Cloud computing module 3

1. Different type of cloud storage.

Public Cloud Storage

\* Storage provided by a third-party provider over the internet

\* Scalable and on-demand

\* Examples: Amazon S3, Google Cloud Storage, Microsoft Azure Blob Storage

Private Cloud Storage

\* Storage provisioned and managed within a private network

\* More secure and controlled than public cloud storage

\* Examples: VMware vCloud, Microsoft System Center

Hybrid Cloud Storage

\* Combination of public and private cloud storage

\* Allows for data to be stored and moved between public and private clouds

\* Examples: AWS Storage Gateway, Azure StorSimple

1. What is role base access control and identity and access management and MFA.

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

A security approach that grants access to resources based on a user's role within an organization

Users are assigned roles, and each role has specific permissions and access rights

Access is determined by the role, not individual user identity

**Identity and Access Management (IAM)**

* A framework of policies, processes, and technologies that manage digital identities and access to resources
* Ensures that only authorized users have access to sensitive information and systems

Components: authentication, authorization, accounting & auditing.

**Multi-Factor Authentication (MFA)**

* A security process that requires multiple authentication factors to access a resource.

Factors : password, pin biometric, OTP.

1. What is physical and virtual host allocation?

**Physical Host Allocation**

* Assigning physical resources (e.g., CPU, memory, storage) of a physical server to a specific workload or application
* Each physical host is a separate server with its own resources

**Virtual Host Allocation**

* Assigning virtual resources (e.g., virtual CPU, memory, storage) from a physical host to a virtual machine (VM) or container
* Multiple virtual hosts can run on a single physical host, sharing resources

1. How to access resource of cloud computing?

1.Choose a Cloud Provider

Select a cloud provider (e.g., AWS, Azure, Google Cloud, IBM Cloud)

2. Create an Account

sign up for an account

Fill out the registration form with required information (e.g., name, email, password)

3. Set up Authentication

Verify your email address (if required)

Set up multi-factor authentication (MFA) for added security

4. Select Resources

Browse the provider's dashboard or catalog to choose resources (e.g., virtual machines, storage, databases)

5. Configure Resources

Set up resource settings (e.g., instance type, storage size, network settings)

Configure security groups and access controls

6. Access Resources

Web Portal: Log in to the provider's dashboard

Command-Line Interface (CLI): Use command-line tools

Software Development Kits (SDKs): Use libraries for programming languages

1. Type of backup in cloud?

1. Full Backup

Complete copy of all data and applications

Initial backup, followed by incremental or differential backups

2. Incremental Backup

Copies only changed data since last backup

Reduces storage space and time

3. Differential Backup

Copies all changes since last full backup

Faster restore times than incremental backups

1. What is disaster recovery?

Disaster Recovery is a comprehensive plan and process to quickly restore business operations, systems, and data after a catastrophic event or disaster, such as: cyberattacks, natural disasters, hardware and software failures