SECTION A

Very Short Answer Questions

Attempt all seven (7) questions [2 × 7 = 14]

**A. Enlist any two characteristics of cloud computing.**

1. **On-Demand Self-Service:** Users can provision computing resources such as server time and network storage automatically without requiring human interaction with each service provider.
2. **Broad Network Access:** Cloud services are available over the network and can be accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and workstations).

**B. State any two benefits of a Virtual Data Centre.**

1. **Cost Efficiency:** Virtual Data Centres reduce the need for physical hardware and associated maintenance costs, leading to significant cost savings.
2. **Scalability:** Virtual Data Centres can easily scale resources up or down based on demand, providing flexibility for growing businesses.

**C. Give any two types of SLA.**

1. **Service-Based SLA:** A single SLA that covers all customers using a particular service.
2. **Customer-Based SLA:** An SLA specific to an individual customer covering all the services they use.

**D. State any two features of open source cloud Eucalyptus.**

1. **Hybrid Cloud Support:** Eucalyptus enables users to create private, hybrid, or public clouds that can integrate with AWS, offering the flexibility of deployment.
2. **High Compatibility with AWS:** Eucalyptus supports AWS-compatible services, making it easy to migrate or integrate applications with AWS cloud services.

**E. Differentiate between Public cloud and Private cloud. (Any two points)**

1. **Ownership:** Public clouds are owned and operated by third-party cloud service providers, whereas private clouds are owned and managed by the organization itself.
2. **Security:** Private clouds offer more control over security as they are hosted on private infrastructure, whereas public clouds share resources among multiple tenants, which may pose security risks.

**F. Define VSAN.**

* **Virtual Storage Area Network (VSAN):** A VSAN is a logical partition in a physical storage area network, enabling multiple storage networks to share the same physical resources while maintaining isolation and security.

**G. State any two uses of a Cloud portal.**

1. **Centralized Management:** A cloud portal allows users to manage and monitor their cloud resources, such as virtual machines, storage, and applications, from a single interface.
2. **Self-Service Provisioning:** Users can provision and manage cloud services and resources independently through the cloud portal, reducing the need for IT support.

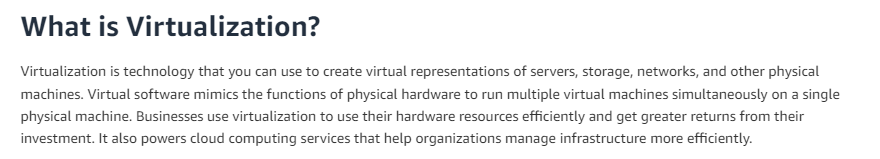
SECTION B

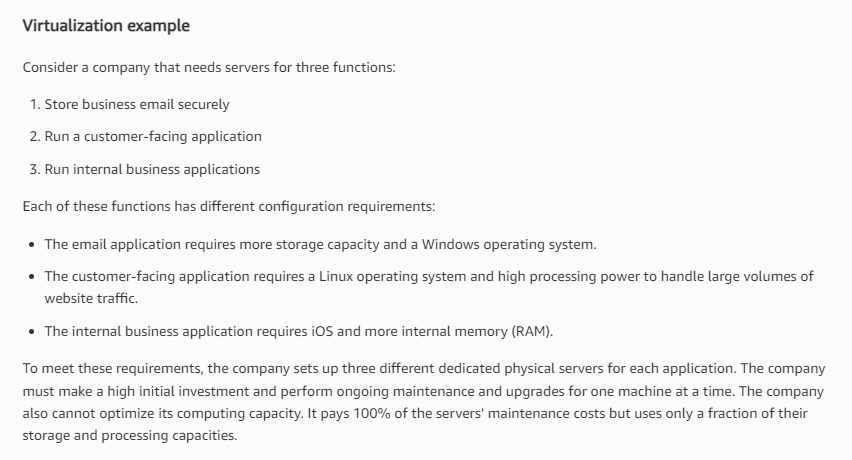
Short Answer Questions

Attempt only seven (7) questions out of eight (9) questions [7 × 8 = 56]

Q. 1   Short Answer Question (Chapter 1: Introduction)

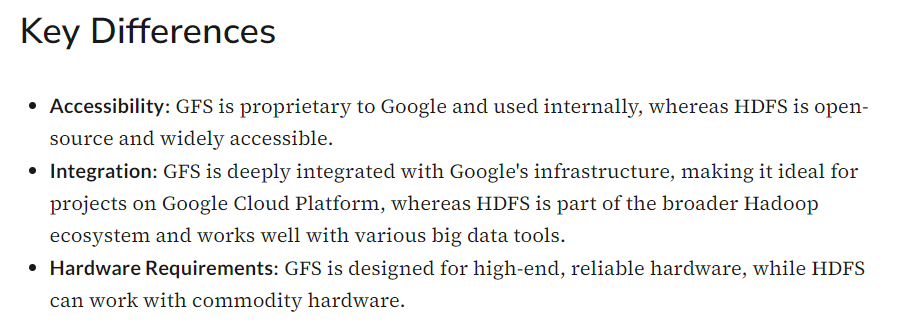
What is virtualization? Provide one real-world example where virtualization is applied.

