Ishita Hardasmalani

C14-2103058

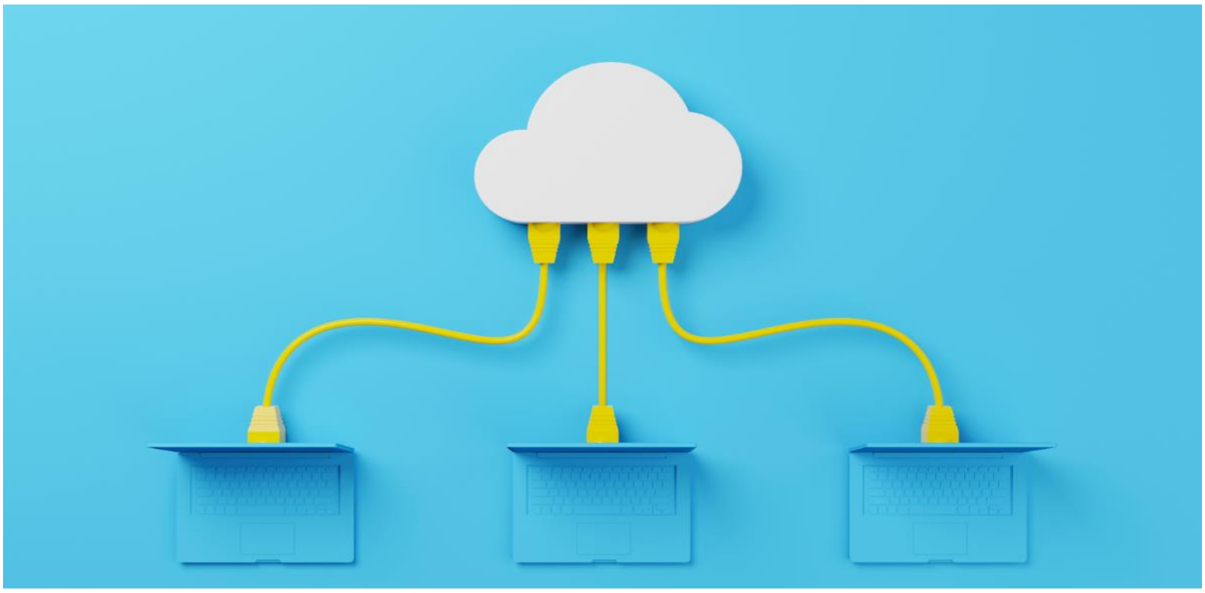
EXPERIMENT NO. 1

Aim: Introduction and overview of cloud computing

Theory:

Definition of Cloud Computing

Cloud computing refers to the delivery of computing services, including storage, processing power, and applications, over the internet. Instead of relying on a local server or a personal computer to handle data and perform various tasks, cloud computing allows users to access and use resources hosted on remote servers. Cloud computing has become a fundamental technology in modern IT infrastructure, offering flexibility, scalability, and cost efficiency for businesses and individuals alike.



Characteristics of Cloud Computing

1. On-Demand Self-Service: Users can provision and manage computing resources as needed without human intervention.
2. Broad Network Access: Cloud services are accessible over the internet from various devices.
3. Resource Pooling: Computing resources are shared and allocated dynamically to serve multiple customers efficiently.
4. Rapid Elasticity: Cloud resources can be quickly scaled up or down to adapt to changing demands.
5. Measured Service: Cloud usage is monitored, controlled, and reported, allowing users to pay for actual consumption.
6. Ubiquitous Access: Cloud services can be accessed from anywhere with an internet connection.

7. Multi-Tenancy: Multiple users or tenants share the same infrastructure while maintaining isolation and security.
8. Fault Tolerance and Reliability: Cloud infrastructure is designed to be resilient, minimizing downtime and ensuring high availability.
9. Security: Cloud providers implement robust security measures to protect data, applications, and infrastructure.
10. Scalability: Cloud services can easily scale to accommodate growing workloads or scale down during periods of low demand.
11. Cost-Effective: Users pay for the resources they consume, avoiding the need for large upfront investments in infrastructure.
12. Continuous Updates and Improvements: Cloud services are regularly updated, providing access to the latest features and security enhancements.

