Security In The Cloud

1.Resource Monitoring Techniques

ANS: Resource monitoring is the process of continuously tracking the usage, performance, and health of system resources to ensure availability and efficiency.
Key Monitoring Techniques:

I. **CPU Monitoring**
   - Tracks CPU utilization, load average, and process usage.
   - Helps detect performance bottlenecks and overloads.

II. **Memory Monitoring**
   - Monitors RAM usage, cache, swap usage, and memory leaks.

III. **Disk Monitoring**
   - Checks disk space usage, IOPS, read/write latency.
   - Prevents disk-full and performance issues.

IV. **Network Monitoring**
   - Monitors bandwidth usage, latency, packet loss, and errors.
   - Detects congestion and security threats.

V. **Application Monitoring**
   - Tracks application response time, errors, and availability.

VI. **Log Monitoring**
   - Analyzes system and application logs for errors and security events.

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

ANS: Accessing cloud compute instances from the internet requires secure remote access tools.
Linux Access:
Tool: SSH (Secure Shell)

- Port: **22**
- Authentication: Password or SSH key pair

Example: ssh user@ip_address
Windows Access:
Tool: RDP (Remote Desktop Protocol)

- Port: **3389**
- Authentication: Username and password

Tool Used: Remote Desktop Client

3.Encryption Technologies and Methods

ANS: Encryption is the process of converting data into an unreadable format to protect confidentiality.
Types of Encryption:
1. Symmetric Encryption

- Uses **one key** for encryption and decryption

- Fast and efficient

Examples:

- AES (Advanced Encryption Standard)
- DES (Data Encryption Standard)

2. Asymmetric Encryption

- Uses **public key and private key**
- More secure but slower

Examples:

- RSA
- ECC (Elliptic Curve Cryptography)

Encryption Methods:

I. **Data at Rest Encryption**
  - Protects stored data (disks, databases)
  - Example: Disk encryption (AES-256)

II. **Data in Transit Encryption**
  - Protects data during transfer
  - Example: SSL/TLS, HTTPS

III. **End-to-End Encryption**
  - Data encrypted at sender and decrypted only at receiver

IV. **Key Management Systems (KMS)**
  - Secure storage and rotation of encryption keys

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

ANS:

A. Network Security in Cloud:

- Virtual Private Cloud (VPC)
- Firewalls / Security Groups
- Network ACLs
- VPN and Private Connectivity
- DDoS protection
- Traffic monitoring and intrusion detection

B. Compute Security:

- OS hardening and patch management
- Identity and Access Management (IAM)
- MFA for admin access
- Anti-malware and endpoint protection
- Secure boot and vulnerability scanning

C. Storage Security:

- Encryption at rest and in transit
- Access control using IAM policies
- Private storage access (no public exposure)
- Backup and disaster recovery
- Data integrity and versioning