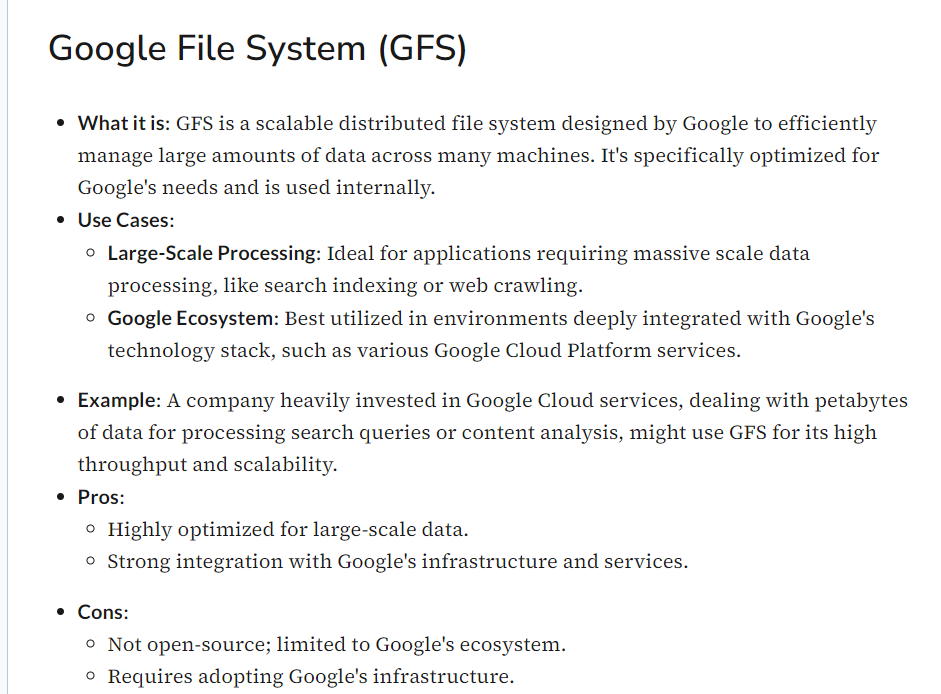


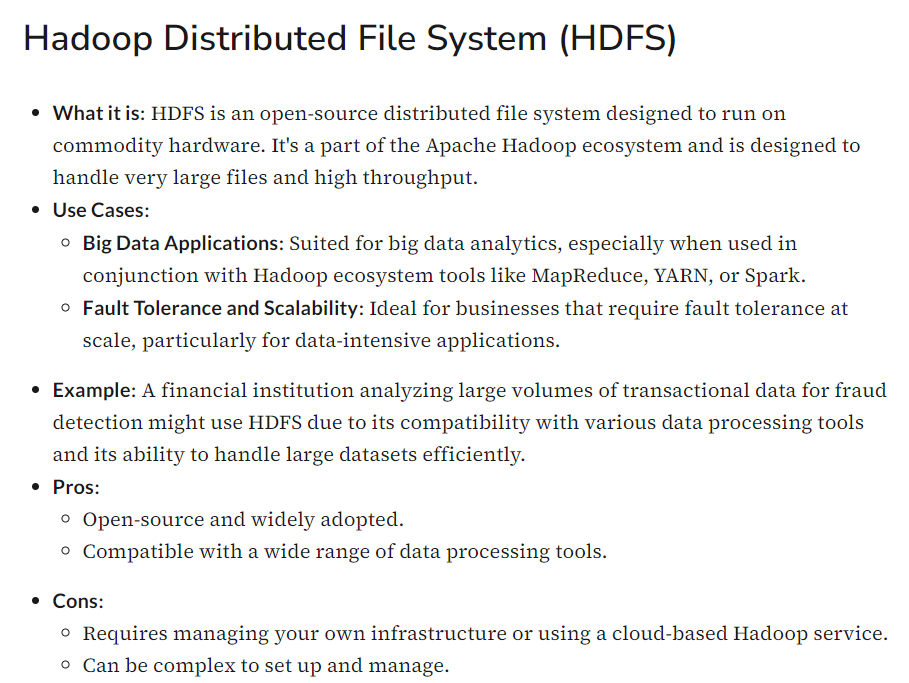


Q. 2   Short Answer Question (Chapter 4: Cloud Service Administration)

Compare and contrast the Google File System (GFS) and the Hadoop Distributed File System (HDFS).



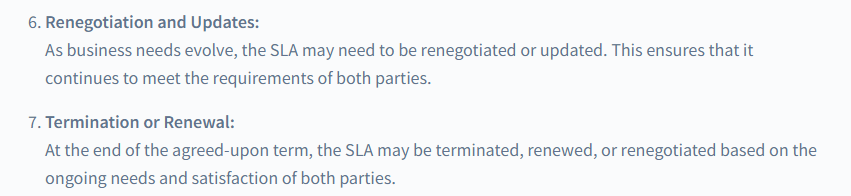




Q. 3   Short Answer Question (Chapter 4: Cloud Service Administration)

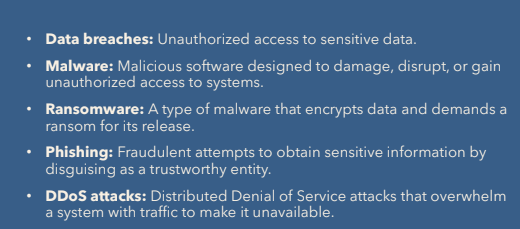
Outline the life cycle stages of a Service Level Agreement (SLA) in cloud computing.

