Module – 4 Storage in the cloud

1. Resource Monitoring Techniques.

Ans - **Resource Monitoring Techniques** are essential for tracking the usage and performance of system resources such as CPU, memory, disk, and network. These techniques help ensure optimal system performance, detect bottlenecks, and support capacity planning.

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

To access compute instances (Windows/Linux) from the internet, you can use the following tools and protocols:

**A. Remote Access Tools:**

| **OS** | **Tool/Protocol** | **Description** |
| --- | --- | --- |
| **Windows** | **RDP (Remote Desktop Protocol)** | Allows GUI-based remote access. Default port: 3389 |
| **Linux** | **SSH (Secure Shell)** | Command-line based secure access. Default port: 22 |
| **Cross-platform** | **VPN (e.g., OpenVPN, WireGuard)** | Secure, encrypted connection to private network |
| **Web-based** | **Remote Desktop Services, Guacamole, Bastion Hosts** | Provide browser-based or proxy access |
| **Cloud-native** | **AWS Systems Manager (SSM), Azure Bastion, Google IAP** | Agent-based, secure access without public IPs |

**B. Security Best Practices:**

* **Use Strong Authentication:** Use SSH key pairs or multi-factor authentication (MFA) for secure login.
* **Restrict Access with Firewalls:** Use security groups (AWS), NSGs (Azure), or firewall rules to allow access from trusted IPs only.
* **Avoid Public IPs:** Use VPNs or bastion hosts instead of exposing servers directly to the internet.
* **Audit & Logging:** Enable session logging, command auditing, and access logs.
* **Patch & Harden Systems:** Regularly update and harden OS configurations (e.g., disable root login for SSH).
* **Use Zero Trust Principles:** Verify every access request, regardless of source.

**3. Encryption Technologies and Methods**

Encryption ensures data confidentiality by converting it into unreadable ciphertext.

**A. Types of Encryption:**

| **Type** | **Description** | **Example** |
| --- | --- | --- |
| **Symmetric Encryption** | Same key for encryption and decryption | AES, DES |
| **Asymmetric Encryption** | Public key for encryption, private key for decryption | RSA, ECC |
| **Hashing** | One-way function used for data integrity | SHA-256, bcrypt |

**B. Encryption Methods:**

* **Data at Rest:**
  + Full Disk Encryption (e.g., BitLocker, LUKS)
  + File/Volume Encryption (e.g., VeraCrypt, EFS)
  + Cloud-native encryption (e.g., AWS KMS, Azure Key Vault)
* **Data in Transit:**
  + TLS/SSL (e.g., HTTPS, SMTPS)
  + VPN Encryption (e.g., IPsec, SSL VPN)
* **Data in Use (Emerging):**
  + Homomorphic encryption
  + Confidential computing (e.g., Intel SGX, AMD SEV)

**C. Key Management:**

* Manual key rotation is risky. Use **Key Management Services (KMS)** for secure storage, access control, and automatic rotation of keys.

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

**A. Network Security in Cloud:**

* **Security Groups / Firewalls**: Control traffic to/from instances.
* **VPC (Virtual Private Cloud)**: Isolated network segments.
* **NACLs (Network ACLs)**: Stateless filtering at subnet level.
* **VPN/Direct Connect/ExpressRoute**: Secure private connectivity.
* **IDS/IPS**: Detect and prevent intrusions (e.g., AWS GuardDuty).
* **WAF**: Protect against web-based threats (e.g., SQLi, XSS).

**B. Compute Security:**

* **Instance Hardening**: Disable unused ports, services, default credentials.
* **Patch Management**: Automate OS and software updates.
* **Endpoint Protection**: Use antivirus, EDR, and host firewalls.
* **IAM Roles**: Assign least-privilege roles to compute resources.
* **Runtime Protection**: Detect anomalies during execution (e.g., memory exploits).

**C. Storage Security:**

* **Encryption at Rest**: Apply server-side encryption with customer or cloud-managed keys.
* **Access Controls**: Use ACLs, IAM policies, and bucket policies.
* **Versioning & Backups**: Maintain historical data and enable recovery.
* **Object Locking**: Prevent object deletion (compliance, retention).
* **Data Loss Prevention (DLP)**: Monitor and protect sensitive data.