1. **When data is stored in cloud, what three (3) security precautions must you take? Be as detailed as possible (9 points)**

   Answer: When storing data in the cloud, three essential security precautions to take are:

   There are three security precautions explaining below:

   Encryption: All sensitive data should be encrypted both at rest and in transit to protect it from unauthorized access. Encryption transforms data into a format that unauthorized users cannot read without the proper decryption key. This applies to both data at rest when it is stored and data in transit while it's being transmitted. Cloud providers offer built-in encryption, but customers should also apply their own encryption measures to ensure end-to-end security. This helps protect sensitive data, like personal information from potential breaches.

   Access Controls: Implement strict identity and access management (IAM) policies. Use multi-factor authentication (MFA) for all accounts, adopt role-based access control (RBAC) to limit privileges, and regularly audit accounts and permissions to prevent unauthorized access.

   Regular Audits and Monitoring: Conduct frequent security audits to identify vulnerabilities and ensure compliance with security standards. Deploy monitoring solutions that provide real-time alerts for suspicious activities, such as unauthorized data access or irregular network traffic. Use automated tools to continuously monitor configurations and address any misconfigurations promptly

2. **Name five (5) advantages of using Cloud Computing (5 points)**

   Answer: Cloud computing using five advantages are given below:

   - Cost-effective (Switching from CapEx to OpEx)
   - Scalability
   - Accessibility
   - Flexibility
   - Disaster Recovery

3. **Describe the difference between scalability and elasticity? (6 points)**

   Answer:

Scalability	Elasticity
Ability to handle increased workload over time	Automatic adjustment of resources based on real-time demand
Long-term strategic need	Short-term tactical need

Adding more servers to handle growth	Scaling resources up during peak hours, then down afterward
Vertical and Horizontal.	Scaling up or down automatically as needed.
Increasing server count from 5 to 10 for higher traffic.	Adding servers during peak hours and reducing afterward.

4. **What are the different layers of cloud computing? (6 points)**

   Answer: The different layers of cloud computing are:

   - **Infrastructure as a Service (IaaS):** This is the foundational layer that provides virtualized computing resources over the internet, such as servers, storage, and networking.
     Example - Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform.
   - **Platform as a Service (PaaS):** Provides a platform allowing customers to develop, run, and manage applications.
     Example - Google App Engine, Microsoft Azure App Service, Heroku
   - **Software as a Service (SaaS):** Provides software applications over the internet, on a subscription basis.
     Example - Google Workspace (Docs, Gmail), Microsoft 365, Dropbox.

5. **What resources are provided by Infrastructure as a Service? (8 points)**

   Answer: IaaS provides the fundamental building blocks of computing infrastructure are:

   - Compute resources (virtual machines): Virtual machines (VMs) with customizable CPU, memory, and storage configurations.
   - Networking: Virtual networks, load balancers, IP addresses, VPNs, and firewalls for secure data transfer.
   - Storage systems: Scalable storage options, such as block storage, object storage, and file storage.
   - Security services: Identity and access management (IAM), encryption, firewalls, and intrusion detection systems.
   - Backup and Recovery: Automated backup services, disaster recovery options, and snapshot functionalities.
   - Scalability and Load Balancing: Features that automatically scale resources based on demand and distribute traffic effectively.
   - Monitoring and Analytics: Tools for monitoring system performance, usage statistics, and resource health.
   - Data Center Management: Virtual data centers that allow users to manage multiple resources in a centralized environment.

6. **Describe how important is Platform as a Service to a customer? (8 points)**

Answer: PaaS is important to a customer because it provides the hardware, software, and infrastructure for running applications. The importance of PaaS to customers include:

- Simplifies Development: Customers focus on application development instead of infrastructure management since the service provider handles the backend operations like resource provisioning, scaling, and load balancing.
- Cost Savings: Customers do not need to invest in physical infrastructure or spend on maintenance, as everything is managed by the cloud provider.
- Faster Deployment: PaaS accelerates the process of developing and deploying applications by providing pre-configured platforms and built-in software components.
- Scalability: The platform automatically adjusts resources to handle varying workloads, making it easier to scale applications up or down depending on demand.
- Security and Maintenance: The service provider manages security, updates, and system maintenance, allowing businesses to focus on application development rather than infrastructure management.
- Collaboration: Developers can work collaboratively from different locations using the same platform, as the environment is cloud-based and accessible from anywhere.
- Flexibility and Customization: PaaS supports multiple programming languages and frameworks, giving developers flexibility in their choice of tools.

