

# Cloud Computing

## CT2 Suggestions:

1. Compare server virtualization with storage virtualization.

Ans: Sure! Here's the short and easy **table format** 🌟

Point	Server Virtualization	Storage Virtualization
<b>Meaning</b>	Divides one physical server into many virtual servers.	Combines many storage devices into one virtual storage.
<b>Focus</b>	CPU, memory, and system resources.	Data and storage space.
<b>Main Tool</b>	Hypervisor (e.g., VMware, Hyper-V).	Storage controller or software.
<b>Purpose</b>	To run many virtual machines on one server.	To manage and use storage efficiently.
<b>Example</b>	VMware vSphere, Microsoft Hyper-V.	VMware vSAN, IBM SAN Volume Controller.
<b>Output</b>	Multiple virtual servers.	One large virtual storage pool.

1. Explain different types of virtualization technologies used in cloud environments.

Ans:

### **Different Types of Virtualization Technologies Used in Cloud Environments**

1. **Server Virtualization** – Divides one physical server into many virtual machines (VMs) to run different OS and apps.
  - *Example:* VMware vSphere, Microsoft Hyper-V.
2. **Storage Virtualization** – Combines multiple storage devices into one virtual storage pool for easy management.
  - *Example:* VMware vSAN, IBM SAN Volume Controller.
3. **Network Virtualization** – Creates multiple virtual networks on a single physical network for flexibility and security.
  - *Example:* VMware NSX, Cisco ACI.
4. **Application / Desktop Virtualization** – Runs applications or desktops on central servers, allowing remote user access.
  - *Example:* Citrix Virtual Apps, VMware Horizon.

1. Evaluate the importance of virtualization in cloud storage management.

Ans: **Importance of Virtualization in Cloud Storage Management**

1. **Efficient Resource Utilization** – Combines multiple storage devices into one virtual pool to reduce wastage and use capacity effectively.
2. **Simplified Management** – Centralized control makes it easier to allocate, monitor, and manage storage resources.
3. **Scalability & Flexibility** – Storage can be easily increased or decreased based on user or application demand.

4. **Data Protection & Recovery** – Enables backup, replication, and quick disaster recovery to ensure data safety.

1. What are different storage models used for big data.

Ans: **Different Storage Models Used for Big Data**

1. **File Storage** – Stores data in files and folders in a distributed system; suitable for unstructured data.
  - o *Example:* Hadoop Distributed File System (HDFS).
2. **Block Storage** – Breaks data into fixed-size blocks and stores them separately for faster access.
  - o *Example:* Amazon Elastic Block Store (EBS), SAN.
3. **Object Storage** – Stores data as objects with metadata and unique IDs; ideal for large-scale unstructured data.
  - o *Example:* Amazon S3, OpenStack Swift.
4. **Database Storage** – Stores structured or semi-structured data using databases for easy querying and management.
  - o *Example:* MongoDB, Cassandra, HBase.

1. Outline the key features of distributed programming.

Ans: **Key Features of Distributed Programming**

1. **Resource Sharing** – Allows multiple systems to share resources like files, data, and hardware across a network.
2. **Concurrency** – Enables several processes to run at the same time on different machines.
3. **Scalability** – System performance can be improved easily by adding more nodes or machines.
4. **Transparency** – Hides the complexity of the distributed system from the user (e.g., location or access transparency).

1. Infer the role of parallel programming in cloud computing.

Ans: **Role of Parallel Programming in Cloud Computing**

1. **Improves Performance** – Divides large tasks into smaller parts and executes them simultaneously on multiple processors or nodes.
2. **Efficient Resource Utilization** – Makes full use of cloud's distributed computing power to process data faster.
3. **Supports Big Data Processing** – Essential for handling large datasets in applications like Hadoop and Spark.
4. **Reduces Execution Time** – Parallel execution speeds up complex computations and improves overall system efficiency.

 **Example:** Hadoop MapReduce, Apache Spark.

1. Show how NoSQL databases differ from relational databases in cloud applications.

Ans: **Difference between NoSQL Databases and Relational Databases**

Point	Relational Database (RDBMS)	NoSQL Database
<b>Data Model</b>	Stores data in tables with rows and columns.	Stores data as key-value, document, column, or graph.
<b>Schema</b>	Fixed schema — structure must be defined before storing data.	Schema-less — flexible structure for unstructured data.
<b>Scalability</b>	Vertically scalable (add more power to one server).	Horizontally scalable (add more servers easily).
<b>Data Type</b>	Best for structured data.	Handles structured, semi-structured, and unstructured data.
<b>Query Language</b>	Uses SQL (Structured Query Language).	Uses non-SQL queries (e.g., JSON, APIs).
<b>Examples</b>	MySQL, Oracle, PostgreSQL.	MongoDB, Cassandra, CouchDB.

