Cloud Computing

Cloud Computing is a technology that allows users to access computing resources (like servers, storage, databases, software) over the Internet, instead of owning physical hardware or software.

1. Overview of Cloud Computing

🔹 What is Cloud Computing?

Cloud Computing is the **delivery of IT resources on demand** over the internet, with a pay-as-you-go pricing model. These resources include:

- Servers
- Storage
- Databases
- Networking
- Software
- Analytics
- Intelligence

🔹 Example:

Google Drive is a cloud storage service that allows users to store files online and access them from any device with an internet connection.

2. Advantages of Cloud Computing

Advantage	Description
Cost-Effective	No need to buy or maintain expensive hardware. Pay only for what you use.
Scalability	Easily scale resources up or down based on demand (e.g., during sales or traffic spikes).
Accessibility	Access services anytime, anywhere through the internet.
Automatic Updates	Cloud providers handle software updates and security patches.
Disaster Recovery	Data backup and recovery are managed by the cloud provider.
Collaboration	Multiple users can access and edit files in real-time from different locations.

3. Disadvantages of Cloud Computing

Disadvantage	Description
Internet Dependency	Requires a stable internet connection.
Security Risks	Data stored off-site may be vulnerable if not properly protected.
Limited Control	Users have less control over infrastructure and data handling.
Ongoing Costs	Can become expensive over time due to subscription-based billing.
Vendor Lock-in	Hard to migrate data or applications from one provider to another.

4. Characteristics of Cloud Computing

Characteristic	Explanation
On-Demand Self-Service	Users can access services whenever needed without human interaction.
Broad Network Access	Services are available over the internet and accessible from any device.
Resource Pooling	Resources (storage, CPU, memory) are shared among multiple users.
Rapid Elasticity	Resources can be quickly scaled up or down.
Measured Service	Usage is monitored and billed accordingly (like electricity or water).

5. Service Models of Cloud Computing

Cloud services are delivered in **three main models**:

1. IaaS (Infrastructure as a Service)

- Provides virtualized computing resources over the internet.
- Users manage the OS, storage, applications; provider manages hardware.

Examples: Amazon EC2, Microsoft Azure VMs
Use Case: Hosting websites, virtual machines

2. PaaS (Platform as a Service)

- Offers a platform where users can develop, run, and manage applications without handling the infrastructure.

Examples: Google App Engine, Heroku
Use Case: App development and testing

3. SaaS (Software as a Service)

- Delivers software applications over the internet, on a subscription basis.

Examples: Gmail, Google Docs, Microsoft 365
Use Case: Email, word processing, CRM

6. Deployment Models of Cloud Computing

There are **four types** of cloud deployment based on how services are hosted and accessed:

1. Public Cloud

- Resources are owned and managed by a third-party provider (e.g., AWS, Google Cloud).
- Shared by multiple organizations.

Example: Gmail, Dropbox

2. Private Cloud

- Cloud infrastructure is used exclusively by one organization.
- Can be hosted on-premises or by a third party.

Example: A bank with its own secure cloud environment

3. Hybrid Cloud

- Combines public and private clouds.
- Sensitive data stays in private; other services in public.

Example: Company stores customer data on a private cloud but uses Google Cloud for analytics.

4. Community Cloud

- Shared infrastructure between organizations with similar requirements.

Example: Government departments sharing a cloud for data exchange

7. Security and Privacy in Cloud Computing

◆ Security Concerns:

- **Data Breaches:** Unauthorized access to stored data.
- **Insider Threats:** Employees with malicious intent.
- **Insecure APIs:** Weak access controls in applications.
- **Denial of Service Attacks (DoS):** Overwhelming the system with traffic.

◆ Security Measures:

- **Data Encryption:** Encrypting data during transfer and storage.
- **Authentication & Authorization:** Multi-factor login and user roles.
- **Regular Security Audits:** Monitoring systems for threats.
- **Backup & Recovery Plans:** To restore data in case of failure.

◆ Privacy Issues:

- Cloud providers may store data across borders (data sovereignty issues).
- Users may not know where exactly their data is stored.
- Risk of third-party data access if policies are unclear.