

**Hardware Networking**

**System Management and Public Cloud**

**SUBMITTED TO**

**KAMLESH SHUKLA SIR**

**SUBMITTED BY**

**MANAV BANDHANIA**

**1. Different Types of Cloud Storage**

Cloud storage refers to the process of storing data on remote servers accessed via the internet. The main types of cloud storage are:

**a. Object Storage**

* Stores data as objects, each with metadata and a unique identifier.
* Commonly used for unstructured data like images, videos, and backups.
* Examples: Amazon S3, Google Cloud Storage, Azure Blob Storage.

**b. Block Storage**

* Data is stored in blocks, similar to traditional hard drives.
* Used for high-performance applications like databases and virtual machines.
* Examples: AWS Elastic Block Store (EBS), Azure Disk Storage.

**c. File Storage**

* Data is stored in a hierarchical file structure (folders and directories).
* Used for shared network storage in enterprises.
* Examples: AWS Elastic File System (EFS), Google Cloud Filestore, Azure Files.

**d. Cold/Archival Storage**

* Designed for long-term storage with lower access frequency.
* Costs less but has higher retrieval times.
* Examples: Amazon Glacier, Azure Archive Storage.

**2. Role-Based Access Control (RBAC), Identity and Access Management (IAM), and Multi-Factor Authentication (MFA)**

**a. Role-Based Access Control (RBAC)**

RBAC is a security approach where access to resources is granted based on user roles. Users are assigned roles, and each role has specific permissions.

* **Example:**
  + An "Admin" can create, modify, and delete users.
  + A "User" can only view data.
  + A "Guest" has restricted access.
* **Advantages of RBAC:**
  + Reduces the risk of unauthorized access.
  + Simplifies permission management.
  + Helps comply with security policies.

**b. Identity and Access Management (IAM)**

IAM is a framework that manages users' identities and their access to cloud resources.

* **Key Functions of IAM:**
  + User authentication and authorization.
  + Role assignment and permission control.
  + Single Sign-On (SSO) and policy enforcement.
* **Examples:**
  + AWS IAM, Azure Active Directory (AD), Google Cloud IAM.

**c. Multi-Factor Authentication (MFA)**

MFA adds an extra security layer by requiring multiple authentication factors.

* **Types of Authentication Factors:**
  1. **Something You Know:** Password, PIN.
  2. **Something You Have:** OTP (One-Time Password), security token.
  3. **Something You Are:** Fingerprint, facial recognition.
* **Example:**
  1. Logging in requires both a password and a one-time OTP sent to your phone.

**3. Physical vs. Virtual Host Allocation**

Cloud resources are hosted on either physical or virtual machines.

**a. Physical Host Allocation**

* Directly assigns workloads to physical servers.
* Suitable for dedicated hosting environments where high performance is needed.
* Example: Bare-metal servers in data centers.

**b. Virtual Host Allocation**

* Uses virtualization to create multiple virtual machines (VMs) on a single physical server.
* Allows efficient resource usage and cost savings.
* Example: Running multiple VMs on an AWS EC2 instance.

**4. How to Access Resources in Cloud Computing?**

Cloud computing resources can be accessed through:

**a. Web-Based UI**

* Cloud providers offer a graphical interface for users.
* Example: AWS Management Console, Azure Portal, Google Cloud Console.

**b. Command-Line Interface (CLI)**

* Cloud providers offer CLI tools for scripting and automation.
* Example: AWS CLI, Google Cloud SDK, Azure CLI.

**c. APIs (Application Programming Interfaces)**

* Developers can programmatically access cloud services using APIs.
* Example: AWS SDK, Google Cloud API, Azure REST API.

**d. Remote Desktop and SSH**

* Remote access methods allow users to manage cloud-hosted servers.
* Example:
  + **RDP (Remote Desktop Protocol)** for Windows servers.
  + **SSH (Secure Shell)** for Linux servers.

**5. Types of Backup in Cloud**

Cloud backup ensures data protection and disaster recovery. There are three main types:

**a. Full Backup**

* Backs up all selected data every time.
* Requires high storage space and time.

**b. Incremental Backup**

* Only backs up new or modified files since the last backup.
* Faster and consumes less storage.
* Example: If a full backup was taken on Monday, an incremental backup on Tuesday will only store new/changed files.

**c. Differential Backup**

* Backs up all changes since the last full backup.
* Uses more storage than incremental but restores faster.

**Other Backup Types:**

* **Snapshot Backup:** Captures the state of a VM or storage at a point in time.
* **Mirror Backup:** Creates an exact real-time replica of data.

**6. What is Disaster Recovery (DR)?**

Disaster Recovery (DR) is the strategy and processes to restore IT operations after failures due to cyberattacks, natural disasters, or human errors.

**a. Disaster Recovery Strategies**

* **Backup and Restore:** Regular backups stored in the cloud.
* **Pilot Light:** Minimal cloud setup that can scale up during a disaster.
* **Warm Standby:** Partially active cloud environment ready to take over.
* **Hot Standby (Active-Active):** Fully operational backup environment running parallel.

**b. Disaster Recovery Sites**

1. **Cold Site:** Minimal infrastructure, requiring time to restore operations.
2. **Warm Site:** Partially configured with essential services.
3. **Hot Site:** Fully operational site, ready to switch immediately.

**c. Example of DR**

* A company running applications in AWS sets up a DR site in another AWS region.
* If the primary region fails, traffic automatically shifts to the backup region.