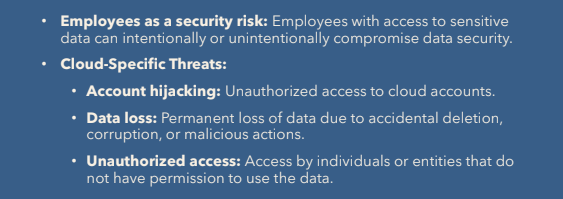


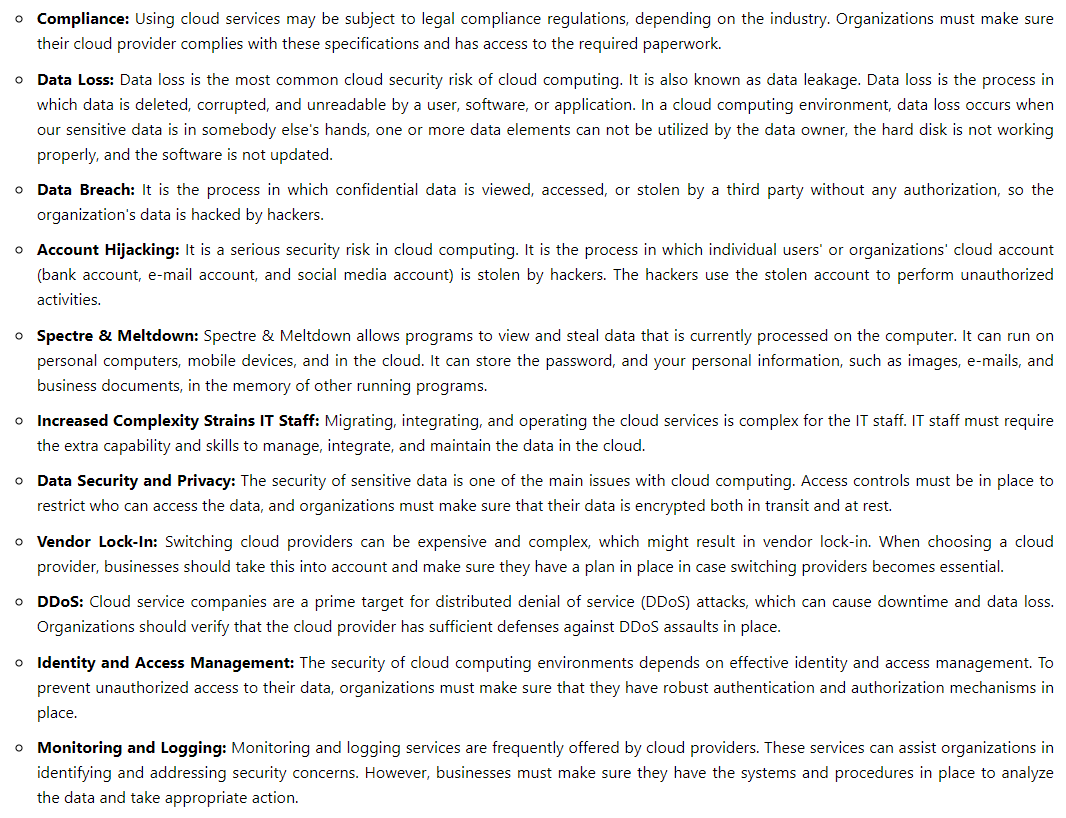


Q. 4   Short Answer Question (Chapter 7: Data Management)

Identify and explain the key risks associated with cloud computing.







Q. 5   Short Answer Question (Chapter 2: Business Values, Introduction)

Discuss the characteristics of different Cloud Service Models (e.g., IaaS, PaaS, SaaS).

Cloud computing offers various service models to cater to different business needs. The primary models are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Each model has distinct characteristics that make it suitable for specific types of applications and use cases.

**1. Infrastructure as a Service (IaaS)**

**Characteristics:**

* **Virtualized Computing Resources**: IaaS provides virtualized computing resources over the internet, including virtual machines (VMs), storage, and networks. Users can scale these resources up or down as needed.
* **User-Controlled Infrastructure**: Users have full control over the operating system, storage, and installed applications. They can configure and manage the underlying hardware according to their requirements.
* **Pay-As-You-Go Pricing**: IaaS typically follows a pay-as-you-go pricing model, where users are charged based on the resources they consume, such as compute power, storage, and network bandwidth.
* **High Flexibility**: IaaS offers a high level of flexibility, allowing users to choose the specific configurations of their virtual machines and other infrastructure components.
* **Automation and Orchestration**: IaaS platforms often provide tools for automating the deployment and management of infrastructure, including auto-scaling, load balancing, and backup services.

**Examples:**

* Amazon Web Services (AWS) EC2
* Microsoft Azure Virtual Machines
* Google Compute Engine (GCE)

**2. Platform as a Service (PaaS)**

**Characteristics:**

* **Development and Deployment Platform**: PaaS provides a platform that includes operating systems, databases, web servers, and development tools, allowing developers to build, deploy, and manage applications without worrying about the underlying infrastructure.
* **Abstracted Infrastructure Management**: Users do not manage the underlying hardware or operating systems. Instead, they focus on developing and deploying their applications.
* **Integrated Development Environment (IDE)**: PaaS platforms often come with integrated development environments (IDEs) and APIs that simplify the application development process.
* **Scalability and Flexibility**: PaaS platforms automatically scale the infrastructure based on application demand, allowing developers to focus on coding rather than infrastructure management.
* **Supports Multiple Programming Languages**: PaaS supports multiple programming languages, frameworks, and libraries, enabling developers to choose the best tools for their applications.

