

BE - SEMESTER-VII (NEW)
EXAMINATION - SUMMER 2022
Subject Code:3170717
Date: 08/06/2022
Subject Name: Cloud Computing

Q.1

(a) Define load balancing. What is need of loan balancing in cloud computing? 03

ANS: Load balancing is the process of distributing workloads across multiple servers. It prevents any single server from getting overloaded and possibly breaking down. It improves service availability and helps prevent downtimes. It uses server to route traffic to multiple server which in turn share workload.

- Without load balancers, newly spun virtual servers wouldn't be able to receive the incoming traffic in a coordinated fashion or if at all. Some virtual servers might even be left handling zero traffic while others become overloaded.

- A load balancer performs the following functions:

- (i) Distributes client requests or network load efficiently across multiple servers

- (ii) Ensures high availability and reliability by sending requests only to servers that are online

- (iii) Provides the flexibility to add or subtract servers as demand dictates

- **Benefits of Load Balancing:**

- (i) Reduced downtime

- (ii) Scalable

- (iii) Redundancy

- (iv) Flexibility

- (v) Efficiency

(b) What are the challenges to data security in cloud? 04

ANS: Data level Security and sensitive data is the domain of the enterprise not the cloud computing provider.

- Data level security is required to protect the data where ever the data flow that include Force encryption for data and permit only specific users to access the data. It can provide compliance with Payment Card Industry Data Security Standard (PCIDSS).

- Key mechanism to store data are Access control, Auditing, Authentication and Authorization

- Challenges of data security are Data residency, Data privacy, Industry and regulation compliance.

1. Data residency: Many companies face legislation by their country of origin or the local country that the business entity is operating in, requiring certain types of data to be kept within defined geographic borders. There are specific regulations that must be followed, centered around data access, management and control.

2. Data privacy: Business data often needs to be guarded and protected more stringently than non-sensitive data. The enterprise is responsible for any breaches to data and must be able ensure strict cloud security in order to protect sensitive information.

3. Industry and regulation compliance: Organizations often have access to and are responsible for data that is highly regulated and restricted.

(c) How machine Imaging help to achieve the goal of cloud computing? 07

ANS: Machine Imaging:

- Machine imaging is a process that is used to achieve the goal of system portability, provision, and deploy systems in the cloud through capturing the state of systems using a system image.
- A system image makes a copy or a clone of the entire computer system inside a single file.
- The image is made by using a program called system imaging program and can be used later to restore a system image.
- For example, Amazon Machine Image (AMI) is a system image that is used in the cloud computing.
- The Amazon Web Services uses AMI to store copies of a virtual machine.
- An AMI is a file system image that contains an operating system, all device drivers, and any applications and state information that the working virtual machine would have.
- The AMI files are encrypted and compressed for security purpose and stored in Amazon S3 (Simple Storage System) buckets as a set of 10MB chunks.
- Machine imaging is mostly run-on virtualization platform due to this it is also called as Virtual Appliances and running virtual machines are called instances.
- Because many users share clouds, the cloud helps you track information about images, such as ownership, history, and so on.
- The IBM SmartCloud Enterprise knows what organization you belong to when you log in.
- You can choose whether to keep images private, exclusively for your own use, or to share with other users in your organization.
- If you are an independent software vendor, you can also add your images to the public catalogue.

Q.2

(a)What are Hypervisors? List it's importance. 03

ANS: A hypervisor is a form of virtualization software used in Cloud hosting to divide and allocate the resources on various pieces of hardware and provides partitioning, isolation or abstraction.

- ❖ This technique allows multiple guest operating systems (OS) to run on a single host system at the same time, sometimes also called a **virtual machine manager (VMM)**
- ❖ A hypervisor allows a single host computer to support multiple virtual machines (VMs) by sharing resources including memory and processing.
- ❖ **Importance:** Hypervisors make it possible to use more of a system's available resources and provide greater IT mobility since the guest VMs are independent of the host hardware. This means they can be easily moved between different servers. Because multiple virtual machines can run off of one physical server with a hypervisor, a hypervisor reduces:
 - Space
 - Energy
 - Maintenance requirements

(b)What is Eucalyptus? Explain in brief.04

ANS: Eucalyptus stands for **Elastic Utility Computing Architecture for Linking Programs To Useful System.**

