Cloud computing

Module -4

1.-Resource Monitoring Techniques

- ➔ ✅ **What is Resource Monitoring?**

It means **watching and tracking** our cloud resources — like CPU, memory, storage, and network — to make sure everything is working well.

🔍 Why it's important:

- To **avoid slowdowns** or crashes
- To **save money** (only pay for what we use)
- To **spot problems early**

🛠️ Common Resource Monitoring Techniques:

1. Agent-Based Monitoring

- **What it is:** A small program (called an "agent") is installed on a server to collect data.
- **Example:** It watches CPU usage, disk space, and more.
- **Pros:** Detailed monitoring
- **Cons:** Uses some system resources

2. Agentless Monitoring

- **What it is:** No software is installed; instead, the system is monitored from outside (like over the network).
- **Example:** Using APIs or remote tools to check status.
- **Pros:** Easy to set up
- **Cons:** Less detailed than agent-based

3. Cloud Provider Monitoring Tools

- **What it is:** Tools built into cloud platforms to watch our resources.
- **Examples:**
  - **AWS CloudWatch**
  - **Azure Monitor**
  - **Google Cloud Operations**
- **Pros:** Deep integration with cloud services

4. Performance Dashboards

- **What it is:** A visual screen showing live data like CPU load, memory usage, etc.
- **Example:** A graph showing traffic spikes on your website.
- **Pros:** Easy to understand, great for quick checks

5. Alerts & Notifications

- **What it is:** we get an alert (email, text) if something goes wrong.
- **Example:** “CPU usage is over 90%” → we get a message.
- **Pros:** Helps fix problems quickly

2. How to access computers (Windows and Linux) from the internet? describe tools and its security

➔✅ How to Access Windows and Linux from the Internet

🖥️ 1. For Windows Servers – Use Remote Desktop (RDP)

- **Tool: Remote Desktop Protocol (RDP)**
- **How it works:**
  - we open the **Remote Desktop app** on our computer.
  - Enter the **public IP address** of the Windows server.

    - Login with **username and password**.
- **Example:** Used to manage a Windows server on AWS or Azure.

💻 2. For Linux Servers – Use SSH (Secure Shell)

- **Tool: SSH (via terminal or apps like PuTTY)**
- **How it works:**
    - Open a terminal (or PuTTY app on Windows).
    - Type: `ssh username@public-ip-address`
    - Use a **password** or **SSH key** for login.
- **Example:** Used to control a Linux server on Google Cloud, AWS, etc.

🔒 Security Tools and Best Practices

Security Feature	What It Does	Simple Explanation
Firewall Rules	Control who can connect	Allow only trusted IPs to access the server
SSH Keys (Linux)	Secure login without password	Use a digital “key” instead of typing a password
Strong Passwords	Prevent easy break-ins	Use complex and long passwords
Multi-Factor Authentication (MFA)	Adds extra layer	we log in with password + phone code
Change Default Ports	Reduce attack risk	Don’t use common ports like 22 (SSH) or 3389 (RDP) openly

Use VPN	Hide access behind private network	Only connect after logging into a secure network
Regular Updates	Fix security holes	Keep Windows/Linux systems up to date

3. Encryption Technologies and Methods

- ➔ **Encryption** is like **locking your data** with a secret key, so only the right person can unlock and read it.
- Think of it like sending a secret message that only someone with the right "code" can understand.

Types of Encryption (Technologies & Methods)

✅ 1. Symmetric Encryption

- **How it works:**
  Same key is used to **lock (encrypt)** and **unlock (decrypt)** the data.
- **Example:** AES (Advanced Encryption Standard)
- **Used in:** Files, databases, or data at rest.
- **Simple analogy:** One key to lock and unlock a diary.

✅ 2. Asymmetric Encryption

- **How it works:**
  Uses **two keys** – a **public key** to lock (encrypt) and a **private key** to unlock (decrypt).
- **Example:** RSA (Rivest-Shamir-Adleman)
- **Used in:** Emails, digital signatures, secure websites (HTTPS).
- **Simple analogy:** Anyone can put a message in our locked mailbox (public key), but only we can open it (private key).

✅ 3. Hashing

- **How it works:**
  Converts data into a fixed string of characters. It **cannot be reversed**.

- **Example:** SHA-256

- **Used for:** Password storage, data integrity checks.

- **Simple analogy:** Like turning a sentence into a unique fingerprint.

✅ 4. Encryption in Transit

- **What it is:** Encrypts data while it's **moving** (e.g., being sent over the internet).

- **Example:** HTTPS, SSL/TLS

- **Why:** Protects data from hackers during transfer.

✅ 5. Encryption at Rest

- **What it is:** Encrypts data while it's **stored** (e.g., on a hard drive or in the cloud).

- **Example:** AWS S3 encryption, BitLocker

- **Why:** Protects data in case the device or server is stolen.

✅ 6. End-to-End Encryption (E2EE)

- **What it is:** Only the sender and receiver can read the data. Not even the service provider can see it.

- **Example:** WhatsApp messages, Signal app

- **Why:** Maximum privacy for communication.

4.Describe network security in cloud, compute security and storage security

➔1. Network Security in Cloud

What it is:

Protecting our data **while it moves** through the cloud network.

Key Techniques:

- **Firewalls:** Block unwanted traffic.
- **VPN (Virtual Private Network):** Creates a private, secure tunnel over the internet.
- **Encryption in Transit:** Scrambles data while it travels (like HTTPS).
- **Security Groups & Rules:** Control which IPs or ports can talk to our cloud systems.

Simple Example:

Like building a fence around our house and only letting trusted people in.

2. Compute Security in Cloud

What it is:

Protecting our **virtual machines (VMs)** or **cloud servers** from threats.

Key Techniques:

- **Strong login controls:** Use strong passwords, SSH keys, or multi-factor authentication.
- **OS updates and patches:** Keep cloud machines updated to fix bugs or holes.
- **Antivirus and firewalls:** Protect against viruses and malware.
- **Isolation:** Keep different apps or users in separate VMs or containers.

Simple Example:

Like locking and securing our personal laptop, but in the cloud.

3. Storage Security in Cloud

What it is:

Keeping your **stored data** (files, databases) safe from hackers or loss.

Key Techniques:

- **Encryption at Rest:** Data is scrambled while stored.

- **Access control:** Only the right users or apps can see or change data.
- **Backups:** Regular copies of our data to recover if something goes wrong.
- **Audit logs:** Keep track of who accessed or changed the data.

Simple Example:

Like putting our files in a locked, alarmed cabinet with a camera on it.