Cloud Security and Resource Management

1. Resource Monitoring Techniques

Resource monitoring techniques in cloud computing involve tools and methods to track the usage and performance of cloud resources such as CPU, memory, disk I/O, and network traffic. Common techniques include:

- Agent-based monitoring (e.g., using installed software agents on virtual machines).
- Agentless monitoring (e.g., via APIs).
- Real-time dashboards.
- Alerts and thresholds.

Tools: Prometheus, Grafana, AWS CloudWatch, Azure Monitor, Google Stackdriver.

2. How to access compute (Windows and Linux) from internet? Describe tools and its security

Accessing Windows:

- Use Remote Desktop Protocol (RDP) through port 3389.
- Secure with firewalls, Network Security Groups (NSGs), and VPNs.
- Tools: Microsoft Remote Desktop, AnyDesk.

Accessing Linux:

- Use Secure Shell (SSH) via port 22.
- Secure with key-based authentication, changing default ports, and enabling firewalls.
- Tools: PuTTY, OpenSSH, MobaXterm.

Security:

- Use Multi-Factor Authentication (MFA).
- Restrict access with IP whitelisting.
- Regular patching and updates.
- Use Bastion Hosts or Jump Boxes for secure access.

3. Encryption Technologies and Methods

Encryption ensures data confidentiality by converting data into unreadable code. Key methods include:

- Symmetric Encryption: Same key for encryption and decryption (e.g., AES).
- Asymmetric Encryption: Public/private key pair (e.g., RSA).
- Hashing: One-way encryption for data integrity (e.g., SHA-256).
- Transport Encryption: TLS/SSL for data in transit.
- Storage Encryption: Encrypting stored data with keys (e.g., AWS KMS, Azure Key Vault).

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

Network Security:

- Use of firewalls, Virtual Private Clouds (VPC), subnets, and security groups.
- Encryption of data in transit.
- Intrusion detection and prevention systems (IDS/IPS).

Compute Security:

- Hardening operating systems.
- Patching vulnerabilities.
- Using endpoint protection and monitoring tools.
- Isolating workloads.

Storage Security:

- Encryption of data at rest and in transit.
- Access control policies.
- Regular backups.
- Integrity checks and versioning.