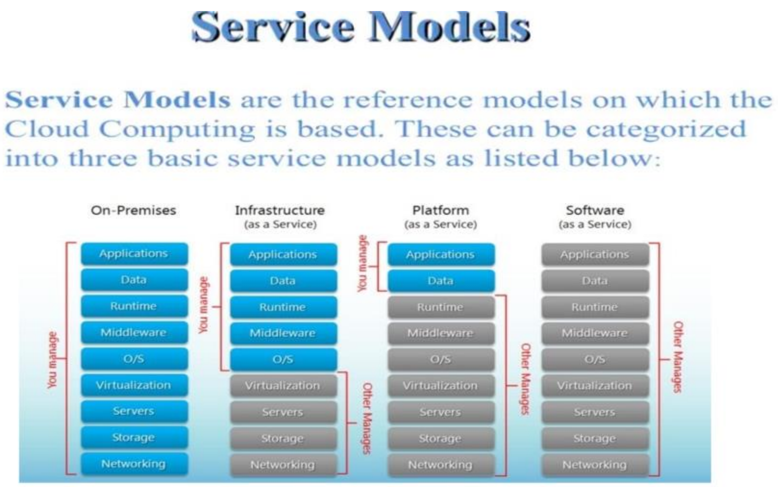
- Service Excellence
- Easy maintenance
- Flexibility
- Economical and Security
- Availability



<u>1.2:Cloud Computing delivery models and services</u>:

provide various ways for users to access and utilize resources, depending on their needs.

The three primary delivery models of cloud computing are **IaaS (Infrastructure as a Service)**, **PaaS (Platform as a Service)**, and **SaaS (Software as a Service)**. Each model offers a different level of control, flexibility, and management over cloud resources.

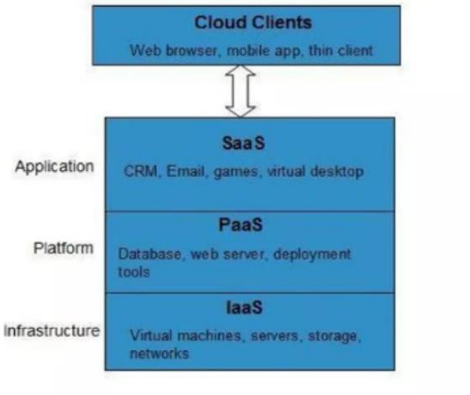


Service Models

Service Models are the reference models on which the Cloud Computing is based. These can be categorized into three basic service models as listed below:

1.Infrastructure as a Service(IaaS):

- **Definition**: IaaS provides virtualized computing resources over the internet, such as servers, storage, and networking. It allows users to rent IT infrastructure instead of purchasing and maintaining it themselves.



Cloud Clients
Web browser, mobile app, thin client
Application
SaaS
CRM, Email, games, virtual desktop
Platform
PaaS
Database, web server, deployment tools
Infrastructure
IaaS
Virtual machines, servers, storage, networks

- **Key Features**:
  - Virtual machines, storage, and networks.
  - High scalability and flexibility.
  - Users manage the applications, data, runtime, and middleware, while the provider manages the infrastructure.
- **Characteristics of IaaS**
- There are the following characteristics of IaaS -
- Resources are available as a service

- Services are highly scalable
- Dynamic and flexible
- GUI and API-based access
- Automated administrative tasks

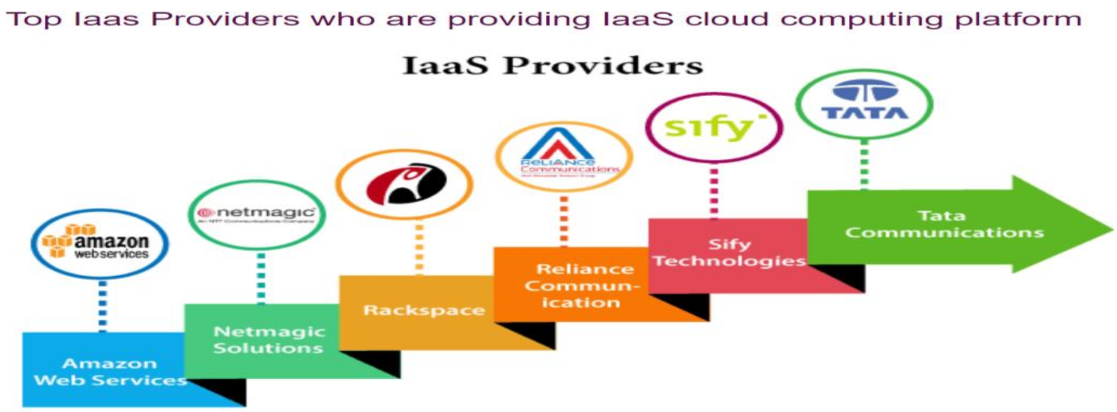
Advantages of IaaS are:

- **Dynamic:** Users can dynamically opt & configure devices such as CPU, storage drive, etc.
- **Easy Access:** Users can easily access the vast cloud computing power.
- **Renting:** Flexible and efficient while renting IT infrastructures.
- Full control of computer resources along with **portability.**

Cons of IaaS:

- **Internet connection** is a must.
- IaaS depends on **virtualization services**.
- This service **restricts user-privacy & customization**
- **IaaS provider provides the following services -**

1. **Compute:** Computing as a Service includes virtual central processing units and virtual main memory for the Vms that is provisioned to the end-users.
2. **Storage:** IaaS provider provides back-end storage for storing files.
3. **Network:** Network as a Service (NaaS) provides networking components such as routers, switches, and bridges for the Vms.
4. **Load balancers:** It provides load balancing capability at the infrastructure layer.



- **Examples**:
  - Amazon Web Services (AWS)
  - Microsoft Azure
  - Google Cloud Platform (GCP)

IaaS Examples
OpSource
NTT Communications
GO GRID
terremark
BLIZZARD ENTERTAINMENT
at&t

2. Platform as a Service (PaaS):

- **Definition**: PaaS provides a platform that allows developers to build, test, and deploy applications without managing the underlying hardware or software infrastructure.
- **Key Features**:
  - Development frameworks, middleware, and databases.
  - Simplified application development.
  - The cloud provider manages the infrastructure, including servers, networks, and storage, while developers focus on their applications.

- **Characteristics of PaaS**
  - There are the following characteristics of PaaS -
  - Accessible to various users via the same development application.
  - Integrates with web services and databases.
  - Builds on virtualization technology, so resources can easily be scaled up or down as per the organization's need.
  - Support multiple languages and frameworks.
  - Provides an ability to "**Auto-scale**".

- **Advantages of PaaS –**
- Programmers need not worry about what specific database or language the application has been programmed in.
- It offers developers the to build applications without the overhead of the underlying operating system or infrastructure.

Provides the freedom to developers to focus on the application’s design while the platform takes care of the language and the database

1) Simplified Development

PaaS allows developers to focus on development and innovation without worrying about infrastructure management.

2) 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.

3) 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.

4) Instant community

PaaS vendors frequently provide online communities where the developer can get the ideas to share experiences and seek advice from others.

5) Scalability

Applications deployed can scale from one to thousands of users without any changes to the applications

- **Disadvantages**

1) Vendor lock-in

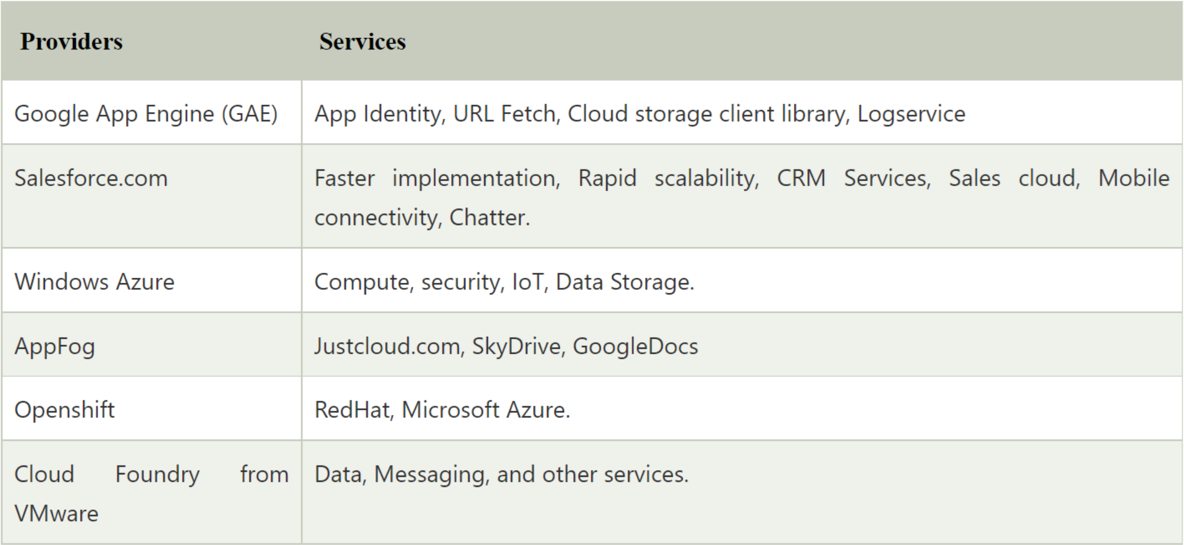
One has to write the applications according to the platform provided by the PaaS vendor, so the migration of an application to another PaaS vendor would be a problem.

