Assignment - 3

Name : Bansi Tejani

Roll No. : 191

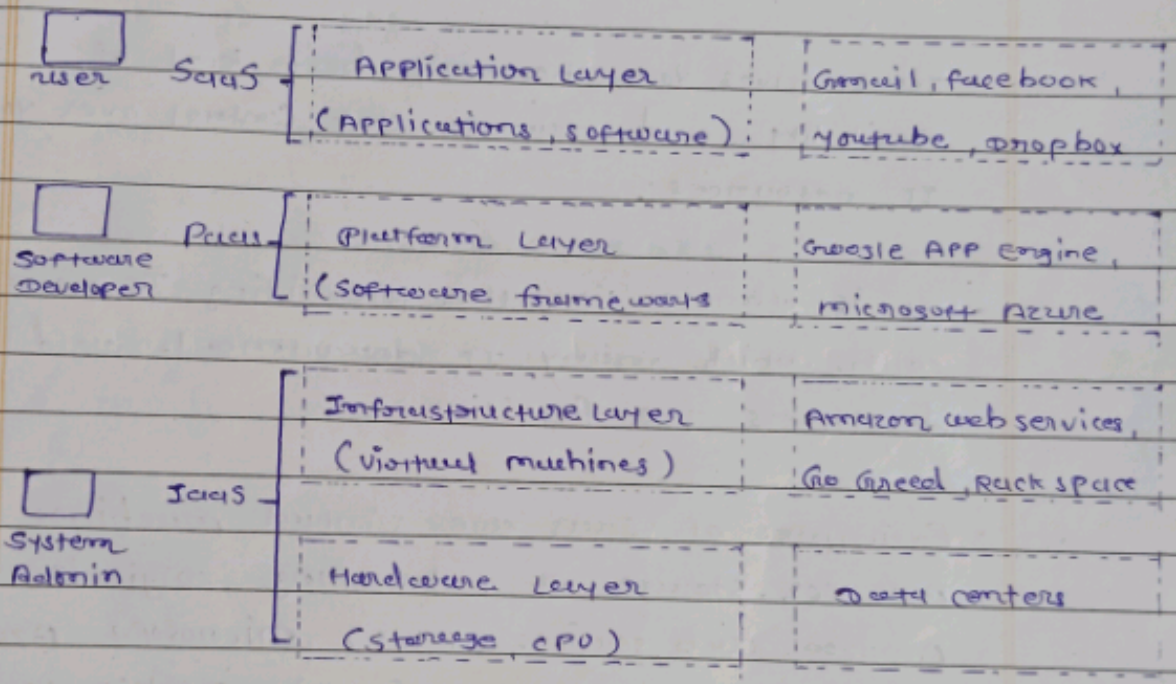
Div. : C

Semester : Bsc. IT (sem - 6)

Subject : (604) . fundamentals of cloud computing.

Q-1 Explain cloud service models in detail

→ Cloud Computing services are offered to users in different forms. NIST defines at least three cloud service models as follows..



→ There are three types of cloud service models:

1) Infrastructure As A service (IaaS)
2) Platform As A service (PaaS)
3) Software As A service (SaaS)

1. Infrastructure As A service (IaaS):

- It is the most flexible type of cloud service which lets you rent the hardware and contains the basic building blocks for cloud and IT.

- It gives complete control over the hardware that runs your application (servers, VMs, storage, networks & operating systems).

- It's an instant computing infrastructure, provisioned and managed over the internet

- IaaS gives you the very best level of flexibility and management control over your IT resources.

- It is almost like the prevailing IT resource with which many IT departments and developers are familiar.

- Examples of IaaS are Virtual machines or AWS EC2, Storage as Networking, Digitalocean, Amazon web services (AWS), Microsoft Azure Google Compute Engine (GCE), Rackspace and cisco Metacloud.

* Advantages of IAAS :

- Cost Savings :

- IaaS is more cost-effective than building your own data center.
- You pay only for what you need - storage space, CPU power, bandwidth and other resources.

- This makes it easier to scale up or down as needed.

- On-demand access :

- You can instantly provision new resources whenever they're needed without having to invest in new hardware and software or hire additional IT staff members.
- The cloud provider takes care of all the maintenance and upgrades required to keep your servers online.

