# Cloud Security Essentials

**1-Resource Monitoring Techniques**

ANS:

Resource monitoring ensures that cloud resources (CPU, memory, storage, network) are efficiently used and performing optimally. Common techniques include:

1. Performance Metrics Monitoring:
   - Tracks CPU usage, memory usage, disk I/O, and network traffic.
   - Tools: Amazon CloudWatch, Azure Monitor, Nagios.
2. Application Monitoring:
   - Monitors the health and performance of applications running on cloud servers.
   - Tools: New Relic, AppDynamics, Dynatrace.
3. Log Monitoring:
   - Collects and analyzes system, application, and security logs.
   - Tools: ELK Stack (Elasticsearch, Logstash, Kibana), Splunk.
4. Threshold-Based Alerts:
   - Sends alerts when resource usage exceeds predefined thresholds.
   - Helps prevent performance degradation or failures.
5. Auto-Scaling Monitoring:
   - Automatically adjusts resources based on demand (e.g., adding more VMs when traffic spikes).
   - Tools: AWS Auto Scaling, Azure Autoscale.
6. Network Monitoring:
   - Monitors network traffic, bandwidth usage, and packet loss.
   - Tools: PRTG Network Monitor, SolarWinds.

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

ANS:

Cloud compute instances can be accessed remotely using specific tools and secure methods:

For Windows Instances:

- Tool: Remote Desktop Protocol (RDP)
- How to Access:
    1. Enable RDP on the Windows VM.
    2. Use Remote Desktop Connection client from your computer.
    3. Enter the public IP or DNS of the VM and login credentials.
- Security Measures:
    - Use strong passwords.
    - Enable Network Level Authentication (NLA).
    - Restrict access via firewall rules or security groups.
    - Use VPN for an extra secure connection.

For Linux Instances:

- Tool: Secure Shell (SSH)
- How to Access:
    1. Enable SSH on the Linux VM.
    2. Use an SSH client (like PuTTY for Windows or terminal on Linux/Mac).
    3. Connect using ssh username@public-ip with private key or password.
- Security Measures:
    - Use SSH keys instead of passwords.
    - Change the default SSH port (22) to reduce attacks.
    - Enable firewall rules to allow access from specific IPs.
    - Use VPN or bastion host for added security.

**3-Encryption Technologies and Methods**

ANS :

Encryption is the process of converting data into a coded form to prevent unauthorized access. It ensures confidentiality, integrity, and security of data in cloud computing.

Encryption Technologies:

1. AES (Advanced Encryption Standard):
   - Symmetric encryption (same key for encryption and decryption).
   - Commonly used for data at rest (stored data).
   - Example: AES-256 for cloud storage encryption.
2. RSA (Rivest–Shamir–Adleman):
   - Asymmetric encryption (public and private key pair).
   - Often used for secure data transmission.
3. TLS/SSL (Transport Layer Security / Secure Sockets Layer):
   - Encrypts data in transit between client and server.
   - Example: HTTPS connections.
4. Homomorphic Encryption:
   - Allows data to be processed while encrypted, without decrypting it.

Encryption Methods:

1. Data at Rest Encryption:
   - Protects stored data (on disks, databases, or cloud storage).
2. Data in Transit Encryption:
   - Protects data moving across networks (using SSL/TLS, VPN).
3. End-to-End Encryption (E2EE):
   - Ensures only the sender and receiver can read the data.

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

ANS:

4.1 Network Security:

Protects data and resources while transmitted over networks.

- Techniques:
  - Firewalls and security groups to control traffic.
  - VPNs for secure remote access.
  - Intrusion Detection/Prevention Systems (IDS/IPS).
  - DDoS protection to prevent attacks.

4.2 Compute Security:

Protects cloud servers, VMs, and applications from threats.

- Techniques:
  - Regular OS and software patching.
  - Anti-virus and malware protection.
  - Role-Based Access Control (RBAC) and Identity Access Management (IAM).
  - Secure configurations of hypervisors and VMs.

4.3 Storage Security:

Protects data stored in cloud storage systems.

- Techniques:
  - Encryption of data at rest and in transit.
  - Access control policies and IAM roles.
  - Data redundancy and backup for reliability.
  - Audit logs and monitoring of storage access.