2) 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.

3) 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.



Providers	Services
Google App Engine (GAE)	App Identity, URL Fetch, Cloud storage client library, Logservice
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.

- **Examples**:
  - Google App Engine
  - Microsoft Azure App Service
  - Heroku

3. Software as a Service (SaaS):

- **Definition**: SaaS delivers software applications over the internet. Users access applications through a web browser, eliminating the need for installation or maintenance.
- **Key Features**:
  - Fully managed software applications.
  - Accessible from any device with internet access.
  - The provider manages everything from infrastructure to the application itself.

- **Characteristics of SaaS**
  - There are the following characteristics of SaaS -
  - 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

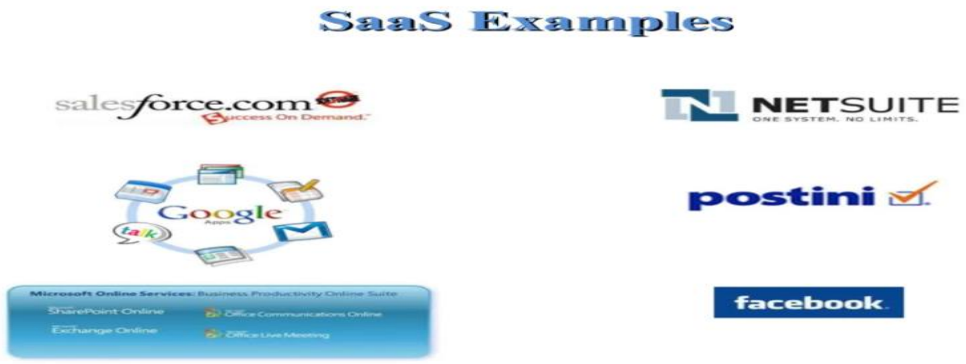
Advantages:

- **Easy to buy**: SaaS's cost is based on monthly or yearly fees allowing new organizations to access the world of business at a low-cost, at least lesser than licensed application.
- **Minimization of Hardware Requirement**: All SaaS software is hosted remotely & so there is no or lesser need for hardware for the organizations.
- **Special Software**: No special software versions are required, as all the users will use the same software version. SaaS reduces IT costs by outsourcing hardware & software maintenance.
- **Low Maintenance**: SaaS removes the daily problem of installing, maintaining, and updating software. The set-up cost of SaaS is also less in comparison to enterprise software.