1. Relate big data issues to cloud programming models.

**Ans: Relation of Big Data Issues to Cloud Programming Models**

1. **Scalability** – Cloud models can grow easily to handle large data volumes.

*Example:* Hadoop clusters expand as data grows.

1. **Data Distribution** – Data is stored and processed across many servers.

*Example:* MapReduce divides tasks across servers.

1. **Fault Tolerance** – Cloud systems recover data if a node fails.

*Example:* Hadoop stores copies of data blocks.

1. **Fast Processing** – Parallel processing in cloud (like Hadoop, Spark) speeds up big data tasks.

*Example:* Apache Spark processes data quickly in memory.

1. Outline the functioning of GFS in distributed storage.

**Ans: Functioning of Google File System (GFS) in Distributed Storage**

1. **Master-Slave Architecture** – One **master node** manages metadata, while multiple **chunk servers** store actual data.
2. **Data Splitting** – Files are divided into fixed-size **chunks** (usually 64 MB) and stored across multiple servers.
3. **Replication for Fault Tolerance** – Each chunk is **replicated** on several servers (usually 3) to prevent data loss.
4. **Client Interaction** – Clients communicate with the master for chunk locations and then read/write data directly from/to chunk servers.

 **Example:** Used by **Google** for handling massive amounts of data in services like Search and Gmail.

1. Show the connection between cloud scalability and parallel programming.

Ans: **Connection Between Cloud Scalability and Parallel Programming**

1. **Divide and Conquer** – Parallel programming splits tasks into smaller parts to run at the same time.
2. **Handles Growth** – Cloud scalability adds more servers to manage increasing workloads.
3. **Faster Processing** – Parallel execution with scalable resources reduces task completion time.
4. **Resource Efficiency** – Uses additional cloud nodes only when needed, optimizing resources.

**Example:** Hadoop MapReduce and Apache Spark run tasks in parallel across scalable cloud clusters to process big data efficiently.

 **In short:** Parallel programming + cloud scalability = **fast, efficient, and scalable processing of large workloads.**

1. Classify programming models used in cloud environments.

Ans:

Programming models in cloud environments define how applications are developed and executed using cloud resources. The main types are:

1. Task-Based Model: Divides applications into independent tasks for parallel execution. (e.g., MapReduce)

2. Thread-Based Model: Uses multiple threads within a process to run concurrently. (e.g., Java Threads)

3. Data Parallel Model: Performs the same operation on multiple data parts. (e.g., Hadoop, Spark)

4. Workflow Model: Represents applications as a series of connected tasks. (e.g., Airflow)

5. Service-Oriented Model: Builds applications from reusable services communicating via APIs. (e.g., REST, SOAP)

6. Event-Driven Model: Executes code in response to events. (e.g., AWS Lambda)

1. Explain the role of HDFS in storing large data sets.

Ans: **Role of HDFS in Storing Large Data Sets**

1. **Distributed Storage** – Splits large files into **blocks/chunks** and stores them across multiple nodes in a cluster.
2. **Fault Tolerance** – Each block is **replicated** (usually 3 copies) on different nodes to prevent data loss.
3. **Scalability** – Can easily **add more nodes** to store growing amounts of data.
4. **High Throughput** – Enables **parallel access** to data blocks, improving read/write speed for big data processing.

 **Example:** Hadoop Distributed File System (HDFS) is used in **Hadoop clusters** for big data analytics.

1. Relate the use of big data tools to efficient cloud application development.

Ans: **Use of Big Data Tools in Efficient Cloud Application Development**

1. **Data Processing** – Tools like **Hadoop and Spark** enable fast processing of large datasets in the cloud.
2. **Scalability** – Big data tools work on **distributed systems**, allowing applications to handle growing data easily.
3. **Fault Tolerance** – Tools provide **data replication and recovery**, ensuring reliable cloud applications.
4. **Analytics & Insights** – Big data tools help **analyze data quickly**, supporting smarter decision-making in applications.

