Ch-1 Introduction

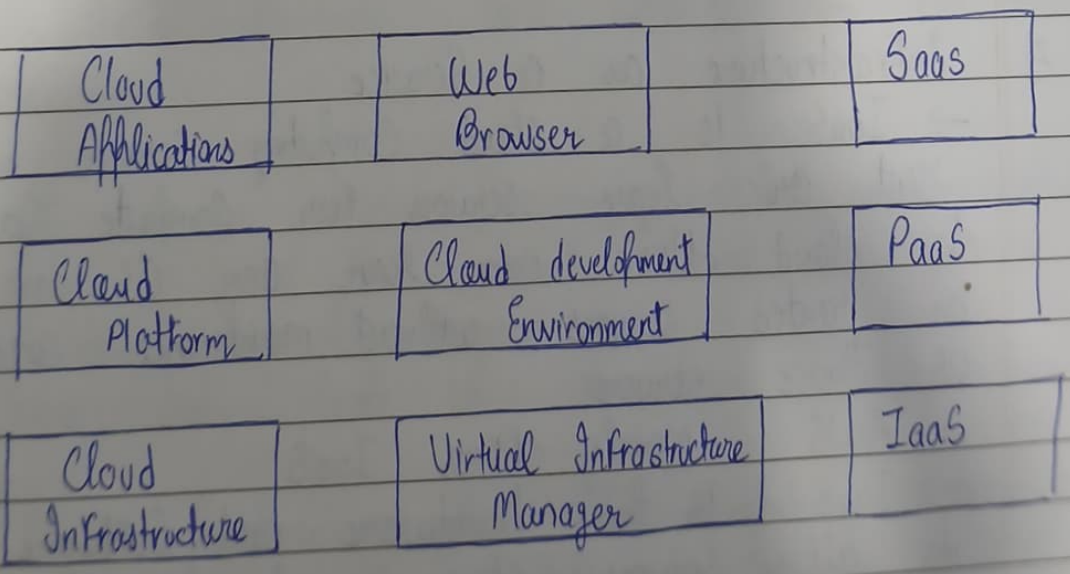
Q-1 Define the term cloud computing ?

Ans → Cloud Computing is a technology that allows you to store and access data and applications over the Internet instead of using your computer's hard drive or local server

→ Cloud Computing refers to applications and services that run on a distributed network using virtualized resources and accessed by common Internet protocols and networking standards.

Q-2 Explain the cloud computing stack ?

Ans



→ Cloud services are designed to provide easy, scalable access to applications, resources and services and are fully managed by a cloud services provider.
→ Cloud Computing, often described as stack, has a broad range of services built on top of one another under the name cloud

1) Software as a Service
→ SaaS utilizes the internet to deliver applications, which are managed by a third party vendor, to its users.
→ A majority of SaaS applications run directly through your web browser, which means they do not require any downloads or installations on the client side
→ Salesforce.com uses SaaS model. SaaS applications are designed for end-users, delivered over the web

2) Infrastructure as a Service
→ IaaS is a cloud computing service where enterprises rent or lease servers for compute and storage in the cloud. Users can run any OS or applications on rented servers without maintenance and operating costs of those servers.
→ AWS mainly offers IaaS
→ IaaS is the hardware and software that powers it all - servers, storage, networks, operating systems

3) Platform as a Service
→ PaaS, provide cloud components to certain software while being used mainly for applications.

→ PaaS delivers a framework for developers that they can build upon and use to create customized applications

→ All servers, storage, and networking can be managed by the enterprise or a third-party provider while the developers can maintain the management of the applications

→ Google AppEngine, an example of Platform as a Service

→ PaaS is the set of tools and services designed to make coding and deploying those applications quick and efficient.

Q-3 What do you understand by Utility Computing?

Ans Utility Computing, as name suggests, is a type of computing that combine/provide resources to users on their demands and charge them for specific usage.

→ It is a service-provisioning model where computing resources (storage, CPU, network, software) are offered like a metered service

→ Users can scale up or down based on their needs

→ Main purpose is to make computing resources and infrastructure management available to customer as per their need, and charge them for specific usage rather than flate rate

→ Its characteristics include, scalability, demand pricing, standardized utility computing services, automation, etc.

Examples

1) AWS For Hosting

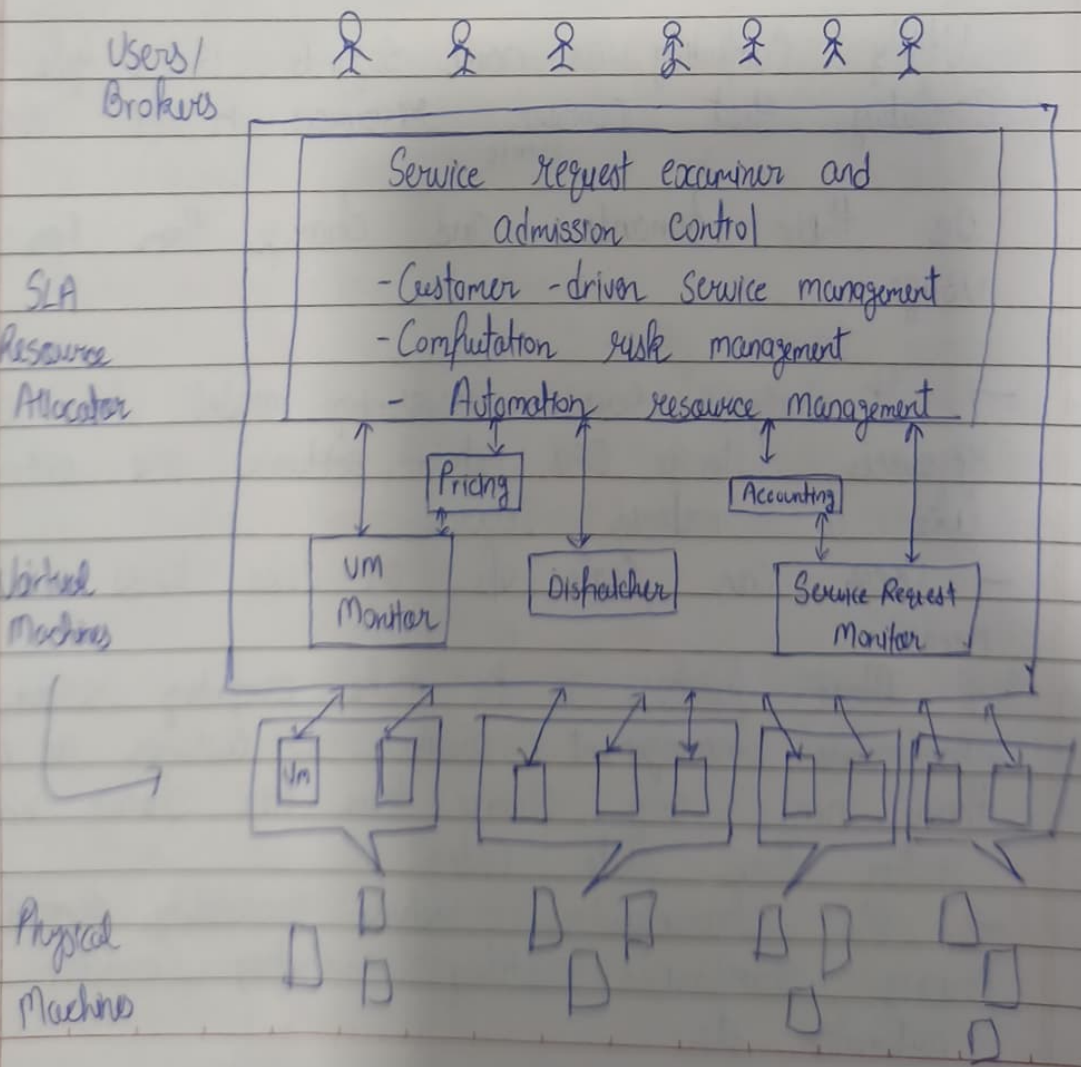
2) Microsoft Azure for Machine Learning

3) Google Cloud Platform For Data Storage and Backup.

→ It allows organization to allocate and segregate computing resources and infrastructure to various users on basis of their requirements.

Q-4 Discuss Cloud Computing Architecture

Ans



1.1.2 Cloud Computing Architecture

- Fig. 1.1.4 shows architectural framework of cloud computing.

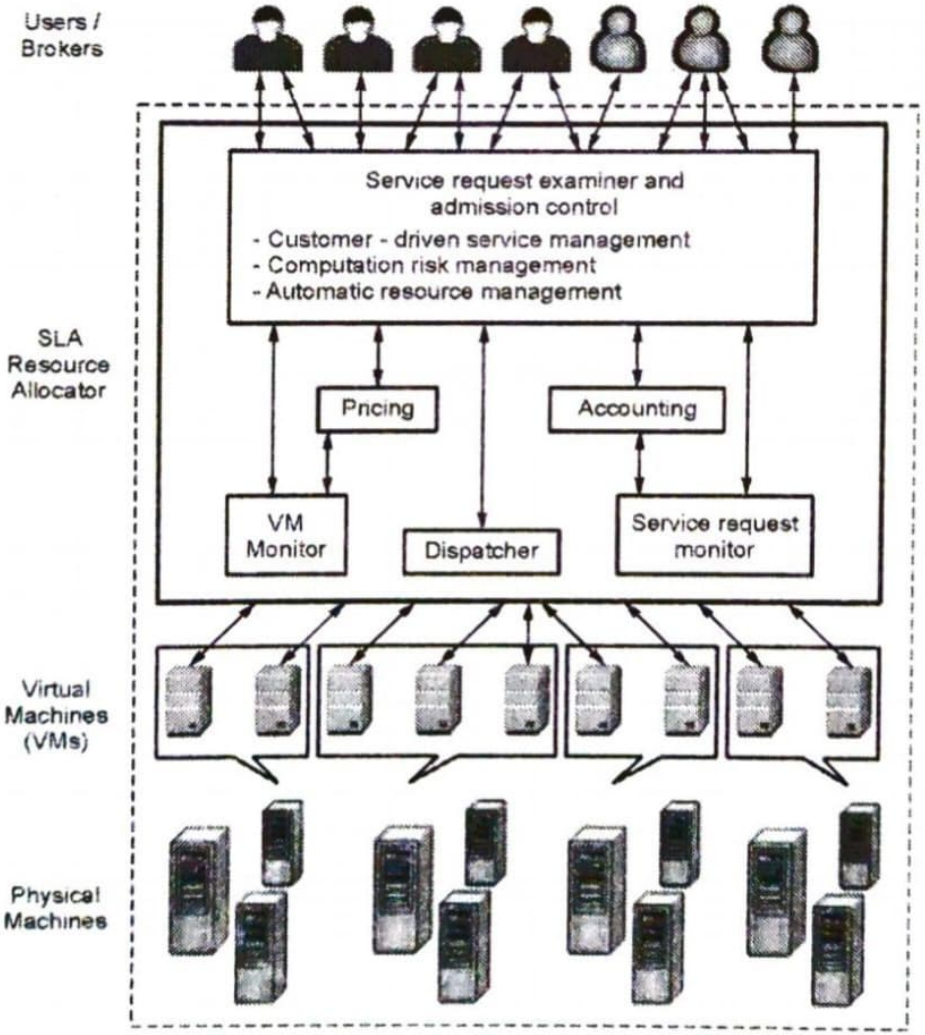


Fig. 1.1.4 Architectural framework

1) Users/ Brokers: They submit their service requests from anywhere in the world to the cloud
2) SLA resource allocator: It is a kind of interface between users and cloud service provider which enable the SLA oriented resource management
3) Service request examiner and admission control: It interprets the submitted request for QoS requirements before determining whether to accept or reject the request. Based on resource availability in the cloud and other parameters decide
4) Pricing: It is in charge of billing based on resource utilization and some factors. Some ~~requests~~ factors are request time, type etc
5) Accounting: Maintains the actual usage of resources by request so that the final cost can be charged to the users
6) VM Monitor: Keeps tracks on the availability of VM's and their resources
7) Dispatcher: The dispatcher mechanism starts the execution of admitted requests on allocated VM's
8) Service Request Monitor: The request monitor mechanism keeps track on execution of request in order to be in tune with SLA

Q-5 What are the challenges and risks in implementing cloud?

Ans 1) Security and Privacy Issues
→ Data stored on third party servers increases risk of data breaches, unauthorized access and data leakage

2) Data Loss and Recovery Risks
→ Data stored in cloud may be lost due to accidental deletion, hardware failure or cyberattacks
→ Backup and disaster recovery depend on the cloud provider's reliability

3) Downtime and Service Availability
→ Cloud services may suffer outages, making applications inaccessible
→ Organizations have limited service control over provider uptime

4) Vendor Lock-in
→ Migration from one cloud provider to another is difficult due to different API's, platforms and tools
→ Can lead to long-term dependency on single vendor

5) Performance Issues
→ Cloud Performance may be affected by latency, bandwidth limitations and network congestion
→ Not suitable for real time systems with strict response requirements

6) Hidden Costs and Budget Overruns
→ Pay-as-you-go model can lead to high unexpected bills if resources are not monitored properly
→ Additional costs for storage, data transfer and premium features

7) Integration Challenges
→ Integration cloud with existing on-premise systems is complex

→ Requires data migration, reconfiguration and interoperability testing

5) Lack of Control
→ Users do not control the underlying infrastructure
→ Limited ability to customize hardware, security and system configurations

Q-6 Define Cloud Computing and write its Characteristics

Ans Characteristics
1) On Demand Self Service
→ A consumer can unilaterally provision computing capabilities, such as service time and network storage, as needed without requiring human interaction with each service's provider
2) Ubiquitous network access: Capabilities are available over the network and accessed through standard mechanisms that ~~provide~~ promote use by heterogeneous thin or thick client platforms
3) Location-independent resource pooling: The provider's computing resources are pooled to serve all consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.
4) Rapid Elasticity: Capabilities can be rapidly and elastically provisioned to quickly scale up, and rapidly released to quickly scale down
5) Pay per use: Capabilities are charged using a metered, Fee-For-Service or advertising-based billing model to promote optimization of resource use

Q-1 Discuss cloud Deployment Models

Ans → Cloud Deployment Models refers to the location and management of clouds infrastructure
→ Deployment models are defined by ownership and control of architectural design and the degree of available customization

1) Public Cloud
→ The cloud infrastructure is made available to the generate public or a large industry group and is owned by an organization selling cloud services
→ Public Cloud is a huge data centre that offers the same services to all its users. The services are accessible for everyone and much used for the consumer segment
→ Provided by Commercial Vendors like AWS, Azure, GCP
→ Use Cases: Web apps, Saas apps, testing environments

Advantages: Cost effective, highly scalable, no maintenance overhead, pay-as-you go pricing

Best For: Startups, small businesses, applications with fluctuating demands, web-based applications

2) Private Cloud
→ Cloud Infrastructure dedicated exclusively to a single organization. It can be physically located on-premises or hosted by a third-party provider, but the resources are not shared with other organizations

Advantages:
1) Greater Control
2) Enhanced security and privacy
3) Customizable to specific business needs
4) better compliance with regulatory requirements

Best For: Large Enterprises, government agencies, organizations handling sensitive data (healthcare, finance), Companies with strict compliance requirements

3) Hybrid Cloud
→ Combines public and private clouds, allowing data and applications to move between them
→ Organizations can keep sensitive data in a private cloud while leveraging public cloud resources for less critical operations

Advantages: Flexibility, optimized costs, better scalability, maintains security for sensitive workloads while using public cloud for bursting capacity.

Best For: Organizations with varying requirements, Companies needing to balance security with scalability

4) Community Cloud
→ The cloud infrastructure is shared by several organization and supports a specific community that has shared concerns (eg: mission, security requirements, policy or compliance considerations)
→ It may be managed by the organizations or third party and may exist on-premises or off-premises

- Advantages
1) Cost Sharing among community members
2) Better Security than public cloud

- Best for:
→ Government Agencies, healthcare organizations, Financial institutions with shared compliance needs

Q-1 Compare IaaS, PaaS & SaaS.

Ans

Basis	IaaS	PaaS	SaaS
1) Access	IaaS gives access to resources like VM (Virtual Machine) & Virtual Storage	Paas gives access to deployment & development tools	SaaS gives access to the end user
2) Model	It is a service model that provides virtualized computing resources over internet	Delivers tools that are used for development of applications	Hosts software to make it available to clients
3) Technical Understanding	It requires technical knowledge	Some required For basic setup	No requirement Company handle everything
4) Popularity	Popular among developers & researchers	Among devs who focus on development of apps and scripts	among consumers and companies, such as file sharing email and networking

5)	Usage	Used by skilled developer to develop unique application	Used by mid-level developer to built application	Used among the users of entertainment
6)	Customization	High	Medium	Low
7)	Scalability	High	High	Very High
8)	Examples	AWS EC2, Azure VMs	Google App Engine	Gmail, Google Docs, Salesforce

Q-9 Define Cloud Computing and write advantage of it

Ans Check Q-1

Advantages:-
1) Lower Computer Costs
2) Improved Performance
3) Reduced Software Cost
4) Instant Software Updates
5) Improved document format compatibility
6) Unlimited Storage Capacity
For more see image

Q-10 Describe Challenges and application of cloud computing

Ans For challenges see Q-5

Applications of Cloud Computing
1) Cost Flexibility and Access to Powerful Analytics.
2) Business Scalability During Demand Spikes
3) Market Adaptability Across different devices.

1.1.5 Pros and Cons of Cloud Computing

Pros of cloud computing :

1. **Lower computer costs :** Since applications run in the cloud, not on the desktop PC, your desktop PC does not need the processing power or hard disk space demanded by traditional desktop software.
2. **Improved performance :** Computers in a cloud computing system boot and run faster because they have fewer programs and processes loaded into memory.
3. **Reduced software costs :** Instead of purchasing expensive software applications, you can get most of what you need for free.
4. **Instant software updates :** When you access a web-based application, you get the latest version - without needing to pay for or download an upgrade.
5. **Improved document format compatibility :** You do not have to worry about the documents you create on your machine being compatible with other user's applications or operating systems.
6. **Unlimited storage capacity :** Cloud computing offers virtually limitless storage.
7. **Increased data reliability :** Unlike desktop computing, in which if a hard disk crashes and destroy all your valuable data, a computer crashing in the cloud should not affect the storage of your data.
8. **Universal document access :** All your documents are instantly available from wherever you are.
9. **Latest version availability :** The cloud always hosts the latest version of your documents; as long as you are connected, you are not in danger of having an outdated version.
10. **Easier group collaboration :** Sharing documents leads directly to better collaboration.
11. **Device independence :** Move to a portable device and your applications and documents are still available.

4) Masked Complexity for Easy Service Access
5) Context Driven Variability and Personalization
6) Ecosystem Connectivity Across Business Partners

See image for more

Q-11 Difference between Scalability and Elasticity

Ans

	Feature	Scalability	Elasticity
1)	Meaning	Ability of system to handle increased workload by adding resources	Ability to automatically add or remove resources based on demand
2)	Nature	Usually planned and long-term	Automatic and real-time
3)	Resource Adjustment	Mostly manual or predefined	Fully dynamic and automatic
4)	When Used	When workload grows steadily over time	When workload fluctuates rapidly
5)	Example	Adding more servers to support a growing user base	Cloud system increases VMs during peak hours and reduces them when demand drops
6)	Focus	Increasing Capacity	Optimizing Resource Usage & Cost

Q-12 Describe various layers of Cloud Computing

Ans
1) SaaS
2) PaaS
3) IaaS

Cloud Applications (All Six)

1. Cost Flexibility and Access to Powerful Analytics

Cloud computing eliminates the need for organizations to invest in hardware, install software, or pay high license fees. Because of this cost flexibility, online marketplaces can use **advanced analytics tools** directly from the cloud, enabling better decision-making and customer understanding.