Disadvantages

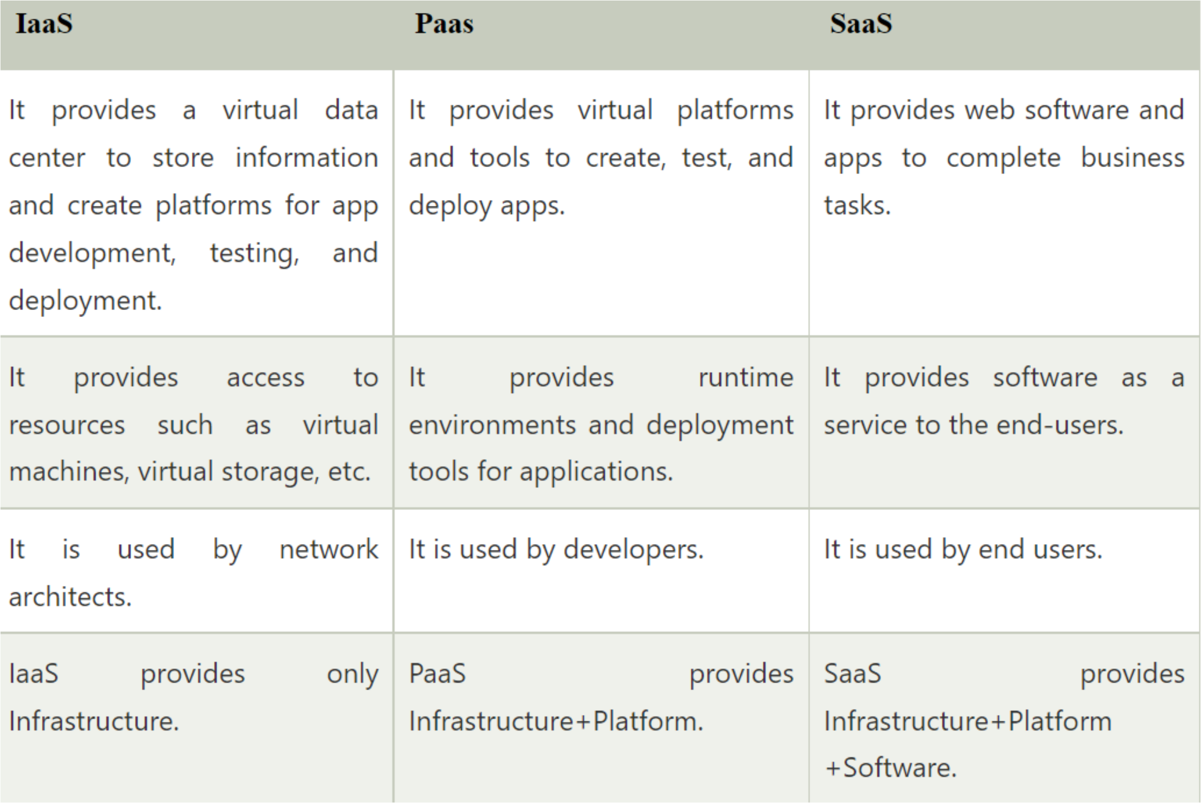
- **Latency factor**: comes due to a variable distance of data between the cloud & the end-user, and hence a possibility of latency may arise while interacting with applications.

- **Internet Connection**: is a major issue. Without an internet connection, SaaS applications are unusable.
- Switching between SaaS vendors in case of any change is very difficult.
- The SaaS cloud service is not very secure as in-house deployment.



- **Examples**:
  - Google Workspace (formerly G Suite)
  - Microsoft Office 365
  - Salesforce

Do you Use the Cloud?

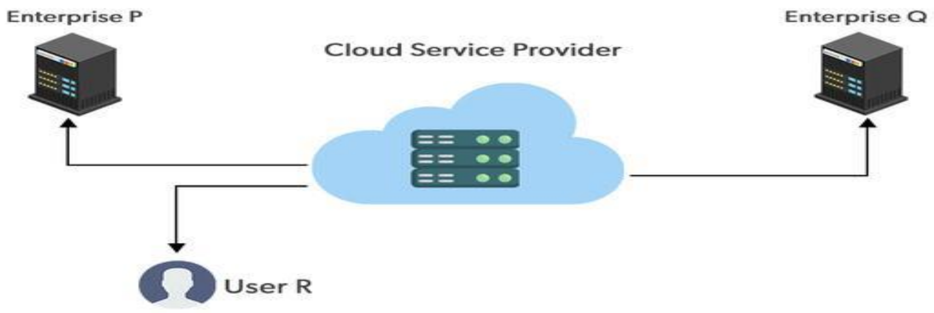


IaaS	Paas	SaaS
It provides a virtual data center to store information and create platforms for app development, testing, and deployment.	It provides virtual platforms and tools to create, test, and deploy apps.	It provides web software and apps to complete business tasks.
It provides access to resources such as virtual machines, virtual storage, etc.	It provides runtime environments and deployment tools for applications.	It provides software as a service to the end-users.
It is used by network architects.	It is used by developers.	It is used by end users.
IaaS provides only Infrastructure.	PaaS provides Infrastructure+Platform.	SaaS provides Infrastructure+Platform +Software.