- It is used to build private, public and hybrid clouds. It can also produce your own data center into private clouds and allow you to extend the functionality to many other organizations.
- Eucalyptus is an open-source infrastructure for the implementation of cloud computing on computer clusters. It is considered one of the earliest tools developed as a surge computing
- Its name is an acronym for “elastic utility computing architecture for linking your programs to useful systems.” implements infrastructure as a service (IaaS) methodology for solutions in private and hybrid clouds.
- It provides a platform for a single interface so that users can calculate the resources available in private clouds and the resources available externally in public cloud services. It is designed with extensible and modular architecture for Web services. It also implements the industry standard (AWS) API. helps it to export a large number of APIs for users
- **Eucalyptus has the following key features:**
 - Support for multiple users with the help of a single cloud
 - Support for Linux and Windows virtual machines
 - Accounting reports
 - Use of WS-Security to ensure secure comm’n bet’n internal resources & processes.
 - The option to configure policies & service level agreements based on users & the environment
 - Provisions for group, user management and security groups

(c)How AWS Billing mechanism works?07

ANS: AWS has a set of solutions to help you with cost management & optimization.

- AWS equips you with tools to organize your resources based on your needs, visualize and analyze cost and usage data in a single pane of glass, and accurately chargeback to appropriate entities (e.g. department, project, and product).
- Rather than centrally policing the cost, you can provide real-time cost data that makes sense to your engineering, application, and business teams.
- The detailed, allocable cost data allows teams to have the visibility and details to be accountable of their own spend.
- Business and organization leaders need a simple and easy way to access AWS billing information, including a spend summary, a breakdown of all service costs incurred by accounts across the organization, along with discounts and credits.
- Customer can choose to consolidate your bills and take advantage of higher volume discounts based on aggregated usage across your bills.
- Leaders also need to set appropriate guardrails in place so you can maintain control over cost, governance, and security.
- AWS helps organizations balance freedom and control by enabling the governance of granular user permission.

- Businesses and organizations need to plan and set expectations around cloud costs for your projects, applications, and more.
- With AWS, customers can take control of your cost and continuously optimize your expenditure.
- There are a variety of AWS pricing models and resources you can choose from to meet requirements for both performance and cost efficiency, and adjust as needed.

OR

(c) Explain SAAS with an example?07

ANS: SaaS is also known as "On-Demand Software".

It is a software distribution model in which services are hosted by a cloud service provider. These services are available to end-users over the internet so, the end-users do not need to install any software on their devices to access these services.

Services provide by SaaS:

Business Services - SaaS Provider provides various business services to start-up the business.

The SaaS business services include **ERP** (Enterprise Resource Planning), **CRM** (Customer Relationship Management), **billing**, and **sales**.

Document Management - SaaS document management is a software application offered by a third party (SaaS providers) to create, manage, and track electronic documents. **Example:** Slack, Samepage, Box, and Zoho Forms.

Social Networks - As we all know, social networking sites are used by the general public, so social networking service providers use SaaS for their convenience and handle the general public's information.

Mail Services - To handle the unpredictable number of users and load on e-mail services, many e-mail providers offering their services using SaaS.

Advantages of SaaS cloud computing layer:

1. SaaS is easy to buy:

SaaS pricing is based on a monthly fee or annual fee subscription, so it allows organizations to access business functionality at a low cost, which is less than licensed applications.

SaaS providers are generally pricing the applications using a subscription fee, most commonly a monthly or annually fee.

2. One to Many:

SaaS services are offered as a one-to-many model means a single instance of the application is shared by multiple users.

3. Less hardware required for SaaS:

The software is hosted remotely, so organizations do not need to invest in additional hardware.

4. Low maintenance required for SaaS:

Software as a service removes the need for installation, set-up, and daily maintenance for the organizations. The initial set-up cost for SaaS is typically less than the enterprise software.

5. No special software or hardware versions required:

SaaS reduces IT support costs by outsourcing hardware and software maintenance and support to the IaaS provider.

6. Multidevice support:

SaaS services can be accessed from any device such as desktops, laptops, tablets, phones, and thin clients.

7. API Integration:

SaaS services easily integrate with other software or services through standard APIs.

8. No client-side installation:

SaaS services are accessed directly from the service provider using the internet connection, so do not need to require any software installation.

Disadvantages of SaaS cloud computing layer:

1) Security:

Actually, data is stored in the cloud, so security may be an issue for some users. However, cloud computing is not more secure than in-house deployment.