NIST Cloud Computing Model

The NIST (National Institute of Standards and Technology) cloud computing model provides a framework for understanding and categorizing the various components and service models within cloud computing. NIST's definition, as outlined in their publication "NIST Special Publication 800-145," identifies essential characteristics, service models, and deployment models that collectively define cloud computing.

NIST's cloud model (definition) is composed of:

- Five essential characteristics
- Three service models
- Four deployment models

NIST's Five Characteristics of Cloud Computing

The five essential characteristics of a cloud service create the cloud computing infrastructure. It includes a physical layer of hardware resources and an abstraction layer which consists of the software deployed across the physical layer. These attributes are:

1. On-Demand Self-Service

Self-service means that the cloud user can acquire the service independently: without going through an IT department, call center, or other middle man. To support self-service:

- The cloud provider must have an automated interface, such as a web portal or mobile app.
- The user should be able to access the interface at any time.
- The user should also be able to cancel the cloud service at any time.

2. Broad Network Access

The cloud service must be broadly available over the communication network. Users should be able to access it from any location and internet-enabled device.

3. Resource Pooling

Multiple customers share the cloud service resources in a multi-tenancy model. This model raises privacy and security concerns, so users must protect their cloud data and assets by taking necessary security precautions.

4. Rapid Elasticity

Elasticity refers to the flexibility of the cloud service to scale up or down automatically to meet the user's needs. That allows the user to access the right level and kind of resources, including processing power, memory, network bandwidth, and storage, to accommodate the user's varying workloads.

5. Measured Service

A measured cloud service provides a metering capability that underpins the provider's pay-as-you-go pricing model. This model provides users with greater transparency and control over their cloud costs.

What Is the NIST's Cloud Computing Architecture Model?

The initial portion of the NIST SP 500-292 defines five major roles within a cloud computing architecture model:

1. Cloud Consumer
2. Cloud Provider
3. Cloud Auditor
4. Cloud Broker
5. Cloud Carrier

We would need dedicated topics to discuss each of these roles in detail, so let's briefly list the cloud providers and the different deployment models to understand NIST's point of view on the cloud computing architecture model.

Cloud Providers in the NIST Cloud Computing Reference Architecture

NIST identifies three distinct cloud service provider categories:

1. Software-as-a-Service (SaaS)

In the SaaS model, the cloud provider manages the underlying software and IT infrastructure. Users access the SaaS offering via a web browser. Local installation is not required, and organizations don't have to worry about managing data centers, IT operations, or maintenance.

Some popular examples of SaaS applications include:

- Amazon Web Services (AWS)
- Salesforce
- Microsoft Office 365
- Google applications (G-Suite), including Gmail
- Dropbox
- SAP
- Adobe Creative Cloud

2. Platform-as-a-Service (PaaS)

PaaS provides a powerful development platform with programming languages, web-based APIs, and processes that allow software developers to create cloud-based applications. The PaaS provider fully manages the underlying infrastructure. Moreover, the platform automatically configures infrastructure resources across user-created environments.

Some popular PaaS providers include:

- AWS Elastic Beanstalk
- Oracle Cloud Platform (OCP)
- Google App Engine
- Microsoft Azure
- Red Hat OpenShift PaaS

3. Infrastructure-as-a-Service (IaaS)

Users can rent the cloud IT infrastructure, such as servers, networking, and storage, from an IaaS provider on a pay-as-you-go basis, so the user doesn't incur the cost of on-premises installation or maintenance.

Examples of popular IaaS providers include:

- AWS EC2
- Google Compute Engine
- DigitalOcean
- Microsoft Azure

NIST Models for Deployment

The NIST cloud computing definition includes four cloud deployment models representing four types of cloud environments. Users can choose the model with features and capabilities best suited to their needs.