Cloud Deployment Models:

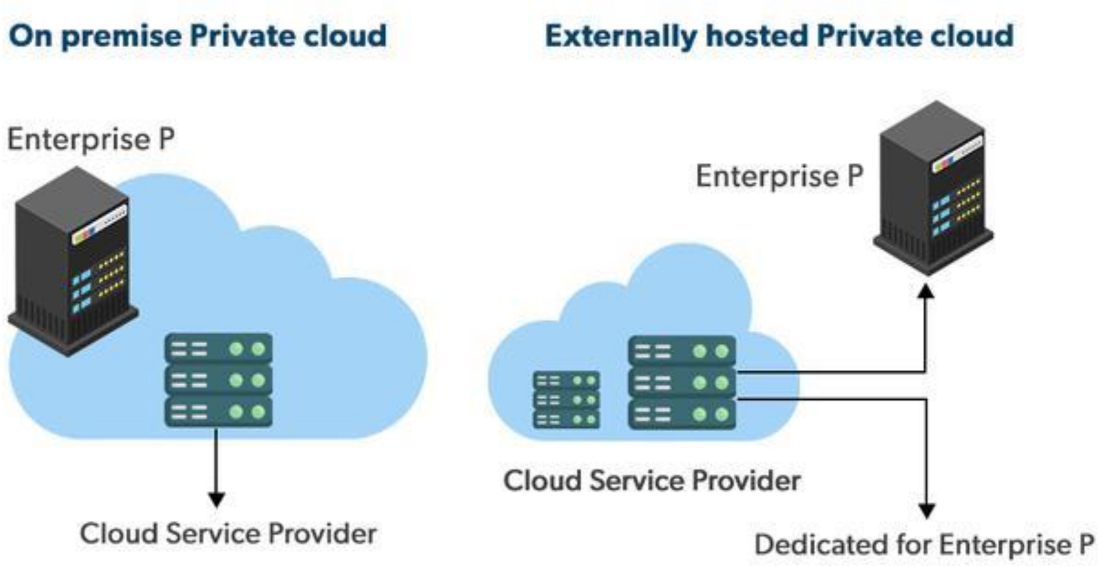
1. **Public Cloud**: Services are delivered over the internet and shared among multiple users or organizations. It is cost-effective but less secure compared to other models.
   - Examples: AWS, Azure, GCP.

- Public clouds are managed by third parties which provide cloud services over the internet to the public, these services are available as pay-as-you-go billing models.
- They offer solutions for minimizing IT infrastructure costs and become a good option for handling peak loads on the local infrastructure. 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.
- The fundamental characteristics of public clouds are **multitenancy**. A public cloud is meant to serve multiple users, not a single customer. A user requires a virtual computing environment that is separated, and most likely isolated, from other users.



2. **Private Cloud**: Cloud infrastructure is dedicated to a single organization, providing greater control and security. It can be hosted on-premise or by a third-party provider.
   - Examples: VMware, OpenStack.

   Private clouds are distributed systems that work on private infrastructure and provide the users with dynamic provisioning of computing resources. Instead of a pay-as-you-go model in private clouds, there could be other schemes that manage the usage of the cloud and proportionally billing of the different departments or sections of an enterprise. Private cloud providers are HP Data Centers, Ubuntu, Elastic-Private cloud, Microsoft, etc.



The advantages of using a private cloud are as follows:

Customer information protection: In the private cloud security concerns are less since customer data and other sensitive information do not flow out of private infrastructure.

Infrastructure ensuring SLAs: Private cloud provides specific operations such as appropriate clustering, data replication, system monitoring, and maintenance, disaster recovery, and other uptime services.

Compliance with standard procedures and operations: Specific procedures have to be put in place when deploying and executing applications according to third-party compliance standards. This is not possible in the case of the public cloud.

Disadvantages of using a private cloud are:

The restricted area of operations: Private cloud is accessible within a particular area. So the area of accessibility is restricted.

Expertise requires: In the private cloud security concerns are less since customer data and other sensitive information do not flow out of private infrastructure. Hence skilled people are required to manage & operate cloud services.

3.Hybrid Cloud: Combines public and private cloud environments, allowing data and applications to be shared between them. This model offers flexibility, scalability, and enhanced security.