**Examples:**

* Google App Engine
* Microsoft Azure App Service
* Heroku

**3. Software as a Service (SaaS)**

**Characteristics:**

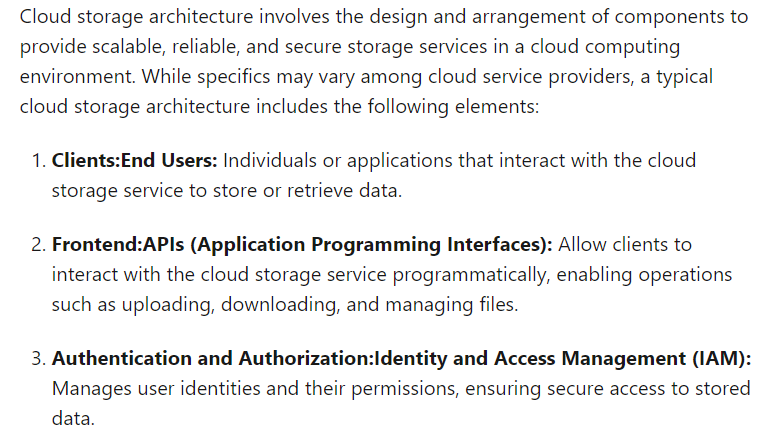
* **Fully Managed Software**: SaaS provides fully managed software applications over the internet, eliminating the need for users to install, manage, or update the software. Everything is handled by the service provider.
* **Subscription-Based Model**: SaaS is usually offered on a subscription basis, where users pay a recurring fee to access the software. The subscription often includes maintenance, updates, and support.
* **Accessibility and Multi-Tenancy**: SaaS applications are accessible via web browsers, making them platform-independent. They are typically multi-tenant, meaning multiple users or organizations share the same application instance while keeping their data isolated.
* **Automatic Updates**: The service provider handles all software updates and security patches, ensuring that users always have access to the latest version of the software without any manual intervention.
* **Collaboration and Integration**: SaaS applications often come with collaboration features and can integrate with other SaaS or on-premises applications, enhancing productivity and workflow efficiency.

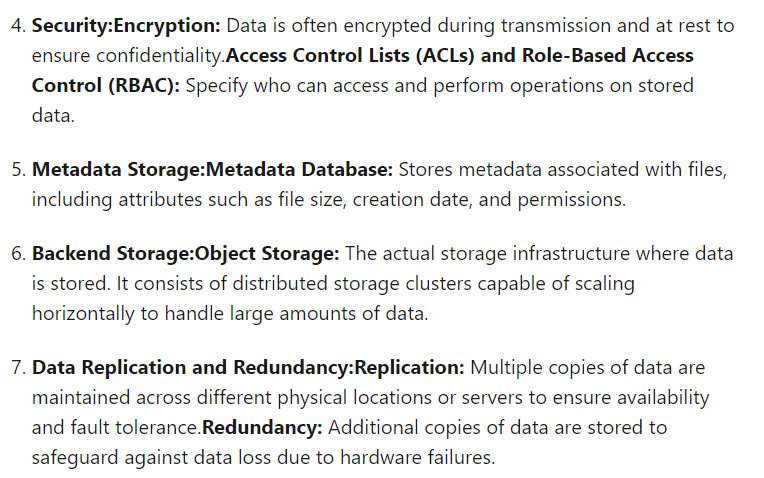
**Examples:**

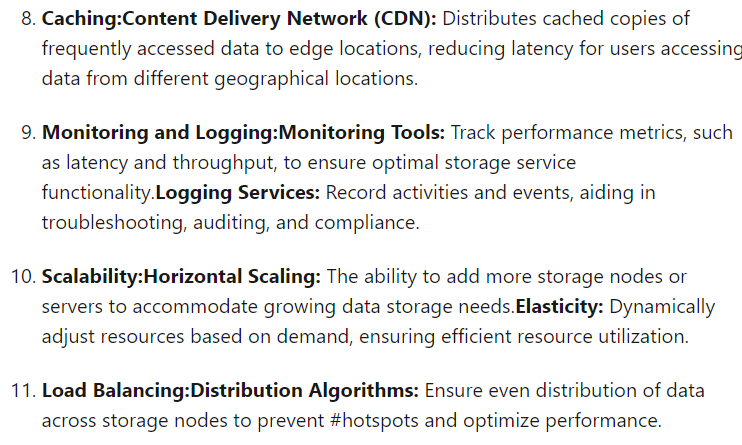
* Google Workspace (formerly G Suite)
* Microsoft 365
* Salesforce

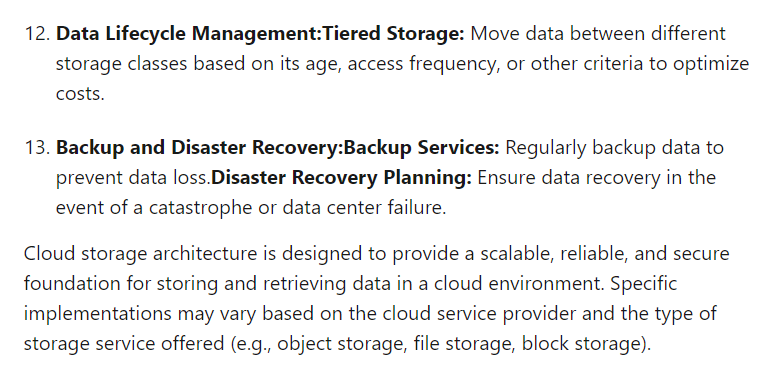
Q. 6   Short Answer Question (Chapter 8: Information Storage In Cloud Computing)

Explain the architecture of a storage system in cloud computing.