1. Private Cloud

A private cloud is a single-tenant environment provisioned by a single organization.

Security is one of the most significant benefits of a private cloud; the company's data cannot be accessed by anyone other than its authorized users. That's why the private cloud is a good choice for organizations whose data or assets are too valuable or sensitive to put on a public cloud and for firms aiming for HIPAA or PCI DSS compliance.

Some private cloud providers are:

- VMWare
- Dell
- Oracle
- IBM
- Microsoft
- Cisco
- AWS

2. Public Cloud

In this multi-tenant deployment model, the cloud is owned by the cloud service provider. The underlying resources are shared by multiple customers who pay for the resources they use on a pay-as-you-use basis.

The provider owns, controls, and protects the data security requirements among different customers. The provider is also responsible for administration, maintenance, troubleshooting, capacity planning, and data backups.

As of fourth-quarter 2022, the top three public cloud providers are AWS, Microsoft Azure, and Google Cloud, which own 32, 23, and 10 percent of the market share, respectively. Other up-and-coming public cloud providers include:

- Alibaba Cloud
- IBM
- DigitalOcean
- Dell
- Adobe

3. Hybrid Cloud

In a hybrid cloud, the cloud infrastructure is composed of two or more distinct public or private clouds, bound together by technology supporting data and application portability. It provides greater flexibility, portability, and scalability than the other deployment models.

Examples of hybrid cloud providers include:

- AWS VPC
- EMC
- BMC
- F5
- NetApp

4. Community Cloud

A community cloud is used by a community of users from organizations with shared concerns. This multi-tenant platform allows multiple companies or special interest user groups to collaborate securely on projects or research.

Community clouds are common in government, healthcare, and education for use cases such as:

- Customer service
- Partner relationship management
- Channel sales
- Dealer contract renewals
- Employee engagement
- Collaboration and business decision-making

NIST Models for Orchestration

The NIST cloud computing definition provides a view on orchestration as a key architectural component to describe how different cloud providers interact at each layer of the cloud infrastructure, namely:

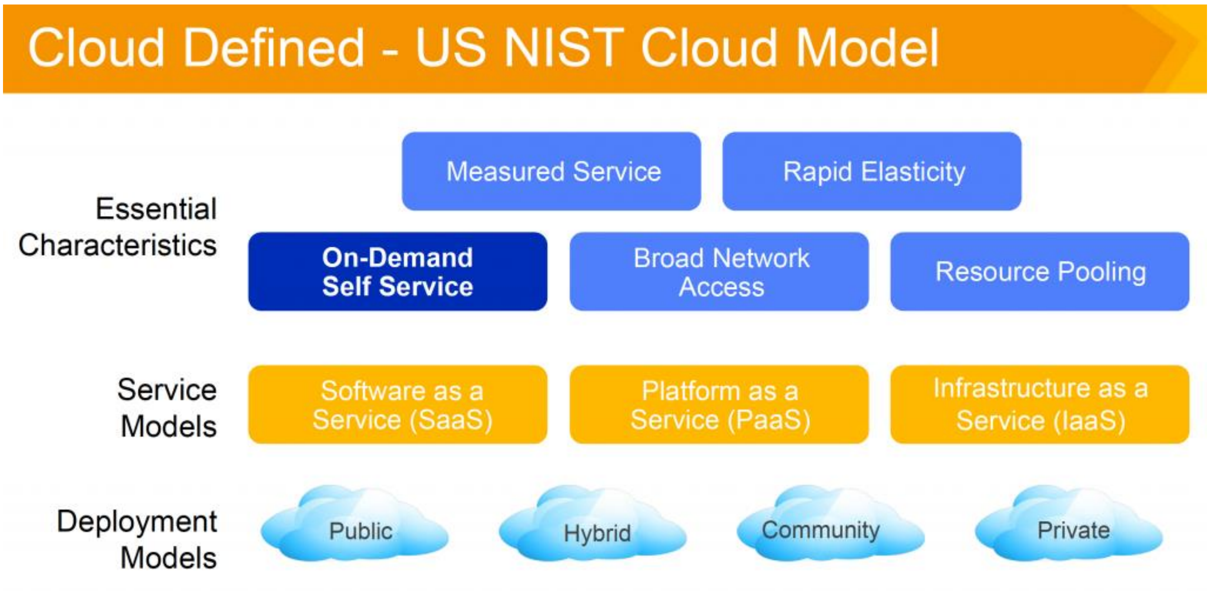
Service Layer

Determines the services made available depending on the Cloud Provider type (SaaS, PaaS, or IaaS)

Resources Layer
Abstract the data and the allocation of resources among the different cloud providers
Physical Layer
Define the interaction between actual endpoints and devices across these providers
NIST Models for Management
NIST defines management as another key architectural component and describes it in three different categories:

1. **Interoperability**. Defines the management, security, and accessibility of information across different formats
2. **Provisioning**. Defines the adherence of service-level agreements between different cloud service models
3. **Support**. Defines accountability and reporting of capacity and availability across the different cloud service models

Benefits of NIST's Cloud Computing Definition
NIST's cloud computing definition allows organizations to compare various cloud services and deployment strategies. A deep understanding of this definition can help organizations better appreciate the benefits of this technology,


Cloud Defined - US NIST Cloud Model
Essential Characteristics
Measured Service
Rapid Elasticity
On-Demand Self Service
Broad Network Access
Resource Pooling
Service Models
Software as a Service (SaaS)
Platform as a Service (PaaS)
Infrastructure as a Service (IaaS)
Deployment Models
Public
Hybrid
Community
Private

Different models of cloud computing

Cloud computing offers three primary service models, each catering to different layers of abstraction and responsibilities. These service models are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Here's a detailed explanation of each:

1. Infrastructure as a Service (IaaS):

- Definition: IaaS provides virtualized computing resources over the internet. Users can rent virtual machines, storage, and networks. It gives clients the flexibility to manage and control the operating systems, applications, and development frameworks, while the cloud provider manages the underlying infrastructure.

- Characteristics:

  - Users have control over the operating systems and applications.

  - Infrastructure resources are scalable based on demand.

  - Users pay for the resources they consume.

- Example: Amazon Web Services (AWS) EC2, Microsoft Azure Virtual Machines.

2. Platform as a Service (PaaS):

- Definition: PaaS offers a platform with tools and services for application development, testing, and deployment. It abstracts away the underlying infrastructure, allowing developers to focus on building and deploying applications without managing the hardware, operating systems, or networking components.

- Characteristics:

  - Developers focus on application development, not infrastructure management.

  - Automatic scaling and load balancing are typically handled by the platform.

  - Reduced complexity for developers.

- Example: Google App Engine, Heroku.

3. Software as a Service (SaaS):

- Definition: SaaS delivers software applications over the internet, eliminating the need for users to install, maintain, and update the software on their devices. Applications are accessed through a web browser, and users typically pay a subscription fee.