---

2. Business Scalability During Demand Spikes

Cloud platforms allow companies—such as online video retailers—to **scale resources up or down** instantly. This helps them handle sudden spikes in demand (e.g., during new releases or festival seasons) without performance issues or infrastructure overload.

---

3. Market Adaptability Across Different Devices

Cloud enables online entertainment platforms to deliver services on **any type of customer device**, including smartphones, tablets, laptops, and smart TVs. This adaptability helps businesses reach diverse user groups quickly and efficiently.

4. Masked Complexity for Easy Service Access

Cloud computing hides the internal complexity of systems. Users can access services without worrying about how they are built or how they run. This simplifies usage and makes even advanced cloud technologies easy for end users to access.

---

5. Context-Driven Variability and Personalization

With vast storage and processing capabilities, cloud systems can store user preferences and behavior patterns. This enables **personalized experiences**, such as intelligent assistants, recommendation systems, and customized services.

---

6. Ecosystem Connectivity Across Business Partners

Cloud platforms support seamless **information exchange and integration** across multiple business partners and stakeholders. This enhances collaboration, supply-chain management, and data sharing between organizations.

Discuss functions provided by PaaS.

Here is a clear, **exam-ready** answer on **functions provided by PaaS (Platform as a Service)**:

Functions Provided by PaaS

Platform as a Service (PaaS) offers a complete platform for developing, running, and managing applications. It provides tools and environments so developers can focus on coding rather than infrastructure.

1. Application Development Environment

- Provides **IDEs, editors, libraries, APIs**.
- Supports multiple programming languages (Java, Python, Node.js, etc.).

2. Application Deployment & Hosting

- Offers automated tools to **deploy, run, test, and host** applications.
- Handles underlying OS, runtime, and updates automatically.

3. Scalability & Load Balancing

- Automatically scales applications based on demand.
- Balances traffic to ensure performance.

4. Database Services

- Provides managed **databases** (SQL/NoSQL).
- Includes backup, replication, and monitoring.

4. Database Services

- Provides managed **databases** (SQL/NoSQL).
- Includes backup, replication, and monitoring.

5. Middleware Services

- Offers **integration tools** like message queues, API management, and authentication services.
- Helps connect different components in an application.

6. Version Control & Collaboration

- Provides tools for **source code management**, team collaboration, CI/CD pipelines.

7. Security & Access Control

- Built-in security, identity management, encryption, and permissions.
- Manages patches and security updates automatically.

8. Development Frameworks

- Provides prebuilt frameworks like Spring, Django, .NET, etc.
- Makes development faster with reusable components.

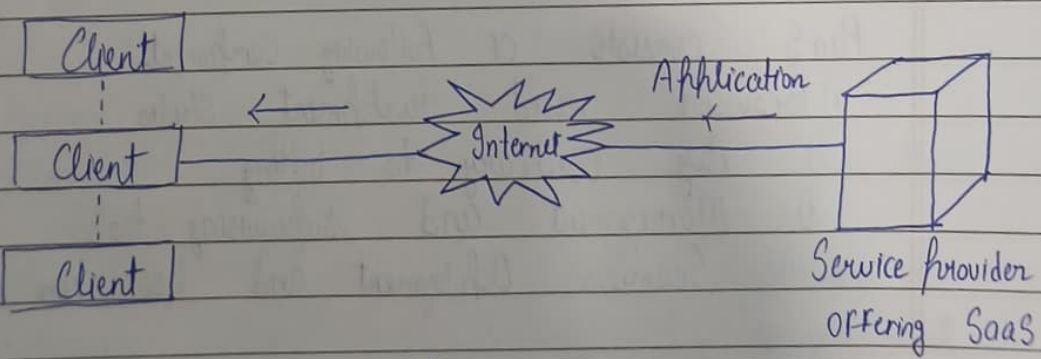
9. Monitoring & Management Tools

- Real-time monitoring of performance, logs, errors, and usage metrics.

10. Integration with Other Cloud Services

- Easy connection with storage, analytics, AI/ML tools, and other cloud resources.

1) SaaS (Software as a Service)
→ Model in which an application is hosted as a service to customers who access it via the Internet
→ the provider does all the patching and upgrades upgrades as well as keeping the infrastructure running
→ In this model, the user, the client or consumer runs an application from a cloud infrastructure. Though an interface such as a web browser, the client or user may access this application from a variety of devices
→ the complete application is offered as on demand service. This saves the client from having to invest in any software licenses or servers up front, and can save the provider money since they are maintaining and providing only a single application
→ Microsoft, Google and Zoho offer SaaS



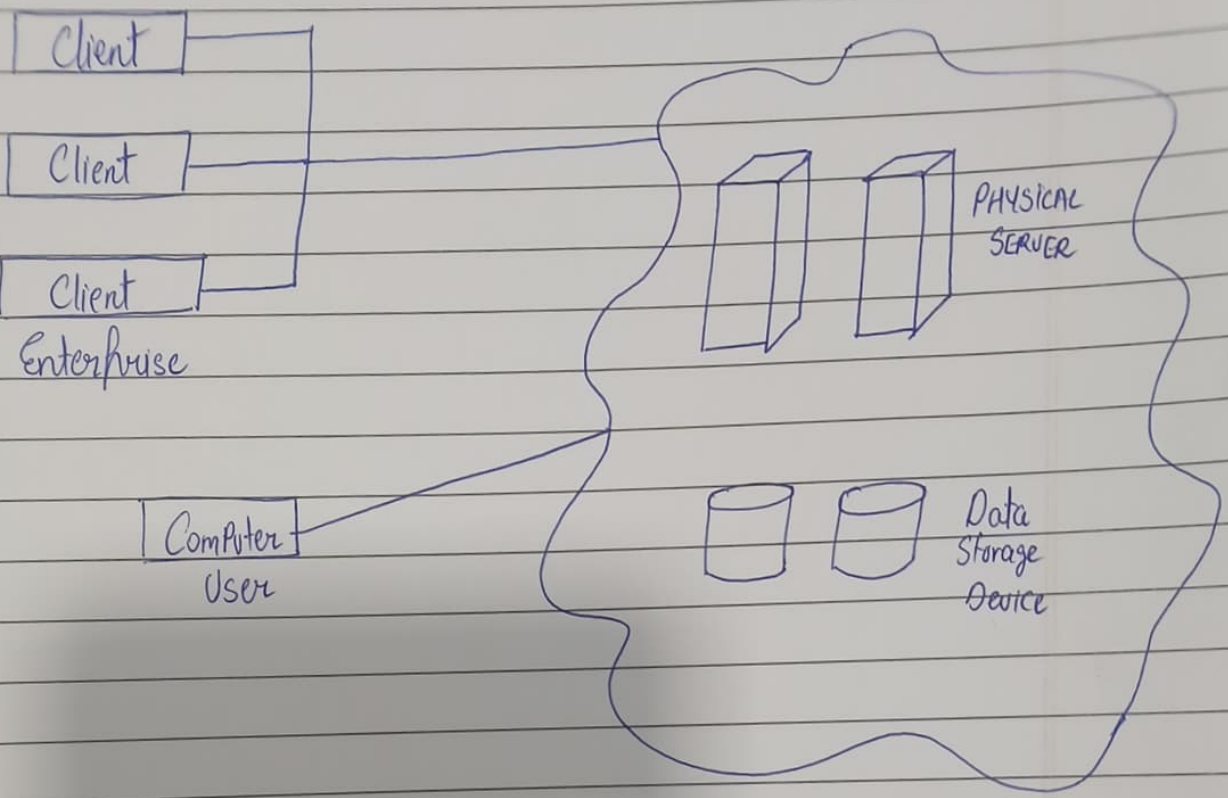
2) PaaS (Platform as a Service)
→ PaaS is another application delivery model and also known as cloud-ware. Supplies all the resources required to build applications and services completely from the Internet, without having to download or install software
→ Services include: Application Design, development, testing, deployment and hosting, team collaboration, web service integration, database integration, security, scalability, storage.

state management and versioning.
→ This model involves software encapsulated and offered as a service, from which higher levels of service may then be built. The user, customer, or client in this model is the one building applications which then run on providers infrastructure
→ This in turn provides customers and clients with the capability to deploy applications onto the cloud infrastructure using programming tools and languages, which the provider supports
→ The customer still does not manage the framework, network, servers or operating system, but has control over deployed applications and sometimes over the hosting environment itself

Examples. Google's App Engine or Force.com

PaaS consists of following components:-
1) Browser based development studio
2) Pay contrary to billing
3) Management and supervising tools
4) Seamless Deployment and host run time environment

3) Infrastructure As a Service (IaaS)
→ IaaS is a cloud computing service model that gives virtualized computing resources over the web with IaaS, associations can get to and manage versatile infrastructure asset like Virtual Machine, storage and network administration parts without the need to put resources into or keep up with actual equipment.



Examples: Amazon EC2, RackSpace Mosso, GoGrid.

IaaS Server Types

1) Physical Server: Actual Hardware is allocated for the customer's dedicated use
2) Dedicated Virtual Server: The Customer is allocated a Virtual Server, which runs on Physical server that may or may not have other virtual servers
3) Shared Virtual Server: The Customer can access a virtual server on a device that may be shared with other customers

Briefly explain the features of IaaS? 7m

Here is a **perfect 7-mark answer** for **Features of IaaS (Infrastructure as a Service)** — detailed, clear, and exam-ready:

Features of IaaS (Infrastructure as a Service)

Infrastructure as a Service (IaaS) provides virtualized computing resources over the internet. It is the foundational layer of cloud computing and offers flexible, scalable infrastructure to users.

---

1. On-Demand Self-Service

Users can provision computing resources such as virtual machines, storage, and networks **whenever needed**, without requiring manual intervention from the provider. This increases flexibility and reduces setup time.

---

2. Scalability and Elasticity

IaaS supports both **horizontal and vertical scaling**.

- Users can add more VMs, increase CPU, RAM, or storage based on workload.
- It helps organizations manage growing or fluctuating demands efficiently.

---

3. Pay-As-You-Go Pricing

IaaS charges users **only for the resources they consume** (CPU hours, storage, bandwidth).
This eliminates upfront hardware costs and reduces financial risk for businesses.

4. Virtualization

IaaS relies heavily on virtualization technology.

Virtual machines are created on physical hardware allowing:

- Better resource utilization
- Fault isolation
- Quick provisioning
- Easy backup and migration

---

5. Accessible Over the Internet

All IaaS resources are accessed through the internet using dashboards, APIs, or command-line tools.

This supports remote infrastructure management and global access.

---

6. High Reliability and Availability

IaaS providers offer **redundant servers, automatic failover, and backup systems**.

This ensures applications run continuously even if hardware fails.

Many services provide **99.9% uptime SLAs**.

---

7. Full Control Over Infrastructure

Users get complete control over:

- Operating systems
- Middleware
- Applications
- Security configurations

This makes IaaS suitable for businesses needing custom environments.

---

8. Security and Data Protection

IaaS offers built-in security features such as:

- Firewalls
- Identity and Access Management (IAM)
- Encryption
- Network security controls

Providers also handle physical security of data centers.

---

9. Global Availability

Most IaaS providers have **data centers in multiple regions,** allowing customers to deploy applications closer to users.
This improves performance and reduces latency.

Conclusion

IaaS offers flexible, scalable, cost-effective virtual infrastructure that allows organizations to run customized applications without investing in physical hardware. Its key features—scalability, on-demand provisioning, virtualization, and high availability—make it ideal for startups, enterprises, and IT administrators.

What are the features of cloud computing? 7m

Here is a **complete, exam-ready 7-mark answer** for **Features of Cloud Computing**.
You can write these points exactly as they are.

Features of Cloud Computing (7 Marks)

Cloud computing provides on-demand access to shared computing resources over the internet. Its major features include the following:

---

1. On-Demand Self-Service

Users can automatically provision computing resources—like servers, storage, and applications—without needing human interaction with the service provider.
This increases speed, flexibility, and independence for users.

---

2. Broad Network Access

Cloud services are accessible from anywhere through the internet using devices such as laptops, smartphones, tablets, and thin clients.
This ensures mobility and universal access.

---

3. Resource Pooling

Cloud providers use a **multi-tenancy model** where computing resources are pooled and shared among multiple users.
Resources like storage, memory, and bandwidth are dynamically assigned and reassigned based on demand.

3. Resource Pooling

Cloud providers use a **multi-tenancy model** where computing resources are pooled and shared among multiple users.
Resources like storage, memory, and bandwidth are dynamically assigned and reassigned based on demand.

---

4. Rapid Elasticity

Cloud resources can scale **up or down instantly** based on workload requirements.
This elasticity helps handle sudden spikes in demand and prevents resource wastage during low usage.

---

5. Measured Service (Pay-as-you-go)

Cloud systems automatically measure usage of resources like CPU time, storage, and bandwidth.
Users are billed only for what they consume, reducing unnecessary costs.

---

6. Scalability

Cloud infrastructure can grow with the business.
Organizations can increase computing power, storage, or servers as their needs expand, without major investments in hardware.

---

7. High Reliability and Availability

Cloud platforms offer reliable services with features like:

- Redundant servers
- Automatic backups
- Failover mechanisms
- Global data centers
  This ensures high uptime and continuous operation.

8. Security

Cloud providers offer strong security features such as:

- Encryption
- Identity and Access Management (IAM)
- Firewalls
- Regular patches and updates

  They also protect the physical infrastructure in secure data centers.

Conclusion

Cloud computing provides flexible, scalable, and cost-effective services with strong accessibility and reliability. These features make it widely used in business, education, entertainment, and almost all digital applications.

Explain IaaS technology in cloud computing with a real-world example.
7marks

Here is a **perfect 7-mark, exam-ready answer** for:

"Explain IaaS technology in cloud computing with a real-world example."

IaaS Technology in Cloud Computing

Infrastructure as a Service (IaaS) is a cloud computing model that provides **virtualized hardware resources** over the internet. It is the **lowest layer** of cloud service delivery and offers essential IT infrastructure such as virtual machines, storage, networks, and servers on a pay-per-use basis.

IaaS eliminates the need for organizations to buy, install, and maintain physical hardware. Instead, they can rent computing resources from a cloud provider whenever required.

Features / Working of IaaS

1. Virtualized Computing Resources

IaaS provides virtual machines (VMs) that users can configure with desired CPU, RAM, and operating system.

2. On-Demand Provisioning

Resources can be instantly created or removed through a dashboard or API without manual hardware setup.

3. Scalability

Organizations can scale resources up or down depending on workload demands.
Example: add more servers during peak usage.

3. Scalability

Organizations can scale resources up or down depending on workload demands.
Example: add more servers during peak usage.

4. Pay-As-You-Go Pricing

Users only pay for the amount of computing they consume—such as instance hours, storage space, or bandwidth.

5. Full User Control

Users control:

- OS installation
- Software and middleware
- Security settings
- Application deployment

The cloud provider only manages the underlying hardware.

6. High Reliability

IaaS providers offer fault-tolerant systems, data backup, disaster recovery, and 99.9% uptime guarantees.

7. Global Access

Infrastructure can be accessed remotely from any location via the internet.

Real-World Example of IaaS

Amazon Web Services – EC2 (Elastic Compute Cloud)

AWS EC2 is one of the most widely used IaaS services. It offers scalable virtual servers where businesses can deploy applications.

How it works in real life:
Consider a **startup launching an e-commerce website**:

- Instead of buying physical servers costing lakhs of rupees, they rent EC2 instances.
- They select VM size (e.g., 4 vCPUs, 16 GB RAM) and OS (Linux/Windows).
- During festival sales like **Diwali,** traffic increases.
  → They can instantly add more EC2 servers to handle heavy load.
- After the sale, they scale down and pay only for the hours used.
- AWS also handles hardware failures, backups, and network management.

This gives the company **flexibility, lower cost, and high performance** without any physical infrastructure.

Conclusion

IaaS provides scalable and cost-efficient IT infrastructure through virtualization. With on-demand provisioning, pay-per-use pricing, and high reliability, it is widely used for hosting websites, running enterprise applications, data analytics, and disaster recovery. Real-world services like AWS EC2, Google Compute Engine, and Microsoft Azure VMs demonstrate the power and convenience of IaaS in modern cloud computing.

Explain Grid computing and Utility computing.

Here is a clear, **exam-ready explanation** of **Grid Computing** and **Utility Computing**:

Grid Computing

Grid computing is a distributed computing model where a large number of geographically scattered computers work together to solve a complex problem.
These computers are connected through a network and share their processing power, storage, and resources.

Key Points:

- Combines many independent computers into a **virtual supercomputer**.
- Designed for tasks that require **high processing power**.
- Resources come from different organizations or locations.
- Supports **parallel processing** — tasks are divided into smaller parts and processed simultaneously.
- Commonly used in **scientific research**, weather forecasting, simulations, biotechnology, physics experiments (e.g., CERN).

Example:

NASA or research labs using thousands of computers worldwide to process satellite images or scientific datasets.