 **Example:** Using **Apache Spark** in cloud-based analytics apps improves speed and scalability.

 **In short:** Big data tools make cloud applications **fast, scalable, reliable, and data-driven**.

1. Assess the resource efficiency of deploying 20 VMs on two hosts, each with 16 cores and 64 GB RAM, with each VM needing 2 cores and 4 GB RAM.

Ans:

**Given:**

- **Hosts:** 2
- **Each host:** 16 cores, 64 GB RAM
- **VMs:** 20
- **Each VM needs:** 2 cores, 4 GB RAM

**Step 1: Calculate total resources per host**

- CPU: 16 cores
- RAM: 64 GB

**Step 2: Calculate total resources needed for 20 VMs**

- CPU:  $20 \times 2$  cores = 40 cores
- RAM:  $20 \times 4$  GB = 80 GB

**Step 3: Compare with available resources**

- **Total available across 2 hosts:**
  - CPU:  $16 \times 2 = 32$  cores
  - RAM:  $64 \times 2 = 128$  GB
- **Required:** CPU = 40 cores → **exceeds capacity**
- RAM = 80 GB → fits within capacity

#### Step 4: Resource efficiency assessment

1. **CPU overcommitment needed** – 40 cores required, only 32 available → CPU resources are **overcommitted**, which may lead to performance degradation.
2. **RAM utilization** – 80 GB required out of 128 GB → RAM is **efficiently utilized** (~62.5% used).
3. **Overall efficiency** – RAM is fine, but CPU is insufficient unless overcommitment is allowed; risk of bottlenecks under heavy workloads.

#### Conclusion:

- **RAM:** Efficient
- **CPU:** Insufficient without overcommitment
- **Overall:** Can deploy, but performance may degrade for CPU-intensive workloads.

If you want, I can also make a **super short table version** for easy exam revision. Do you want me to do that?

You said:

yes

ChatGPT said:

Here's a **short and easy table version** for quick exam revision:

Resource	Available (2 Hosts)	Required (20 VMs)	Assessment
CPU Cores	32	40	Overcommitted → possible performance issues
RAM	128 GB	80 GB	Efficient utilization (~62.5%)
Overall	–	–	RAM okay, CPU may bottleneck; careful workload planning needed

 In short: Deploying 20 VMs on 2 hosts **fits RAM but exceeds CPU**, so performance could degrade under heavy CPU load.

1. Critique the decision to deploy high-I/O database VMs on shared virtualized storage rather than dedicated disks.

Ans: **Critique of Deploying High-I/O Database VMs on Shared Virtualized Storage**

1. **Performance Issues** – Shared storage can become a **bottleneck** under heavy I/O load, slowing database performance.

- Resource Contention** – Multiple VMs using the same storage may **compete for I/O**, causing latency spikes.
- Fault Isolation** – Failures or misconfigurations in shared storage can **affect multiple VMs**, reducing reliability.
- Cost vs. Flexibility** – Shared storage is **cost-effective and flexible**, but may not meet the performance demands of high-I/O databases.

 **Example:** A high-traffic MySQL or Oracle database VM may perform better on **dedicated SSDs** rather than shared SAN/NAS storage.

- Assess the performance implications if 10 application VMs share a single 1 Gbps virtual network interface card (vNIC) in a hypervisor setup.

Ans: Here's a **short table version** for quick exam revision 

Factor	Impact on 10 VMs Sharing 1 Gbps vNIC
<b>Bandwidth</b>	Contention reduces per-VM throughput (<100 Mbps each if all active)
<b>Latency</b>	Increases due to network congestion and queueing
<b>Performance</b>	High-traffic apps (video, DB) may experience slowdowns
<b>Overall</b>	Shared vNIC limits network performance; dedicated or higher-speed vNIC recommended

 **In short:**Sharing a single 1 Gbps vNIC among 10 VMs **causes contention, higher latency, and potential performance degradation.**

- Differentiate between network-level, host-level, and application-level security in cloud computing. Provide examples of security measures used at each level.

Ans: Here's a **short and easy table format** for quick revision 

Security Level	Focus	Examples
<b>Network-Level</b>	Protects data <b>in transit</b> over networks	Firewall, VPN, IDS/IPS, DDoS protection
<b>Host-Level</b>	Protects <b>servers or VMs</b> from attacks	Antivirus, OS hardening, patch updates, access control
<b>Application-Level</b>	Protects <b>applications and data</b>	Input validation, encryption, WAF, authentication

 **In short:**

- **Network:** Secures communication
- **Host:** Secures servers/VMs
- **Application:** Secures apps and data

1. Analyze the role of access control mechanisms in maintaining data security in a cloud environment. How do they differ from authentication methods?

