Cloud computing

Module -3

1. **Different type of cloud storage**

➔ 1. Public Cloud Storage

- **What it is:** Storage offered by companies like Google, Amazon, or Microsoft to everyone.
- **Example:** Google Drive, Dropbox, iCloud.
- **Good for:** Personal use or small businesses.
- **Pros:** Easy to use, cheap or free.
- **Cons:** Less control over security and privacy.

2. Private Cloud Storage

- **What it is:** Cloud storage that a company sets up just for itself.
- **Example:** A company creates its own storage system behind a firewall.
- **Good for:** Large companies with strict security needs.
- **Pros:** More control and privacy.
- **Cons:** More expensive, needs IT staff.

3. Hybrid Cloud Storage

- **What it is:** A mix of public and private cloud storage.
- **Example:** A company stores sensitive files in a private cloud and other data in a public cloud.
- **Good for:** Businesses that want both security and flexibility.
- **Pros:** Balance between cost and control.
- **Cons:** Can be complex to manage.

4. Community Cloud Storage

- **What it is:** Shared cloud storage used by a group with similar needs (like hospitals or banks).

- **Example:** Several hospitals sharing a cloud system to store patient data.
- **Good for:** Organizations with shared goals or rules.
- **Pros:** Cost-sharing, common security policies.
- **Cons:** Limited to specific communities.

2. What is role base access control and identity and access management and MFA

1. Role-Based Access Control (RBAC)

- **What it means:** Giving people access to only what they need based on their job.
- **Example:**
    - A **teacher** can enter grades.
    - A **student** can only see their grades.
    - An **admin** can do everything.
- **Why it's useful:** It keeps data safe by not giving everyone full access.

2. Identity and Access Management (IAM)

- **What it means:** A system to manage **who we are** (identity) and **what we can do** (access).
- **Example:**
    - we log into our email → the system checks our **identity** (username/password).
    - Then it checks what **we're allowed to do** (read, send, or delete emails).
- **Why it's useful:** Helps make sure the right people have the right access.

3. Multi-Factor Authentication (MFA)

- **What it means:** Using **more than one way** to prove it's really us.
- **Example:**
    - First, we enter our password.

    - Then, we get a code on our phone.

- **Why it's useful:** Even if someone knows our password, they can't log in without our phone (or second factor).

3. What is physical and virtual host allocation?

➔ 1. Physical Host Allocation

- **What it means:** Using a **real, physical computer (server)** to run our applications or store data.

- **Example:**

    - A company buys a server and sets it up in their office or data center.

- **Why it matters:**

    We have full control over the hardware.

    - But it's more expensive and harder to scale (we need to buy more machines if we grow).

---

2. Virtual Host Allocation

- **What it means:** Using **virtual machines (VMs)** to run apps or services on **shared physical servers**.

- **Example:**

    - One big physical server is split into several "virtual servers," and each one runs like a separate machine.

    - Cloud providers like AWS or Azure do this.

- **Why it matters:**

    - It's cheaper, easier to manage, and we can scale up or down quickly.

    - we don't have to worry about the actual hardware.

4.How to access resources for cloud computing?

➔ ✅ 1. Through the Internet (Web Browser)

- **What happens:** we go to a website (like Google Drive or AWS).
- **Example:** we open our browser and go to `www.dropbox.com` to see our files.
- **Use case:** For simple tasks like checking emails, uploading files, or using cloud apps.

✅ 2. Using Cloud Provider's Dashboard or Portal

- **What happens:** we log in to a special cloud dashboard to manage our resources.
- **Example:** AWS Management Console or Microsoft Azure Portal.
- **Use case:** To create virtual machines, databases, or storage.

✅ 3. Using Remote Desktop or SSH

- **What happens:** we connect to a cloud computer (virtual machine) like ou're sitting in front of it.
- **Example:**
    - Use **Remote Desktop** for Windows servers.
    - Use **SSH (Secure Shell)** for Linux servers.
- **Use case:** For developers or admins to control cloud servers directly.

✅ 4. Using APIs

- **What happens:** Apps talk to cloud services using code.
- **Example:** A weather app fetching data from a cloud database.
- **Use case:** For programmers who want to build apps or automate tasks.

✅ 5. Using Mobile Apps

- **What happens:** we use a cloud provider's app on our phone or tablet.
- **Example:** Google Drive app, Dropbox app, or AWS mobile app.
- **Use case:** To access files or cloud services on the go.

5. Type of backup in the cloud ?

➔ ✅ 1. Full Backup

- **What it is:** Makes a copy of **everything** (all files and data).
- **Example:** If we have 100 files, it backs up all 100 every time.
- **Pros:** Easy to restore everything.
- **Cons:** Takes more time and storage.

✅ 2. Incremental Backup

- **What it is:** Backs up **only the new or changed files** since the last backup.
- **Example:** If we change 5 files, only those 5 get backed up.
- **Pros:** Fast and saves space.
- **Cons:** Slower to restore because it needs all backups in order.

✅ 3. Differential Backup

- **What it is:** Backs up everything that has changed **since the last full backup**.
- **Example:** If we changed 10 files since Monday's full backup, it backs up all 10 each day until the next full backup.
- **Pros:** Faster to restore than incremental.
- **Cons:** Takes more space than incremental.

✅ 4. Mirror Backup

- **What it is:** An **exact copy** of our current data.
- **Example:** If we delete a file on our computer, it's deleted from the backup too.
- **Pros:** Very fast to access and restore.
- **Cons:** Not good if we accidentally delete something.

✅ 5. Continuous Backup (Real-time)

- **What it is:** Data is backed up **as soon as it changes**, in real-time.
- **Example:** we save a document, and it's instantly backed up in the cloud.
- **Pros:** Always up to date.
- **Cons:** Needs more cloud resources and internet.

6. What is disaster recovery?

➔ **Disaster recovery** means having a **plan to get your data and systems back** if something goes wrong — like a cyberattack, fire, flood, or system crash.

💥 Think of it like this:

If our phone gets lost or broken, we can **restore everything** from a backup — contacts, photos, apps.
Disaster recovery does the same thing for businesses and cloud systems.

🛠️ What does it include?

- **Backups** of data (in the cloud or another location)
- **Tools** to quickly restart apps or servers
- **A plan** that tells people what to do in a disaster

🚨 Why it's important:

- Keeps the business running
- Avoids big money losses
- Protects customer trust

🧠 Simple Example:

A hospital's system goes down due to a power failure.
Thanks to disaster recovery:

- Their patient data is restored from cloud backups.
- Critical services are moved to another server.
- They're back up and running within hours.