Ch-2 Software as a Service

Q-1 Justify the statement "SaaS integration is hard"

Ans Means Challenges are there in SaaS integration which makes it hard to implement
Challenges are

1) Lack of Standarization
Every SaaS application uses different APIs, data formats, authentication methods and communication protocols This makes integrating multiple SaaS systems difficult

2) Limited Customization
→ SaaS runs on multi-tenant architecture, so users get limited control over backend functions. This restricts how much you can modify or integrate it with existing enterprise systems

3) API Limitations
SaaS depends heavily on API's which may suffer from:
- Rate Limits
- Version Updates
- Deprecated endpoints
- Performance issues

4) Data Security & Privacy Concerns
→ Data moves accross the internet between SaaS apps.
→ Ensuring compliance, encryption, secure access, and proper identity management is a major challenge

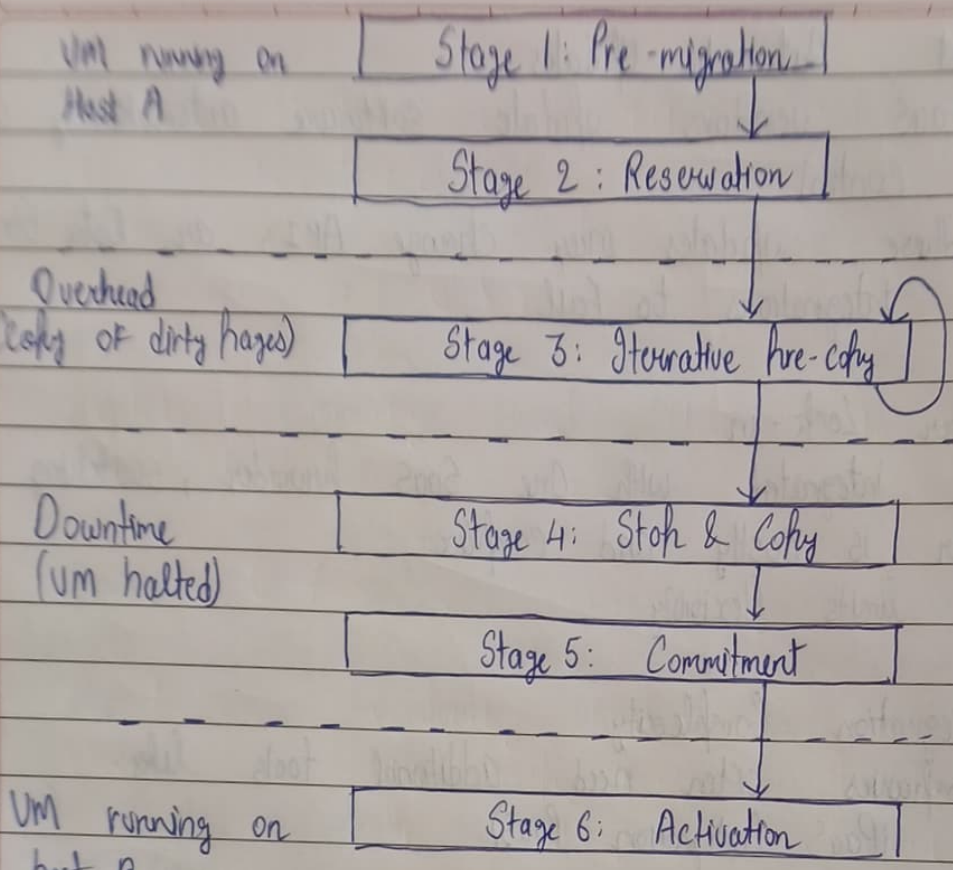
5. Frequent Automatic Updates
→ SaaS vendors update software automatically without user control
→ These updates may change API's or Data Structures causing integrations to fail

6) Vendor Lock-in
→ Once integrated with one SaaS provider, switching to another is costly and complex
This limits flexibility

7) Integration Complexity
Companies often need additional tools like:
→ iPaaS (Integration PaaS)
→ Middleware
→ Custom connectors
This increases cost and technical effort

Q-2 Explain the following Virtual Machine migration services in detail
(i) Hot Migration
(ii) Cold Migration

Ans (1) Hot Migration
→ Hot migration refers to moving a running Virtual Machine (VM) from one physical host to another without shutting it down
→ Without stoppage of OS or applications, they are shifted from Virtual Machines to Physical machines
→ Downtime of clients is easily averdable



Stage 1: Pre-Migration stage: A target host will be preselected where the resources required to receive migration will be guaranteed.

Stage 2: Reservation: A request is submitted to migrate a VM from host-A to Host B. If the request is not fulfilled, then VM will continue to run on Host-A

Stage 3: Iterative Pre-Copy: During the first iteration, all memory pages are transferred from Host-A to Host-B. Subsequent iterations copy are only those pages dirtied during the previous transfers

Stage: 4: Stop & Copy: In this phase, VM will be suspended on Host-A and redirect its network traffic to Host-B

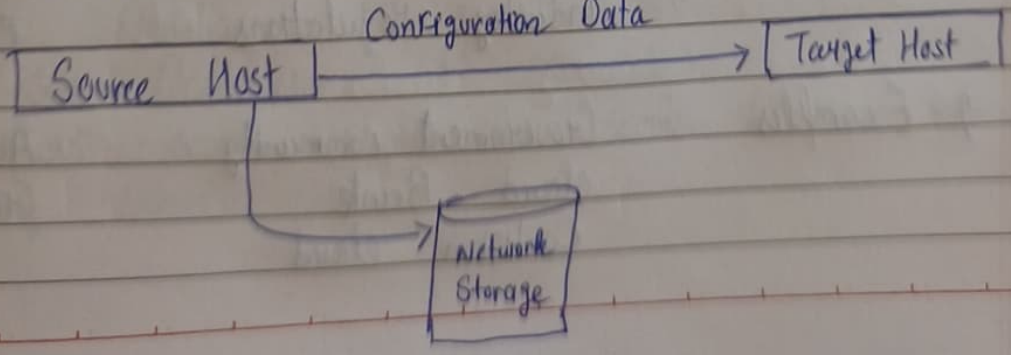
→ CPU state and any remaining inconsistent memory pages are then transferred like a final sync.

→ This process will reach a consistent suspended copy of the VM at both Host-A and Host-B.
→ Host-A will remain primary and it will be resumed in case of failure at this stage.

Stage 5: Commitment to the hosts: Host B sends the signal to Host-A that it has successfully received a consistent VM OS image.
→ Host A acknowledges the signal and destroys the VM. Host B becomes primary host for migrated VM

Stage 6: Activation of VM: The migrated VM on Host-B is now activated. Post-migration code connects to the local resources and resumes the operation.

(ii) Cold Migration
→ Movement of VM from one physical machine to another in powered OFF state is cold migration.
→ The configuration files, log files, disk of VM are moved from source target to target host.
→ The new VM is now registered and also VM is removed from the registry.
→ The first host VM is shut down and again started on next host.
→ Applications and OS are terminated on VM's before moving them to physical devices. User is given choice of movement of disks associated from one data store to another one.



Q-3 Compare various cloud delivery models based on their characteristics

Ans See ch-1 Q-8

Q-4 Explain Community Cloud. How it is different from Public Cloud?

Ans See Q-7

Aspect	Community Cloud	Public Cloud
1) Users	Specific group or orgs with shared goals	Available for everyone (general public)
2) Ownership	Shared by community	Owned and operated by cloud provider (AWS, Azure, Google)
3) Security level	Higher Security	Lower
4) Cost	Cost shared among community members	Pay as you go, usually cheaper.
5) Customization	High	Limited Customization
6) Compliance	Designed for specific industry regulations	General Purpose compliance
7) Examples	Government community cloud, Bank Corhsium cloud	AWS, Azure, Google Cloud.

Q-4 Describe PaaS Application Framework in Detail

Ans The PaaS Application Framework provides a complete environment for building, testing, deploying and managing applications on the cloud.

Components of PaaS Application Framework

1) Application Development tools
→ Code Editors
→ Debuggers
→ Build tools
→ Version Control System (Git)

2) Application Runtime Environment
For Java, Python, Node.js, Ruby, .NET
Developers do not need to install or configure runtime manually

3) Middleware
Middleware Components handle:
Messaging, Authentication, Integration and Workflow Management
Thus allows applications to communicate with databases, APIs and other services easily

4) Database Services
PaaS includes built-in database services:
- SQL Databases (MySQL, PostgreSQL)
- NoSQL Databases (MongoDB, Redis)

Developers can access and scale databases without managing servers

5) Deployment & Management tools
Tools For:
→ Automatic Deployment, Scaling applications, Monitoring Usage, Logging Errors, Auto-Updates

These tools simplify the entire application lifecycle

6) APIs and Web Services
PaaS provides APIs for:
Storage, Authentication, Networking, Payment Processing, Analytics
APIs help integrate cloud services into applications quickly

7) Scalability & Load Balancing
→ PaaS automatically scales the application based on demand:
→ Adds more instances during high load
→ Reduces instances during low load

8) Security Services
Paas includes
→ Identity and access management
→ SSL/TLS encryption
→ Data Backup and Recovery
→ Role-based Access
Developers get secure environments without handling complex security tasks
Examples: Google App Engine, Azure, AWS, Heroku

Q-5 Discuss services Provided by SaaS?

Ans
1) Application Hosting Services
2) On Demand Software Delivery
3) Automatic Updates and Patch Management
4) Multi-tenant Application Services
5) Data Management and Storage Services
6) Security and Access Control
7) Collaboration and Sharing Services
8) Integration Services

See Image for More

Q-6 What are the benefits of Platform as a Service (PaaS)

Ans
1) Faster application Development
2) Reduced Cost
3) Automatic Scalability
4) No Infrastructure Management
5) Built-in and testing & Deployment Tools
6) Collaboration Support
7) High Availability and Disaster Recovery
8) Integration Capabilities

Example: Google App Engine

See Image for More

Discuss services provided by SaaS.

Here is a **perfect exam-ready answer** for **"Services provided by SaaS"** (suitable for 5–7 marks):

Services Provided by SaaS (Software as a Service)

Software as a Service delivers complete, ready-to-use applications over the internet. Users access these applications through a web browser without installing or maintaining any software.

SaaS provides the following key services:

---

1. Application Hosting Services

SaaS hosts complete software applications on the provider's cloud infrastructure.
Users only need a browser to access it—no installation or hardware setup.

Examples: Gmail, Google Docs, Salesforce.

---

2. On-Demand Software Delivery

SaaS applications are delivered on subscription or pay-per-use model.
Users pay only for the features or time they use, reducing software ownership cost.

---

3. Automatic Updates and Patch Management

The SaaS provider is responsible for:

- Software updates
- Bug fixes
- Security patches

Users always get the latest version without manual update effort.

4. Multi-tenant Application Services

A single application instance serves multiple users or organizations securely.

This reduces cost and improves resource utilization.

---

5. Data Management and Storage Services

SaaS platforms provide:

- Cloud storage
- Backup
- Recovery
- Database management

All data is securely stored and managed by the provider.

---

6. Security and Access Control

SaaS provides:

- Authentication and authorization
- Encryption
- Secure access through SSL/TLS

Security is handled centrally by the provider.

---

7. Collaboration and Sharing Services

Many SaaS apps include features that support teamwork:

- Real-time document editing
- File sharing
- Project collaboration
- Messaging tools

Example: Microsoft Office 365, Google Workspace.

8. Integration Services

SaaS apps can integrate with:

- APIs
- Third-party systems
- CRMs
- Financial tools

This enables smooth data exchange.

Short 4-Mark Version

- Hosted software accessible via browser
- Automatic updates and security
- On-demand subscription model
- Multi-tenant support
- Cloud storage and data management
- Collaboration features

Benefits of Platform as a Service (PaaS)

Platform as a Service provides a complete cloud-based environment for developing, running, and managing applications. It offers several advantages for developers and organizations:

---

1. Faster Application Development

PaaS provides ready-to-use tools, libraries, frameworks, and runtime environments.
Developers can build applications quickly without setting up hardware or software manually.

---

2. Reduced Cost

There is no need to buy servers, storage, operating systems, or development tools.
Users pay only for what they use, which greatly reduces development and deployment costs.

---

3. Automatic Scalability

PaaS platforms automatically scale the application based on user load.
This ensures good performance during peak demand without manual intervention.

---

4. No Infrastructure Management

The cloud provider manages:

- Hardware
- Operating systems
- Middleware
- Security updates

Developers can focus entirely on coding, not on managing servers.

---

5. Built-in Testing and Deployment Tools

PaaS offers services for:

- Continuous Integration
- Continuous Deployment
- Automated testing
- Application monitoring

This simplifies the entire application lifecycle.

---

6. Collaboration Support

Multiple developers can work on the same project from different locations.
Shared environments make teamwork easy.

---

7. High Availability and Disaster Recovery

PaaS handles:

- Backup
- Failover
- Load balancing
- Data recovery

This ensures applications remain available even during failures.

---

8. Integration Capabilities

PaaS provides APIs to integrate with:

- Databases
- Payment systems
- Messaging services
- Identity services (OAuth, SSO)

Real-World Example

Example: Google App Engine (GAE)

A company wants to build an online ticket-booking application.

Using **Google App Engine**, developers get:

- Pre-configured runtimes (Python, Java, Node.js)
- Built-in database (Cloud Datastore)
- Automatic scaling when many users request tickets
- Logging, monitoring, and error tracking tools
- Zero server management

Developers only write the application code, and Google App Engine handles everything else.

Short 3–4 Mark Version (if needed)

- Faster development
- Lower cost
- Automatic scalability
- No infrastructure management
- Built-in tools for testing, deployment
- High availability
- Good for team collaboration

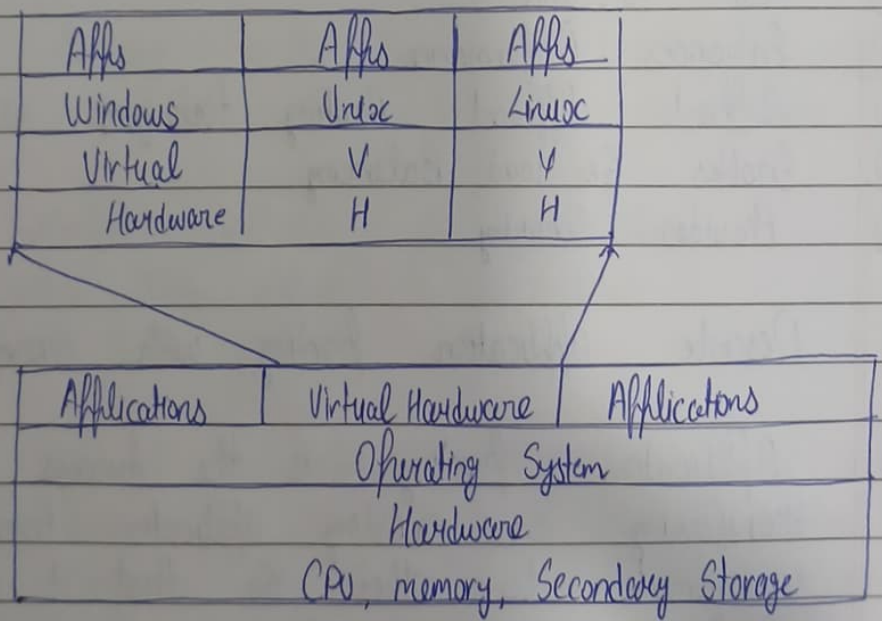
Example: Deploying a web app using **AWS Elastic Beanstalk** or **Google App Engine**.

If you want, I can also give **diagram of PaaS architecture** or **very short paragraph answer**.

Ch-3 Abstraction & Virtualization

Q.1 Describe Virtual Machine and its role in Cloud Computing [W-24]

Ans A Virtual Machine is software based emulation of a physical Computer. It runs an Operating system and applications just like a real machine, but it is created and managed by a hypervisor
→ Each VM has has its own virtual CPU, memory, Storage and network interface, even though the underlying physical resources are shared



Role in Cloud Computing
1) Resource Virtualization
2) Isolation and Security
3) Scalability
4) Flexibility
5) Cost Efficiency
6) Backup & Recovery
7) Supports Multitenancy

Role of Virtual Machines in Cloud Computing

1. Resource Virtualization

VMs allow cloud providers to divide a single physical server into multiple isolated virtual servers.
This improves **resource utilization**, prevents wastage, and ensures each user gets a dedicated environment.

2. Isolation and Security

Each VM is isolated from others.
So if one VM crashes or gets attacked, **other VMs remain unaffected**, ensuring better security and stability.

3. Scalability

Cloud platforms can easily **create, start, stop, or delete** VMs on demand.
This supports **elastic scaling** based on user requirements.

4. Flexibility

Users can install any operating system (Windows/Linux), frameworks, databases, etc., depending on their needs.
This flexibility makes cloud environments suitable for diverse workloads.

5. Cost Efficiency

Instead of buying physical servers, users rent VMs for the required time.
This **pay-as-you-go** model reduces IT infrastructure cost.

6. Backup and Recovery

VMs can be easily **snapshotted, cloned, or migrated**, allowing quick disaster recovery and efficient management.

7. Support for Multi-Tenancy

Multiple users or organizations can run their isolated VMs on the same hardware.

Cloud providers use this feature to maximize return from their data centers.

In Summary

Feature	Description
Definition	Software emulation of a physical machine
Manages by	Hypervisor (Type-1 or Type-2)
Key Role	Virtualization, isolation, resource sharing
Benefits	Scalability, cost reduction, flexibility, security
Use in Cloud	Provisioning servers on demand, running apps, testing, backup, migration

Q-2 Describe the use of Load Balancer [W-24]

Ans A Load Balancer is a cloud service that distributes incoming network traffic or application requests across multiple servers (or VMs) to ensure reliability, availability and optimal performance.

Its main purpose is to prevent any single server from becoming overloaded

Uses:
1) Distributes Workload evenly
2) Ensures High availability
3) Improves Scalability
4) Fault tolerance
5) Enhances Performance
6) Supports different Routing techniques
7) Enables Geo-load Balancing
8) Provides Security

Q-3 Describe application porting with example

Ans Application porting is the process of modifying and transferring an existing application from one computing environments to other so that it works correctly in the new environment

The environments may differ in OS, hardware, cloud platform, programming language or database

Why Porting is Required
→ To move applications to cloud
→ To upgrade old hardware or OS
→ To reduce cost or improve performance

→ To support multiple platforms (eg. Windows & Linux)

Example
On Premise → Cloud Porting
→ A company runs a Java web application on a local Linux server
→ They decide to move it to Aws cloud.

Q-4 Describe Virtual Machine Migration

Ans See Ch-2

Q-5 What is Machine Imaging

Ans Machine Imaging is the process of creating a complete copy or snapshot of a VM which includes
→ OS
→ Installed software and applications
→ System and network configurations
→ Data on attached disks

→ This snapshot is called a machine Image and can be reused to create new identical virtual machines anytime. It plays a vital role in backup, Scaling, disaster recovery and automated deployments
→ A machine Image is a Computer Engine that stores all the configuration, metadata, permissions and data from multiple disks of a VM instance. You can use a machine image in many system maintenance, backup and recovery and instance cloning scenarios

Uses of Load Balancer in Cloud

1. Distributes Workload Evenly

It spreads client requests across multiple servers so that:

- No server is overloaded
- All servers work efficiently
- System performance improves

2. Ensures High Availability

If one server fails or is under maintenance, the load balancer automatically redirects traffic to healthy servers.
This ensures **continuous service without downtime**.

3. Improves Scalability

Cloud environments often scale automatically.
Load balancers:

- Add new servers to the pool when traffic increases
- Remove or reduce servers when traffic decreases

This supports **auto-scaling**.

4. Fault Tolerance

It continuously monitors the health of servers.
If a server becomes slow or unresponsive, it stops sending traffic to it.

5. Enhances Performance

Load balancers optimize:

- Response time
- Throughput
- Resource utilization

Some load balancers even perform caching and SSL offloading to boost performance.

6. Supports Different Routing Techniques

Cloud load balancers use algorithms like:

- **Round Robin**
- **Least Connections**
- **IP Hash**
- **Weighted Round Robin**

These help manage traffic intelligently.

7. Enables Geo-Load Balancing

Traffic can be distributed across servers in different geographic regions.

This reduces latency and improves user experience globally.

8. Provides Security

Load balancers can offer built-in security features like:

- DDoS protection
- SSL/TLS termination
- Web Application Firewall (WAF) integration

Understanding Machine Imaging

- When to use machine imaging in cloud computing?
- machine images are the most ideal resources for the following use cases:
  - Multiple disk backups
  - Instance cloning
- **Multiple Disk backups:** Machine images support backups at the VM instance level. Disks are backed up as differential snapshots.
- When a machine image is used to copy disks, Compute Engine guarantees that the data across disks is captured in a crash-consistent manner at a given time. Compute Engine uses globally consistent timestamps to ensure this guarantee. This consistency is critical if your VM instance is running and you want to ensure that the backup point across disks is maintained. When the backup point across disks is maintained, you can return to the same point in time across disks when you restore a machine image.