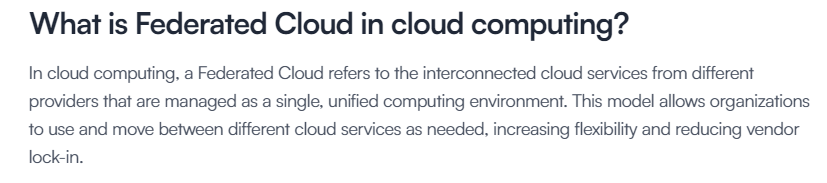


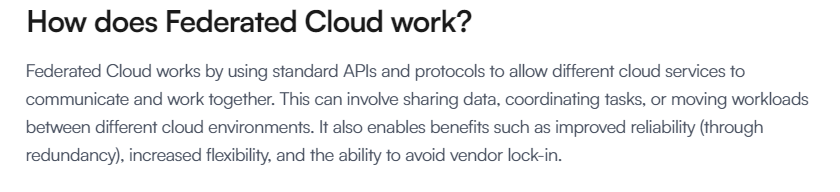


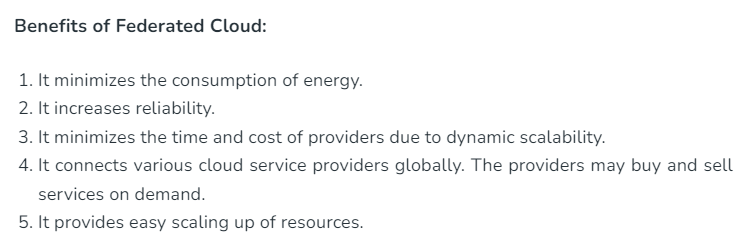


Q.7 Short Answer Question (Chapter 9: Discovery of Private &amp; Hybrid Clouds)

Describe the concept of federated cloud computing and its benefits.

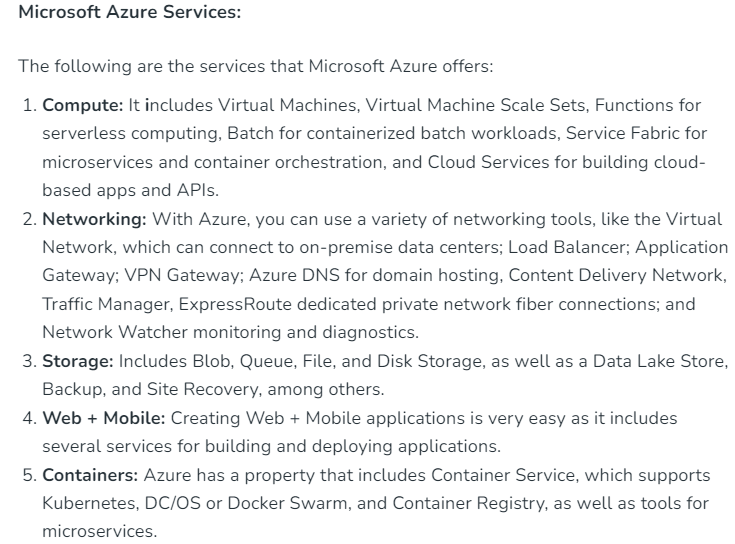


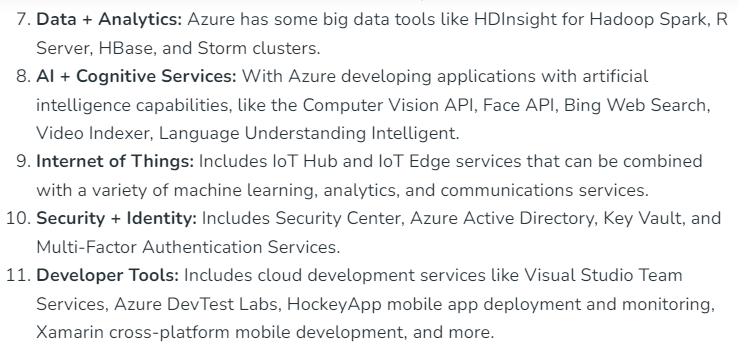




Q. 8   Short Answer Question (Chapter 5: Cloud Computing Technology)

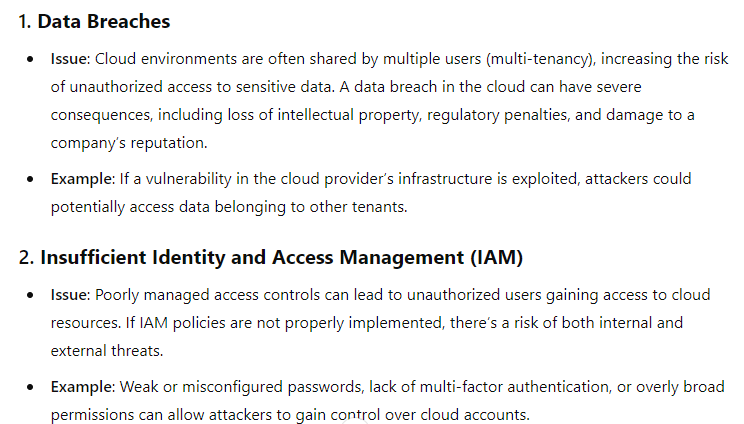
Explain the architecture and functioning of Microsoft Azure with the help of a diagram.