2) Latency issue:

There is a possibility that there may be greater latency when interacting with the application compared to local deployment. Therefore, the SaaS model is not suitable for applications whose demand response time is in milliseconds.

3) Total Dependency on Internet:

Without an internet connection, most SaaS applications are not usable.

4) Switching between SaaS vendors is difficult:

Switching SaaS vendors involves the difficult and slow task of transferring the very large data files over the internet and then converting and importing them into another SaaS also.

Popular SaaS Providers:

Provider	Services
Salseforce.com	On-demand CRM solutions
MS Office 365	Online office suite
Google Apps	Gmail, Google Calendar, Docs, and sites
NetSuite	ERP, accounting, order management, CRM, Professionals Services Automation (PSA), and e-commerce applications.
GoToMeeting	Online meeting and video-conferencing software
Constant Contact	E-mail marketing, online survey, and event marketing
Oracle CRM	CRM applications
Workday, Inc	Human capital management, payroll, and financial management.

Q.3

(a)What is SOAP and REST web services? 03

ANS: SOAP:

- Simple Object Access Protocol (SOAP) is a **lightweight XML-based protocol that is used for the exchange of information in decentralized, distributed application environments.**
- You can transmit SOAP messages in any way that the applications require, as long as both the client and the server use the same method.
- It provides data transport for Web services.
- It can exchange complete documents or call a remote procedure.
- It can be used for broadcasting a message.

- It is platform- and language-independent.
- It is the XML way of defining what information is sent and how.
- It enables client applications to easily connect to remote services and invoke remote methods.

REST:

- REST stands for REpresentational State Transfer.
- REST is web standards-based architecture and uses HTTP Protocols.
- RESTful web services are light weight, highly scalable and maintainable and are very commonly used to create APIs for web-based applications.
- In REST architecture, a REST Server simply provides access to resources and REST client accesses and modifies the resources.

(b)Elaborate Securing Data. 04

ANS: Securing the data is the practice of protecting digital information from unauthorized access, corruption, or theft throughout its entire lifecycle.

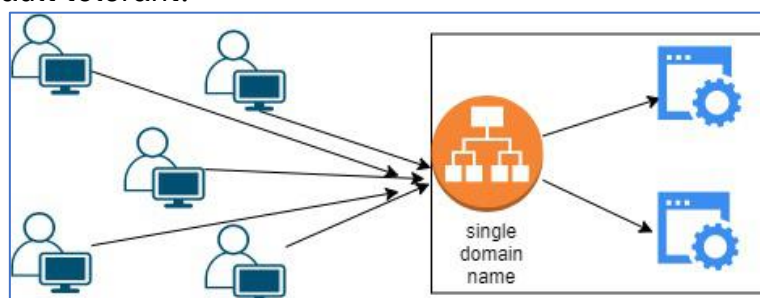
- A comprehensive data security strategy incorporates people, processes, and technologies.
- Regardless of whether your data is stored on-premises, in a corporate data center, or in the public cloud, you need to ensure that facilities are secured against intruders and have adequate fire suppression measures and climate controls in place.
- Database, network, and administrative account access should be given to as few people as possible, and only those who absolutely need it to get their jobs done.
- All software should be updated to the latest version as soon as possible after patches or new versions are released.
- Maintaining usable, thoroughly tested backup copies of all critical data is a core component of any robust data security strategy.
- Training employees in the importance of good security practices.
- Implementing a comprehensive suite of threat management, detection, and response tools

(c)Explain Elastic Load Balancer.07

ANS: Elastic load balancer:

Elastic load balancer is a service provided by Amazon in which the incoming traffic is efficiently automatically distributed across a group of backend servers in a manner that increases speed and performance.

Load Balancer allows you to configure health checks for the registered targets. In case any of registered target fails the health check, the load balancer will not route traffic to that unhealthy target. Thereby ensuring your application is highly available and fault tolerant.



Load balancer acting as single point of routing traffic

Types of load balancer

A. Classic Load Balancer: It is the traditional form of load balancer which was used initially. It distributes the traffic among the instances and is not intelligent enough to support host-based routing or path-based routing.

B. Application Load Balancer: This type of Load Balancer is used when decisions are to be made related to HTTP and HTTPS traffic routing. It supports path-based routing and host-based routing.

C. Network Load Balancer: This type of load balancer works at the transport layer (TCP/SSL) of the OSI model. It's capable of handling millions of requests per second. It is mainly used for load balancing TCP traffic.