Understanding Machine Imaging

- **Multiple disk backup:** Machine images are suitable for creating backups of all disks that are attached to a VM instance. A machine image can be used to backup multiple disks at a time. A persistent disk snapshot can only backup a single disk at a time.
- Example:
  - Imagine a VM named WebServer with:
  - Disk 1: OS (Linux) – 50 GB
  - Disk 2: App Data – 200 GB
  - Disk 3: Logs – 100 GB
  - With snapshots, you need to back up each disk separately (three snapshots).
  - With a machine image, you take one backup that includes all disks in a single step.
- **Differential disk backup:** Machine images store differential snapshots of your previously created machine images or snapshots. When you generate a machine image from a VM instance, the first machine image contains a full copy of all disk data. Subsequent machine images are stored as differential copies for better performance and space efficiency. This mechanism is similar to that used by persistent disk snapshots.
- The first machine image contains a full copy of all disks.
- Later images store only the changes (differences) since the last image — this saves time and storage.
- Example:
  - Day 1: Full backup = 350 GB.
  - Day 2: Only 10 GB of changes → backup stores just 10 GB, not 350 GB again.
  - Day 3: 2 GB changed → backup stores only 2 GB.
  - Similar to incremental backups used in backup software.

Understanding Machine Imaging

- **Instance cloning:** Machine images can be used to clone instances. You can use machine image to make copies of an instance that contains most of the VM configurations of the source instance. These copies can then be used for troubleshooting, scaling VM instances, debugging, or system maintenance.
- Use a machine image to create an identical copy of a VM, including its OS, applications, and most configurations.
- **Why it's useful:**
- Troubleshooting – Test issues without affecting production.
- Scaling – Create more servers quickly for high traffic.
- Maintenance – Prepare updates on a copy before applying to the live server.
- Example:
  - Production VM: Billing-System.
  - You need to test a software patch.
  - Clone the VM from its machine image to create Billing-System-Test.
  - Apply the patch to the clone, test it, then update production once verified.

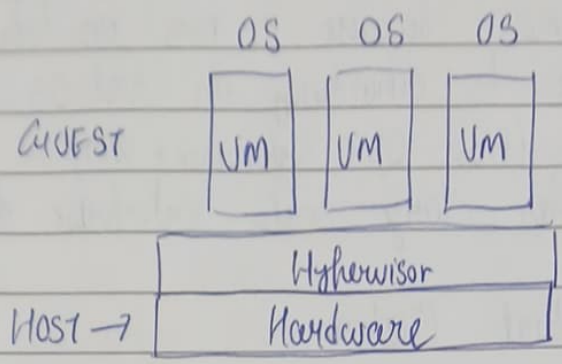
Q-6 Describe various type of hypervisors with their advantage and disadvantage

Ans Type 1 Hypervisor (Bare-Metal)

→ It runs directly on a given hardware platform. A "guest" OS that runs at the second level above the hardware
→ It does not require any base server OS
→ It has direct access to hardware resources
→ Examples of type-1 hypervisors include VMware ESXi, Citrix Xen Server and Microsoft Hyper-V hypervisor

Advantages
→ Very efficient because they have direct access to physical hardware resources (like CPU, Memory, Network, and Physical Storage)
→ More security because there is no kind of third party resource so that attacker couldn't compromise with anything

Cons / Disadvantages:
One problem with Type-1 Hypervisors is that they usually need a dedicated separate machine to perform their operation and to instruct different VM's and control the host hardware resources

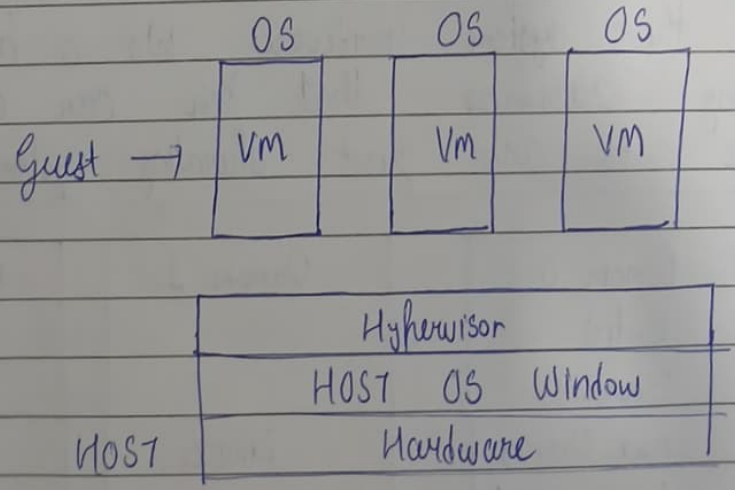


2) Type-2 Hyperwisor (Hosted)

→ Such kind of hyperwisor don't run directly over the underlying hardware rather they run as an application in a Host system (Physical machine)

→ Basically, the software is installed on an Operating system

→ Hyperwisor asks the OS to make hardware calls. An example of Type-2 Hyperwisor includes VMware Player or Parallels Desktop



0 Advantages

1) Easy to install and use like normal software
2) Good for testing, learning and development
3) No need for special hardware
4) Cheaper or free options available.

Disadvantages

→ Lower Performance because it runs on top of host OS
→ Less secure due to dependency on host OS
→ More Overhead (host OS + hypervisor + VM)
→ Not ideal for large scale enterprise deployments

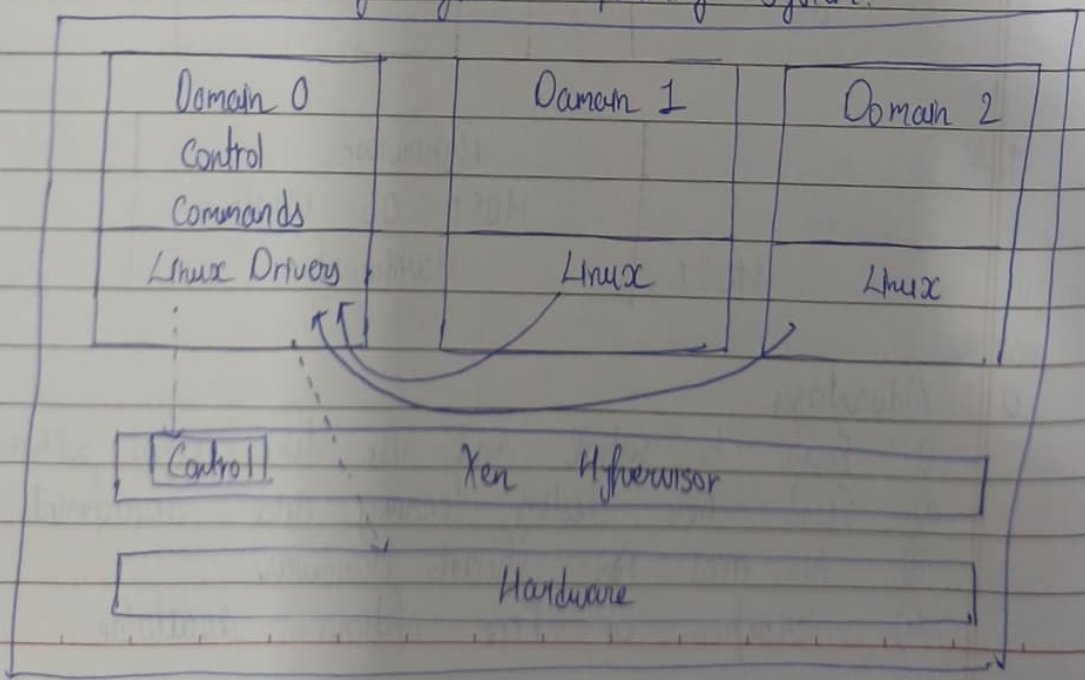
Q-7 Describe Virtual Cluster

Ans See Image

Q-8 Discuss Xen in brief

Ans Xen is a type I hypervisor that creates logical pools of systems resources so that many virtual machine can share the same physical resources

→ Xen is a hypervisor that runs directly on the system hardware. It inserts a virtualization layer between the system hardware and virtual machines, turning the system hardware into a pool of logical computing resources that Xen can dynamically allocate to any guest operating system.



Virtual Clusters and Resource management

- Virtual clusters are built with VMs installed at distributed servers from one or more physical clusters.
- The VMs in a virtual cluster are interconnected logically by a virtual network across several physical networks.

Properties of virtual clusters

- The virtual cluster nodes can be either physical or virtual machines. Multiple VMs running with different OSes can be deployed on the same physical node.
- A VM runs with a guest OS, which is often different from the host OS, that manages the resources in the physical machine, where the VM is implemented.
- The purpose of using VMs is to consolidate multiple functionalities on the same server. This will greatly enhance server utilization and application flexibility.
- VMs can be replicated in multiple servers for the purpose of promoting distributed parallelism, fault tolerance, and disaster recovery.
- The size (number of nodes) of a virtual cluster can grow or shrink dynamically, similar to the way an overlay network varies in size in a peer-to-peer (P2P) network.
- The failure of any physical nodes may disable some VMs installed on the failing nodes. But the failure of VMs will not pull down the host system.

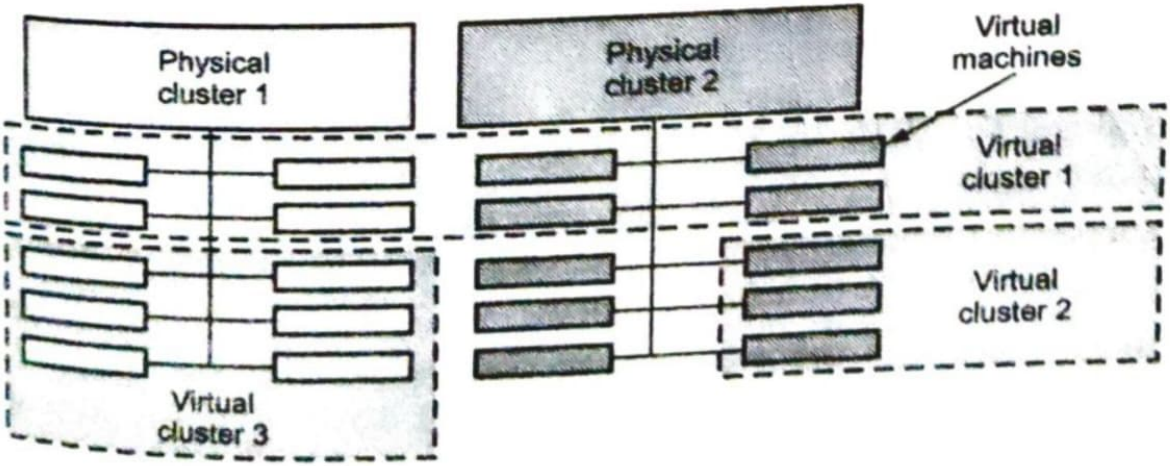


Fig. 3.6.1 cloud platform example with three virtual clusters over two physical clusters

→ Xen provides a virtual environment located between the hardware and the OS
→ Xen doesn't include any device drivers; it provides a mechanism by which a guest-OS can have direct access to the physical devices
→ The core components of Xen are the hypervisor, kernel and applications. Many guest operating systems can run on the top of the hypervisor; but it should be noted that one of these guest OS controls the others

Q-3 Explain the following terms
1) Hardware Virtualization
2) Multi-tenant
3) Autonomic Computing

Ans 1) Hardware Virtualization
→ The process of creating virtual versions of physical hardware components like servers, storage devices or network resource using software

2) Multi-tenant
→ An architecture where a single instance of software serves multiple customers (tenants), with each tenants data and configuration kept isolated and secure

3) Autonomic Computing
→ Computer systems that can manage themselves automatically with minimal human intervention, similar to how the human autonomic nervous system controls breathing without conciens thought.

3.7 Virtualization for Data Center Automation

- Data centers have grown rapidly in recent years, and all major IT companies are pouring their resources into building new data centers. Data Centers are specialized environments that safeguard company's most valuable equipment and intellectual property.
- The data center infrastructure is central to the IT architecture, from which all content is sourced or passes through. Proper planning of the data center infrastructure design is critical, and performance, resiliency, and scalability need to be carefully considered.
- Data center automation is the process by which routine workflows and processes of a data center, scheduling, monitoring, maintenance, application delivery are managed and executed without human administration.
- Data-center automation means that huge volumes of hardware, software, and database resources in these data centers can be allocated dynamically to millions of Internet users simultaneously, with guaranteed QoS and cost effectiveness.
- Data center automation increases agility and operational efficiency. It reduces the time IT needs to perform routine tasks and enables them to deliver services on demand in a repeatable, automated manner. These services can then be rapidly consumed by end users.
- Why data center automation is important
  a) Delivers insight into server nodes and configurations
  b) Automates routine procedures like patching, updating, and reporting
  c) Produces and programs all data center scheduling and monitoring tasks
  d) Enforces data center processes and controls in agreement with standards and policies

Difference Between Type 1 and Type 2

Feature	Type 1 Hypervisor (Bare-Metal)	Type 2 Hypervisor (Hosted)
Installation	Installed directly on the physical hardware	Installed on top of an existing operating system
Hardware Access	Direct access to hardware resources	Accesses hardware resources through the underlying OS
Performance	Higher performance	Lower performance due to additional layer
Security	More secure as isolated from the OS	Less secure as vulnerabilities in the OS can impact VMs
Management Complexity	More complex due to lower-level interaction	Easier to manage as it leverages existing OS tools
Compatibility	Limited due to specific hardware drivers needed	Broad - as it runs on top of a standard OS
Cost	More expensive due to commercial licensing	Can be free or open-source (limited features)
Best suited for	Enterprise environments with high performance and security requirements	Development, testing environments, or personal use on individual workstations

Difference Between Single-Tenant and Multi-Tenant Applications

Feature	Single-Tenant Application	Multi-Tenant Application
Definition	Each customer (tenant) gets a **separate** application instance and database.	Multiple customers share the **same** application instance and database with logical separation.
Isolation	**High isolation** – data and resources are not shared.	**Low/Moderate isolation** – tenants share infrastructure.
Customization	Highly customizable for each customer.	Limited customization (shared architecture).
Security	Strong security because data is fully isolated.	Good security but needs strong measures to prevent data leakage across tenants.
Cost	Higher cost (separate resources per tenant).	Lower cost (resources shared across tenants).
Maintenance	More maintenance (update each tenant separately).	Easier maintenance (one update applies to all tenants).
Scalability	Harder to scale – must scale each tenant separately.	Highly scalable – adding new tenants is easy.
Examples	Dedicated ERP for a company, private cloud apps, on-premise CRM.	Gmail, Salesforce, Zoom, Office 365.

Short Note on KVM

KVM (Kernel-based Virtual Machine) is an open-source virtualization technology built into the **Linux kernel**. It turns the Linux operating system into a **Type-1 (bare-metal) hypervisor**, allowing multiple virtual machines to run on a single physical server.

KVM uses **hardware-assisted virtualization** features such as Intel VT-x or AMD-V to achieve high performance.

Key Features

- **Full virtualization:** Each VM runs its own OS (Linux, Windows, etc.).
- **High performance:** Uses hardware virtualization and Linux kernel optimizations.
- **Strong security:** Inherits Linux security features like SELinux.
- **Scalable:** Supports large numbers of VMs on powerful servers.
- **Open-source and free:** Widely used in cloud platforms like OpenStack.

Components

- **QEMU:** Emulates hardware devices for VMs.
- **KVM kernel module:** Provides the virtualization capability.

Example Use

Cloud providers (like OpenStack-based private clouds) use KVM to create and manage multiple isolated virtual machines on a single server.

3.1.2 Load Balancing

- Load balancing can be defined as the process of task distribution among multiple computers, processes, disk or other resources in order to get optimal resource utilization and to reduce the computation time.
- Fig. 3.1.2 shows load balancing in cloud computing.

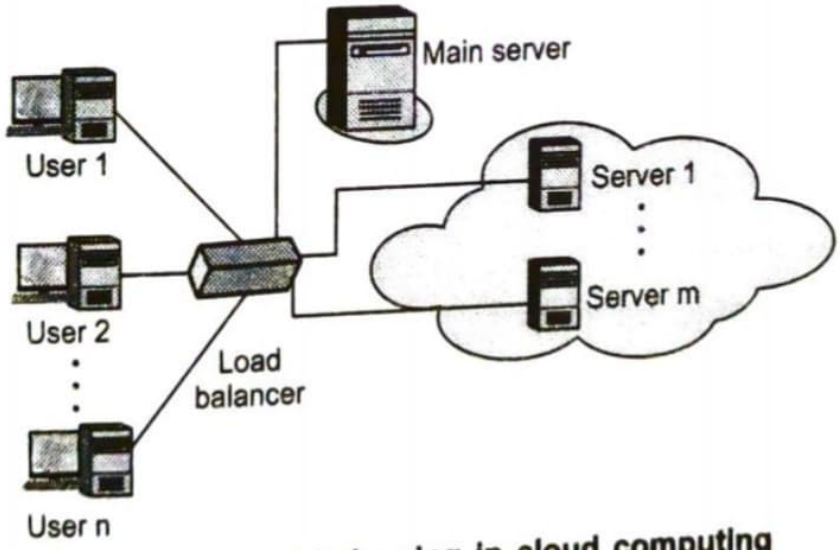


Fig. 3.1.2 Load balancing in cloud computing

- Load balancing is an important means to achieve effective resource sharing and utilization.
- Cloud load balancing is the process of distributing workloads and computing resources in a cloud computing environment. Load balancing allows enterprises to manage application or workload demands by allocating resources among multiple computers, networks or servers.
- The technology used to distribute service requests to resources is referred to as load balancing. Load balancing can be implemented in hardware.
- Google, Yahoo!, Amazon, and Microsoft experience millions of user hits per day. Across the web, sites experience a wide range of network traffic requirements.

- To handle such web requests, the sites use a technique known as load balancing, to share the requests across multiple servers.
- Load balancing uses a server to route traffic to multiple servers which, in turn, share the workload
- In general, load balancing algorithms can be divided into following three types :
  1. Centralized approach : In this approach, a single node is responsible for managing the distribution within the whole system.
  2. Distributed approach : In this approach, each node independently builds its own load vector by collecting the load information of other nodes. Decisions are made locally using local load vectors. This approach is more suitable for widely distributed systems such as cloud computing.
  3. Mixed approach : A combination between the two approaches to take advantage of each approach.
- Load balancing is an optimization technique; it can be used to increase utilization and throughput, lower latency, reduce response time and avoid system overload.
- The following network resources can be load balanced :
  a. Network interfaces and services such as DNS, FTP and HTTP
  b. Connections through intelligent switches
  c. Processing through computer system assignment
  d. Storage resources
  e. Access to application instances
- Without load balancing, cloud computing would very difficult to manage. Load balancing provides the necessary redundancy to make an intrinsically unreliable system reliable through managed redirection. It also provides fault tolerance when coupled with a failover mechanism.