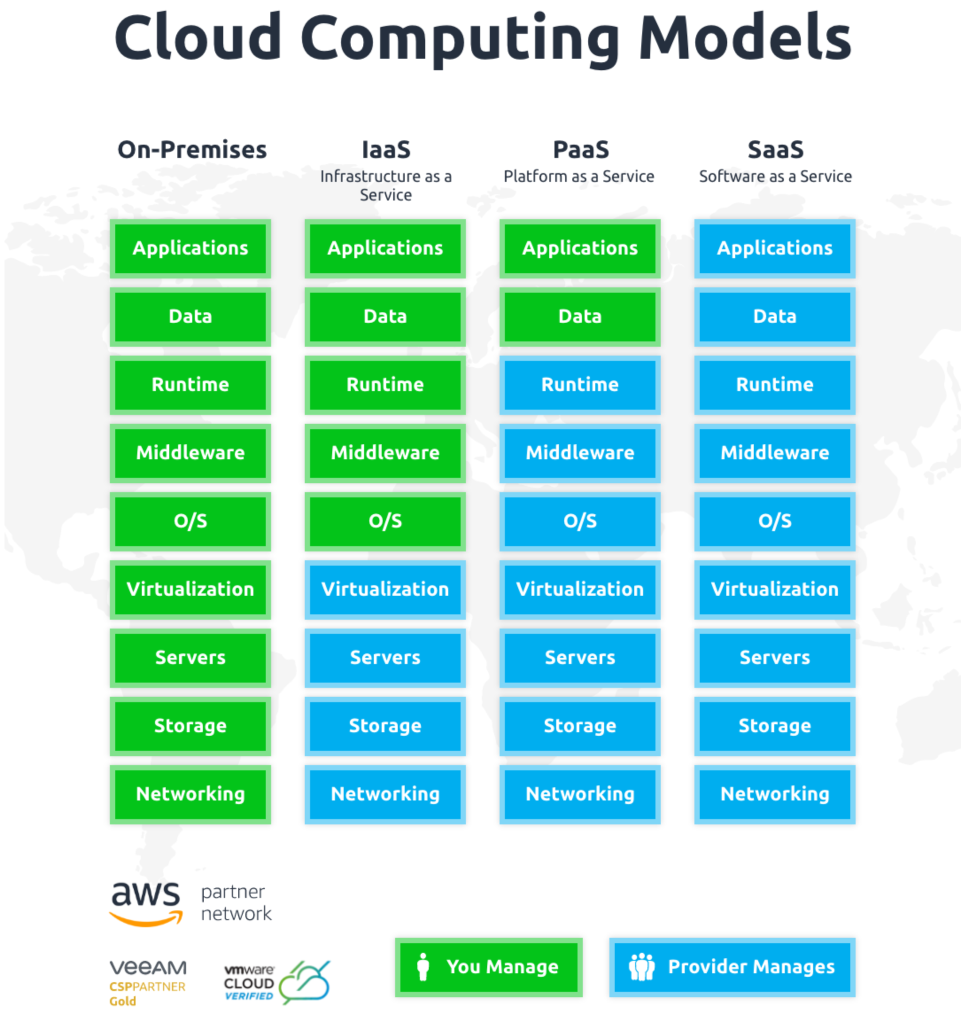
- Characteristics:

  - Users access software applications via a web browser.

- Maintenance and updates are handled by the service provider.
- Subscription-based pricing model.

- Example: Salesforce, Google Workspace, Microsoft 365.

These service models operate at different layers of the cloud computing stack, providing varying levels of abstraction and management responsibilities. The choice of service model depends on the specific needs of the user or organization, with considerations for control, customization, and management complexity. IaaS is closer to traditional infrastructure management, PaaS offers a more streamlined development experience, and SaaS provides complete software solutions without the need for local installations.



