**Storage In The Cloud**

**1. Resource Monitoring Techniques**

Resource monitoring in cloud computing ensures that system performance, availability, and health are maintained. Common techniques include:

* **Agent-Based Monitoring**:
  + Small software agents installed on cloud resources collect metrics (CPU, memory, disk, etc.).
  + Examples: AWS CloudWatch Agent, Zabbix, Datadog agent.
* **Agentless Monitoring**:
  + Collects data without installing agents, often through APIs or protocols like SNMP.
  + Lower overhead, but may offer less detail.
* **Log-Based Monitoring**:
  + Analyzing logs (event logs, system logs) to detect issues or performance problems.
  + Tools: ELK Stack, CloudWatch Logs, Azure Monitor Logs.
* **Performance and Health Dashboards**:
  + Graphical interfaces showing real-time metrics and historical data.
  + Tools: Grafana, Prometheus, AWS CloudWatch, Azure Monitor.

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

* **Accessing Windows Instances:**
  + **Tool**: Remote Desktop Protocol (RDP)
  + **Port**: 3389
  + **Security**:
    - Use strong passwords
    - Restrict RDP access using Security Groups or Firewalls
    - Enable Network Level Authentication (NLA)
    - Use VPN or Bastion Host for extra security
* **Accessing Linux Instances:**
  + **Tool**: SSH (Secure Shell)
  + **Port**: 22
  + **Security**:
    - Use SSH key pairs instead of passwords
    - Disable root login
    - Change default SSH port
    - Use firewalls and IP whitelisting
    - Use Bastion Host or VPN for added security
* **Security Enhancements for Both:**
  + Multi-Factor Authentication (MFA)
  + Regular patching and updates
  + Logging and monitoring of login attempts

**3. Encryption Technologies and Methods**

Encryption is used to protect data at rest, in transit, and during processing.

* **Types of Encryption**:
  + **Symmetric Encryption**: Uses the same key for encryption and decryption (e.g., AES).
  + **Asymmetric Encryption**: Uses a public and private key pair (e.g., RSA, ECC).
* **Data at Rest**:
  + Encryption of stored data (disks, files, databases).
  + Tools: AWS KMS, Azure Storage Encryption, BitLocker.
* **Data in Transit**:
  + Encryption during data transfer (HTTPS, TLS, VPN).
  + Ensures secure communication between endpoints.
* **Client-Side & Server-Side Encryption**:
  + **Client-Side**: Data is encrypted before upload.
  + **Server-Side**: Cloud provider encrypts data upon receipt.
* **Key Management**:
  + Cloud providers offer services to manage encryption keys (e.g., AWS KMS, Azure Key Vault, Google Cloud KMS).

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

* **Network Security**:
  + **Firewalls & Security Groups**: Control inbound/outbound traffic.
  + **Virtual Private Cloud (VPC)**: Isolated network segment in the cloud.
  + **VPNs and Direct Connect**: Secure connections to cloud environments.
  + **Intrusion Detection/Prevention (IDS/IPS)**: Detect and block malicious activity.
  + **DDoS Protection**: Prevent denial-of-service attacks.
* **Compute Security**:
  + **Access Controls**: RBAC, IAM policies.
  + **Patching**: Regular OS and application updates.
  + **Antivirus/Antimalware**: Security agents on virtual machines.
  + **Instance Isolation**: Each VM is logically separated from others.
* **Storage Security**:
  + **Data Encryption**: For data at rest and in transit.
  + **Access Control Policies**: Manage who can read/write storage resources.
  + **Versioning and Object Locking**: Protect against accidental or malicious deletion.
  + **Backup and Replication**: Secure data redundancy and recovery.