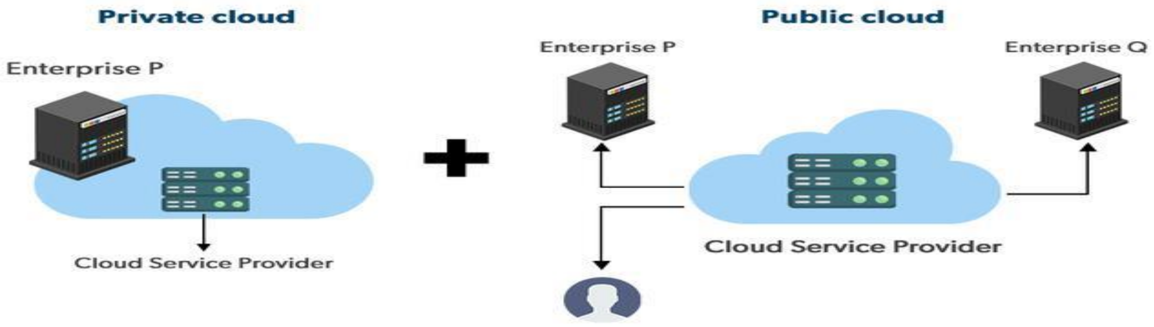
- Examples: Microsoft Azure Stack, AWS Outposts.

A hybrid cloud is a heterogeneous distributed system formed by combining facilities of the public cloud and private cloud. For this reason, they are also called **heterogeneous clouds.**

A major drawback of private deployments is the inability to scale on-demand and efficiently address peak loads. Here public clouds are needed. Hence, a hybrid cloud takes advantage of both public and private clouds.

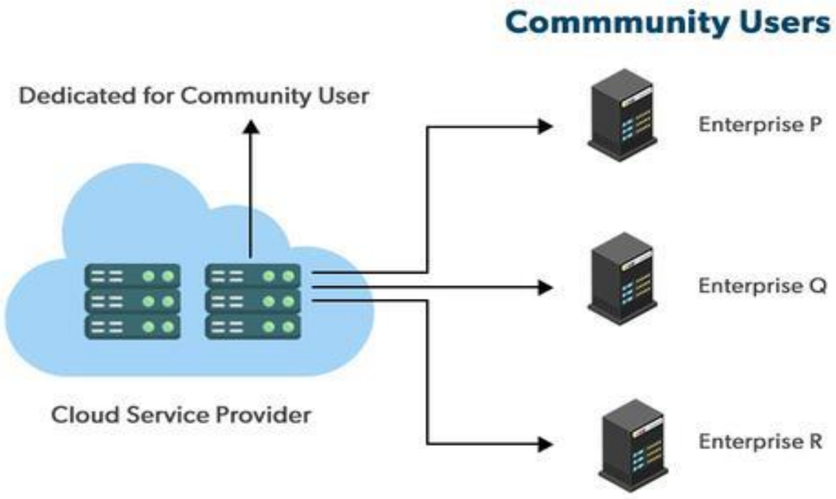
A hybrid cloud is a heterogeneous distributed system formed by combining facilities of the public cloud and private cloud. For this reason, they are also called **heterogeneous clouds.**

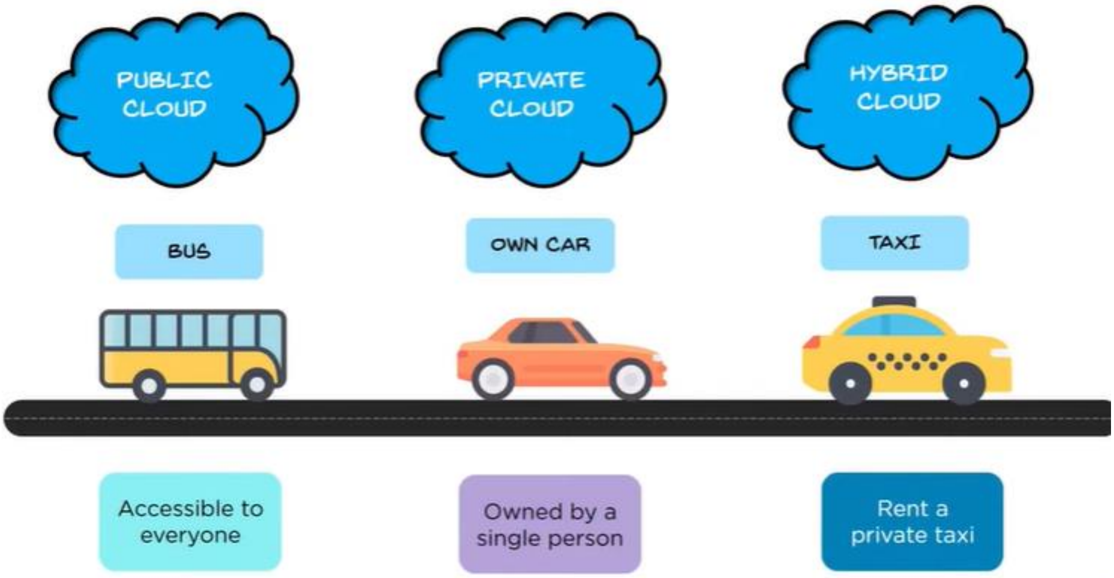
A major drawback of private deployments is the inability to scale on-demand and efficiently address peak loads. Here public clouds are needed. Hence, a hybrid cloud takes advantage of both public and private clouds.



