Cloud computing module 4

1. Resource Monitoring Techniques

Resource monitoring techniques help track and manage resource usage, ensuring efficient utilization and optimal performance

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

To access compute resources from the internet, you'll need to use remote access tools and protocols.

RDP : for windows gui based remote desktop access

SSH : for linux cli based remote access

Other tools : any desk, team viewer

1. Encryption Technologies and Methods.

Encryption Technologies:

1. Advanced Encryption Standard (AES): Symmetric key block cipher for encrypting data at rest and in transit.
2. Transport Layer Security (TLS): Cryptographic protocol for secure web communication.
3. Secure Sockets Layer (SSL): Predecessor to TLS, still used for secure web communication.
4. Public Key Infrastructure (PKI): Asymmetric key cryptography for secure data exchange.
5. Hash Functions: One-way encryption for data integrity and authenticity (e.g., SHA-256, MD5).

Encryption Methods:

1. Symmetric Key Encryption: Same key for encryption and decryption (e.g., AES).
2. Asymmetric Key Encryption: Pair of keys for encryption and decryption (e.g., RSA).
3. Block Cipher: Encrypts data in fixed-length blocks (e.g., AES).
4. Stream Cipher: Encrypts data in real-time, bit-by-bit (e.g., RC4).
5. Describe network security in cloud, compute security and storage security.

Network Security in Cloud:

1. Virtual Private Cloud (VPC): Isolated network within a cloud provider.
2. Firewalls: Control incoming and outgoing network traffic.
3. Access Control Lists (ACLs): Filter traffic based on IP addresses and ports.
4. Security Groups: Group-based network access control.
5. Network Segmentation: Divide network into smaller, secure segments.
6. Encryption: Protect data in transit with SSL/TLS, IPsec, or VPNs.

Compute Security:

1. Instance Security: Secure virtual machines and containers.
2. Identity and Access Management (IAM): Control access to compute resources.
3. Key Management: Securely manage encryption keys.
4. Patch Management: Regularly update operating systems and software.
5. Configuration Management: Monitor and enforce secure configurations.

Storage Security:

1. Data Encryption: Encrypt data at rest and in transit.
2. Access Control: Control access to storage resources.
3. Authentication: Verify identity before accessing storage.
4. Authorization: Grant access based on user roles and permissions.
5. Data Backup and Recovery: Regularly backup and test data recovery.