D. Gateway Load Balancer: Gateway Load Balancers provides you the facility to deploy, scale, and manage virtual appliances like firewall. Gateway Load Balancers combines a transparent network gateway and then distributes the traffic.

OR

Q.3

(a)What is SOAP? Explain in brief. 03

ANS: Simple Object Access Protocol (SOAP) is a **lightweight XML-based protocol that is used for the exchange of information in decentralized, distributed application environments.**

- You can transmit SOAP messages in any way that the applications require, as long as both the client and the server use the same method.
- It provides data transport for Web services.
- It can exchange complete documents or call a remote procedure.
- It can be used for broadcasting a message.
- It is platform- and language-independent.
- It is the XML way of defining what information is sent and how.
- It enables client applications to easily connect to remote services and invoke remote methods.

(b)Explain Physical versus Virtual Clusters 04

ANS: Difference between Physical vs. Virtual Clusters:

Physical Clusters	Virtual Clusters
A physical cluster is a collection of physical servers interconnected by physical network.	Virtual clusters are built mainly with multiple VMs installed at servers belonging to one or more physical clusters.
The failure of any physical nodes may disable some VMs installed on the failing nodes.	The failure of VMs will not pull down the host system/physical machine.
The PMs are known as host systems	The VMs are known as guest systems
PM nodes can't be added, removed, or migrated easily over the time.	VM nodes can be added, removed, or migrated dynamically over the time

(c) Explain Amazon S3? Explain Amazon S3 API? What are the operations we can execute through API? 07

ANS: Amazon Simple Storage Service (S3)

Amazon S3 has a simple web services interface that you can use to store and retrieve any amount of data, at any time, from anywhere on the web.

Amazon S3 is intentionally built with a minimal feature set that focuses on simplicity and robustness.

Following are some of advantages of the Amazon S3 service:

- **Create Buckets** – Create and name a bucket that stores data. Buckets are the fundamental container in Amazon S3 for data storage.
- **Store data in Buckets** – Store an infinite amount of data in a bucket. Upload as many objects as you like into an Amazon S3 bucket. Each object can contain up to 5 TB of data. Each object is stored and retrieved using a unique developer-assigned key.
- **Download data** – Download your data any time you like or allow others to do the same.
- **Permissions** – Grant or deny access to others who want to upload or download data into your Amazon S3 bucket.
- **Standard interfaces** – Use standards-based REST and SOAP interfaces designed to work with any Internet-development toolkit.

Amazon S3 Application Programming Interfaces (API):

- The Amazon S3 architecture is designed to be programming language-neutral, using their supported interfaces to store and retrieve objects.
- Amazon S3 provides a REST and a SOAP interface.
- They are similar, but there are some differences. For example, in the REST interface, metadata is returned in HTTP headers. Because we only support HTTP requests of up to 4 KB (not including the body), the amount of metadata you can supply is restricted.

Operations we can execute through API:

- Login into Amazon S3.
- Uploading.
- Retrieving.
- Deleting etc.

Q.4

(a) Give A Brief Introduction to Windows Azure Operating System. 03

ANS: Microsoft Azure:

- Microsoft Azure is a Microsoft cloud service provider that provides cloud computing services like computation, storage, security and many other domains.
- It provides services in the form of Infrastructure as a service, Platform as a Service and Software as a service. It even provides serverless computing meaning, you just put your code and all your backend activities as managed by Microsoft Azure.
- Azure queue storage is a service for storing large numbers of message that can be accessed from anywhere in the world via HTTP.

- Azure has low operational cost because it runs on its own servers whose only job is to make the cloud functional and bug-free, it's usually a whole lot more reliable than your own, on-location server.

- **Use for**

- Build a web application that runs and stores data
- Create virtual machine to develop and test or run
- Develop massively scalable applications with many users
- Azure keep backups of all your valuable data. In disaster situations, you can recover all your data in a single click without your business getting affected.

(b)How would you secure data for transport in the cloud? 04

ANS: Data transport is the process of moving data from one location to another. The challenges of securing data in the cloud include ensuring that data is encrypted while in transit, as well as ensuring that data is stored securely at the destination.