Q-10 Explain about Virtualization in context of data center automation

Ans See Image

Q-11 Difference between type-1 and type-2 Hypervisors

Ans See Image

Q-12 Difference between Single Tenant and Multi-tenant Applications

Ans See Image

Q-13 Write a short note on KVM

Ans See Image

Q-14 Explain in brief about the load balancing in cloud computing

Ans See Image

Q-15 What are the various types of virtualizations

Ans 1) CPU virtualization
→ Converts physical CPU → multiple vCPUs
→ Allows multiple VMs to run independently on same processor
→ Managed by hypervisor using CPU scheduling

2) Memory Virtualization
→ Creates a virtual view of memory for each VM
→ Each VM believes it has its own RAM
→ Hypervisor maps VM memory → physical memory
→ Enables memory over commitment

3) Storage Virtualization
→ Combines multiple physical storage into one unified storage pool
→ VM's see virtual disks, not physical ones
→ Supports snapshots, cloning, thin provisioning

4) Network Virtualization
→ Creates virtual network, switches, NIC's and routers inside a VM environment
→ Allows VMs to communicate over isolated virtual networks

5) I/O Virtualization
→ Shares physical I/O devices (disk, NIC, USB) between VMs
→ Hypervisor handles interrupts and device requests
→ Improve performance using techniques like SR-IOV

6) Desktop Virtualization
→ Allow a user to run a Virtual Desktop remotely (VDI)
→ Eg: Windows Virtual Desktop

7) Application Virtualization
→ Runs applications in isolated containers without installing them on OS

3) Monitoring & Optimization Phase
→ Monitor CPU, memory, storage, network, logs and cost
→ adjust VMs, autoscaling rules or storage types
→ Enable alerts, backups and disaster recovery

Q-13 Write about Application porting in cloud [3 times]

Ans Application porting means moving an existing application from one environment to another environment without changing its main functionality

1) Local Server → Cloud
2) One cloud provider → Another cloud provider, or
3) Old OS/Platform → New OS/Platform

o Need
1) To use cloud benefits (scalability, cost saving)
2) To upgrade to modern platforms
3) To migrate from outdated hardware
4) To improve performance or security

o Steps of Application Porting
1) Analyze the existing application
→ Check OS, programming language, dependencies, database, libraries etc
2) Identify cloud requirements
→ Choose required VM size, OS, runtime or PaaS tools
3) Modify Configuration
→ Update environment variables, libraries, database connection to match the new platform

4) Test in new environment
→ Ensure the application runs correctly and performs well
5) Deploy & Monitor
→ Launch the application on cloud and verify performance

Example
→ Suppose a company has a website running on local server using
OS: Windows, Web Server: Apache, Database: My SQL

→ To move this website to AWS cloud, the company performs following application porting:
1) Creates an AWS EC2 instance
2) Installs Apache, PHP and My SQL
3) Uploads website files
4) Updates database configuration
5) Runs and tests the website in the cloud

After porting, the same website runs on AWS without changing its main code

Ch-4 Cloud Infrastructure and Cloud Resource Management.

Q-1 Describe dynamic resource allocation in cloud?

Ans Dynamic resource allocation is a cloud computing technique where computing resources such as CPU, memory, storage and bandwidth are automatically assigned or adjusted based on the current workload or user demand.

In this method, resources are scaled up when demand increases and scaled down when demand decreases. This process is usually managed by cloud platforms using virtualization, monitoring tools, and automation policies.

Importance
1) Efficient Utilization of resources
2) Cost Optimization
3) Improved Performance
4) High Availability

Q-2 What is SLA? Why it is important? [S-24, S-25, W-24]

Ans A Service Level Agreement (SLA) is a formal contract between a cloud service provider and the customer that defines the level of service the provider will deliver.

It specifies measurable metrics like availability (uptime), performance, response time, data security, duties and responsibilities of both parties

Why is SLA important?
SLA is important because:-
1) Defines clear expectations
→ Users know exactly what performance, uptime (eg 99.9%) and service quality they will receive

2) Protects the customer
→ If the cloud provider fails to meet the promised service levels, customers may receive penalties, refunds, or credits

3) Improves trust and transparency
→ SLA builds confidence between the user and provider by clearly stating roles, responsibilities and guarantees

4) Helps in monitoring and management
→ Users can measure whether the cloud provider is delivering services as agreed.

Q.3 Write about Emerging cloud management standards

Ans 1) Open Cloud Computing Interface (OCCI)
→ Developed by Open Grid Forum (OGF)
→ A standard API for managing cloud resources such as compute, storage and network
→ Help manage IaaS services across different cloud providers
→ Ensures interportability between public, private & hybrid clouds

Service Level Agreement (SLA) in Cloud Computing – Long Answer

A **Service Level Agreement (SLA)** is a formal contract between the **cloud service provider (CSP)** and the **cloud consumer** that defines the level of service expected during the usage of cloud resources. It is one of the most critical components of cloud computing because it ensures transparency, trust, accountability, and measurable performance guarantees.

An SLA clearly specifies the **services offered**, **performance metrics**, **security responsibilities**, **penalties**, **support mechanisms**, and **obligations** of both parties. SLAs help customers evaluate whether the cloud provider meets business and technical requirements.

---

1. Purpose of SLA

The main goals of SLA in cloud environments are:

- To ensure **predictable and measurable service quality**.
- To define **roles and responsibilities** of provider and user.
- To outline **performance targets** and how they will be monitored.
- To protect users from service failures through **penalties or compensation**.
- To enable long-term trust and stable service delivery.

4.3.2 Emerging Cloud Management Standards

- The following working groups produce the standards and technologies promoted by the cloud management initiative :
  1. **Cloud Management Working Group (CMWG) :** Models the management of cloud services and the operations and attributes of the cloud service lifecycle through its work on the Cloud Infrastructure Management Interface (CIMI).

2. **Cloud Auditing Data Federation Working Group (CADF) :** Defines the CADF standard, a full event model anyone can use to fill in the essential data needed to certify, self-manage and self-audit application security in cloud environments.
3. **Software Entitlement Working Group (SEWG) :** Focuses on the interoperability with which software inventory and product usage are expressed, allowing the industry to better manage licensed software products and product usage.
4. **Open Virtualization Working Group (OVF) :** Produces the OVF standard, which provides the industry with a standard packaging format for software solutions based on virtual systems.

2) Open Virtualization Format (OVF)
→ A DMTF standard for packaging and distributing virtual machines
→ Makes VM images portable across platforms like VMware, Virtualbox, KVM, Xen.
→ Simplifies migration between cloud providers

3) Cloud Infrastructure Management Interface (CIMI)
→ Developed by Distributed Management Task Force (DMTF)
→ Provides a common model and API to manage cloud infrastructure
→ Supports operations like provisioning, monitoring and lifecycle management
→ Help avoid vendor lock-in because it works across many cloud services

4) Topology and Orchestration Specification for Cloud Applications (TOSCA)
→ Developed by OASIS
→ Describes application architecture and how it should be deployed in cloud.
→ Helps automate deployment, scaling and orchestration of complex ~~architect~~ applications
→ Provides multi-cloud portability

5) Cloud Auditing Data Federation (CADF)
→ Also developed by DMTF
→ Provides a standard format for audit logs and monitoring data in cloud environments
→ Ensures consistent security and compliance reporting across different clouds

6) Simple Cloud Identity Management (SCIM)
→ A standard for managing user identities across cloud apps
→ Helps in user provisioning, de-provisioning, authentication and access control
→ Widely used in SaaS applications and enterprise cloud services

7) NIST Cloud Computing Standards
→ The National Institute of Standards & Technology provides guidelines and framework for
- Cloud Architecture
- Security Policies
- Performance and service measurement
- Interferability and portability

NIST standards are widely adopted by government and enterprise users

Q-4 Explain the architectural design of compute and storage clouds

Ans → Major design goals of a cloud computing platform is Scalability, virtualization, efficiency and reliability
Cloud supports Web 2.0 applications
→ Cloud Management Layer
→ Cloud management receives user requests and identifies the required resources
→ It uses provisioning services to allocate compute or storage resources in cloud
→ Must support both physical and virtual machines

2) Scalable and Efficient Infrastructure
→ Cloud platforms use large-scale HPC (High Performance Computing) Infrastructure
→ Hardware and Software are combined for easy and efficient operation
→ Scalability benefits from cluster architecture to handle many users simultaneously
→ Multitasking is essential to support distributed system performance

3) Performance Metrics
1) System throughput & efficiency
2) Multitasking scalability
3) System availability
4) Security Index
5) Cost-effectiveness

4) Enabling technologies
→ Broadband Internet, wireless networking, declining storage cost, and improved software drive cloud adoption
→ Resource Virtualization enables rapid deployment and disaster recovery
→ SOA (Service-Oriented Architecture) and Web 2.0 standard supports SaaS delivery

5) Dynamic Resource Planning
→ Users can demand more capacity at peak times
→ Providers increase utilization using multiplexing, virtualization and dynamic provisioning
→ Unneeded capacity can be removed to reduce cost

4) Data Center Infrastructure
→ Cloud resources are hosted in large data centers owned by third party vendors
→ Consumers access services without needing to know the underlying technology

5) What is cloud Resource Management? Explain inter cloud resource management with its challenges
[W-22, S-23, W-24]

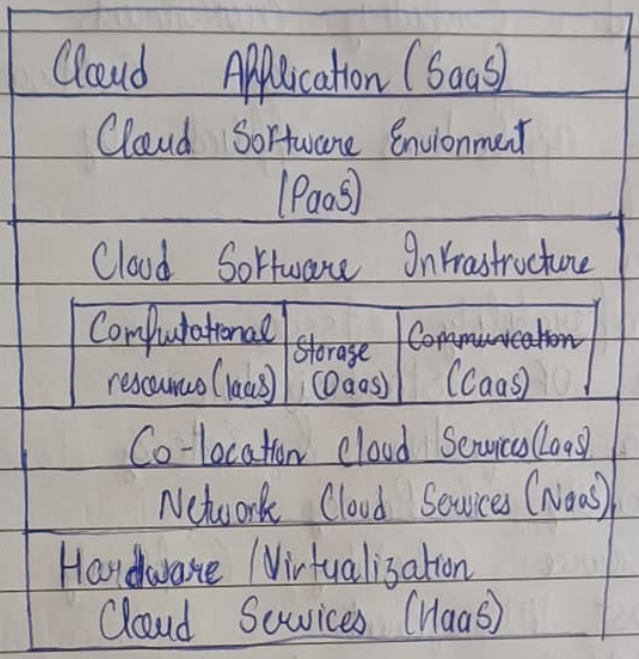
Ans Cloud Resource Management is the process of allocating, monitoring, optimizing and controlling cloud resources such as CPU, memory, storage, bandwidth and Virtual Machines to ensure efficient operation.

It ensures:
→ Applications get the required resources
→ Workload is balanced
→ Cost is minimized
→ Performance and availability are maintained.

Cloud providers use Virtualization, auto-scaling, load balancing and monitoring tools to manage resources dynamically based on demand

Inter Cloud Resource Management
→ The inter cloud is a cloud of cloud constructed to support resource sharing between the clouds
→ The resources under the inter cloud environment are managed in distributed model without any central authority
→ The inter cloud communication and resource identification is a complex task.

→ The software agents are small piece of code that can be used to perform any task.
→ The agent models are applied to execute the tasks as small fragments for a specific requirement



→ The bottom most layer provides Hardware As a Service (HaaS). The next layer is for interconnecting all the hardware components, and is simply called Network as a Service (NaaS). Virtual LAN's fall within the scope of NaaS
→ The next layer up offers Location as a Service (LaaS) which provides a collocation service to house, power and secure all the physical hardware and network resources. The cloud infrastructure can be further divided into data as a service and Communication as a service in addition to Compute and Storage in IaaS
→ The top layer is for SaaS applications. For example, CRM is heavily practiced in business promotion direct sales and marketing services. CRM offered the first SaaS on the cloud successfully.

Q-6

Ans

1)
2)
3)
4)
5)
6)
7)
8)
9)

→ PaaS is provided by Google, Salesforce.com and FB, among others. IaaS is provided by Amazon, Windows Azure and RackRack among others

→ Runtime Support Services: As in cluster environment, there are also some runtime supporting services in the cloud computing environment.
Runtime support is software needed in browser-initiated applications applied by thousands of cloud customers

o Challenges
1) Interoperability Issues
2) Lack of Standarization
3) Data Migration & Latency
4) Security & Privacy
5) Resource Scheduling Complexity
6) Cost Management
7) SLA (Service Level Agreement) Conflicts
8) Management Overhead

Q-6 List down the advantages of inter Cloud or Cloud Brokering

Ans
1) Cost Optimization
2) Improved Performance
3) High Availability and Realiability
4) Avoids Vendor-Lock In
5) Better resource Utilization
6) Unified Management
7) Security & Compliance Support
8) Service Customizations
9) Flexibility & choice

3. Challenges in Inter-Cloud Resource Management

1. Interoperability Issues

Different clouds use different APIs, formats, VM images, and tools.

Hard to make them work together seamlessly.

2. Lack of Standardization

No universal standard for resource naming, monitoring, or security policies across clouds.

3. Data Migration & Latency

Moving large datasets between clouds is slow, expensive, and may cause delays.

4. Security & Privacy

Data is exposed while traveling between clouds.

Each cloud has different security rules → difficult to maintain uniform protection.

5. Resource Scheduling Complexity

Coordinating multiple clouds to assign CPU, memory, or VMs optimally is complex.

6. Cost Management

Different clouds have different pricing models.

Predicting and optimizing cost across clouds becomes difficult.

7. SLA (Service Level Agreement) Conflicts

Different providers offer different uptime, performance, and security guarantees.

Matching them is challenging.

8. Management Overhead

Monitoring, configuring, and controlling multiple clouds increases complexity.

List down the advantages of Inter Cloud or Cloud Brokering.

Here are the **advantages of Inter-Cloud / Cloud Brokering** in a clear, exam-friendly way:

Advantages of Inter-Cloud / Cloud Brokering

1. **Cost Optimization**
   Cloud brokers compare pricing across multiple cloud providers and select the most economical option for the required service.
2. **Improved Performance**
   Workloads can be placed on clouds that offer lower latency, better bandwidth, or faster compute depending on user location or application needs.
3. **High Availability & Reliability**
   If one cloud fails, services can automatically shift to another cloud—ensuring continuity.
4. **Avoids Vendor Lock-In**
   Users are not tied to a single provider; they can switch between clouds based on cost, features, or performance.
5. **Better Resource Utilization**
   Applications can scale across multiple clouds, allowing efficient use of compute, storage, and network resources.
6. **Unified Management**
   A cloud broker provides a single interface/dashboard to manage resources coming from different clouds (AWS, Azure, GCP, etc.).
7. **Security & Compliance Support**
   Brokers can ensure that the selected cloud meets the required security standards, policies, or regulatory needs.
8. **Service Customization**
   Brokers can bundle services from different providers and offer customized solutions (e.g., storage from one cloud, compute from another).
9. **Flexibility & Choice**
   Users get access to a wide range of services and configurations from multiple clouds through one broker.

Q.7 What do you mean by High Availability and Dynamic Resource Allocation in cloud Computing ?

Ans 1) High Availability means that cloud services and applications remain accessible and operational at all times, even if some components fail
Clouds providers achieve HA by using:
→ Redundant Servers and data centers
→ Load Balancing
→ Automatic failover mechanisms
→ Data Replication across regions

- Purpose:
  To ensure minimal downtime, continuous services and applications remain accessible and reliability for users

- Example
  → If one Virtual Machine or server crashes, another server automatically takes over without interupting the service

2) Dynamic Resource Allocation in Cloud Computing
→ It means allocating computing resources (CPU, memory, storage, network bandwidth) automatically based on demand
Cloud Systems constantly monitor workload and adjust resources as needed.

(scaling up)
- When workload increase → cloud allocates more resources
- When workload decrease → cloud releases unused resources (down)

Purpose: To ensure performance efficiency, avoid resource wastage, and reduce costs

Example:
During peak traffic, a cloud based web app automatically gets more instances to handle users; when traffic drops, extra instances are removed

Q-8 Enlist the design challenges of cloud Infrastructure and Resource Management

Ans
1) Scalability
2) Resource Provisioning
3) Heterogenity of Resources
4) Load Balancing
5) Fault Tolerance & High Availability
6) Energy Efficiency
7) Security & Privacy
8) Interoperability & Portability

Q-9

Design Challenges of Cloud Infrastructure & Resource Management

1. Scalability

- Ensuring the system can scale up/down automatically based on workload.
- Handling sudden spikes without degrading performance.

2. Resource Provisioning

- Allocating CPU, memory, storage, and network resources efficiently.
- Avoiding over-provisioning (wasting resources) or under-provisioning (performance issues).

3. Heterogeneity of Resources

- Managing varied hardware, virtualization technologies, and cloud services.
- Integrating different platforms (VMs, containers, GPUs, etc.).

4. Load Balancing

- Distributing workload evenly across servers.
- Preventing hotspots and ensuring optimal utilization.

5. Fault Tolerance & High Availability

- Designing systems that continue running even when components fail.
- Implementing redundancy, replication, and failover mechanisms.

6. Energy Efficiency

- Minimizing power consumption in data centers.
- Using energy-aware scheduling and resource allocation.

7. Security & Privacy

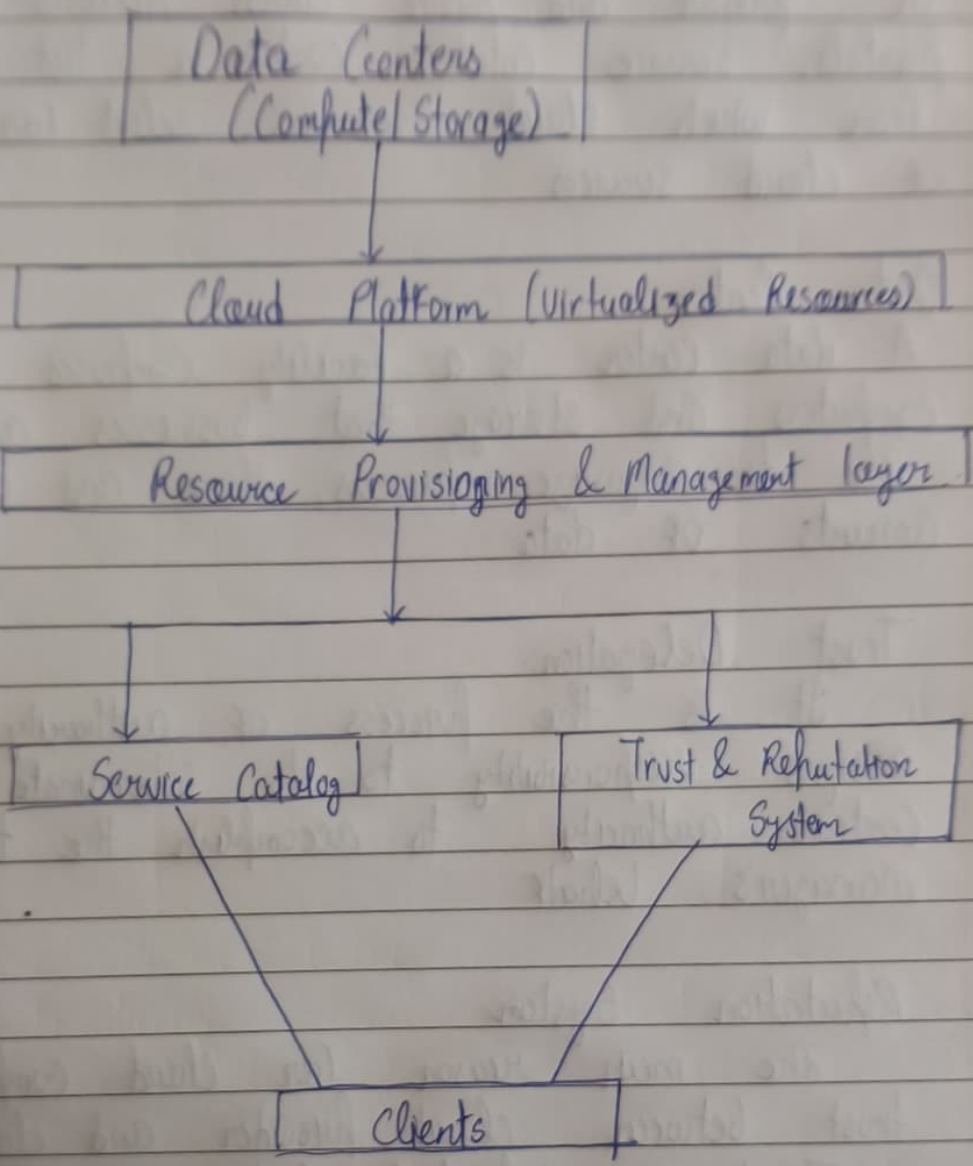
- Securing data, VMs, APIs, and communication between components.
- Ensuring access control, authentication, and compliance.

