**Unit-III**

1.List different cloud file system.. Explain Ghost file system

2. Explain different storage sub system.

3. Explain distributed Data storage.

4. How Data Management done in Cloud Storage

5.Explain the Cloud Storage from LANs to WANs

6.Write Data intensive technology for cloud Computing

7. What are three Types of Cloud Storage

8.What is Data store? Type of Data store.

**Unit IV**

1.What are risk in cloud computing

2.What is Risk Management in Cloud computing.

3.Explain the process of Risk Management

4.Explain the Cloud Security Services

5.Explain Data security and Application security Maintained in cloud computing.

6.What are the secure cloud software requirements

7.Explain the different key security Challenges for cloud computing.

---------------------------------------------------------------------------------------------------------------------------------------

**Unit III: Cloud Storage and Data Management**

**1. Cloud File Systems & Ghost File System**

* Cloud file systems: Google File System (GFS), Hadoop Distributed File System (HDFS), Amazon S3, Microsoft Azure Blob Storage, Ghost File System (GFS).
* **Ghost File System (GFS)**:
  + Ghost File System is a cloud-based file system designed to provide transparent access to files across distributed environments.
  + Uses distributed metadata to efficiently locate and manage files while supporting features like data deduplication and automatic replication.
  + It employs caching mechanisms to improve performance, making it suitable for cloud infrastructure deployments.
  + Optimized for distributed environments.
  + Eg. The files that you store on google docs, are not necessarily stored in the same spot. They are present across *many* distributed storages.

**2. Storage Subsystems**

* **Direct Attached Storage (DAS)**: Locally attached to a server.
  + DAS is the basic storage system providing block-level storage and used for building SAN and NAS.
  + The performance of SAN and NAS depends on DAS.
  + Performance of DAS will always be high, because it is directly connected to the system.
* **Network Attached Storage (NAS)**: Shared storage accessed over a network.
  + For file-level storage, NAS is used.
  + SAN and DAS act as base system for NAS.
  + NAS is also called as ‘File Server’.
  + The main advantages of NAS are that multiple hosts can share a single volume at the same time, whereas when using SAN or DAS only one client can access the volume at a time.
* **Storage Area Network (SAN)**: High-speed dedicated storage network.
  + When multiple hosts want to connect a single storage device, then SAN is used.
  + SAN provides block-level storage and simultaneous access is not permitted and hence it is suitable for clustering environment.
  + SAN technologies are FC (Fibre Channel), iSCSI (Internet SCSI) and AoE (ATA over Ethernet).

**Cloud Storage**: Scalable storage accessed via the internet. (Above SAN & NAS)

* + Scalable, internet-based storage.
  + Includes Block, File, and Object storage.
  + Examples: Amazon S3, Google Cloud Storage, Azure Blob Storage.

**3. Distributed Data Storage**

* Data is partitioned and stored across multiple nodes.
* Ensures fault tolerance and redundancy.
* Uses replication and consistency models.
* Examples: HDFS, Amazon S3, Cassandra.

**4. Data Management in Cloud Storage**

Data storage is expensive; therefore, storage administrators are trying to use tiered storage.

* **Data Replication**: Copies across multiple servers for reliability.
* **Data Consistency**: Ensuring synchronization across copies.
* **Data Deduplication**: Removing duplicate data for efficiency.
* **Data Tiering**: Moving data across storage types based on usage.

**5. Cloud Storage: LANs to WANs**

Cloud storage enables data storage and retrieval over a network.

* **LAN-based Cloud Storage**: High-speed, low-latency data access.  
  Operates within a private network.
* **WAN-based Cloud Storage**: Uses internet-based data access, higher latency.  
  Data is stored in remote cloud servers.
* **Hybrid Storage**: Combines local and remote storage for efficiency.

**6. Data-Intensive Technologies for Cloud Computing**

* **Hadoop MapReduce**: Processes large-scale data in parallel.
* **Apache Spark**: Faster data analytics using in-memory processing.
* **Google BigQuery**: SQL-based analytics for big data.
* **NoSQL Databases**: MongoDB, Cassandra, DynamoDB.

**7. Three Types of Cloud Storage**

* **Block Storage**: Raw storage for databases and virtual machines.
* **File Storage**: Hierarchical, shared storage (e.g., NFS, SMB).
* **Object Storage**: Scalable storage for unstructured data (e.g., Amazon S3).

**8. Data Store & Types**

* **Data Store**: A system for storing and managing data.
* **Types**:
  + **Relational Databases**: SQL-based (e.g., MySQL, PostgreSQL).
  + **NoSQL Databases**: Non-relational (e.g., MongoDB, Cassandra).
  + **Key-Value Stores**: Simple, fast storage (e.g., Redis, DynamoDB).
  + **Document Stores**: Stores semi-structured data (e.g., CouchDB).
  + **Graph Databases**: Stores relationships efficiently (e.g., Neo4j).

---------------------------------------------------------------------------------------------------------------------------------------

**Unit IV: Cloud Security & Risk Management**

**1. Risks in Cloud Computing**

* **Data Breaches**: Unauthorized access to data.
* **Data Loss**: Accidental deletion or corruption.
* **Service Downtime**: Cloud provider outages.
* **Compliance Issues**: Failure to meet regulations.
* **Insider Threats**: Employees misusing access.

**2. Risk Management in Cloud Computing**

* **Risk Identification**: Finding vulnerabilities and threats.
* **Risk Assessment**: Analyzing impact and likelihood.
* **Risk Mitigation**: Implementing security measures.
* **Risk Monitoring**: Continuous evaluation and improvement.

**3. Process of Risk Management**

* **Risk Analysis**: Identifying critical assets.
* **Threat Assessment**: Evaluating potential threats.
* **Risk Prioritization**: Ranking risks based on impact.
* **Mitigation Planning**: Deploying countermeasures.
* **Monitoring & Review**: Regular security assessments.

**4. Cloud Security Services**

* **Identity and Access Management (IAM)**: Controls user access.
* **Data Encryption**: Protects data at rest and in transit.
* **Threat Detection**: Monitors for security incidents.
* **Disaster Recovery**: Backup and failover solutions.

**5. Data Security & Application Security in Cloud Computing**

* **Data Security**:
  + Encryption, authentication, and access controls.
  + Regular security audits.
* **Application Security**:
  + Secure coding practices.
  + Regular patching and updates.
  + API security and firewalls.

**6. Secure Cloud Software Requirements**

* **Authentication & Authorization**: Role-based access control.
* **Data Encryption**: AES, TLS, SSL for secure communication.
* **Regular Audits**: Security assessments <M,Nand compliance checks.
* **Secure APIs**: Proper authentication for API endpoints.

**7. Key Security Challenges in Cloud Computing**

* **Multi-Tenancy Risks**: Shared infrastructure vulnerabilities.
* **Data Sovereignty**: Compliance with data regulations.
* **Access Control**: Preventing unauthorized access.
* **Insider Threats**: Employees misusing privileges.
* **Zero-Day Exploits**: Newly discovered security flaws.