7. **What does Software as a Service provide? (8 points)**

Answer: SaaS provides customers with access to software over the internet. Users do not install the software on their local devices.

- Access to software over the internet without local installation.
- On-demand functionality, allowing users to access the software whenever needed.
- Ready-to-use applications without local installation.
- Enables scalability based on user needs.
- A complete software offering accessible over the internet.
- Automatic updates and maintenance handled by the provider.
- No need for installation or manual upgrades.
- Subscription-based access with automatic updates.
- Examples include Microsoft Office 365, Salesforce, and Google Docs.

8. **How does cloud computing provide on-demand functionality? (5 points)**

Answer: Cloud computing provides on-demand functionality given below:

- Users can provision and manage resources through easy-to-use web interfaces.
- Instantly allocates computing, storage, and network resources based on user needs.
- Automatically scales resources up or down based on demand.

- Users pay only for the resources they consume.
- Automates resource allocation, load balancing, and maintenance.
- Provides real-time data on resource usage and performance.
- Allows developers to manage resources through code.
- Enables quick setup of applications using pre-configured templates.

9. Why is virtualization an important consideration for cloud computing platforms? (6 points)

Answer: Virtualization is an important consideration for cloud computing platforms for several reasons:

- Breaks Down Physical Barriers: Virtualization abstracts physical resources, allowing them to be shared and managed more efficiently. It enables the pooling of computing resources like CPU, memory, and storage, breaking the limitations imposed by physical infrastructure.
- Cost Savings: By consolidating servers and optimizing resources, virtualization reduces both capital expenses (CapEx) and operational expenses (OpEx).
- Scalability: Virtual machines can be created, scaled, and removed quickly, allowing cloud providers to adjust resources in real-time to meet varying customer demands.
- Disaster Recovery: Virtualization facilitates rapid backup, replication, and restoration of virtual machines (VMs), minimizing downtime and reducing the risk of data loss.
- Enhanced Security: Virtual machines operate in isolation, preventing security threats from spreading between VMs and the underlying hardware.
- Flexibility and Agility: Virtualization enables rapid provisioning and deployment of resources, allowing businesses to quickly respond to new requirements or market shifts.

10. Research and supply the names of the five (5) largest Cloud Providers in the industry today (by percentage market share), along with their respective offerings. (10 points).

Answer: The five largest cloud service providers by global market share are:

i. Amazon Web Services (AWS) - 30% market share
   - AWS Provides a comprehensive suite of cloud services including computing power, storage solutions and database.

ii. Microsoft Azure - 21% market share
   - Azure provides a wide range of cloud services, such as virtual machines, AI capabilities, and analytics.

iii. Google Cloud Platform (GCP) - 12% market share
   - GCP offers services like data storage, machine learning tools, and application development platforms.

iv. Alibaba Cloud - 4% market share
   - Alibaba Cloud delivers services including elastic computing, data storage, and large-scale computing.

v. IBM Cloud - Market share not specified, but consistently in the top 5

- IBM Cloud provides services including IaaS, PaaS, and SaaS, with a focus on AI, blockchain, and IoT solutions.

These providers dominate the cloud computing industry, offering diverse services that cater to various business needs worldwide.

11. What are some common cloud security threats, and how can they be mitigated? (5 points)

Answer: Some common cloud security threats and their mitigation strategies include:

Data Breaches:

- Threat: Unauthorized access to sensitive data due to poor security controls.
- Mitigation: Use strong encryption for data at rest and in transit, along with strict access controls and multi-factor authentication (MFA).

Account Hijacking:

- Threat: Cybercriminals can gain control over user accounts through phishing or weak passwords.
- Mitigation: Use strong password policies, enforce MFA, and monitor account activity for unusual behavior.