Ans: **Role of Access Control Mechanisms in Cloud Security**

1. **Defines Permissions** – Access control determines **who can access what resources** and what actions they can perform.
  - *Example:* Role-Based Access Control (RBAC) assigns permissions based on user roles.
2. **Protects Sensitive Data** – Ensures that only **authorized users** can read, modify, or delete data.
3. **Enforces Security Policies** – Helps maintain compliance by restricting access according to organization policies.
4. **Monitors and Audits Access** – Tracks user actions for accountability and detection of unauthorized attempts.

### Difference from Authentication

Aspect	Access Control	Authentication
Purpose	Determines <b>what a user can do</b> after login	Verifies <b>who the user is</b>
Focus	Authorization of resources and actions	Identity verification
Example	RBAC, ABAC (Attribute-Based Access Control)	Passwords, OTP, biometric login

### ✓ In short:

- **Authentication:** Confirms identity.
- **Access Control:** Grants or restricts permissions based on identity.

### Example in cloud:

- User logs in with a password (**authentication**) → Can access only their own S3 bucket (**access control**).

1. Evaluate the effectiveness of existing authentication mechanisms (e.g., multi-factor authentication, biometric access) in securing cloud services against unauthorized access.

Ans: **Effectiveness of Authentication Mechanisms in Cloud Security**

1. **Multi-Factor Authentication (MFA)** – Combines two or more factors (password + OTP/smartphone) to reduce the risk of unauthorized access.
  - *Effectiveness:* Stronger than password-only; prevents most credential-based attacks.
  - *Example:* AWS MFA for cloud console access.
2. **Biometric Authentication** – Uses unique physical traits (fingerprint, facial recognition) for identity verification.
  - *Effectiveness:* Difficult to forge; enhances security for sensitive cloud services.
  - *Example:* Azure Active Directory with fingerprint or face login.
3. **Password-Based Authentication** – Single-factor using username/password.
  - *Effectiveness:* Weak alone; vulnerable to phishing, brute force, or credential leaks.
4. **Token-Based Authentication** – Uses temporary tokens or keys to access cloud services.

- *Effectiveness*: Limits exposure time and prevents replay attacks.
- *Example*: OAuth tokens for cloud APIs.

1. Compare data privacy issues in mobile and media clouds.

Ans: **Data Privacy Issues in Mobile and Media Clouds**

Aspect	Mobile Cloud	Media Cloud
Type of Data	Personal info, contacts, location, messages	Photos, videos, audio, large media files
Privacy Concern	Unauthorized access to personal data, location tracking, app permissions	Copyright infringement, sharing without consent, leakage of sensitive media
Data Volume	Moderate, mostly structured or semi-structured	Large volume, mostly unstructured
Security Measures	App permissions, encryption, secure authentication	DRM (Digital Rights Management), access control, encryption
User Risk	Identity theft, tracking	Unauthorized sharing, intellectual property loss

**Q1. Write the difference between network level, host level and application level security in Cloud.**

Ans:

Level	Meaning	Techniques Used	Purpose
<b>Network Level Security</b>	Protects the entire network and data while it is transferred between users and servers.	Firewalls, VPNs, intrusion prevention systems, and encryption of data in transit.	Prevents unauthorized access, sniffing, and denial-of-service attacks.
<b>Host Level Security</b>	Secures individual cloud servers or virtual machines used for computation or storage.	Antivirus software, operating system patching, and monitoring of logs.	Prevents internal misuse or malware infection on cloud hosts.
<b>Application Level Security</b>	Protects the web applications and APIs running on the cloud.	Input validation, authentication, and secure coding practices.	Prevents SQL injection, cross-site scripting, and data leakage.

**Explanation:** All three levels work together to create a layered defense system ensuring complete cloud protection from both internal and external threats.

## Q2. Write the role of access control mechanism in maintaining cloud security.

Ans:

1. **Definition** – Access control defines *who* can access *what* resources in the cloud environment. It prevents unauthorized entry and misuse.
2. **Identity Verification** – Every user or process must be authenticated before getting access to cloud resources.
3. **Role-Based Access Control (RBAC)** – Users are assigned roles such as admin, developer, or viewer; each role has limited permissions.
4. **Least Privilege Principle** – Ensures users only have the minimum access needed to complete their job.
5. **Result** – It reduces insider threats, prevents data breaches, and maintains overall cloud security integrity.