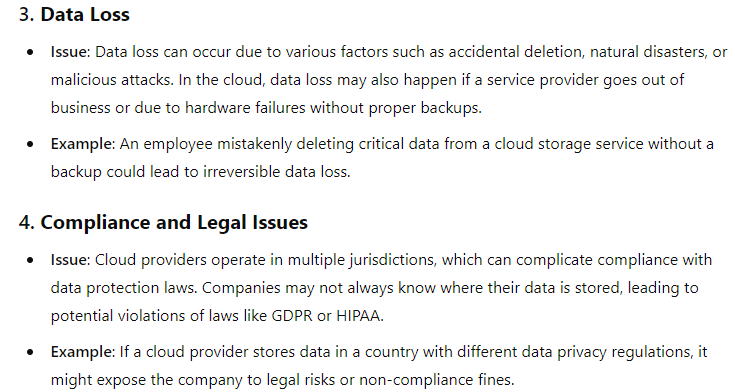


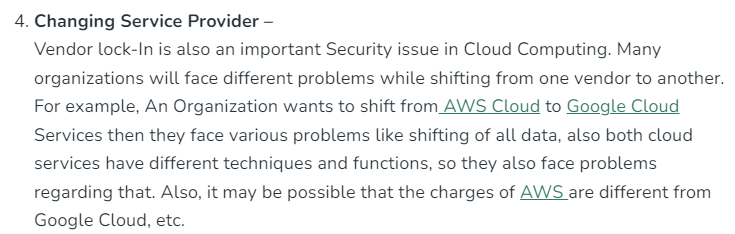


Q. 9   Short Answer Question (Chapter 10: Cloud Computing Standards)

Discuss general security issues in cloud computing, providing at least four examples.







Group C

Long Analytical or Case Question

Attempt any two (2) questions out of three (3) questions [2 × 15 = 30]

Q. 1 Long or Analytical Answer Question (Chapter 6: Accessing &amp; The Cloud Chapter 8: Information Storage in Cloud Computing)

An Enterprise Enhancing Cloud Security and Storage

A. The enterprise is assessing security risks in their cloud system. Discuss the types of analysis required and identify the challenging areas.

B. They are considering storage zones with encryption keys to protect cloud storage. Explain this approach with diagrams.

C. C) The enterprise needs to manage identities in the cloud. Discuss the reasons and methods for identity management. (5 + 5 + 5)

**A. Assessing Security Risks in Cloud Systems**

When an enterprise is assessing security risks in their cloud system, the following types of analysis are required:

**1. Threat Analysis:**

* **Purpose**: Identify potential threats that could exploit vulnerabilities in the cloud environment.
* **Focus**: Includes threats such as unauthorized access, data breaches, insider threats, and Distributed Denial of Service (DDoS) attacks.
* **Challenging Area**: The dynamic nature of cloud environments and the need to account for both internal and external threats make threat analysis complex.

**2. Vulnerability Analysis:**

* **Purpose**: Identify weaknesses in the cloud infrastructure, applications, and services that could be exploited.
* **Focus**: Assess software vulnerabilities, misconfigurations, inadequate encryption, and unpatched systems.
* **Challenging Area**: Ensuring all vulnerabilities are identified across a distributed and often opaque cloud environment can be difficult.

**3. Compliance Analysis:**

* **Purpose**: Ensure that the cloud system adheres to industry regulations and standards such as GDPR, HIPAA, and PCI-DSS.
* **Focus**: Analyze data handling, storage, and processing practices to ensure they meet legal requirements.
* **Challenging Area**: Different jurisdictions may have conflicting regulations, making global compliance a significant challenge.

**4. Risk Assessment:**

* **Purpose**: Evaluate the potential impact and likelihood of identified risks materializing.
* **Focus**: Includes assessing the business impact of data breaches, downtime, and legal consequences.
* **Challenging Area**: Quantifying the risk impact, especially for intangible assets like reputation, and prioritizing which risks to mitigate first.

**5. Penetration Testing:**

* **Purpose**: Simulate cyberattacks to test the effectiveness of security measures.
* **Focus**: Identify weaknesses that might not be apparent through other analyses.
* **Challenging Area**: Ensuring that tests are comprehensive and do not disrupt live services.

**B. Storage Zones with Encryption Keys**

**Approach Explanation:**

* **Storage Zones**: In cloud storage, data is often divided into different zones or regions, which are physical or logical divisions used to store and manage data. These zones can be set up to isolate data based on its sensitivity or regulatory requirements.
* **Encryption Keys**: Data stored in each zone is encrypted using unique encryption keys. Encryption transforms data into a format that can only be read or decrypted by someone who has the corresponding key.
* **How It Works**:
  + **Data Segmentation**: Data is first classified and segmented based on its sensitivity and then stored in designated zones.
  + **Encryption**: Before being stored, the data is encrypted using encryption keys specific to each storage zone.
  + **Key Management**: The encryption keys are securely managed and rotated regularly to minimize the risk of key compromise.

**Diagram Explanation:**

* **Diagram Overview**: The diagram should illustrate multiple storage zones (Zone A, Zone B, Zone C), each with its own encryption keys (Key A, Key B, Key C). Data enters a zone, gets encrypted, and is stored securely.
* **Flow**: Data -> Segmentation -> Encryption -> Storage Zone -> Retrieval (Decryption with the correct key).

This approach ensures that even if data in one zone is compromised, it cannot be decrypted without the specific key, adding a robust layer of security.

**C. Identity Management in the Cloud**

**Reasons for Identity Management:**

1. **Access Control**: To ensure that only authorized users can access cloud resources, thereby protecting sensitive data and applications.
2. **Compliance**: To meet regulatory requirements for data protection and user privacy by controlling and auditing access to cloud systems.
3. **Scalability**: To efficiently manage access across a growing number of users, devices, and services as the enterprise scales its cloud operations.
4. **User Experience**: To provide seamless access to cloud services through single sign-on (SSO) and unified identity management, improving productivity.
5. **Security**: To prevent unauthorized access and potential breaches by enforcing strong authentication and authorization mechanisms.