Denial of Service (DoS) Attacks:

- Threat: Attackers flood the system with traffic, making services unavailable to legitimate users.
- Mitigation: Use firewalls, traffic monitoring tools, and cloud-based load balancing to detect and mitigate such attacks.

Data Loss:

- Threat: Accidental deletion, hardware failure, or corruption of data by users or cyberattacks can lead to data loss.
- Mitigation: Regularly back up data and use automated recovery solutions such as snapshots and apply version control to important files.

Insecure APIs:

- Threat: Weak or improperly secured APIs can be exploited to gain unauthorized access.
- Mitigation: Secure APIs with authentication, input validation, and regular security testing.

These mitigation strategies help organizations protect their data, maintain service availability, and ensure the integrity of their cloud systems.

12. What is multi-cloud, and what are its advantages and challenges? (10 points)

Answer: Multi-cloud refers to the use of cloud services from multiple cloud providers. Here are some advantages and challenges:

Multi-Cloud: Multi-cloud refers to the use of cloud services from two or more different providers simultaneously. This strategy allows organizations to leverage the strengths of various cloud providers to optimize performance, cost, and redundancy.

Advantages:

- Avoids Vendor Lock-In: Reduces dependence on a single provider.
- Flexibility: Organizations can choose best-in-class services from different providers.
- Cost Efficiency: Organizations can optimize costs by selecting the most cost-effective service for each specific need.
- Optimized Performance: Allows businesses to choose the best services from different providers based on workload requirements, improving overall performance.
- Increased Resilience: Spreading workloads across

13. What are the key considerations for migrating applications to the cloud? (5 points)

Answer: The key considerations for migrating applications to the cloud are:

- Evaluate your application ecosystem to understand how compatibility issues might affect performance and reliability after migration.
- Understand legal and regulatory compliance standards relevant to your industry, and ensure the chosen cloud provider meets those obligations.
- Carefully evaluate short-term and long-term costs, understanding that initial migration may incur additional expenses before realizing long-term savings.
- Establish clear performance benchmarks before migration to provide a basis for comparison post-migration.
- Implement backup and disaster recovery plans to ensure high availability and business continuity during and after migration.
- Consider the potential challenges of being tied to a single vendor and explore multi-cloud or hybrid solutions if necessary.

14. What are the security challenges of cloud computing, and how can they be addressed? (9 points)

Answer: Cloud computing introduces several security challenges due to its shared infrastructure, multi-tenancy, and remote accessibility. Below are the major challenges and strategies to mitigate are:

Data Breaches: Unauthorized access to sensitive data stored in the cloud.

Solution: Implement strong encryption for data at rest and in transit and use multi-factor authentication (MFA) and robust access controls.

Data Loss: Accidental deletion, malicious attacks, or system failures can lead to permanent data loss.

Solution: Perform regular backups, use automated recovery tools, and configure disaster recovery solutions to ensure data availability.

Denial of Service (DoS) Attacks: Attackers may overwhelm cloud resources, making services unavailable to legitimate users.

Solution: Use advanced firewalls, load balancers, and traffic filtering to mitigate these attacks.

Insecure APIs: Vulnerabilities in APIs can lead to unauthorized access or data leaks.

Solution: Implement secure coding practices, validate input data, and enforce proper authentication and authorization on all APIs.

Account Hijacking: Attackers may gain control over cloud user accounts, leading to unauthorized access and misuse.

Solution: Use strong passwords, enable MFA, and continuously monitor accounts for suspicious activity.

Insider Threats: Malicious actions or negligence by employees.

Solution: Enforce strict access controls, conduct regular audits, and implement user activity monitoring.

Lack of Compliance: Organizations must ensure they meet various legal and regulatory requirements depending on their industry and region.

Solution: Regular compliance audits and use cloud providers that meet industry standards and certifications.

Shared Technology Vulnerabilities: Vulnerabilities in shared infrastructure could allow attackers to compromise other tenants' environments.

Solution: Regularly patch shared resources, use robust isolation techniques, and employ continuous vulnerability scanning.

Limited Visibility and Control: Lack of direct control over cloud infrastructure.

Solution: Use comprehensive monitoring tools. Employ cloud access security brokers (CASBs) for better visibility and control.