4.Community Cloud: Infrastructure is shared by several organizations with similar needs, often in the same industry. This model provides a balance of privacy and cost-efficiency.

Community clouds are distributed systems created by integrating the services of different clouds to address the specific needs of an industry, a community, or a business sector. But sharing responsibilities among the organizations is difficult. In the community cloud, the infrastructure is shared between organizations that have shared concerns or tasks. The cloud may be managed by an organization or a third party.





Cloud Services:

1. **Compute**: Virtual machines, containers, and serverless computing for running applications and workloads.
2. **Storage**: Scalable storage services, including object storage, block storage, and file storage.
3. **Networking**: Virtual private networks (VPNs), load balancers, and DNS services.
4. **Databases**: Managed database services, including SQL and NoSQL databases.
5. **Security**: Identity and access management, firewalls, encryption, and threat detection services.

Cloud computing delivery models and services are designed to meet the diverse needs of businesses, enabling them to choose the right combination of infrastructure, platforms, and applications for their specific requirements.

1.3: Ethical issues

Unauthorized access, data corruption, infrastructure failure, or unavailability are some of the risks related to relinquishing the control to third party services; moreover, it is difficult to identify the source of the problem and the entity causing it.

Cloud computing is based on a paradigm shift with profound implications on computing ethics.

The main elements of this shift are:

1. The control is relinquished to third party services;
2. The data is stored on multiple sites administered by several organizations; and
3. Multiple services interoperate across the network.

Cloud Computing is Internet-based computing, where shared resources, software, and information are provided to computers and other devices on demand.

These are major issues in Cloud Computing:

1. Privacy: The user data can be accessed by the host company with or without permission. The service provider may access the data that is on the cloud at any point in time. They could accidentally or deliberately alter or even delete information.

2. Compliance: There are many regulations in places related to data and hosting. To comply with regulations (Federal Information Security Management Act, Health Insurance Portability and Accountability Act, etc.) the user may have to adopt deployment modes that are expensive.

3. Security: Cloud-based services involve third-party for storage and security. Can one assume that a cloud-based company will protect and secure one's data if one is using their services at a very low or for free?

They may share users' information with others. Security presents a real threat to the cloud.

4. Higher Cost: If you want to use cloud services uninterruptedly then you need to have a powerful network with higher bandwidth than ordinary internet networks, and also if your organization is broad and large so ordinary cloud service subscription won't suit your organization.

Otherwise, you might face hassle in utilizing an ordinary cloud service while working on complex projects and applications. This is a major problem before small organizations, that restricts them from diving into cloud technology for their business.

5. Recovery of lost data in contingency: Before subscribing any cloud service provider goes through all norms and documentations and check whether their services match your requirements and sufficient well-maintained resource infrastructure with proper upkeeping.

Once you subscribed to the service you almost hand over your data into the hands of a third party.

If you are able to choose proper cloud service then in the future you don't need to worry about the recovery of lost data in any contingency.

6.Upkeeping(management) of Cloud: Maintaining a cloud is a herculin task because a cloud architecture contains a large resources infrastructure and other challenges and risks as well, user satisfaction, etc.

As users usually pay for how much they have consumed the resources.

So, sometimes it becomes hard to decide how much should be charged in case the user wants scalability and extend the services.

7. Lack of resources/skilled expertise: One of the major issues that companies and enterprises are going through today is the lack of resources and skilled employees.