8. Interoperability & Portability

- Allowing applications to move across clouds (public, private, hybrid).
- Avoiding vendor lock-in.

7) Security & Privacy
8) Interoperability & Portability

Draw and Explain Generic Cloud Reference Architecture?



1) Clients
A client is a computer or a program that, as part of its operation, relies on sending a request to another program or a computer hardware or software that accesses a service made available by server (which may or may not be located on another computer)

2) Service Catalogs:
The use of service catalog for cloud computing services is an integral part of deploying services

on private and public clouds. Accessed by self-service portals, service catalogs contain a list of cloud services from which cloud consumers select for self-provisioning of cloud services

3) Data Center
A data center is a facility composed of networked computers and storage that businesses and other organizations use to organize, process, store and disseminate large amounts of data

4) Trust Delegation:
It is the process of authority wherein manager assigns responsibility to its subordinate along with the certain authority to accomplish the task on the manager's behalf

5) Reputation System
The main reason for cloud computing is to create trust between cloud provider and cloud consumer
Trust is important factor in cloud computing and it is mostly depending on observation of reputation and the self assessment by cloud providers

Ch-5 Security

Q-1 How are VPN dependable and secure? [S-24]

Ans
1) Strong Encryption
2) Secure Tunneling
3) Authentication and Authorization
4) Data Integrity Protection
5) IP Address Masking
6) Protection Against Cyber Attacks
7) Realiability through Redundancy
8) Centralized Policy Enforcement

Q-2 What are Digital Signatures [S-24] [W-24, S-25]

Ans A Digital Signature is a cryptographic technique used to validate the authenticity, integrity and non-rejudication of digital message or document.
→ It is electronic equivalent of a handwritten signature, but far more secure because it uses mathematical algorithm and encryption

Key Characteristics
1) Authentication
→ Confirms the identity of sender
→ Only the owner of private key could have generates the signature
2) Integrity
→ Ensures the message was not changed after signing
→ Even a small modification will cause verification to fail

3 Non - Refudiation
→ The sender cannot deny sending the message because only they hosses the private key used to generate the signature key

o Working
→ Sender creates a hash of message
→ Hash is encrypted with sender's private key, forming the digital signature
→ Reciever decrypts the message using the sender's public key
→ If both matches hash, the message is valid and unchanged.

o Applications
1) Secure emails & docs
2) Banking
3) E-governance services
4) Software/code Signing
5) Digital Certificates and SSL

Q-3 Name few common threats and vulnerabilities in cloud? [S-24]

Ans
1) Data Breaches
2) Data Loss
3) Insecure APIs
4) Account Hijacking
5) Insider threats
6) Denial of Service Attacks
7) Malware Injection
8) Misconfiguration

How are VPN secure and dependable?

Here is a **clear, concise, exam-ready explanation** of **How VPNs are secure and dependable** (perfect for 4–6 marks).

How VPNs Are Secure and Dependable

A **Virtual Private Network (VPN)** provides secure and reliable communication over an untrusted public network like the Internet. It achieves this through encryption, authentication, tunneling, and traffic protection mechanisms.

---

1. Strong Encryption (Confidentiality)

VPNs use strong encryption algorithms like **AES-256**, **IPSec**, or **SSL/TLS** to protect data.
Even if attackers intercept the traffic, they cannot read it.
This ensures **data privacy**.

---

2. Secure Tunneling

VPNs create an encrypted **tunnel** between the user and the VPN server.
Protocols such as **OpenVPN, IPSec, L2TP, and IKEv2** wrap data inside secure packets.
This prevents eavesdropping and ensures safe transmission over public networks.

---

3. Authentication and Authorization

VPNs verify user identity using:

- Passwords
- Digital certificates
- Multi-factor authentication

This ensures **only authorized users** can connect, making the network dependable and protected from intruders.

---

4. Data Integrity Protection

VPNs use hashing techniques like **HMAC** and **SHA-256** to ensure that data is not altered during transmission.
If someone tries to modify the packets, the VPN detects it immediately.
This ensures **integrity and trustworthiness**.

---

5. IP Address Masking

VPNs hide the user's real IP address and replace it with the VPN server's IP.
This protects identity, location, and prevents direct attacks on the user's device.

---

6. Protection Against Cyber Attacks

VPNs defend against:

- Man-in-the-middle attacks
- Packet sniffing
- Spoofing
- Session hijacking

Because attackers cannot decrypt or modify the traffic.

---

7. Reliability Through Redundancy

Enterprise VPNs use:

- Multiple servers
- Failover mechanisms
- Load balancing

This ensures **high availability**, stable performance, and dependable connectivity even if one server fails.

---

8. Centralized Policy Enforcement

Organizations can apply:

- Firewall rules
- Access control
- Logging and monitoring
- Traffic filtering

This ensures consistent security for all remote users.

Common Threats and Vulnerabilities in Cloud Computing

1. Data Breaches

Unauthorized access to sensitive data stored in the cloud.

2. Data Loss

Accidental deletion, hardware failures, or malicious attacks leading to permanent loss of data.

3. Insecure APIs

Poorly designed or unsecured APIs expose cloud services to attacks like injection and misuse.

4. Account Hijacking

Attackers steal login credentials and gain unauthorized access to cloud resources.

5. Insider Threats

Employees or authorized users misuse their access intentionally or accidentally.

6. Denial of Service (DoS/DDoS) Attacks

Overloading cloud servers, making services unavailable.

7. Misconfiguration

Incorrect settings (public buckets, open ports, weak IAM rules) lead to vulnerabilities.

8. Malware Injection

Malicious code or VMs injected into cloud services to steal data or disrupt operations.

Q-4 Briefly Explain steps to implement identity management and access control mechanisms [4 times]

Ans AWS Identity and Access management (IAM) is a web service that helps you securely control access to AWS resources

→ When you first create an AWS account, you begin with a single sign-in identity that has complete access to all AWS services and resources in the account. This identity is called the AWS account root user and is accessed by signing in with email address and password that you create for account.
→ For each AWS account, you can create multiple users with different credentials. For each user, you can give different rights.

IAm Users: are account objects that allow an individual user to access your AWS environment with a set of credentials. You can issue user accounts to anyone you want to view or administer objects and resources within your Environment. Permission can be applied to a user individually, but the best practice for permission assignments is to assign them via the use of groups

IAm groups: are objects that have permissions assigned to them via policies allowing the members of the group access to specific resources. Having users assigned to these groups allows for a uniform approach to access management and control

IAM roles: are again objects created within IAM which have policy permissions to them. However, instead of being associated with users as groups are, roles are assigned to instance to adopt the permissions given by the role without the need to have access keys stored locally on the instance

→ Security groups are used to control access to EC2 instances Because AWS users Not layers 3, any instance within a user account can communicate with any other instance

- AWS Identity Access Management allows to establish access rules and permissions to specific users & applications
  1) Set up permissions for users and applications
  2) Create user groups for common rules assignment
  3) Cloud trail allows to monitor the access
  4) Identity Federation: allows users to log in with their company credentials
  5) Temporary Security Credentials, obtained by calling AWS STS APIs like AssumeRole or GetFederationToken

Q5 Describe Data Security in Cloud

Ans Data Security in cloud computing refers to the set of policies, technologies, and controls used to protect data stored, processed and transmitted over cloud environments.

→ Since cloud data resides outside an organizations physical premises, strong security measures are essential to prevent unauthorized access, misuse or loss

1) Data Confidentiality
2) Data Integrity
3) Data Availability
4) Secure Storage & Transmission
5) Access Control & Monitoring

Q-6 Write Cloud Security Challenges?

Ans 1) Data Protection
Securing your data both at rest and in transit

2) User Authentication
Limiting access to data and monitoring who access data

3) Disaster and Data Breach
Contingency Planning

See Image For more

Q-7 Discuss Disaster Recovery Cloud

Ans Business Continuity (BC) is more proactive and generally refers to processes and procedures an org. must implement to ensure that mission-critical function can continue during and after a disaster. BC involves more comprehensive planning geared towards long term challenges to an organizations success
→ Disaster Recovery is more reactive and comprises specific steps an organization must take to resume operations following an incident. Disaster recovery actions take place after the incident and response times can range from seconds to days.

1) Data Confidentiality

- Ensures that only authorized users can access the data.
- Achieved using encryption (AES, RSA), access control, passwords, and multi-factor authentication.
- Prevents unauthorized access even if data is intercepted.

2) Data Integrity

- Ensures that data is not changed, corrupted, or tampered during storage or transmission.
- Uses hashing algorithms (SHA), digital signatures, and checksums.
- Maintains accuracy and trustworthiness of cloud data.

3) Data Availability

- Ensures that data is accessible anytime without interruption.
- Achieved using backups, replication, redundant storage, and disaster recovery.
- Protects against hardware failures, outages, and accidental deletion.

4) Secure Storage & Transmission

- Data is encrypted both **at rest** (stored) and **in transit** (during transfer).
- Secure protocols like HTTPS, SSL/TLS, and IPSec ensure safe communication.
- Prevents eavesdropping and MITM attacks.

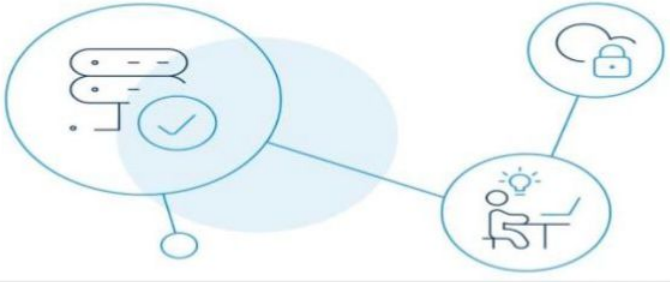
5) Access Control & Monitoring

- Role-based access control (RBAC) limits who can access what.
- Continuous monitoring and logging help detect suspicious activity.
- Regular audits ensure compliance with security policies.

Cloud Security Challenges and Risks

Cloud computing security challenges fall into three broad categories:

1. **Data Protection**:
   Securing your data both at rest and in transit.
1. **User Authentication**:
   Limiting access to data and monitoring who access the data.
1. **Disaster and Data Breach:**
   Contingency Planning



Data Protection

Cloud data protection practices leverage tools and techniques for the purpose of protecting cloud-based corporate data. These practices should provide coverage for all data, including data at-rest and data in-transit, whether the data is located in an in-house private store or managed by a third-party contractor.

Due to the above-mentioned challenged, the Cloud Security Alliance has given recommendations in protecting sensitive data. These simple yet strong recommendations are the following:

- *Sensitive data should be encrypted before it is transmitted from the organization to the cloud service provider.*
- *Sensitive data should be encrypted in use, at rest and in transit.*
- *The decryption keys should never be accessible to the cloud service provider and its staff.*
- *Sensitive data should be encrypted with random, long keys and approved algorithms.*

Although there are cloud storage security issues when it comes to encryption, it still remains the top tool for data protection.

User Authentication

- Cloud computing is helping businesses to store a large amount of data at relatively low costs but it is essential these service providers offer methods to ensure users are authenticated.
- Data resting in the cloud needs to be accessible only by those authorized to do so, making it critical to both restrict and monitor who will be accessing the company's data through the cloud. In order to ensure the integrity of user authentication, companies need to be able to view data access logs and audit trails to verify that only authorized users are accessing the data.
- ***The purpose of cloud-based authentication is to protect companies from hackers trying to steal confidential information. Cloud authentication allows authorized users across networks and continents to securely access information stored in the cloud with authentication provided through cloud-based services.***

Disaster and Data Breach

What is a data breach?

It is an accident in which the information is accessed and extracted without authorization. This event usually results in a data leak .

- No matter how well-prepared your organization is, disaster can strike at any time. Perhaps a single employee makes an honest mistake or a hacker with a revolutionary new method targets your servers.
- Data breaches are more than just a scenario that haunts your IT department's nightmares, they are very real and cost your organizations both money and credibility - which is why preparation is key.

Disaster and Data Breach

According to a survey by Ermetic, nearly 80% of businesses have experienced at least one cloud data breach in the last 18 months, while 43% of businesses report more than 10 breaches.

According to the 300 CISOs surveyed, the three biggest causes of breaches were:

- Security configuration errors (67%)
- Lack of adequate visibility into access settings and activities (64%)
- Identity and access management (IAM) and permission errors (61%)

1) Data Confidentiality
2) Data Integrity
3) Data Availability
4) Secure Storage & Transmission
5) Access Control & Monitoring

Q.6 Write Cloud Security Challenges?

Ans 1) Data Protection
Securing your data both at rest and in transit

2) User Authentication
Limiting access to data and monitoring who access data

3) Disaster and Data Breach
Contingency Planning

See Image For more

Q.7 Discuss Disaster Recovery Cloud

Ans Business Continuity (BC) is more proactive and generally refers to processes and procedures an org. must implement to ensure that mission-critical function can continue during and after a disaster. BC involves more comprehensive planning geared towards long term challenges to an organizations success
→ Disaster Recovery is more reactive and confesses specific steps an organization must take to resume operations following an incident. Disaster recovery actions take place after the incident and response times can range from seconds to days.

→ Disaster Recovery is a piece of business continuity Planning and concentrates on accessing data easily following a disaster

→ These practices enable an organization to get back on its feet after problems occur and improve operations while decreasing the chance of emergencies

Q-1 Discuss Disaster Recovery Plan

→ Disaster Recovery plan is a plan designed to recover all the vital business during a disaster with in a limited amount of time. This plan has all the procedures required to handle the emergency situations

→ A disaster recovery process should have provable recovery capability and hence it provides the most efficient method to be adopted immediately after a disaster occurs

→ Mostly the DRP has technology oriented methodologies and concentrates on getting the systems up as soon as possible, within a reasonable amount of time.

→ Recovery Time Objective (RTO) & Recovery Point Objective (RPO) are the targets of DRP

→ The most successful disaster recovery strategy is one that will never be implemented, therefore, risk avoidance is a critical element in disaster recovery process

Q-2 Write a short note on data security and application security

Ans 1) Data Security in Cloud

Data Security refers to protecting cloud-stored and cloud processed data from unauthorized access, modification and loss

Because data resides on shared servers, strong security measures are required.

Key Points
1) Confidentiality
2) Integrity
3) Availability
4) Secure Storage & Transmission
5) Access Control

2) Application Security in Cloud
→ Application security ensures that cloud-based applications operate safely without vulnerabilities that attackers can exploit.
→ Cloud apps face risks from insecure code, weak APIs and improper configuration.

Key Points:
1) Secure Coding Practices
2) API security
3) Authentication & Authorization
4) Vulnerability Scanning
5) Web Application Firewall (WAF)

Q-9 Describe the Identity Management lifecycle

Ans The Identity Management lifecycle refers to the complete process of creating, managing, controlling and removing user identities within an organization or cloud environment.

1) Data Security in Cloud

Data security refers to protecting cloud-stored and cloud-processed data from unauthorized access, modification, and loss. Because data resides on shared servers, strong security measures are required.

Key Points:

- **Confidentiality:**
  Data is protected from unauthorized users using encryption (AES, RSA), access controls, and multi-factor authentication.
- **Integrity:**
  Ensures data is not altered during storage or transmission.
  Uses hashing (SHA), digital signatures, and checksums to detect tampering.
- **Availability:**
  Data should be accessible anytime. Achieved using backups, replication, disaster recovery, and redundant storage.
- **Secure Storage & Transmission:**
  Data is encrypted both **at rest** and **in transit** with SSL/TLS, HTTPS, and IPSec.
- **Access Control:**
  RBAC, IAM policies, logging, and continuous monitoring prevent unauthorized access.

2) Application Security in Cloud

Application security ensures that cloud-based applications operate safely without vulnerabilities that attackers can exploit. Cloud apps face risks from insecure code, weak APIs, and improper configuration.

Key Points:

- **Secure Coding Practices:**
  Applications must be developed using safe coding techniques to avoid SQL injection, XSS, and buffer overflow attacks.
- **API Security:**
  Most cloud apps rely on APIs.
  APIs must have strong authentication, input validation, rate limiting, and encryption to prevent misuse.
- **Authentication & Authorization:**
  Uses IAM, OAuth, MFA, and RBAC to ensure only authorized users access the application.
- **Vulnerability Scanning:**
  Continuous scanning and patching fix software bugs and security holes.
- **Web Application Firewalls (WAF):**
  Protects cloud applications from common web attacks by filtering harmful traffic.

The lifecycle has following stages:
1) Identity Creation (Provisioning)
2) Identity Management (Maintenance/Update)
3) Identity Removal (De-Provisioning/Termination)

Q-10 Compare the types of identity Providers in detail

Ans See Image

1) SAML-based identity Providers
2) OAuth/OpenID Connect Identity Providers
3) Social Identity Providers
4) Enterprise/Corporate IP
5) Cloud IP

Q-11 Compare the models of encryption & key management in detail

Ans 1) Provider-Managed Keys
2) Customer-Managed Keys (CMK)
3) Customer-Supplied Keys
4) Hold your own Keys (HYOK)
5) Hybrid key Model

See Image

Q-12 Write a note on Vendor Lock-in with respect to Cloud Security Risk

Ans Vendor Lock-in refers to a situation cloud customer becomes

The **Identity Management (IdM) lifecycle** refers to the complete process of creating, managing, controlling, and removing user identities within a organization or cloud environment.
It ensures that the **right person gets the right access at the right time.**

The lifecycle has the following stages:

1) Identity Creation (Provisioning)

- The lifecycle begins when a new user (employee, student, customer) joins the system.
- An identity is created with a unique ID (username) and initial credentials.
- Basic access rights and roles are assigned based on job role or requirements.

2) Identity Management (Maintenance / Update)

- During this stage, the user continues to use the identity.
- Access permissions may change due to promotions, department changes, new responsibilities, or policy updates.
- Password resets, privilege updates, authentication changes, and access monitoring also happen here.

3) Identity Removal (De-provisioning / Termination)

- When the user leaves the organization or no longer needs access, their identity must be removed.
- Login credentials are disabled, roles revoked, and all access rights withdrawn.
- Prevents unauthorized access and protects sensitive data from former users.

Comparison of Identity Providers

Type of Identity Provider	Description	How it Works	Use Cases
1. SAML-based Identity Providers	Use SAML (Security Assertion Markup Language) for authentication. Mostly used in enterprises.	User requests access → IdP authenticates using SSO (Single Sign-On) → Sends SAML token to service provider.	Corporate logins, enterprise applications, employee access systems.
2. OAuth / OpenID Connect Identity Providers	Use OAuth 2.0 and OIDC for secure authorization and identity verification.	User logs in → IdP issues access token / ID token → App verifies the token to authenticate user.	Mobile apps, cloud apps, APIs, modern web applications.
3. Social Identity Providers	IdPs run by social platforms such as Google, Facebook, Apple, LinkedIn, etc.	Users authenticate using their social accounts → Identity provider sends verified profile details to the application.	Easy login for apps, websites, consumer services.
4. Enterprise/Corporate Identity Providers	Centralized identity systems used inside companies (e.g., Active Directory, LDAP).	User credentials stored in enterprise servers → Access provided based on roles and policies.	Internal networks, secure company systems, employee authentication.
5. Cloud Identity Providers	Identity services provided by cloud vendors like AWS IAM, Azure AD, Google Cloud IAM.	Authentication + access policies controlled through cloud platform → Tokens or keys used to access cloud resources.	Cloud-based applications, multi-cloud access control.

