**Module 4**

1.  **AWS CloudWatch**: Monitors AWS resources and applications in real time.

 **Azure Monitor**: Collects and analyzes telemetry data from Azure resources.

 **Google Cloud Operations Suite**: Provides logging, monitoring, and diagnostics for Google Cloud resources.

2. - Remote Desktop Protocol (RDP) for Windows

**Tool**: Microsoft Remote Desktop

**Access**: Use RDP to connect to Windows instances via the internet. Typically, this involves using the instance's public IP address.

**Security**:

**Network Security Groups (NSGs)**: Configure rules to restrict access to specific IP addresses.

**Strong Passwords**: Ensure that user accounts have strong, complex passwords.

**Multi-Factor Authentication (MFA)**: Use MFA to enhance security.

**VPN**: Consider using a Virtual Private Network to access the network securely before using RDP.

**- SSH (Secure Shell) for Linux**

**Tool**: SSH Clients (like PuTTY, OpenSSH)

**Access**: Connect to Linux instances using the SSH protocol, typically via a terminal or dedicated SSH client.

**Security**:

**Key-based Authentication**: Use SSH keys instead of passwords for stronger security.

**Firewall Rules**: Configure firewalls (e.g., AWS Security Groups) to allow SSH access only from specific IPs.

**Fail2Ban**: Implement tools like Fail2Ban to protect against brute-force attacks.

**Port Change**: Change the default SSH port (22) to a non-standard port to reduce automated attacks.

3.**Data-at-Rest Encryption**

**Data-in-Transit Encryption**

. **End-to-End Encryption (E2EE)**

Homomorphic Encryption

**Tokenization**

**Secure Enclaves**

Key Management Solutions (KMS)

4. Network Security in Cloud

**Firewalls:**

**Virtual Private Cloud (VPC)**

**Intrusion Detection and Prevention Systems (IDPS)**

**Network Segmentation**

**VPNs (Virtual Private Networks)**

**Encryption[[1]](#footnote-1)**

-Compute Security in Cloud

**Access Control**

Identity and Access Management (IAM)

Patch Management

**Security Groups and Network ACLs**

**Instance Hardening**

**Monitoring and Logging**

-Storage Security in Cloud

**Data Encryption:**

**Access Control and Permissions:**

**Data Backup and Recovery**

**Data Loss Prevention (DLP)**

**Audit and Compliance**

1. [↑](#footnote-ref-1)