## Q3. Uses of Authentication mechanism in Cloud services.

Ans:

1. **User Identification** – Confirms the real identity of users accessing the cloud to avoid impersonation.
2. **Data Protection** – Prevents unauthorized users from reading or modifying confidential data.
3. **Access Control** – Works together with authorization to allow only legitimate operations.
4. **Multiple Methods** – Can use passwords, OTPs, biometrics, or tokens depending on the sensitivity of the data.
5. **Outcome** – Builds trust between users and providers, maintaining secure communication channels in cloud applications.

## Q4. Write the difference between Authentication and Authorization.

Ans:

Aspect	Authentication	Authorization
<b>Definition</b>	Process of verifying the identity of a user.	Determines what the authenticated user is allowed to do.
<b>Timing</b>	Happens before authorization.	Happens after authentication.
<b>Purpose</b>	Confirms “Who you are.”	Confirms “What you can access.”
<b>Example</b>	Logging in with username and password.	Accessing admin dashboard after login.
<b>Techniques</b>	Passwords, OTP, biometrics.	Role-based or policy-based permissions.

**Explanation:** Both work together to ensure secure and controlled access to cloud resources.

## **Q5. What are the different threats and malware for the cloud services.**

Ans:

1. **Data Breach** – Unauthorized access to confidential data due to weak security policies.
2. **Malware Injections** – Attackers insert malicious code or programs into cloud software to steal or corrupt data.
3. **Account Hijacking** – Login credentials are stolen through phishing or brute force attacks.
4. **Denial of Service (DoS)** – Overloads the cloud servers with heavy traffic to make them unavailable.
5. **Insider Threats** – Employees or administrators misusing their privileges for personal gain or revenge.

## **Q6. Explain how application level threats can lead to data breaches.**

Ans:

1. **Weak Input Validation** – If user input is not validated properly, attackers can inject harmful scripts or SQL queries.
2. **Insecure APIs** – Poorly designed APIs can expose sensitive data directly to the attacker.
3. **Unpatched Software** – Applications that are not updated may have known vulnerabilities that hackers exploit.
4. **Weak Authentication** – Applications without strong login security make it easy for intruders to access user accounts.
5. **Result** – Such vulnerabilities lead to unauthorized data access, modification, or complete loss of confidential information.

## **Q7. Write the difference between DoS and DDoS.**

Ans:

Aspect	DoS (Denial of Service)	DDoS (Distributed Denial of Service)
<b>Number of Attackers</b>	Single source launches the attack.	Multiple infected systems attack simultaneously.
<b>Severity</b>	Limited impact due to one origin.	Very powerful and harder to stop.
<b>Detection</b>	Easier to detect and block.	Difficult to trace as it uses many IPs.
<b>Example</b>	One user sending continuous requests to a server.	Botnet of computers flooding a website with traffic.
<b>Effect</b>	Temporary unavailability.	Complete service shutdown and heavy loss.

## **Q8. Categorize various types of threat agents.**

Ans:

1. **External Attackers** – Hackers or cybercriminals trying to steal or corrupt data.
2. **Internal Threats** – Authorized users misusing their access or credentials.
3. **Automated Bots** – Software that continuously scans and attacks systems automatically.
4. **Malware Developers** – Individuals who design and distribute viruses or ransomware.
5. **Competitors or Hacktivists** – Try to damage reputation or steal intellectual property.

## **Q9. Compare traditional security models with access control mechanisms in Cloud.**

Ans:

Aspect	Traditional Security Models	Cloud Access Control Mechanisms
<b>Environment</b>	Local, on-premise infrastructure.	Virtual, remote, and scalable.
<b>User Access</b>	Based on physical presence or static login.	Managed dynamically through identity and role management.
<b>Scalability</b>	Limited and manually configured.	Highly scalable using automation and policies.
<b>Security Updates</b>	Manual patching required.	Centralized automatic updates handled by provider.
<b>Control</b>	Organization manages everything.	Shared between user and cloud service provider.

## **Q10. Analyze different encryption techniques in Cloud data privacy.**

Ans:

- Symmetric Encryption (AES)** – Uses one secret key for both encryption and decryption, fast and efficient.
- Asymmetric Encryption (RSA)** – Uses two keys: a public key to encrypt and a private key to decrypt.
- Hashing Techniques (SHA, MD5)** – Converts data into fixed hash values to verify integrity.
- Homomorphic Encryption** – Allows computation on encrypted data without decrypting it.
- Conclusion** – Encryption ensures that even if hackers gain access, the data remains unreadable and protected.