**Methods for Identity Management:**

1. **Single Sign-On (SSO)**:
   * **Explanation**: Allows users to log in once and gain access to multiple applications without re-authenticating.
   * **Benefit**: Simplifies the user experience and reduces the risk of password fatigue.
2. **Multi-Factor Authentication (MFA)**:
   * **Explanation**: Requires users to provide two or more verification factors to gain access.
   * **Benefit**: Adds an extra layer of security, making it harder for attackers to gain unauthorized access.
3. **Role-Based Access Control (RBAC)**:
   * **Explanation**: Users are granted access based on their roles within the organization.
   * **Benefit**: Ensures users only have access to the resources necessary for their job, minimizing potential damage from a compromised account.
4. **Identity Federation**:
   * **Explanation**: Links multiple identity management systems across different domains, allowing users to authenticate using their credentials from one domain to access resources in another.
   * **Benefit**: Facilitates collaboration and access control across multiple cloud services and platforms.
5. **Identity and Access Management (IAM) Tools**:
   * **Explanation**: Use of IAM platforms (e.g., Azure AD, AWS IAM) to manage identities, policies, and access controls centrally.
   * **Benefit**: Provides a unified and scalable solution for managing identities across diverse cloud environments.

Q. 2 Long or Analytical Answer Question (Chapter 3: Cloud Computing Technology &amp; Chapter 2: Business Values, Introduction)

A. Discuss Identity as a Service (IDaaS) in detail. Explain its components and benefits.

B. Explain the concepts of Workloads, Pods, and Silos in cloud environments.

C. Discuss open SaaS and explain the role of Mashups in creating composite applications. (5 + 5 + 5)

**A. Discuss Identity as a Service (IDaaS) in Detail**

**Identity as a Service (IDaaS)** is a cloud-based service that provides identity and access management (IAM) functionalities. It enables organizations to manage user identities and control access to applications and resources across various environments, including on-premises and cloud-based services.

**Components of IDaaS:**

1. **User Authentication**:
   * **Explanation**: Verifies the identity of users before granting access to resources.
   * **Methods**: Typically involves multi-factor authentication (MFA), single sign-on (SSO), and password management.
2. **Single Sign-On (SSO)**:
   * **Explanation**: Allows users to authenticate once and gain access to multiple applications without needing to log in again.
   * **Benefit**: Simplifies the login process, enhances user experience, and reduces the need for multiple passwords.
3. **Access Control**:
   * **Explanation**: Manages permissions and enforces policies that determine what resources a user can access.
   * **Types**: Includes role-based access control (RBAC) and attribute-based access control (ABAC).
4. **User Provisioning and De-provisioning**:
   * **Explanation**: Automates the creation, management, and removal of user accounts and access permissions.
   * **Benefit**: Ensures that users have the appropriate access when they join or leave an organization.
5. **Federated Identity Management**:
   * **Explanation**: Links multiple identity management systems across different organizations or domains.
   * **Benefit**: Allows users to use their credentials from one domain (e.g., corporate login) to access resources in another domain (e.g., partner systems).
6. **Directory Services**:
   * **Explanation**: Stores and manages user information, credentials, and access rights.
   * **Integration**: IDaaS often integrates with on-premises directory services like Active Directory (AD) or LDAP.
7. **Reporting and Analytics**:
   * **Explanation**: Provides insights into identity-related activities, access patterns, and potential security risks.
   * **Benefit**: Helps in auditing, compliance, and detecting suspicious activities.

**Benefits of IDaaS:**

1. **Enhanced Security**:
   * **Explanation**: By implementing MFA, SSO, and strong access controls, IDaaS reduces the risk of unauthorized access and potential breaches.
2. **Cost Efficiency**:
   * **Explanation**: IDaaS eliminates the need for expensive on-premises IAM infrastructure, leading to reduced costs in hardware, software, and maintenance.
3. **Scalability**:
   * **Explanation**: IDaaS can easily scale to accommodate growing numbers of users, devices, and applications, making it suitable for organizations of any size.
4. **Improved User Experience**:
   * **Explanation**: SSO and streamlined access control improve the user experience by reducing the need for multiple logins and passwords.
5. **Compliance and Auditability**:
   * **Explanation**: IDaaS offers detailed reporting and monitoring capabilities, which help organizations comply with regulatory requirements and perform audits.

**B. Explain the Concepts of Workloads, Pods, and Silos in Cloud Environments**

**Workloads:**

* **Explanation**: A workload in cloud computing refers to the processing or computing tasks that an application or service must perform. Workloads can range from simple tasks, like serving a static web page, to complex operations, like processing large datasets or running machine learning algorithms.
* **Types**: Workloads can be categorized into compute-intensive, memory-intensive, storage-intensive, or network-intensive workloads.
* **Significance**: Managing and optimizing workloads is crucial for ensuring efficiency, performance, and cost-effectiveness in a cloud environment.

**Pods:**

* **Explanation**: In cloud-native environments, particularly with container orchestration platforms like Kubernetes, a pod is the smallest deployable unit. A pod encapsulates one or more containers, along with shared storage, network, and specifications on how to run them.
* **Function**: Pods enable better resource utilization and scaling by packaging multiple containers that need to work together. They can be easily scaled up or down based on demand.
* **Significance**: Pods provide a modular and efficient way to manage workloads in a microservices architecture, enhancing agility and scalability.

**Silos:**

* **Explanation**: In the context of cloud environments, silos refer to isolated units or departments within an organization that operate independently with little to no collaboration or information sharing with other units. In a cloud context, it could also refer to isolated cloud environments or services that don’t integrate well with others.
* **Challenges**: Silos can lead to inefficiencies, as they prevent seamless data and resource sharing, leading to duplicated efforts and inconsistent practices across the organization.
* **Overcoming Silos**: Modern cloud strategies encourage breaking down silos through integrated services, shared data platforms, and cross-functional teams.