Comparison of Encryption & Key Management Models (4 Marks)

Model	Key Creation	Key Storage	Who Controls Keys?
1. Provider-Managed Keys	Created by CSP	Stored in CSP KMS	Cloud Provider controls everything
2. Customer-Managed Keys (CMK)	Created by Customer	Stored in CSP KMS	Customer controls key usage & rotation
3. Customer-Supplied Keys (BYOK)	Created offline by Customer	Imported to CSP KMS	Customer fully controls original key
4. Hold Your Own Key (HYOK)	Created by Customer	Stored on customer's on-prem HSM	Only Customer controls keys, CSP has zero access
5. Hybrid Key Model	Master key by Customer, data key by CSP	Split storage (Customer + CSP)	Shared control between CSP and Customer

making it difficult to move to another provider without significant cost, effort or technical challenges. It is considered a major cloud security and operational risk

See Image for more

Q-14 Write a short note on Identity Broker

Ans An Identity Broker is a service that acts as an intermediary between a user and multiple identity providers (IdPs). It helps users access different cloud applications without creating separate accounts for each service

- Key Points
  1) Mediates Authentication
  2) Supports Single Sign-On (SSO)
  3) Centralized Identity Management

See Image

Q-15 Discuss Autonomic Security Storage Area Networks in brief

Ans Autonomic Security Storage Area Networks refers to SAN systems that can protect, monitor and manage their own security automatically with minimal human intervention
→ The purpose of SAN is to allow multiple servers access to a pool of storage in which any server can potentially access any storage unit

Vendor Lock-in – Cloud Security Risk (Short Note / Long Note)

Vendor lock-in refers to a situation where a cloud customer becomes **dependent on a single cloud provider** for services, tools, or infrastructure, making it difficult to move to another provider without significant cost, effort, or technical challenges. It is considered a major **cloud security and operational risk**.

---

1. Meaning of Vendor Lock-in

When organizations deploy applications, store data, or use proprietary cloud services, they often rely on the provider's:

- APIs
- Data formats
- Storage systems
- Identity services
- Proprietary managed services (e.g., AWS Lambda, Azure Cosmos DB)

Over time, this tight dependency **reduces portability** and makes switching vendors very complex.

---

2. Why Vendor Lock-in is a Security Risk

Vendor lock-in affects security because:

a) Limited Control Over Security Measures

Different providers have different:

- encryption mechanisms
- key management tools
- identity management

  If an organization cannot switch providers easily, it may be forced to **accept security limitations** of that provider.

---

b) Restricted Data Portability

Data stored in proprietary formats may be:

- hard to export
- expensive to transfer
- slow to migrate
  This increases risks of:
- **Data loss**
- **Data exposure during migration**
- **Incomplete data deletion**

---

c) Dependency on Provider's Security Policies

Organizations must completely rely on the provider for:

- patch management
- updates
- vulnerability remediation
  If a provider experiences a breach or fails to meet security compliance, the customer has **no quick alternative**.

---

d) Higher Impact During Outages or Incidents

If the provider faces:

- service outage
- cyberattack
- region failure
  the customer cannot failover easily to another cloud.
  This reduces availability and resilience.

---

e) Compliance and Legal Risks

Different countries have different laws regarding:

- data residency
- audit requirements
- encryption standards
  If a cloud provider cannot meet new compliance needs, the organization remains **locked** and faces legal issues.

3. Factors Causing Vendor Lock-in

- Proprietary APIs and services
- Special programming interfaces
- Unique storage formats
- High data transfer costs (egress charges)
- Lack of interoperability between cloud platforms
- Dependence on provider's managed services (PaaS, serverless, databases)

---

4. Mitigation Strategies

Organizations can reduce vendor lock-in risks by:

1. Using **open standards** and **portable technologies** (Docker, Kubernetes).
2. Avoiding provider-specific services where unnecessary.
3. Storing data in **standard formats** (JSON, CSV, Parquet).
4. Using **multi-cloud** or **hybrid cloud** architectures.
5. Designing applications using **microservices** for easier migration.
6. Negotiating SLAs and exit clauses with providers.

---

5. Conclusion

Vendor lock-in is a significant cloud security risk because it limits an organization's ability to:

- switch providers
- maintain flexibility
- manage compliance
- ensure security independence

  Proper planning and adoption of open technologies can significantly reduce this risk.

If you want, I can convert this into a **2-mark, 4-mark, or 10-mark** version according to your exam format.

11. Write a short note on Identity broker. (3m)

Identity Broker – Short Note (3 Marks)

An **Identity Broker** is a service that **acts as an intermediary** between a user and multiple identity providers (IdPs). It helps users access different cloud applications without creating separate accounts for each service.

Key Points:

1. **Mediates Authentication**
   - The broker verifies the user's identity by communicating with trusted IdPs (like Google, Azure AD, or corporate LDAP).
   - It converts the authentication token into the format required by the target cloud service.
2. **Supports Single Sign-On (SSO)**
   - Users log in once, and the broker handles access to multiple applications.
   - This reduces login fatigue and enhances productivity.
3. **Centralized Identity Management**
   - Provides a single point to control user access, roles, and permissions across different cloud platforms.
   - Improves security by enforcing uniform policies and reducing identity duplication.

12. Discuss autonomic security storage area networks in brief (3m)

Autonomic Security in Storage Area Networks (SANs) – 3 Marks

Autonomic Security Storage Area Networks refer to SAN systems that can **protect, monitor, and manage their own security automatically**, with minimal human intervention. These SANs use the principles of autonomic computing — *self-configuration, self-healing, self-protection, and self-optimization* — to ensure secure storage operations.

Key Points:

1) Self-Protection Mechanism

The SAN continuously monitors for threats such as unauthorized access, abnormal data transfers, or suspicious patterns. It automatically blocks risky activities, enforces access control policies, and isolates compromised components.

2) Self-Configuration and Self-Healing

The system can automatically configure security settings like authentication, encryption, and zoning. If any security failure occurs (e.g., failed disk, corrupted data block), the SAN repairs or reconfigures itself without disrupting storage services.

3) Automated Policy Enforcement

Autonomic SANs apply security rules—like data encryption, user permissions, and audit logging—without manual effort. This reduces human errors, ensures consistent protection, and maintains compliance with security standards.

→ SAN consists of a communication infrastructure, which provides physical connections ; and a management layer, which organizes the connections, storage elements and computer systems so that the data transfer is secure and robust.

→ SAN consists of three main components : Servers, Network Infrastructure and Storage

Key Points
1) Self-Protection Mechanism
2) Self-Configuration and Self-Healing
3) Automated Policy Enforcement

Q-16 Write challenges to data security in cloud

Ans See Image

1) Data Breaches
2) Data Loss are Leakage
3) Insecure APIs and Interface
4) Insider threats
5) Multi-tenacy Risks
6) Lack of visibility and Control
7) Compliance and Legal Challenges
8) Data Remanence

Q-17 List the Cloud Security Risks and briefly explain them

Ans 1) Data Breaches
2) Data Loss and Data Unavailability
3) Insecure APIs and Interfaces

Misconfiguration of Cloud Resources
Multi-tenacy and Virtualization Risks
Insider threats
Account Hijacking and Identity Attacks
Compliance and Legal Issues
Denial of Service (DoS/DDoS) Attacks

Write challenges to data security in cloud.

Here is an **exam-ready answer** for:

Challenges to Data Security in Cloud

Data security in cloud computing faces several challenges due to shared infrastructure, remote storage, and multi-tenant environments. Ensuring confidentiality, integrity, and availability of data becomes complex. The major challenges are:

---

1. Data Breaches

Cloud data is stored over the Internet, making it a target for cyberattacks. Unauthorized access due to weak authentication, vulnerabilities, or misconfigurations can lead to large-scale data breaches.

---

2. Data Loss or Leakage

Data may be lost due to:

- accidental deletion
- hardware failures
- software errors
- malicious attacks (ransomware)
  Since data is stored remotely, recovery becomes harder if proper backups are not maintained.

---

3. Insecure APIs and Interfaces

Cloud services are accessed via APIs.
If APIs are:

- poorly designed
- not encrypted
- lack authentication
  attackers can exploit them to steal or modify data.

4. Insider Threats

Employees of the cloud provider or the customer may misuse access privileges. Insiders can intentionally:

- leak data
- modify sensitive information
- disable security controls

---

5. Multi-Tenancy Risks

Multiple users share the same physical hardware. Weak isolation between tenants may cause:

- data leakage
- side-channel attacks
- unauthorized access across virtual machines

---

6. Lack of Visibility and Control

In cloud, the provider controls most of the infrastructure. Customers may not know:

- where exactly data is stored
- which security controls are active
- how access is monitored

  This reduces transparency and security assurance.

---

7. Compliance and Legal Challenges

Different countries have different data privacy laws.
Storing data across borders can cause violations of:

- GDPR
- HIPAA
- PCI-DSS

  Meeting compliance requirements becomes difficult.

---

8. Data Remanence

Old or deleted data may remain in storage temporarily, leading to potential recovery by attackers if cloud storage is not securely wiped.

---

1. Data Breaches

Sensitive information stored in the cloud may be accessed by unauthorized users due to weak access controls, software vulnerabilities, or misconfigured storage.
Data breaches cause:

- loss of confidentiality
- financial penalties
- legal consequences

---

2. Data Loss and Data Unavailability

Data may be permanently lost due to accidental deletion, hardware failures, malicious attacks (e.g., ransomware), or natural disasters.
If the organization does not maintain proper backups or redundancy, recovery becomes extremely difficult, affecting business continuity.

---

3. Insecure APIs and Interfaces

Cloud platforms expose APIs for management and data access.
If APIs are not properly secured (no encryption, weak authentication, improper input validation), attackers can exploit them to:

- steal data
- modify configurations
- hijack services

---

4. Misconfiguration of Cloud Resources

This is one of the most common risks.
Examples include:

- publicly open storage buckets (e.g., S3)
- overly permissive IAM roles
- exposed databases
  Misconfigurations occur due to user error, lack of understanding, or poor security policies, leading to unintended data exposure.

5. Multi-Tenancy and Virtualization Risks

Cloud providers host multiple users (tenants) on the same physical hardware.
If isolation between virtual machines or containers fails, one tenant could access another tenant's data, leading to confidentiality breaches.

---

6. Insider Threats

Employees of cloud providers or the customer can intentionally or accidentally misuse their access rights.
Insiders may:

- leak data
- alter configurations
- disable security controls
  This makes insider threats dangerous and difficult to detect.

---

7. Account Hijacking and Identity Attacks

Attackers use phishing, malware, credential theft, or weak passwords to gain access to cloud accounts.
Once an account is hijacked, the attacker can:

- manipulate data
- impersonate users
- perform unauthorized operations
  This undermines authentication and access control mechanisms.

---

8. Denial of Service (DoS/DDoS) Attacks

Attackers flood cloud services with excessive traffic, making them unavailable to legitimate customers.
This affects availability, performance, and may cause financial loss due to increased resource consumption.

---

9. Compliance and Legal Issues

Cloud data may be stored across multiple countries with different data protection laws.
Organizations must meet standards such as:

- GDPR
- HIPAA
- PCI-DSS
  Non-compliance can lead to penalties and lega putes.

Date
Page

Ch-6 & Ch-7

Q-1 Write a Short note on Amazon SQS [5-2h, 4m]

Ans → Amazon SQS (Simple Queue Service)

Amazon SQS is fully managed message queing service provided by AWS that enables you to decouple and scale microserwises, distributed Systems and Serverless application

Key Features

1) Decoupling Components: SQS allows different parts of an application to Communicate asynchronously without being directly connected, improving realibility and Scalability

2) Scalability: Automatically Scales to handle any volume of messages without requiring provisioning or management

3) Rediabity: Messages are stored redundantly across multiple AWS availability zones, ensuring high durability and availability

- Two Queue Types

1) Standard Queues: Offer maximum throughput, best-effort ordering and at-least once delivery

2) Fifo Queues: Gurantee exactly once processing and preserwe order of message

Q-2 Write a brief overview of Google Cloud Management

Ans Google Cloud Management refers to the set of the tools, services and frameworks provided by Google Cloud Platform (GCP) to efficiently manage cloud resources, monitor performance, secure data and optimize overall operations

1) Centralized Management Through Google Cloud Console
2) Resource Automation Using Cloud Deployment Manager
3) Monitoring and Logging with Cloud Operations Suite
4) Identity and Access Management (IAM)
5) Cost Management and Billing tools
6) Security and Compliance Tools
7) Scalable Application Management with Kubernetes (GKE)

Q-3 Write a brief overview of Amazon AWS array of services

Ans 1) Compute Services
→ Amazon EC2 (Elastic Compute Cloud):
Virtual servers in the cloud with flexible sizing and configurations for running applications
→ AWS Lambda: Serverless computing that runs code in response to events without provisioning servers
→ AWS ECS/EKS: Container orchestration services for Docker containers and Kubernetes deployments

Google Cloud Management – Overview (7 Marks)

Google Cloud Management refers to the set of tools, services, and frameworks provided by **Google Cloud Platform (GCP)** to efficiently manage cloud resources, monitor performance, secure data, and optimize overall operations. It focuses on automation, scalability, centralized control, and cost-effective resource utilization. GCP offers a rich ecosystem that helps developers, administrators, and enterprises manage applications, networks, storage, and security from a unified interface.

1) Centralized Management Through Google Cloud Console

Google Cloud Console is a web-based dashboard that allows users to manage all cloud services in one place. It provides a graphical interface for launching VM instances, configuring networking, managing databases, and monitoring system health. It simplifies complex configurations through visual tools, making cloud management more intuitive and accessible for administrators.

2) Resource Automation Using Cloud Deployment Manager

Google's Deployment Manager is an Infrastructure-as-Code (IaC) tool used to create, configure, and deploy cloud resources using templates (YAML or Python). It automates large deployments, ensures consistency across environments, reduces manual errors, and enables repeatable resource provisioning. This is essential for managing scalable and distributed cloud applications.

3) Monitoring and Logging with Cloud Operations Suite

GCP offers a powerful monitoring system called **Cloud Operations Suite** (formerly Stackdriver). It includes:

- **Cloud Monitoring** – tracks CPU usage, latency, uptime, and service performance.
- **Cloud Logging** – stores logs from applications, VMs, containers, and network devices for analysis.
- **Error Reporting & Debugger** – helps identify and fix issues quickly.
  This suite ensures high reliability and facilitates proactive management of cloud workloads.

4) Identity and Access Management (IAM)

Google IAM provides fine-grained access control to cloud resources. Administrators can assign roles like Viewer, Editor, or Custom Roles to maintain security. IAM ensures the **principle of least privilege**, protecting resources from unauthorized access. Policies can be applied at project, folder, or organizational levels.

5) Cost Management and Billing Tools

Google Cloud provides detailed billing dashboards, cost breakdowns, and forecasting tools. Administrators can set budgets, get alerts for overspending, and optimize costs using recommendations from **Recommender AI**. GCP also offers sustained-use discounts and committed-use contracts that help control long-term expenses.

6) Security and Compliance Tools

GCP includes several built-in security services such as:

- **Cloud KMS** for encryption key management.
- **Cloud Armor** for DDoS protection.
- **Security Command Center** for vulnerability detection and threat analysis.
  These tools ensure data security, regulatory compliance, and protection against malware or cyber-attacks in cloud environments.

7) Scalable Application Management with Kubernetes (GKE)

Google Kubernetes Engine (GKE) enables automated orchestration of containers. It handles scaling, load balancing, upgrades, and failover with minimal manual intervention. GKE plays a major role in managing modern microservices-based applications and supports high-availability deployments.

3) Storage Services
→ Amazon S3 (Simple Storage Service) : Object Storage with high durability For backup, archiving and data lakes
→ AWS Glacier: Low cost archival storage For long-term data retention
→ Amazon EBS (Elastic Block Store): Persistent block storage volumes For EC2 instances
→ Amazon EFS (Elastic File System): Scalable, fully managed file storage For use with AWS cloud services

Database Services
→ Amazon RDS: Managed relational databases supporting MySQL, PostgreSQL, Oracle, SQL, Server and more

→ Amazon Aurora: High Performance MySQL and PostgreSQL compatible relational database

→ Amazon RedShift: Data Warehousing Service For analytics and business intelligence

4) Networking and Content Delivery
→ Amazon VPC : Isolated virtual networks For launching AWS resources
→ AWS Route 53: Scalable DNS and domain name registeration service
→ Amazon Cloud Front: Global Content delivery Network (CDN) For low latency content delivery.

5) Security, Identity and Access Management
→ AWS IAM : Control users access & permissions to AWS resources

→ AWS Shield: DDoS protection service for application
→ AWS WAF: Web app. firewall to protect against common exploits

6) Analytics & Machine Learning Services
→ Amazon Athena: For serverless SQL queries on S3 data
→ Amazon SageMaker: Build, train and deploy machine learning models at scale
→ Amazon EMR: Big data processing using Hadoop and Spark frameworks

7) Developer tools
→ AWS Cloud9: Cloud based integrated development environment (IDE)
→ AWS CodeBuild: Fully managed build service for compiling code and running tests.

Q-4 What is AWS auto scaling ?

Ans AWS Scaling refers to ability of Amazon Web Services to automatically increase or decrease computing resources based on the demand of an application. It ensures that applications always have the right amount of capacity - neither over-provisioned nor under-provision

1) Vertical & Horizontal Scaling
→ Vertical Scaling (Scale up/Down): Increasing or decreasing the power of a single instance (eg adding more CPU or RAM to an EC2 instance)
→ Horizontal Scaling (Scale out/In): Adding or removing multiple instances of same application to distribute load

2) Auto Scaling Feature
→ AWS provides Auto Scaling Groups (ASGs) which monitor application performance and automatically launch new instances when demand increases and terminate instances when demand drops. This ensures cost-efficiency and consistent performance

3) Benefits of Scaling
→ AWS scaling improves high availability, maintains optimal performance, and reduces operational cost by using pay-as-you-go resources based on real-time workloads

Q.5 What is Eucalyptus? Discuss in brief

Ans. Eucalyptus stands for "~~Eucalyptus~~ Elastic Utility Computing Architecture For linking your programs to useful systems"
→ It is used to build private, public and hybrid clouds
→ It can also produce your own data center into a private cloud and allow you to extend the functionality to many other organizations
→ Eucalyptus is open-source software for building AWS-compatible private and hybrid clouds. As an Infrastructure as a Service (IaaS) product, Eucalyptus allows your users to provision your compute and storage resources on-demand
o Eucalyptus has following key features
a) Supports for multiple users with help of single cloud
b) Support for Linux & Windows VMs
c) Accounting Reports

d) Use of WS-security to ensure secure communication between internal resources and processes
e) the option to configure policies and service level agreements based on users and environment
f) Provisions for graph, user management and security groups

Q-6 Write Features of Cloud Simulator

Ans 1) Virtualized Cloud Environment
2) Resource Management and Scheduling
3) Performance Evaluation tools
4) Customizability and Extensibility

Q-7 Write Services Provided by Azure Cloud

Ans 1) Compute Services
→ Azure VM's: Scalable virtual servers with customizable CPU, RAM and OS.
→ Azure App Services: Fully managed platformed for hosting web apps APIs, and mobile backends
→ Azure Kubernetes Services (AKS): Managed Kubernetes for container orchestration

2) Storage Services
→ Blob Storage: Object Storage for unstructured data like images, videos, logs
→ File Storage: Manged file shares accessible like via SMB protocol
→ Disk Storage: Persistent storage for VM's

Features of Cloud Simulator (4 Marks)

A cloud simulator is a software tool used to model, test, and analyze cloud computing environments without using real cloud infrastructure. It helps researchers and students study cloud behavior, resource allocation, and service performance cost-effectively.