- When transporting data in a cloud computing environment, keep two things in mind: Make sure that no one can intercept your data as it moves from point A to point B in the cloud, and make sure that no data leaks (malicious or otherwise) from any storage in the cloud.
- A virtual private network (VPN) is one way to secure data while it is being transported in a cloud. A VPN converts the public network to a private network instead. A well-designed VPN will incorporate two things:
 - A firewall will act as a barrier between the public and any private network.
 - Encryption protects your sensitive data from hackers; only the computer that you send it to should have the key to decode the data.
- Check that there is no data leak with the encryption key implemented with the data you send while it moves from point A to point B in a cloud.

(c)Mention working mechanism of AWS Cloud Trail with its benefits. 07

ANS: AWS CloudTrail is an AWS service that helps you enable governance, compliance, and operational and risk auditing of your AWS account.

Working of CloudTrail:

You can create two types of trails for an AWS account:

- **A trail that applies to all regions:**

- When you create a trail that applies to all regions, CloudTrail records events in each region and delivers the CloudTrail event log files to an S3 bucket that you specify.
- If a region is added after you create a trail that applies to all regions that new region is automatically included, and events in that region are logged.
- This is the default option when you create a trail in the CloudTrail console.

- **A trail that applies to one region:**

- When you create a trail that applies to one region, CloudTrail records the events in that region only.
- It then delivers the CloudTrail event log files to an Amazon S3 bucket that you specify.
- If you create additional single trails, you can have those trails deliver CloudTrail event log files to the same Amazon S3 bucket or to separate buckets.
- This is the default option when you create a trail using the AWS CLI or the CloudTrail API.

- Beginning on April 12, 2019, trails will be viewable only in the AWS Regions where they log events.
- If you create a trail that logs events in all AWS Regions, it will appear in the console in all AWS Regions.
- If you create a trail that only logs events in a single AWS Region, you can view and manage it only in that AWS Region.
- If you have created an organization in AWS Organizations, you can also create a trail that will log all events for all AWS accounts in that organization.
- This is referred to as an organization trail. Organization trails can apply to all AWS Regions or one Region.
- Organization trails must be created in the master account, and when specified as applying to an organization, are automatically applied to all member accounts in the organization.
- Member accounts will be able to see the organization trail, but cannot modify or delete it.
- By default, member accounts will not have access to the log files for the organization trail in the Amazon S3 bucket.
- You can change the configuration of a trail after you create it, including whether it logs events in one region or all regions.
- You can also change whether it logs data or CloudTrail Insights events.
- Changing whether a trail logs events in one region or in all regions affects which events are logged.
- By default, CloudTrail event log files are encrypted using Amazon S3 server-side encryption (SSE).
- You can also choose to encrypt your log files with an AWS Key Management Service (AWS KMS) key.
- You can store your log files in your bucket for as long as you want.
- You can also define Amazon S3 lifecycle rules to archive or delete log files automatically.
- If you want notifications about log file delivery and validation, you can set up Amazon SNS notifications.
- CloudTrail typically delivers log files within 15 minutes of account activity.
- In addition, CloudTrail publishes log files multiple times an hour, about every five minutes.
- These log files contain API calls from services in the account that support CloudTrail.

Benefits of CloudTrail:

Simplified compliance:

- With AWS CloudTrail, simplify your compliance audits by automatically recording and storing event logs for actions made within your AWS account.
- Integration with Amazon CloudWatch Logs provides a convenient way to search through log data, identify out-of-compliance events, accelerate incident investigations, and expedite responses to auditor requests.

Security analysis and troubleshooting:

- With AWS CloudTrail, you can discover and troubleshoot security and operational issues by capturing a comprehensive history of changes that occurred in your AWS account within a specified period of time.

Visibility into user and resource activity:

- AWS CloudTrail increases visibility into your user and resource activity by recording AWS Management Console actions and API calls.

OR

Q.4

(a) Explain the difference between cloud and traditional data centers.03

ANS: Difference between Cloud and Data Center:

Cloud	Data Center
Cloud is a virtual resource that helps businesses to store, organize, and operate data efficiently.	Data Center is a physical resource that helps businesses to store, organize, and operate data efficiently.
The scalability of the cloud required less amount of investment.	The scalability of Data Center is huge in investment as compared to the cloud.
The maintenance cost is less than service providers maintain it.	The maintenance cost is high because developers of the organization do maintenance.
Third-Party needs to be trusted for the organization's data to be stored.	The organization's developers are trusted for the data stored in data centers.
Performance is huge as compared with investment.	Performance is less than compared to investment.
It requires a plan to customize the cloud.	It is easily customizable without any hard plan.
It requires a stable internet connection to provide the function.	It may and may not require an internet connection.
Cloud is easy to operate and is considered a viable option.	Data Centers require experienced developers to operate and are considered not a viable option.
Data is generally collected from the internet	Here, data is collected from the Organization's network.
It finds use in scenarios where security is not a critical aspect. Hence, small web applications can be hosted easily.	It finds use in scenarios where the project requires a high level of security.

