Assignment : Cloud Computing

**Submitted By :- Purv Patel**

**Module 4: Resource Management And Security**

**1-Different type of cloud storage**

### > **Types of Cloud Storage**

Cloud storage is categorized based on how data is stored, accessed, and managed. The main types include:

### **1️ Block Storage**

🔹 Stores data in fixed-sized **blocks**, similar to traditional hard drives.  
🔹 Used for **high-performance applications, databases, and virtual machines (VMs)**.  
🔹 Supports **low-latency and high-speed** access.

**Examples:**  
 Amazon **EBS (Elastic Block Store)**  
 Microsoft **Azure Managed Disks**  
 Google **Persistent Disks**

### **2️ File Storage (Network File System - NFS, SMB/CIFS)**

🔹 Data is stored in a **hierarchical file structure** with folders.  
🔹 Used for **file sharing, user directories, and application data**.  
🔹 Accessible over a **network using protocols like SMB (Windows) & NFS (Linux)**.

**Examples:**  
 Amazon **EFS (Elastic File System)**  
 Azure **File Storage**  
 Google **Filestore**

### **3️ Object Storage**

🔹 Stores **data as objects** with metadata & unique identifiers.  
🔹 Highly **scalable, durable, and cost-effective**.  
🔹 Used for **backups, media files, logs, and cloud-native applications**.

**Examples:**  
 Amazon **S3 (Simple Storage Service)**  
 Microsoft **Azure Blob Storage**  
 Google **Cloud Storage**

### **4 Hybrid & Multi-Cloud Storage**

🔹 Combines **on-premises and cloud storage**.  
🔹 Allows businesses to keep sensitive data **on-premises** while leveraging the cloud for scalability.

**Examples:**  
 AWS **Storage Gateway**  
 Azure **StorSimple**  
 Google **Anthos**

### **Conclusion**

🔹 **Block Storage** → Best for **databases, VMs, high-performance apps**.  
🔹 **File Storage** → Best for **file sharing & collaborative environments**.  
🔹 **Object Storage** → Best for **scalability, backups & unstructured data**.  
🔹 **Hybrid Storage** → Best for **flexibility & compliance needs**.

**2-What is role base access control and identity and access management and MFA**

### > Role-Based Access Control (RBAC), Identity & Access Management (IAM), and Multi-Factor Authentication (MFA)

1️ Role-Based Access Control (RBAC)

🔹 RBAC is a security model that grants access to users based on predefined roles instead of individual permissions.  
🔹 Users are assigned roles, and each role has specific permissions to access resources.

Key Features:  
 Least Privilege – Users get only the access they need.  
 Centralized Management – Easier to manage permissions.  
 Compliance & Security – Reduces unauthorized access risks.

Example:

* Admin Role → Full access to servers & databases.
* HR Role → Access to employee records but not financial data.
* Guest Role → Read-only access to reports.

🔹 Used in: Windows Server, Azure AD, AWS IAM, Kubernetes, etc.

2️ Identity and Access Management (IAM)

🔹 IAM is a framework for managing users, authentication, and permissions to access IT resources.  
🔹 Ensures the right individuals have the right access to systems.

Key Features:  
 User Authentication – Verifies user identity.  
 Access Control – Assigns permissions based on roles.  
 Single Sign-On (SSO) – One login for multiple services.

Example:

* AWS IAM → Manages user roles & permissions in AWS cloud.
* Azure AD → Manages identities across Microsoft services.

3️ Multi-Factor Authentication (MFA)

🔹 MFA adds an extra layer of security by requiring multiple authentication factors.  
🔹 Instead of just a password, users must verify identity using at least two or more factors:

Types of Authentication Factors:  
1️ Something You Know → Password, PIN.  
2️ Something You Have → OTP (One-Time Password), security token, smart card.  
3️ Something You Are → Biometric (Fingerprint, Face ID).

Example:

* Logging into Microsoft 365 requires a password + OTP via SMS.
* Google Account login requires password + fingerprint.

**3-What is physical and virtual host allocation?**

### > Physical vs. Virtual Host Allocation

Host allocation refers to assigning computing resources to run applications, services, or virtual machines (VMs). It can be done using physical hosts (bare-metal servers) or virtual hosts (virtualized environments).

1️ Physical Host Allocation

A physical host is a dedicated server that directly runs an operating system (OS) and applications without virtualization.

Key Characteristics:  
 Dedicated resources (CPU, RAM, storage, network).  
 Ideal for high-performance computing, databases, and legacy applications.  
 Less flexible compared to virtual environments.

Example:

* A physical Windows Server assigned to handle enterprise applications.
* A bare-metal server running without virtualization in a data center.

2️ Virtual Host Allocation

A virtual host is a server that runs multiple virtual machines (VMs) using a hypervisor like VMware ESXi, Microsoft Hyper-V, or KVM.

Key Characteristics:  
 Multiple VMs can run on a single physical server.  
 Resource-efficient & scalable (dynamic allocation of CPU, RAM, storage).  
 Used in cloud computing, virtualization, and multi-tenant environments.

Example:

* A Hyper-V host running multiple VMs for different departments.
* An AWS EC2 instance assigned to a client in a cloud data center.

Comparison Table

| Feature | Physical Host Allocation | Virtual Host Allocation |
| --- | --- | --- |
| Resource Usage | Dedicated hardware | Shared among VMs |
| Scalability | Limited | Highly scalable |
| Cost | Expensive (hardware cost) | Cost-effective (better resource utilization) |
| Flexibility | Low | High (dynamic allocation) |
| Management | Manual setup & maintenance | Centralized via hypervisors |

**4-How to access resource of cloud computing?**

### > How to Access Cloud Computing Resources?

Cloud computing resources can be accessed using different methods depending on the service model (IaaS, PaaS, SaaS) and deployment type (Public, Private, Hybrid Cloud).