Every second organization is seeming interested or has already been moved to cloud services.

That’s why the workload in the cloud is increasing so the cloud service hosting companies need continuous rapid advancement.

Due to these factors, organizations are having a tough time keeping up to date with the tools. As new tools and technologies are emerging every day so more skilled/trained employees need to grow. These challenges can only be minimized through additional training of IT and development staff.

8. Pay-per-use service charges: Cloud computing services are on-demand services a user can extend or compress the volume of the resource as per needs.

so you paid for how much you have consumed the resources. It is difficult to define a certain pre-defined cost for a particular quantity of services.

Such types of ups and downs and price variations make the implementation of cloud computing very difficult and intricate.

It is not easy for a firm’s owner to study consistent demand and fluctuations with the seasons and various events.

So it is hard to build a budget for a service that could consume several months of the budget in a few days of heavy use.

1.4:CLOUD VULNERABILITIES

Cloud vulnerabilities refer to the potential weaknesses or security gaps in cloud computing environments that can be exploited by attackers. Here are some common cloud vulnerabilities:

1. Data Breaches:
    - Unauthorized access to sensitive data stored in the cloud, often due to weak authentication, encryption, or inadequate security policies.
2. Insecure APIs:
    - Cloud services often expose APIs for user interactions. If these APIs are insecure, they can be exploited to compromise systems, steal data, or cause service disruptions.
3. Misconfigured Cloud Settings:
    - Misconfigurations, such as incorrect permissions or failure to encrypt sensitive data, can expose critical information to unauthorized users.
4. Account Hijacking:
    - Attackers can compromise cloud user accounts through phishing, social engineering, or weak passwords, giving them unauthorized access to cloud services.
5. Insufficient Identity and Access Management (IAM):
    - Poor management of user privileges, lack of multi-factor authentication (MFA), or over-permissive roles can lead to unauthorized access.
6. Data Loss:
    - Data in the cloud can be lost due to accidental deletion, malicious attacks (such as ransomware), or failure to back up data properly.
7. Denial of Service (DoS) Attacks:
    - Cloud systems can be overwhelmed by DoS attacks, making services unavailable to legitimate users.
8. Shared Technology Vulnerabilities:

- Cloud environments often share infrastructure, platforms, and applications. Vulnerabilities in shared components can result in "cross-tenant" attacks, where one user's compromise affects others.

9. Malicious Insiders:

- Employees or contractors with access to cloud systems could intentionally or unintentionally cause harm by leaking data or damaging cloud resources.

10. Inadequate Security Controls:

- Some cloud service providers may not implement sufficient security controls, leaving customer data vulnerable to attacks.

11. Vendor Lock-In and Data Portability:

- Limited options for migrating data between cloud providers can pose a risk when transitioning or needing redundancy, potentially exposing vulnerabilities during the process.

12. Compliance Risks:

- Non-compliance with industry regulations (e.g., GDPR, HIPAA) can create legal vulnerabilities, especially regarding how data is stored, processed, or accessed in the cloud.

Mitigation Strategies:

- Strong encryption for data at rest and in transit.
- Regular audits and monitoring of cloud environments.
- Applying best practices for IAM and enforcing the principle of least privilege.
- Configuring security policies correctly and ensuring proper access controls.
- Use of MFA and secure, regularly updated APIs.

Cloud vulnerabilities are constantly evolving, so continuous monitoring and regular updates are essential to maintaining security.

QUESTION BANK

1.Describe the Following:

i. Public Cloud ii. Private Cloud iii. Hybrid Cloud iii.Community Cloud

2.List the Characteristics of IAAS and PASS.

3. Explain in detail about cloud Service models.

4. Discuss in detail about Major Ethical Issues in the cloud computing.

5. Summarize in detail about how IAAS provides access to fundamental resources.

6. Compare the differences between PAAS and SAAS.

7.Discuss the essentials characteristics that identify PAAS solution.

8.Summarize the IAAS based solution for cloud computing.

9.Explain the reference Implementation of SAAS with a neat diagram.

10.List the Ethical Issues in the cloud computing.

11.Write the types of cloud based on Deployment model.

12.Explain in detail about cloud delivery model.

13.Explain in detail about cloud volnerabilities.

14.Mention the characteristics of cloud computing.

15.Mention the advantage sand disadvantages of cloud computing.