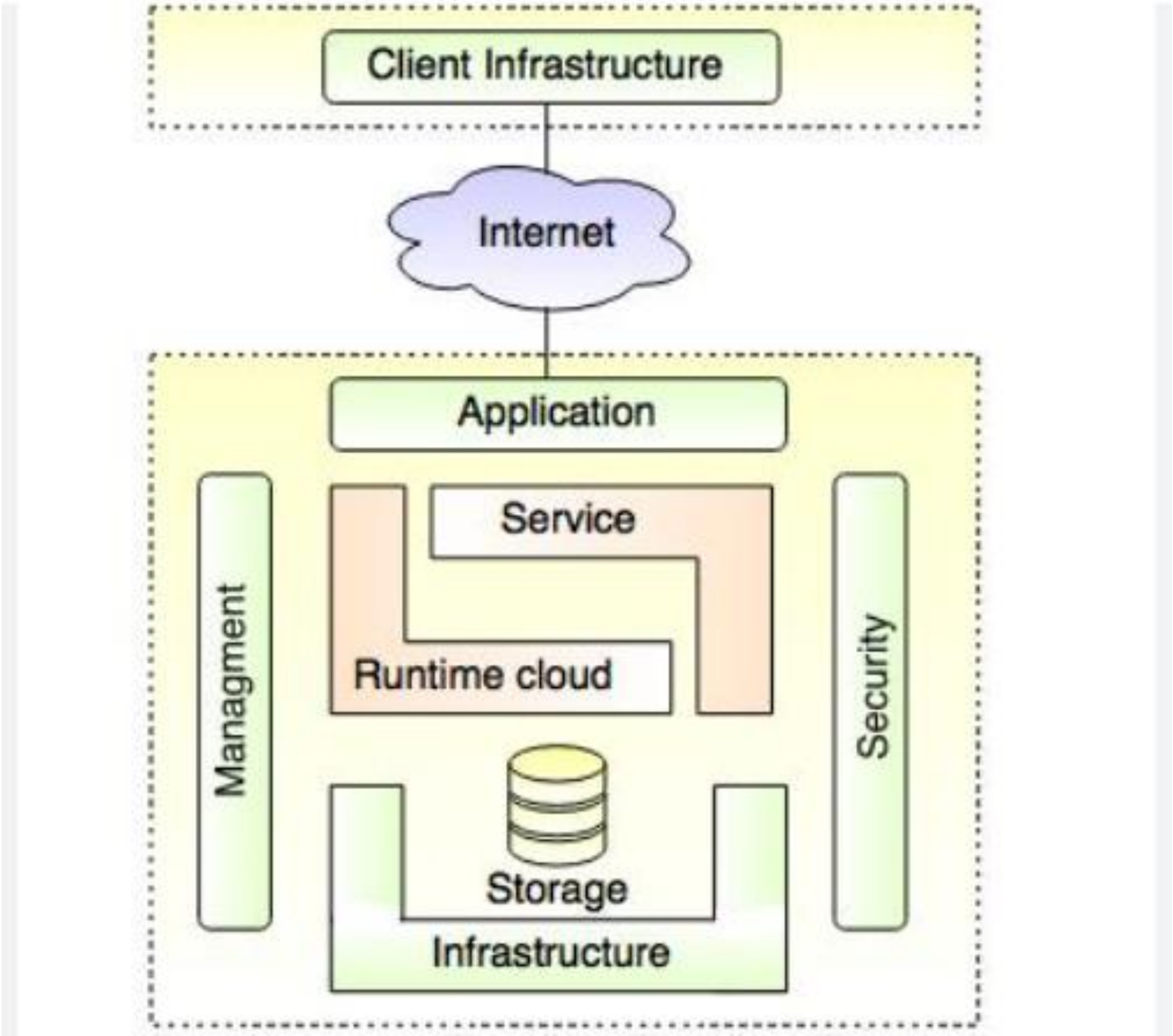
Cloud Computing Models

On-Premises	IaaS Infrastructure as a Service	PaaS Platform as a Service	SaaS Software as a Service
🟩 Applications	🟩 Applications	🟩 Applications	🟦 Applications
🟩 Data	🟩 Data	🟩 Data	🟦 Data
🟩 Runtime	🟩 Runtime	🟦 Runtime	🟦 Runtime
🟩 Middleware	🟩 Middleware	🟦 Middleware	🟦 Middleware
🟩 O/S	🟩 O/S	🟦 O/S	🟦 O/S
🟩 Virtualization	🟦 Virtualization	🟦 Virtualization	🟦 Virtualization
🟩 Servers	🟦 Servers	🟦 Servers	🟦 Servers
🟩 Storage	🟦 Storage	🟦 Storage	🟦 Storage
🟩 Networking	🟦 Networking	🟦 Networking	🟦 Networking

🟩 You Manage

🟦 Provider Manages

Architecture of Cloud Computing



1. Client Infrastructure:

a. Users: Individuals or organizations that access and use cloud computing services.

b. Devices: Laptops, desktops, smartphones, and tablets used to access cloud services.

c. Front End: The user interface and client-side of the cloud computing system. It includes applications and interfaces that users interact with to access cloud services.

d. Middleware: Software that connects the front end and back end, enabling communication and data management. It includes databases, messaging systems, and application servers.

e. APIs (Application Programming Interfaces): APIs allow different components of the cloud architecture to communicate and interact. They facilitate the integration of services and applications.