## **Q11. Explain how encryption techniques enable data privacy.**

Ans:

- Data Conversion** – Transforms readable data into a secure coded format, preventing unauthorized understanding.
- Key Management** – Only users with correct decryption keys can access the actual information.
- Transmission Protection** – Protects data while it travels between client and cloud servers.
- Storage Security** – Keeps stored files encrypted, reducing risk in case of server breaches.
- Result** – Guarantees confidentiality, integrity, and compliance with privacy laws.

## **Q12. What is Multi-Factor Authentication (MFA) and explain its requirement in Cloud.**

Ans:

- Definition** – MFA requires two or more independent credentials before allowing access.
- Examples** – Password + OTP, or Password + Biometric scan.
- Purpose** – Reduces the risk of unauthorized access even if one factor (like a password) is stolen.
- In Cloud** – Protects admin panels, dashboards, and critical accounts that are accessible remotely.
- Result** – Strengthens cloud security by verifying identity through multiple trusted layers.

### **Q13. Write the best ways for managing sensitive data in the Cloud.**

Ans:

1. **Encrypt Before Uploading** – Always encrypt confidential files locally before storing in cloud.
2. **Use Strong Authentication** – Protect accounts with MFA and complex passwords.
3. **Apply Access Restrictions** – Give permissions only to trusted users and groups.
4. **Monitor and Backup Data Regularly** – Helps recover quickly from accidental deletion or attacks.
5. **Choose Reliable Providers** – Select cloud vendors with recognized security certifications (ISO 27001, SOC 2).

### **Q14. Define HIDS in virtualization.**

Ans:

1. **Meaning** – HIDS stands for *Host-Based Intrusion Detection System*.
2. **Purpose** – Monitors and analyzes activities occurring on a single cloud host or virtual machine.
3. **Functionality** – Detects file changes, unauthorized logins, or unusual resource usage.
4. **Working** – Compares system activity logs with known attack signatures.
5. **Importance** – Provides an additional protection layer inside virtualized environments where multiple VMs share the same host.

### **Q15. Discuss the risk and mitigation strategies for different threats in Cloud infrastructure.**

Ans:

1. **Data Breaches** – Mitigation: Use end-to-end encryption, access controls, and regular audits.
2. **Downtime or Outages** – Mitigation: Employ redundancy and backup data centers.
3. **Malware and Viruses** – Mitigation: Install updated antivirus software and intrusion detection.
4. **Account Hijacking** – Mitigation: Implement MFA and regular password changes.
5. **Insider Threats** – Mitigation: Log all activities and apply role-based access restrictions.

### **Q16. Write the importance of data privacy in Cloud.**

Ans:

1. **Confidentiality** – Ensures that sensitive user or business data is kept secret and accessed only by authorized persons.
2. **Legal Compliance** – Fulfills privacy laws such as GDPR, HIPAA, or IT security policies.
3. **Customer Trust** – Builds user confidence in cloud services by ensuring their data is safe.
4. **Prevention of Misuse** – Stops hackers, competitors, or insiders from exploiting stored data.
5. **Business Continuity** – Maintains integrity and reduces financial or reputational loss from leaks.

### **Q17. Explain the responsibility of Cloud service providers to maintain security.**

Ans:

1. **Infrastructure Protection** – Maintain secure servers, networks, and power backups for continuous service.
2. **Data Encryption** – Apply encryption for stored and transmitted information.
3. **Regular Updates** – Patch vulnerabilities and update software to close loopholes.
4. **Monitoring and Auditing** – Continuously monitor for suspicious activities and maintain audit logs.
5. **Compliance and Transparency** – Follow international standards (ISO, NIST) and clearly define shared security responsibilities with customers.

### **Q18. Discuss different authentication mechanisms.**

Ans:

1. **Password-Based Authentication** – Basic method where user provides a password; simple but vulnerable.
2. **Token-Based Authentication** – Uses unique tokens (JWT, OAuth) to maintain session security.
3. **Biometric Authentication** – Uses fingerprints, facial recognition, or voice for identity verification.
4. **Multi-Factor Authentication (MFA)** – Combines two or more methods like password + OTP.

5. **Single Sign-On (SSO)** – Allows a user to log in once and access multiple applications securely (used in Google and Microsoft services).