(b) What are the cons of cloud computing?04

ANS: CONS OF CLOUD COMPUTING:

- **Internet Connectivity:** If you do not have good internet connectivity, you cannot access the data stored on the cloud. However, we have no other way to access data from the cloud.
- **Vendor lock-in:** Organizations may face problems when transferring their services from one vendor to another. As different vendors provide different platforms, that can cause difficulty moving from one cloud to another.
- **Limited Control:** Cloud infrastructure is completely owned, managed, and monitored by the service provider, so the cloud users have less control over the function and execution of services within a cloud infrastructure.

- **Security:** you should be aware that you will be sending all your organization's sensitive information to a third party, i.e., a cloud computing service provider. While sending the data on the cloud, there may be a chance that your organization's info. is hacked by Hackers.

(c)What is Amazon Glacier? How does it work? Differentiate Glacier and S3.07

ANS: Amazon S3 is one of the core services offered by AWS that has a wide variety of use cases, from serving static websites to hosting images, managing data, and much more.

- Amazon S3 Glacier (S3 Glacier) is a secure and durable service for low-cost data archiving and long-term backup.
- In Amazon S3 Glacier, you can store your data cost effectively for months, years, or even decades.
- S3 Glacier helps you offload the administrative burdens of operating and scaling storage to AWS, so you don't have to worry about capacity planning, hardware provisioning, data replication, hardware failure detection and recovery, or time-consuming hardware migrations.
- Amazon Simple Storage Service (Amazon S3) also provides three Amazon S3 Glacier archive storage classes. These storage classes are designed for different access patterns and storage duration. These storage classes differ as follows:
 - (i)S3 Glacier Instant Retrieval** – Use for archiving data that is rarely accessed and requires milliseconds retrieval.
 - (ii)S3 Glacier Flexible Retrieval** – Use for archives where portions of the data might need to be retrieved in minutes. Data stored here can be accessed in as little as 1-5 minutes by using Expedited retrieval.
 - (iii)S3 Glacier Deep Archive** – Use for archiving data that rarely needs to be accessed. Data stored in the S3 Glacier Deep Archive storage class has a default retrieval time of 12 hours.

Diff'n Bet'n Glacier & S3:

Amazon Glacier	Amazon S3
is mainly used for frequent data access	is mainly utilized for long-term data storage.
does not support hosting static online content	supports hosting static online content
It stores data in the form of archives & vaults.	It saves data in the logical buckets.
Amazon Glacier is less expensive.	Amazon S3 is more expensive.
The minimum storage day with Glacier is 90 days.	The minimum storage day with S3 is 30 days
Setting up Amazon Glacier is simple	Setting up Amazon S3 is more complicated
Amazon Glacier is faster in creating & organizing.	Amazon S3 is slower in creating & organizing.

Q.5

(a)Define cloud computing and state it's desirable features 03

ANS: The term Cloud refers to a Network or Internet. In other words, we can say that Cloud is something, which is present at remote locations. Cloud can provide services over public and private networks, i.e., WAN, LAN or VPN.

- **Cloud Computing** refers to manipulating, configuring, and accessing the hardware and software resources remotely. It offers online data storage, infrastructure, and application.

FEATURES OF CLOUD COMPUTING:

- **Resources Pooling:** Cloud provider pulled the computing resources to provide services to multiple customers with the help of a multi-tenant model.
- **On-Demand Self-Service:** user can continuously monitor the server uptime, capabilities, and allotted network storage.
- **Easy Maintenance:** The servers are easily maintained and the downtime is very low and even in some cases, there is no downtime.
- **Large Network Access:** The user can access the data of the cloud or upload the data to the cloud from anywhere just with the help of a device and an internet connection.
- **Availability:** The capabilities of the Cloud can be modified as per the use and can be extended a lot. allows the user to buy extra Cloud storage if needed for a very small amount.
- **Automatic System:** Cloud computing automatically analyzes the data needed and supports a metering capability at some level of services.
- **Economical:** It is the one-time investment as the company has to buy the storage and a small part of it can be provided to the many companies which save the host from monthly or yearly costs.
- **Security:** It creates a snapshot of the data stored so that the data may not get lost even if one of the servers gets damaged.
- **Pay as you go:** the user has to pay only for the service or the space they have utilized.
- **Measured Service:** Supporting charge-per-use capabilities.
- **Latest Version Available:** Provide latest version as long as you are connected.