2. Internet:

a. Communication Channel: The internet serves as the communication channel between users' devices and the cloud infrastructure. It enables data transfer and access to cloud services.

b. Security Measures: Security protocols, such as encryption and secure sockets layer (SSL), are implemented to ensure the confidentiality and integrity of data during transmission over the internet.

3. Backend:

a. Cloud Service Provider (CSP): The entity that owns and operates the cloud infrastructure, offering services to users. Examples include AWS, Azure, Google Cloud, and others.

b. Data Centers : Physical facilities housing servers, storage, networking equipment, and other infrastructure components required to run cloud services.

c. Virtualization Layer: Software that creates and manages virtual instances of computing resources, allowing multiple virtual machines (VMs) to run on a single physical server.

d. Storage: Persistent storage systems used to store data, files, and configurations. Can include various types like object storage, block storage, and file storage.

e. Networking: Infrastructure that enables communication between different components, both within the cloud environment and between the cloud and users.

f. Security and Compliance: Measures and protocols to ensure the security and compliance of data and applications, including firewalls, encryption, and access controls.

g. Scaling and Load Balancing: Mechanisms to dynamically adjust resources based on demand, ensuring optimal performance and resource utilization.

This breakdown illustrates the flow from users and devices through the frontend, internet, and into the backend of the cloud architecture. Middleware and APIs play crucial roles in connecting different layers, and security measures are implemented at various stages to ensure the confidentiality and integrity of data. The backend infrastructure encompasses the core components provided by the cloud service provider, including data centers, virtualization, storage, networking, and security measures.

Benefits of Cloud Computing:

1. Cost Efficiency: Cloud computing eliminates the need for organizations to invest heavily in physical hardware, infrastructure, and maintenance. Users can pay for resources on a pay-as-you-go basis, reducing capital expenses.

2.Scalability and Flexibility: Cloud services provide the ability to scale resources up or down based on demand. This scalability allows organizations to adapt to changing workloads efficiently and ensures optimal resource utilization.

3. Accessibility and Ubiquity: Users can access cloud services from anywhere with an internet connection. This accessibility promotes collaboration and remote work, enabling teams to work seamlessly across different locations.

4. Automatic Updates and Maintenance: Cloud service providers handle infrastructure updates, security patches, and maintenance tasks, relieving organizations from the burden of managing these activities. This ensures that the services are always up-to-date and secure.

5. Disaster Recovery and Redundancy: Cloud providers often have robust disaster recovery mechanisms and redundancy built into their infrastructure. This reduces the risk of data loss and ensures high availability of services, even in the face of hardware failures or natural disasters.

Limitations of Cloud Computing:

1. Security Concerns: Storing sensitive data in the cloud raises security concerns, as organizations may worry about unauthorized access, data breaches, or vulnerabilities in the cloud infrastructure. Security measures must be carefully implemented and continuously monitored.

2. Dependence on Internet Connectivity: Cloud services heavily rely on internet connectivity. Organizations may face disruptions if they experience internet outages or have limited bandwidth. This dependence can affect accessibility and performance.

3. Limited Customization and Control: Users have limited control over the underlying infrastructure in a public cloud. Customization options may be restricted, and organizations may need to conform to the configurations and services provided by the cloud service provider.

4. Potential for Downtime: While cloud providers strive for high availability, no service is immune to downtime. Organizations may experience disruptions in service, impacting operations, especially during outages or maintenance activities by the cloud provider.

5. Data Privacy and Compliance Challenges: Organizations may face challenges regarding data privacy and compliance, especially when dealing with sensitive or regulated data. Meeting legal and regulatory requirements can be complex and may vary across different regions.