1️ Web-Based Access (Cloud Portals & Dashboards)

🔹 Cloud providers offer web-based dashboards for managing resources.  
🔹 Requires an internet connection & login credentials.

Examples:  
 AWS Management Console – Manage EC2, S3, RDS, etc.  
 Azure Portal – Manage VMs, storage, networking.  
 Google Cloud Console – Control cloud resources.

2️ Command-Line Interface (CLI) Access

🔹 CLI allows automation & scripting for managing cloud resources.  
🔹 Requires installation of CLI tools from cloud providers.

Examples:  
 AWS CLI → Manage AWS services via terminal.  
 Azure CLI → Run commands to configure Azure resources.  
 Google Cloud SDK (gcloud CLI) → Manage Google Cloud via CLI.

3️ API Access (Programmatic Access)

🔹 Cloud services provide RESTful APIs for developers to integrate cloud resources into applications.  
🔹 Used for automation, DevOps, and third-party tool integration.

Examples:  
 AWS SDK (Boto3 for Python, Java SDK) → Automate AWS services.  
 Google Cloud APIs → Programmatically access resources.  
 Azure REST API → Manage cloud resources via API calls.

4️ Remote Desktop & SSH Access

🔹 Used to connect to cloud-based virtual machines (VMs).

Examples:  
 Remote Desktop Protocol (RDP) → Access Windows VMs.  
 Secure Shell (SSH) → Connect to Linux-based instances.

5️ Cloud Storage Access (File Transfer & Storage)

🔹 Cloud storage can be accessed via:

* Web interface
* CLI
* APIs
* Mounting cloud storage as a local drive

Examples:  
 Amazon S3 → Access via AWS S3 API, CLI, or web UI.✅ Google Drive / OneDrive → Access via browser, mobile app, or desktop sync.

6️ Virtual Private Network (VPN) & Direct Connections

🔹 Secure access to cloud resources from on-premises environments.

Examples:  
 AWS Direct Connect – Private link to AWS.  
 Azure ExpressRoute – Secure private network to Azure.  
 Google Cloud Interconnect – Direct connection to Google Cloud.

**5-Type of backup in cloud?**

### > Types of Backup in Cloud Computing

Cloud backups ensure data protection, disaster recovery, and business continuity. The main types of cloud backups are:

1️ Full Backup

🔹 A complete copy of all data is backed up every time.  
🔹 Ensures maximum protection but requires more storage and time.

Best For:  
 Critical business data.  
 Initial backup setup.

Example:

* A company backs up all server data to AWS S3 once a week.

2️ Incremental Backup

🔹 Backs up only the data that changed since the last backup (full or incremental).  
🔹 Faster and uses less storage than full backups.

Best For:  
 Daily or frequent backups.  
 Reducing storage costs.

Example:

* After a full backup on Monday, only new or modified files are backed up daily.

3️ Differential Backup

🔹 Backs up all changes made since the last full backup (but not incremental backups).  
🔹 Requires more storage than incremental but is faster to restore.

Best For:  
 Faster recovery than incremental backups.  
 Balancing storage and restore speed.

Example:

* A full backup on Sunday, then a differential backup every day.

4️ Mirror Backup (Real-Time Backup)

🔹 Exact copy (replica) of live data is stored in real time.  
🔹 No historical versions—only the latest version is kept.

Best For:  
 High-availability systems.  
 Disaster recovery solutions.

Example:

* A company mirrors its database to a secondary cloud region.

5️ Synthetic Full Backup

🔹 Creates a new full backup using previous backups + new changes, without re-backing up all data.  
🔹 Faster than full backups and saves bandwidth.

Best For:  
 Cloud-based storage optimization.  
 Reducing backup time & bandwidth.

Example:

* AWS or Azure creates a full backup without re-uploading unchanged files.

6️ Snapshot Backup

🔹 Captures the entire system state (VM, disk, or database) at a specific point in time.  
🔹 Fastest recovery method, commonly used for virtual machines and databases.

Best For:  
 Quick disaster recovery.  
 VM and cloud database backups.

Example:

* AWS EBS Snapshots, Azure VM snapshots, Google Cloud snapshots.

**6-What is disaster recovery?**

### > **What is Disaster Recovery (DR)?**

**Disaster Recovery (DR)** is the **process of restoring IT systems, data, and operations** after a disruption caused by **natural disasters, cyberattacks, hardware failures, or human errors**. It ensures **business continuity and minimal downtime**.

### **🔹 Key Components of Disaster Recovery:**

**Backup & Data Replication** → Copies of critical data stored in **cloud, offsite, or redundant locations**.  
 **Failover Systems** → Secondary systems ready to take over in case of failure.  
 **Disaster Recovery Plan (DRP)** → Documented steps for recovery & risk assessment.  
 **Testing & Drills** → Regular simulations to validate recovery strategies.

### **🔹 Types of Disaster Recovery:**

1️ **Backup-Based DR** → Uses **regular backups** for restoration.  
2️ **Cloud DR** → Utilizes **cloud infrastructure** for fast recovery.  
3️ **Virtualization DR** → Restores systems using **VM snapshots**.  
4️ **Failover & Redundant Systems** → Uses **secondary data centers** for instant recovery.  
5️ **Disaster Recovery as a Service (DRaaS)** → Fully managed DR solutions in the cloud (AWS, Azure, Google Cloud).

### **🔹 Benefits of Disaster Recovery:**

**Minimizes Downtime** → Quickly restores critical services.  
 **Protects Data** → Ensures data integrity and security.  
 **Ensures Compliance** → Meets regulatory standards (e.g., GDPR, HIPAA).  
 **Business Continuity** → Keeps operations running after a disaster.