(b)Write a note on AWS API Security.04

ANS: AWS API Security:

- API Gateway supports multiple mechanisms of access control, including metering or tracking API used by clients using API keys.
- The standard AWS IAM roles and policies offer flexible and robust access controls that can be applied to an entire API set or individual methods.
- Custom authorizers and Amazon Cognito user pools provide customizable authorization and authentication solutions.

(A)Control Access to an API with IAM Permissions:

- You control access to Amazon API Gateway with IAM permissions by controlling access to the following two API Gateway component processes:
 - (a)To create, deploy, and manage an API in API Gateway.
 - (b)To call a deployed API or to refresh the API caching.

(B)Use API Gateway Custom Authorizers:

- An Amazon API Gateway custom authorizer is a Lambda function that you provide to control access to your API methods.

(C)Use Amazon Cognito User Pools:

- In addition to using IAM roles and policies or custom authorizers, you can use an Amazon Cognito user pool to control who can access your API in Amazon API Gateway.
- To use an Amazon Cognito user pool with your API, you must first create an authorizer of the COGNITO_USER_POOLS type and then configure an API method to use that authorizer.

(D)Use Client-Side SSL Certificates for Authentication by the Backend:

- You can use API Gateway to generate an SSL certificate and use its public key in the backend to verify that HTTP requests to your backend system are from API Gateway.

(E) Create and Use API Gateway Usage Plans:

- After you create, test, and deploy your APIs, you can use API Gateway usage plans to extend them as product offerings for your customers.

(c)How AWS deals with Disaster recovery? 07

ANS: Our data is the most precious asset that we have and protecting it is our top priority.

- Creating backups of our data to an off shore data center, so that in the event of an on-premise failure we can switch over to our backup, is a prime focus for business continuity.
- As AWS says, 'Disaster recovery is a continual process of analysis and improvement, as business and systems evolve. For each business service, customers need to establish an acceptable recovery point and time, and then build an appropriate DR solution.'
- Backup and DR on Cloud reduces costs by half as compared to maintaining your own redundant data centers.
- Imagine the kind of cost you would entail in buying and maintaining servers & data centers, providing secure & stable connectivity & not to mention keeping them secure.
- You would also be underutilizing servers; and in times of unpredictable traffic rise it would be strenuous to set up new ones. To all the cloud provides a seamless transition reducing cost dramatically.

4 Standard Approaches of Backup and Disaster Recovery Using Amazon Cloud:

1. Backup and Recovery:

- To recover your data in the event of any disaster, you must first have your data periodically backed up from your system to AWS.
- AWS offers AWS Direct connect and Import-Export services that allow for faster backup.

2. Pilot Light Approach:

- In the preparatory phase your on-premise database server mirrors data to data volumes on AWS. The database server on cloud is always activated for frequent or continuous incremental backup.

3. Warm Standby Approach:

- In this Technique, your application and caching servers are set up and always activated based on your business-critical activities but only a minimum sized fleet of EC2 instances are dedicated.
- The backup system is not capable of handling production load, but can be used for testing, quality assurance and other internal uses.

4. Multi-Site Approach:

- All activities in the preparatory stage are similar to a warm standby; except that AWS backup on Cloud is also used to handle some portions of the user traffic using Route 53.
- When a disaster strikes, the rest of the traffic that was pointing to the on-premise servers are rerouted to AWS and using auto scaling techniques multiple EC2 instances are deployed to handle full production capacity.