1) Virtualized Cloud Environment

Cloud simulators create a **virtual cloud setup** that includes data centers, virtual machines, networks, brokers, and workloads. This allows users to test different configurations, scheduling policies, and resource models just like a real cloud.

2) Resource Management and Scheduling

They support simulation of **resource allocation algorithms**, VM provisioning, load balancing, and task scheduling. Users can analyze how different techniques affect performance, cost, and energy consumption.

3) Performance Evaluation Tools

Simulators provide metrics such as **execution time, throughput, latency, energy usage, cost estimation, and SLA violations**. This helps compare cloud architectures and understand system behavior under various workloads.

4) Customizability and Extensibility

Most cloud simulators (like CloudSim, GreenCloud, iCanCloud) are **open-source and modular**, allowing users to customize components, add new policies, model new cloud services, and simulate complex research scenarios.

d) Use of WS-security to ensure secure communication between internal resources and processes
e) The option to configure policies and service level agreements based on users and environment
f) Provisions for group, user management and security groups

Q.6 Write Features of Cloud Simulator

Ans
1) Virtualized Cloud Environment
2) Resource Management and Scheduling
3) Performance Evaluation tools
4) Customizability and Extensibility

Q.7 Write Services Provided by Azure Cloud

Ans
1) Compute Services
→ Azure VMs: Scalable virtual servers with customizable CPU, RAM and OS.
→ Azure App Services: Fully managed platformed for hosting web apps APIs, and mobile backends
→ Azure Kubernetes Services (AKS): Managed Kubernetes for container orchestration

2) Storage Services
→ Blob Storage: Object Storage for unstructured data like images, videos, logs
→ File Storage: Manged file shares accessible like via SMB protocol
→ Disk Storage: Persistent storage for VMs

3) Database Services
→ Azure SQL Database: Fully managed relational database
→ Cosmos DB: NoSQL distributed database with low latency global access
→ Azure Database for MySQL / PostgreSQL: Simplified database hosting

4) Networking Services
→ Virtual Network (VNet): Builds secure private networks in cloud
→ Load Balancer & Application Gateway: Handles traffic distribution and security filtering
→ Azure CDN: Delivers content globally with low latency

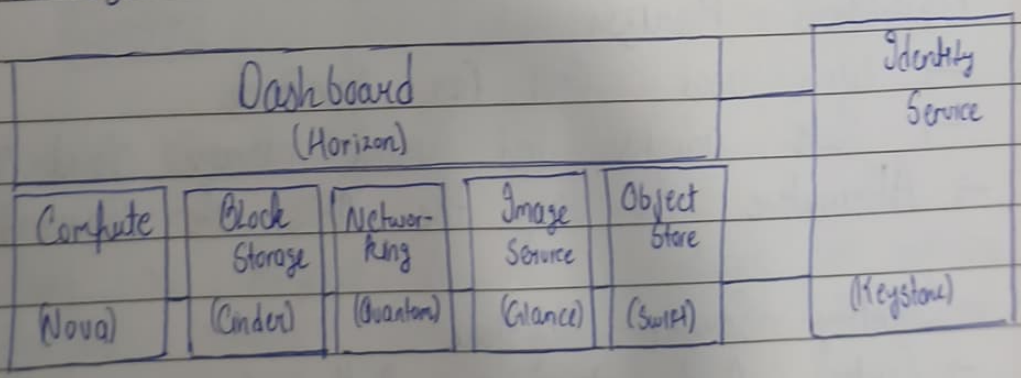
5) AI and Machine Learning Services
→ Azure Machine Learning: Platform to build, train and deploy ML models
→ Cognitive Services: APIs for vision, speech, language and sentiment analysis
→ Bot Services: Frameworks to create conversational AI applications

6) Security and Identity Management
→ Azure Active Directory (AAD): Identity and Access management across users and apps
→ Azure Security Center: Monitors threats, vulnerabilities and compliance
→ Key Vault: Protects encryption keys, passwords and certificates

7) Developer and Devops Services
→ Azure Devops : CI/CD pipelines, code repositories, testing and release management
→ Azure Functions: Serverless computing to run code in response to triggers
→ Logic Apps: Automates workflows across apps and services

Q-8 Discuss Open Stack cloud middleware along with its architecture

Ans OpenStack is an open-source middleware platform used for creating and managing public and private cloud environments
→ It provides IaaS by pooling compute, storage, and networking resources and offering them to users through a centralized dashboard or APIs



Components of Open Stack
1) Compute - Nova
→ Manages Virtual Machines (VMs) and compute resources
→ Handles scheduling, creation, deletion of VM instances
→ Acts as the brain for compute operations in cloud

2) Object Storage - Swift
→ Stores large amounts of unstructured data (files, images, videos, backups)
→ Uses Unique IDs instead of file path to locate data
→ Highly scalable, distributed and good for backups/ archives

3) Block Storage - Cinder
→ Provides block-level storage (like virtual Hard drives)
→ Supports attach/detach of storage volumes to/from VMs
→ Useful for databases, servers and applications needing persistent storage

4) Networking - Neutron
→ Manages all networking functions in OpenStack
→ Handles IP addresses, subnets, routers, firewalls, VPNs
→ Ensures connectivity between all OpenStack components

5) Dashboard - Horizon
→ Web-based GUI for OpenStack
→ Lets admins and users manage cloud resources visually
→ Alternative to using the APIs or command line

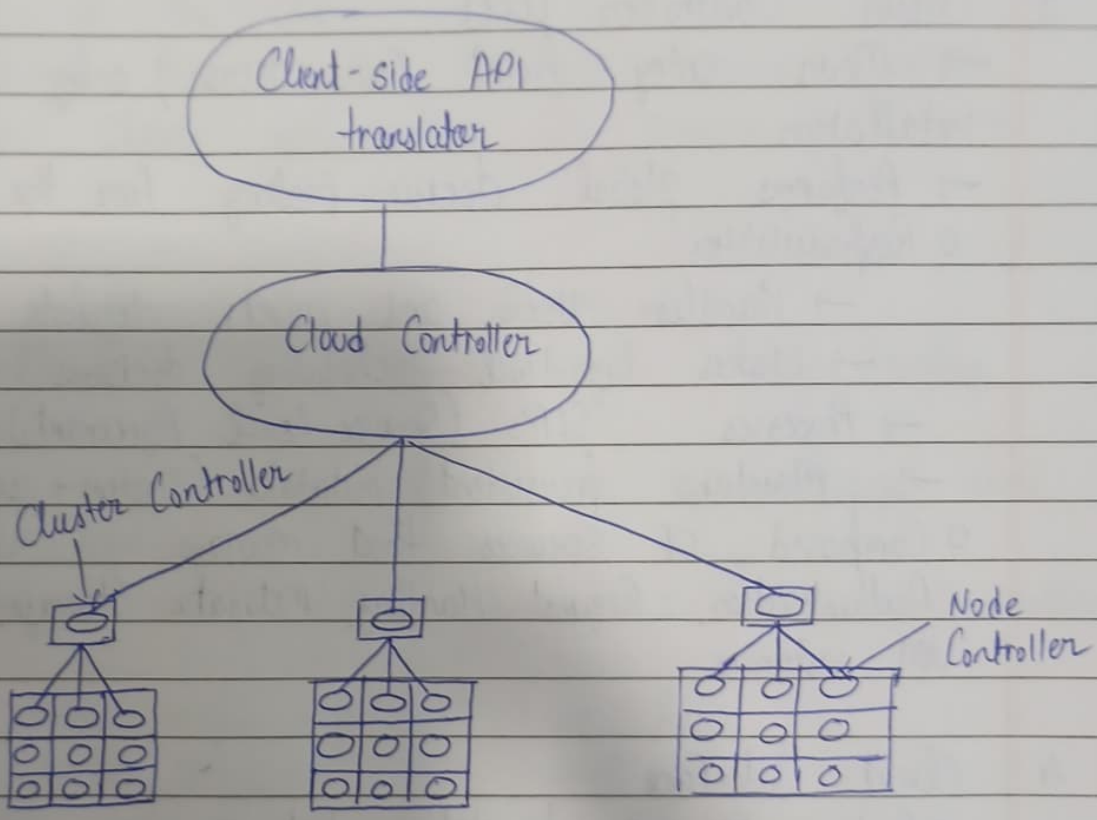
6) Identity Service - KeyStone
→ Central Authorization and Authentication service
→ Manages users, roles, tokens and permissions
→ Ensures secure access to OpenStack Services

7) Image Service - Glance
→ Stores and manages VM images (templates)
→ Used to boot new VM instances from stored disk images

→ Supports Formats like qcow2, VMDK, VDI, RAW, OVF, VHD

Q.9 Discuss Eucalyptus Architecture

Ans See Q.5 for Introduction



Q Components of Eucalyptus

1) Node Controller (NC)
→ Runs on physical machine that hosts VM instances
→ Handles instance startup, shutdown, inspection and cleanup
→ Directly Manages the life cycles of VMs on each node

2) Cluster Controller (CC)
→ Manages a group of node Controllers
→ Typically runs on a cluster head node with access to private and public networks

- Responsibilities:
  - → Collects state info. from NC's
  - → Schedules VM instance requests to specific NCs
  - → Manages network configuration (Public/Private) for instances.

3 Cloud Controller (CLC)
- → Main entry point for users; only ONE per Eucalyptus installation
- → Performs global decision-making for the cloud.
- Responsibilities:
  - → Handles user and admin requests
  - → Makes high-level scheduling decisions
  - → Processes SLA's (Service Level Agreements)
  - → Maintains persistent metadata (system + user)
- Composed of services that manage:
  Authentication, Request Handling, Metadata Storage, Monitoring of VM instances

4 Client Interface
- → Acts as a translator between
  - → External cloud client interfaces (eg Amazon SOAP, HTTP Query API)
  - → Internal Eucalyptus system operations
- → Allows Eucalyptus to accept AWS-style requests by converting them to internal objects

5) Administrative Interface
- → Supports cloud administration tasks, such as:
  - → Adding/removing users
  - → Managing disk images

Provided through
- → A web based interface (via CLC)

→ Command-line tools
→ Unlike the client interface, the interface is unique to Eucalyptus

6) Instance Control (VM Control Service)
→ Part of the CLC
→ Manages the creation of VM instance Metadata
→ Works closely with other CLC services to track VM state

7) SLA Implementation and Management
→ Implemented via extensions to the message handling services
→ Can inspect, modify, approve, or reject messages based on SLA logic
→ Also Interacts with VMControl to enforce SLA conditions

Notes:
→ Worker nodes may not have public IPs
→ Cloud allocations have limited public IPs
→ All instances get a private network interface
→ Uses two types of internal cloud networks

Q-10 What is Google App Engine ? Why it is used

Ans Google App Engine is a PAAS provided by Google that allows developers to build, run and host web applications on Google's cloud infrastructure without managing servers
→ It automatically handles scaling, load balancing, monitoring and resource management

Google App Engine is used because:
1) No server management
2) Automatic Scaling
3) High Availability
4) Easy Deployment
5) Supports Multiple languages
6) Built-In Services
7) Cost-efficient

Q-11 Describe the Key Features and characteristics of Google App Engine

Ans
1) Automatic Scaling
2) Fully Managed Infrastructure
3) Multi-language and Custom-Runtime Support
4) Built-in Cloud Services
5) High Availability and Reliability
6) Security and Acess Control
7) Versioning and Easy Deployment

Q-12 Describe the various Features of Open Stack

Ans Features of Open Stack
1) Open Source Platform
2) Modular Architecture
3) Scalability and Elasticity
4) Multi-tenancy and Security
5) Self-Service and Automation
6) Support for Heterogeneous Environments

Key Characteristics and Features of Google App Engine (7 Marks)

Google App Engine (GAE) is a Platform-as-a-Service (PaaS) offered by Google for building and deploying web applications on Google's cloud infrastructure. Its major characteristics and features are:

1. **Automatic Scaling:**
   GAE automatically increases or decreases the number of application instances based on incoming requests. This ensures the application can handle sudden traffic spikes without manual intervention.
2. **Fully Managed Infrastructure:**
   All system administration tasks such as server provisioning, OS management, patching, load balancing, monitoring, and security updates are handled by Google. Developers only focus on writing code.
3. **Multi-language and Custom Runtime Support:**
   It supports multiple languages like Python, Java, Node.js, Go, Ruby, and PHP. It also allows custom runtimes using Docker containers, giving flexibility in choosing the development environment.
4. **Built-in Cloud Services:**
   GAE includes several integrated services such as Cloud Datastore (NoSQL), Cloud SQL, Memcache, Task Queues, Cron Jobs, and Identity Services. These services simplify application development and reduce dependency on external tools.
5. **High Availability and Reliability:**
   Applications are hosted in Google's globally distributed data centers with built-in redundancy and failover support. This provides high uptime and automatic fault tolerance.
6. **Security and Access Control:**
   GAE provides strong security features like firewalls, identity and access management (IAM), secure sandboxing, and automatic SSL/TLS certificate provisioning. Google continuously manages security patches and threat protection.
7. **Versioning and Easy Deployment:**
   Developers can deploy multiple versions of an application and switch traffic between them for testing or gradual rollout. Deployment is simple using command-line tools, and integration with CI/CD pipelines is supported.

Features of OpenStack (4 Marks)

1. **Open-Source Platform:**
   OpenStack is fully open-source, allowing organizations to modify, customize, and deploy it without licensing costs.
2. **Modular Architecture:**
   It consists of independent components like Nova, Swift, Cinder, Neutron, Glance, and Horizon, providing flexibility and easy integration.
3. **Scalability and Elasticity:**
   It supports large-scale cloud deployments and can automatically scale compute, storage, and network resources based on demand.
4. **Multi-Tenancy and Security:**
   Provides secure isolation for multiple users/projects through Keystone authentication, role-based access control, and secure networking.
5. **Self-Service and Automation:**
   Users can launch VMs, manage storage, and configure networks using APIs or the Horizon dashboard, enabling quick provisioning and automation.
6. **Support for Heterogeneous Environments:**
   Works with multiple hypervisors (KVM, Xen, VMware), various hardware types, and different storage/network backends for maximum flexibility.

Q-13 Compare various Cloud Service Providers

Ans

Feature	AWS	Azure	GCP	IBM Cloud
1) Founded	2006	2010	2011	2011
2) Market Position	Largest and most mature cloud provider	Second largest Strong enterprise presence	Fast-growing strong in AI/ML	Smaller market share, Enterprise focused
3) Core Strengths	Compute (EC2), Storage (S3) Serverless (lambda)	Windows integration, Hybrid cloud, Enterprise tools	AI/ML, Big Data Kubernetes	Security, Hybrid Cloud, Legacy system support
4) Global Reach	Widest global Infra	Very large global presence	Moderate no. of regions	Limited Regions
5) Pricing Model	Complex, Pay-as-you-go, reserved instances	Pay-as-you-go, enterprise discounts	Simple pricing, Sustained use discounts	Moderate, Enterprise pricing
6) Ease of Use	Powerful but Complex	Easy for Enterprises	Developer Friendly	More complex For beginner
7) Best For	Large Enterprises, Scalable apps, big data	Enterprises using Microsoft Ecosystem	Startups, data-driven Companies	Banks Financial Institutions, Gov projects
8) Key Services	EC2, S3, RDS, Lambda	Azure VMs, SQL DB,	BigQuery, GKE, cloud functions	Watson AI, VM, Cloud Foundary

	AWS	Azure	GCP	IBM Cloud
9) Hybrid Cloud Capability	Moderate	Excellent	Good	Excellent
10) AI & ML Support	Strong (SageMaker)	Strong (Cognitive Services)	Best-in class (TensorFlow)	Strong (Watson AI)
11) Vendor Lock-In	Moderate	Moderate	Low to Moderate	High (for enterprise)
12) Typical Users	All Industries, global scale	Corporates, enterprises, IT teams	Devs, Analysts, ML engineers	Large enterprises with mainfra

Q-14 Enlist the features of cloud management products

Ans 1) Resource Provisioning and Automation

2) Monitoring & Performance Management

3) Self-Service Portal

4) Billing & Cost Management

5) Security and Access Control

6) Multi-cloud and Hybrid Cloud Support.

Comparison of Various Cloud Service Providers (7 Marks – Tabular Form)

Feature	Amazon AWS	Microsoft Azure	Google Cloud Platform (GCP)	IBM Cloud
Founded / Launched	2006	2010	2011	2011
Market Position	Largest and most mature cloud provider	Second largest, strong enterprise presence	Fast-growing, strong in AI/ML	Smaller market share, enterprise-focused
Core Strengths	Compute (EC2), Storage (S3), Serverless (Lambda)	Windows integration, Hybrid Cloud, Enterprise tools	AI/ML, Big Data, Kubernetes (GKE)	Security, Hybrid cloud, Legacy system support
Global Reach / Regions	Widest global infrastructure	Very large global presence	Moderate number of regions	Limited regions
Pricing Model	Complex, pay-as-you-go, reserved instances	Pay-as-you-go, enterprise discounts	Simple pricing, sustained-use discounts	Moderate, enterprise pricing
Best For	Large enterprises, scalable apps, big data	Enterprises using Microsoft ecosystem	Startups, data-driven companies	Banks, financial institutions, govt projects
Key Services	EC2, S3, RDS, Lambda, CloudFront	Azure VMs, SQL Database, AD, App Services	BigQuery, GKE, Cloud Functions	Watson AI, VM, Kubernetes, Cloud Foundry
Hybrid Cloud Capability	Moderate	Excellent (Azure Arc, Azure Stack)	Good	Excellent
AI & ML Support	Strong (SageMaker)	Strong (Cognitive Services)	Best in class (Vertex AI, TensorFlow)	Strong (Watson AI)
Ease of Use	Powerful but complex	Easy for enterprises	Developer-friendly	More complex for beginners
Typical Users	All industries, global scale	Corporates, enterprises, IT teams	Developers, analysts, ML engineers	Large enterprises with mainframes
Vendor Lock-In	Moderate	Moderate	Low to moderate	High (for enterprise systems)

Here are **six points** you can write for **"Features of Cloud Management Products" (3 marks)**:

Features of Cloud Management Products

1. **Resource Provisioning & Automation:**
   Ability to automatically allocate, configure, and manage compute, storage, and network resources.
2. **Monitoring & Performance Management:**
   Tracks system performance, resource usage, application health, and generates alerts.
3. **Self-Service Portal:**
   Allows users to deploy and manage cloud resources through a user-friendly dashboard.
4. **Billing & Cost Management:**
   Provides usage tracking, cost estimation, chargeback, and budgeting tools to control expenses.
5. **Security & Access Control:**
   Ensures secure access using authentication, authorization, role-based access control (RBAC), and policy enforcement.
6. **Multi-Cloud & Hybrid Cloud Support:**
   Manages workloads across different cloud providers (AWS, Azure, GCP) and on-premise environments.