**Module -4**

**Cloud computing**

1-Resource Monitoring Techniques

🡪**Resource Monitoring Techniques:**

1. **Agent-Based Monitoring** – Software agent installed on systems to collect data.
2. **Agentless Monitoring** – Uses protocols like SNMP/SSH to gather data without installing agents.
3. **Log Monitoring** – Tracks system/application logs for issues.
4. **Performance Metrics** – Monitors CPU, memory, disk, network usage.
5. **Cloud Monitoring Tools** – AWS CloudWatch, Azure Monitor, etc.

2-How to access compute (windows and Linux) from internet? describe tools and its security

🡪**Accessing Compute (Windows & Linux) from Internet:**

**1. Windows**

* **Tool:** **Remote Desktop Protocol**
* **Port:** TCP **3389**
* **Security:**
  + Use **strong passwords**
  + Enable **Network Level Authentication**
  + Use **VPN** or **bastion host**
  + Enable **firewall rules** and **MFA**

**2. Linux**

* **Tool:** **Secure Shell (SSH)**
* **Port:** TCP **22**
* **Security:**
  + Use **key-based authentication**
  + Disable root login
  + Use **fail2ban**, **firewall**, and **MFA**
  + Access via **bastion host** or **VPN**

3-Encryption Technologies and Methods

🡪**Encryption Methods (Short):**

1. **Symmetric** – Same key
2. **Asymmetric** – Public/private key
3. **Hashing** – One-way encryption
4. **TLS/SSL** – Secures data in transit
5. **Disk Encryption** – Protects data at
6. **E2EE** – Only sender & receiver can read data

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

🡪**1. Network Security in Cloud:**

* Use **firewalls**, **security groups**, **VPNs**, and **NACLs**
* Encrypt data in transit (TLS)
* Monitor traffic with IDS/IPS

**2. Compute Security:**

* Patch OS/VMs regularly
* Use **antivirus**, **MFA**, and **access control**
* Harden VM configurations

**3. Storage Security:**

* **Encrypt data at rest**
* Use **access control policies**
* Regular **backups** and **audits**