OR

Q.5

(a)Mention benefits of cloud computing technology. 03

ANS: ADVANTAGES/PROS OF CLOUD COMPUTING:

- **Back-up and restore data:** Once the data is stored in the cloud, it is easier to get back-up and restore that data using the cloud.
- **Improved collaboration:** Cloud applications improve collaboration by allowing groups of people to quickly and easily share information in the cloud via shared storage.
- **Excellent accessibility:** Cloud allows us to quickly and easily access store information anywhere, anytime in the whole world, using an internet connection.
- **Low maintenance cost:** Cloud computing reduces both hardware and software maintenance costs for organizations.
- **Mobility:** Cloud computing allows us to easily access all cloud data via Mobile.
- **Pay-per-use model:** Cloud computing offers (APIs) to the users for access services on the cloud and pays the charges as per the usage of service.
- **Unlimited storage capacity:** Cloud offers us a huge amount of storage capacity for storing our important data such as documents, images, audio, video, etc. in one place.
- **Data security:** Cloud offers many advanced features related to security and ensures that data is securely stored and handled.

(b)Write a note on AWS Ecosystem.04

ANS: AWS Ecosystem:

- In general, a cloud ecosystem is a complex system of interdependent components that all work together to enable cloud services. In cloud computing, the ecosystem consists of hardware and software as well as cloud customers, cloud engineers, consultants, integrators and partners.
- Amazon Web Services (AWS) is the market leader in IaaS (Infrastructure-as-a-Service) and PaaS (Platform-as-a-Service) for cloud ecosystems, which can be combined to create a scalable cloud application without worrying about delays related to infrastructure provisioning (compute, storage, and network) and management.
- With AWS you can select the specific solutions you need, and only pay for exactly what you use, resulting in lower capital expenditure and faster time to value without sacrificing application performance or user experience.
- New and existing companies can build their digital infrastructure partially or entirely in the cloud with AWS, making the on-premise data center a thing of the past.
- The AWS cloud ensures infrastructure reliability, compliance with security standards, and the ability to instantly grow or shrink your infrastructure to meet your needs and maximize your budget, all without upfront investment in equipment.

(c)What technology services does Amazon provide? What are the business advantages to Amazon and to subscribers of these services? What are the disadvantages of each? What kinds of businesses are likely to benefit from these services? 07

ANS: Amazon has many services for cloud applications. A few key services of the AWS ecosystem and a brief description of how developers use them in their business.

Amazon has a list of services:

1. Compute service
2. Storage
3. Database
4. Networking and delivery of content
5. Security tools
6. Developer tools
7. Management tools

1.Compute Service:

These services help developers build, deploy, and scale an application in the cloud platform.

AWS EC2 is a web service that allows developers to rent virtual machines and automatically scales the compute capacity when required.

AWS Lambda is a serverless compute service. It is also responsible for executing code for applications.

2.Storage:

AWS provides web data storage service for archiving data. Also, its primary advantage is disaster data recovery with high durability.

Amazon S3 is an open cloud-based storage service that is utilized for online data backup.

Amazon EBS provides a high availability storage volume for persistent data. It is mainly used by Amazon EC2 instances.

3. Database:

AWS database domain service offers cost-efficient, highly secure, and scalable database instances in the cloud.

DynamoDB is a flexible NoSQL database service that offers fast and reliable performance with no scalability issues.

RDS is a managed distributed relational database cloud service that helps developers to operate and scale a database in a simple manner.

4.Networking and Delivery of Content:

It offers a highly secure cloud platform and connects your physical network to your private VN with a high transfer speed.

VPC helps a developer to deploy AWS resources, such as Amazon EC2 instances into a private virtual cloud & gives you control over the complete cloud network environment.

Route 53 is a web service with a highly available Domain Name System (DNS) that helps users to route software by translating the text into an IP address.

5.Security, Identity & Compliance:

It helps in monitoring a safe environment for your AWS resources by providing limited access to specific users.

Identity Access Management (IAM) is a framework that helps in maintaining access to AWS services in a secure way.

KMS enables users to create and manage the encryption keys that are used for encrypting data.

6.Developer Tools:

It helps a user build, deploy, and run an application source code automatically. It also updates the server and instance on the workload.

CodeStar is a service designed to where developers can quickly develop, build and deploy applications on AWS

Code Build compiles your code, executes unit tests, and gives output artifacts that are ready to deploy.

7.Management Tools:

Using this service, an individual can optimize costs, minimize risks, and automate all the resources running efficiently on the AWS infrastructure.

Cloud Watch is a monitoring tool for AWS resources and customer applications running on the AWS platform.

Cloud Formation service helps you in monitoring all your AWS resources in one place so your time is not wasted.

AWS used for: AWS offers over 200 fully featured services. It allows you to select the programming language, database, operating system, web application platform, and other needed services. You can build, deploy, and manage applications, websites, and processes on AWS secure platform.