**Cloud Networking**

1. Resource Monitoring Techniques

Resource monitoring ensures efficient use of cloud infrastructure by tracking performance, availability, and usage.

Common Monitoring Techniques:

* Agent-based Monitoring: Software agents installed on servers collect performance data (e.g., CPU, memory, disk).
  + *Example:* Zabbix Agent, Nagios NRPE.
* Agentless Monitoring: Uses standard protocols (like SNMP, WMI) to gather data without installing agents.
* Cloud-native Monitoring Tools:
  + AWS CloudWatch
  + Azure Monitor
  + Google Cloud Operations (formerly Stackdriver)

Metrics Monitored:

* CPU usage, memory, disk I/O, network bandwidth
* Application-level logs
* Uptime & availability

2. How to Access Compute (Windows and Linux) from Internet – Tools & Security

Windows Access:

* Tool: Remote Desktop Protocol (RDP)
* Port: TCP 3389
* Access method:
  + Enable RDP on the instance
  + Assign a public IP or Elastic IP
  + Use Windows Remote Desktop Client

Linux Access:

* Tool: Secure Shell (SSH)
* Port: TCP 22
* Access method:
  + Enable SSH on instance
  + Use tools like PuTTY, OpenSSH
  + Connect using private key:

ssh -i "key.pem" user@public\_ip

Security Measures:

* Use strong passwords or key-based authentication
* Configure firewall rules / security groups to allow access only from trusted IPs
* Change default ports
* Use VPN for secure internal access
* Enable multi-factor authentication (MFA)

3. Encryption Technologies and Methods

Encryption Methods:

| Type | Description | Examples |
| --- | --- | --- |
| Symmetric | Same key for encryption and decryption | AES, DES |
| Asymmetric | Public key to encrypt, private key to decrypt | RSA, ECC |
| Hashing | One-way encryption, used for integrity checks | SHA-256, MD5 |
| Homomorphic | Allows computation on encrypted data | Used in privacy-preserving apps |

Technologies:

* TLS/SSL: Encrypts web traffic (HTTPS)
* BitLocker / LUKS: Full-disk encryption
* VPN Encryption: IPSec, OpenVPN
* Cloud-native encryption:
  + AWS KMS (Key Management Service)
  + Azure Key Vault
  + Google Cloud KMS

4. Network Security, Compute Security, and Storage Security in Cloud

Network Security:

* Use firewalls and security groups
* Implement Virtual Private Cloud (VPC)
* Use VPNs and IP whitelisting
* Enable DDoS protection (e.g., AWS Shield)

Compute Security:

* Use hardened VM images
* Keep OS and applications up-to-date
* Configure IAM roles properly
* Enable antivirus, endpoint protection
* Use key-based authentication over passwords

Storage Security:

* Encrypt data at rest and in transit
* Use object-level permissions (e.g., S3 bucket policies)
* Backup and replication for disaster recovery
* Enable versioning and access logs
* Apply least privilege access to storage resources