**C. Discuss Open SaaS and Explain the Role of Mashups in Creating Composite Applications**

**Open SaaS:**

* **Explanation**: Open SaaS (Software as a Service) refers to SaaS applications that are based on open-source software. Open SaaS solutions provide the benefits of traditional SaaS—such as accessibility, scalability, and reduced infrastructure management—while allowing users to modify, extend, or integrate the software with other tools due to its open-source nature.
* **Advantages**: Open SaaS offers more flexibility, customization, and control over the software, which can be tailored to fit specific business needs. It also fosters a collaborative development environment where users can contribute to the software’s improvement.

**Mashups:**

* **Explanation**: A mashup in the context of cloud computing and SaaS refers to a web application that integrates data, APIs, or functionalities from multiple sources into a single, unified application. Mashups enable the creation of composite applications that leverage the strengths of various services or platforms.
* **Example**: A simple example of a mashup could be a web application that combines mapping data from Google Maps with real-time traffic data from a different service to create a traffic monitoring tool.
* **Role in Composite Applications**:
  + **Integration**: Mashups play a critical role in composite applications by allowing different services to be combined and presented as a single cohesive solution.
  + **Flexibility**: They enable businesses to quickly adapt to changing requirements by integrating new services or replacing outdated ones without overhauling the entire application.
  + **Innovation**: By leveraging existing services, mashups facilitate innovation and reduce development time, as they avoid the need to build every component from scratch.

Q. 3 Long or Analytical Answer Question (Chapter 9: Discovery of Private &amp; Hybrid Clouds)

Design a Virtual Data Centre. Identify the key elements needed and provide a block diagram to

illustrate your design. (15)

Designing a Virtual Data Centre (VDC) involves understanding the components and architecture necessary to create a scalable, secure, and efficient environment for hosting IT resources. A Virtual Data Centre is a collection of virtualized resources, including compute, storage, and networking, that are abstracted and managed as a cohesive unit.

**Key Elements Needed for a Virtual Data Centre**

1. **Compute Resources**:
   * **Virtual Machines (VMs)**: VMs are the primary compute units in a VDC. Each VM runs its own operating system and applications, isolated from other VMs.
   * **Hypervisor**: The hypervisor is the virtualization layer that allows multiple VMs to run on a single physical server. It manages resource allocation and VM isolation.
2. **Storage Resources**:
   * **Virtual Storage**: Virtual storage pools, such as Storage Area Networks (SAN) or Network Attached Storage (NAS), provide storage for VMs and applications.
   * **Data Management Tools**: These tools handle data replication, backup, and recovery, ensuring data availability and integrity.
3. **Networking Resources**:
   * **Virtual Network**: A virtual network includes virtual switches, routers, and firewalls that manage communication between VMs, both within the VDC and with external networks.
   * **Software-Defined Networking (SDN)**: SDN decouples the network control plane from the data plane, allowing centralized management of network traffic, policies, and configurations.
4. **Management and Orchestration**:
   * **Cloud Management Platform (CMP)**: The CMP provides a unified interface for managing and orchestrating VDC resources. It includes tools for provisioning, monitoring, and automating resource management.
   * **Resource Orchestration**: This component ensures optimal allocation of compute, storage, and network resources based on workloads, policies, and service level agreements (SLAs).
5. **Security**:
   * **Virtual Firewalls**: These are used to secure network traffic within the VDC and between the VDC and external networks.
   * **Identity and Access Management (IAM)**: IAM controls user access to VDC resources, ensuring that only authorized personnel can access sensitive data and systems.
   * **Encryption**: Data at rest and in transit are encrypted to protect against unauthorized access and breaches.
6. **Scalability and Load Balancing**:
   * **Auto-Scaling**: Automatically adjusts resource allocation (e.g., adding or removing VMs) based on demand, ensuring optimal performance and cost-efficiency.
   * **Load Balancers**: Distribute workloads across multiple VMs to ensure availability and performance.
7. **Monitoring and Analytics**:
   * **Performance Monitoring**: Tools that track the health and performance of VDC resources, including CPU, memory, storage, and network usage.
   * **Analytics**: Provides insights into resource usage, capacity planning, and potential bottlenecks, enabling proactive management.
8. **Backup and Disaster Recovery**:
   * **Backup Solutions**: Regular backups of VMs and data to prevent data loss.
   * **Disaster Recovery (DR)**: Strategies and systems to restore operations in case of catastrophic failure, including failover to secondary data centers.

**Block Diagram of a Virtual Data Centre**

Below is a description of how you can conceptualize the block diagram for a Virtual Data Centre:

* **Central Management Layer**:
  + Cloud Management Platform (CMP)
  + Resource Orchestration
* **Compute Layer**:
  + Hypervisors
  + Virtual Machines (VMs)
* **Storage Layer**:
  + Virtual Storage (SAN/NAS)
  + Data Management Tools
* **Networking Layer**:
  + Virtual Network (Switches, Routers)
  + Software-Defined Networking (SDN)
* **Security Layer**:
  + Virtual Firewalls
  + IAM (Identity and Access Management)
  + Encryption
* **Scalability Layer**:
  + Auto-Scaling
  + Load Balancers
* **Monitoring and Analytics Layer**:
  + Performance Monitoring
  + Analytics Tools
* **Backup and Disaster Recovery Layer**:
  + Backup Solutions
  + Disaster Recovery (DR)