1. Resource Monitoring Techniques

* Resource monitoring in cloud computing involves tracking the usage and performance of various resources like CPU, memory, storage, and network. Techniques include using cloud provider dashboards (e.g., AWS CloudWatch, Azure Monitor), third-party tools (e.g., Nagios, Datadog), and log-based monitoring for real-time insights. These techniques help in ensuring optimal resource allocation, detecting anomalies, and managing costs.

2. How to Access Compute (Windows and Linux) from the Internet

* To access compute instances (Windows or Linux) from the internet, you typically use Remote Desktop Protocol (RDP) for Windows and Secure Shell (SSH) for Linux. Tools like RDP client (Windows) and PuTTY (Linux/Windows) are commonly used. Security involves:
* Using strong passwords or SSH keys.Configuring firewalls to allow only specific IPs.Employing Multi-Factor Authentication (MFA).

Regularly updating and patching systems.

3. Encryption Technologies and Methods

* Encryption secures data by converting it into a code to prevent unauthorized access. Common technologies include AES (Advanced Encryption Standard) for data at rest and TLS/SSL (Transport Layer Security/Secure Sockets Layer) for data in transit. Methods include symmetric encryption (same key for encryption/decryption) and asymmetric encryption (public/private key pairs).

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

* **Network Security**: Involves using firewalls, Virtual Private Networks (VPNs), Intrusion Detection/Prevention Systems (IDS/IPS), and network segmentation to protect data flow
* : **Focuses on securing** VMs and instances with proper authentication, patch management, anti-malware tools, and OS hardening.
* **Storage Security**: Ensures that data stored in cloud environments is protected using encryption, access controls, and regular audits to detect unauthorized access.