- website hosting :

- Running websites using IaaS can be less expensive than traditional web hosting.

- security :

- The IaaS cloud provider may provide better security than your existing software.

- maintenance :

- There is no need to manage the underlying data center or the introduction of new releases of the development or underlying software.
- This is all handled by the IaaS cloud provider.

• flexibility :

- with cloud computing, you can easily add more resources when demand increases without having to upgrade equipment or hire more IT professionals.

* Disadvantages of IaaS

• Limited infrastructure control :

- Although IaaS providers normally handle upgrades and management of the underlying infrastructure, this might also imply that users have less control over the environment and might not be able to make some adjustments.

• Security issues :

- Users must take responsibility for protecting their data and apps, which can be very demanding.

• limited access :

- cloud computing may not be accessible in certain regions and countries due to legal policies.

2. platform As A Service (Paas):

→ Paas is a cloud service model that gives a ready-to-use development environment where developers can specialize in writing and executing high-quality code to make customized applications.

- It helps to create an application quickly without managing the underlying infrastructure.

- for example, when deploying a web application using Paas, you don't have to install an operating system, web server, or even system updates.

- However, you can scale and add new features to your services.

- This cloud service model makes the method of developing and deploying applications simpler.

- This helps you be more efficient as you don't get to worry about resource procurement, capacity planning, software maintenance involved in running your application.

- Examples of Paas: Elastic Beanstalk or Lambda from AWS, WebApps, functions or Azure SQL DB from Azure, cloud SQL DB from Google cloud, an

oracle database cloud service from Oracle cloud.

* Advantages of Paas :

- faster development time :
  - you don't have to build infrastructure before you can start coding.

- Reduced costs :
  - your IT department won't need to spend time on manual deployments or server management

- Enhanced security :
  - Paas providers lock down your applications so that they're more secure than traditional web apps.

- High availability :
  - A Paas provider can make sure your application is always available, even during hardware failures or maintenance windows

- Automatic updates :
  - Rather than purchasing new software, customers rely on a Saas provider to automatically perform the updates.

* Disadvantages of PaaS :

- Dependency on the provider :
- Customers rely on the PaaS provider to maintain the platform's scalability, availability and dependability ; however, this poses a risk if the provider encounters disruptions or other problems.

- Restricted flexibility :
- The usefulness of PaaS solutions for some organizations may be limited if they cannot handle particular workloads or applications.

- Dependence on internet Connectivity :
- PaaS solutions are typically cloud-based, which means that they require a stable internet connection to function properly.
- This can be problematic for users in areas with poor connectivity or for those who need to access the software in offline environments.

- Security Concerns :
- PaaS providers are responsible for maintaining the security of the data stored on their servers, but there is still a risk of data breaches or other security incidents.

3. Software As A service (SaaS) :

- Saas provides you with a complete product that is run and managed by the service provider.
-
- The software is hosted online and made available to customers on a subscription basis or for purchase in this cloud service model.

- with a saas offering, you don't need to worry about how the service is maintained or how the underlying infrastructure is managed.

- It would help if you believed how you'd use that specific software.

- Examples of Saas : microsoft office 365, oracle ERP / HCM cloud, salesforce, Gmail or Dropbox.

* Advantages of Saas :

• lower Total cost :

- one of the biggest benefits of saas is that it lowers your total cost of ownership (TCO) by eliminating hardware expenses and maintenance costs.

• Better security :

- Another benefit of Saas is improved security.
- since most services are hosted on secure servers in data centers with 24/7 monitoring, there's less chance for hackers to gain access or steal your data.

• Reduced time :

- Users can run most Saas apps directly from their web browser without needing to download and install any software.
- This reduces the time spent in installation and configuration, and can reduce the issues that can get in the way of the software deployment.

• Automatic updates :

- Rather than purchasing new software, customers rely on a Saas provider to automatically perform the updates.

* Disadvantages of Saas :

• Limited customization :

- Saas solutions are usually less customizable.
- As a result, customers may not be able to customize the program to meet their unique requirements and may be forced to operate

within the platform limitations of the SaaS provider.

- Dependency on Internet Connectivity :

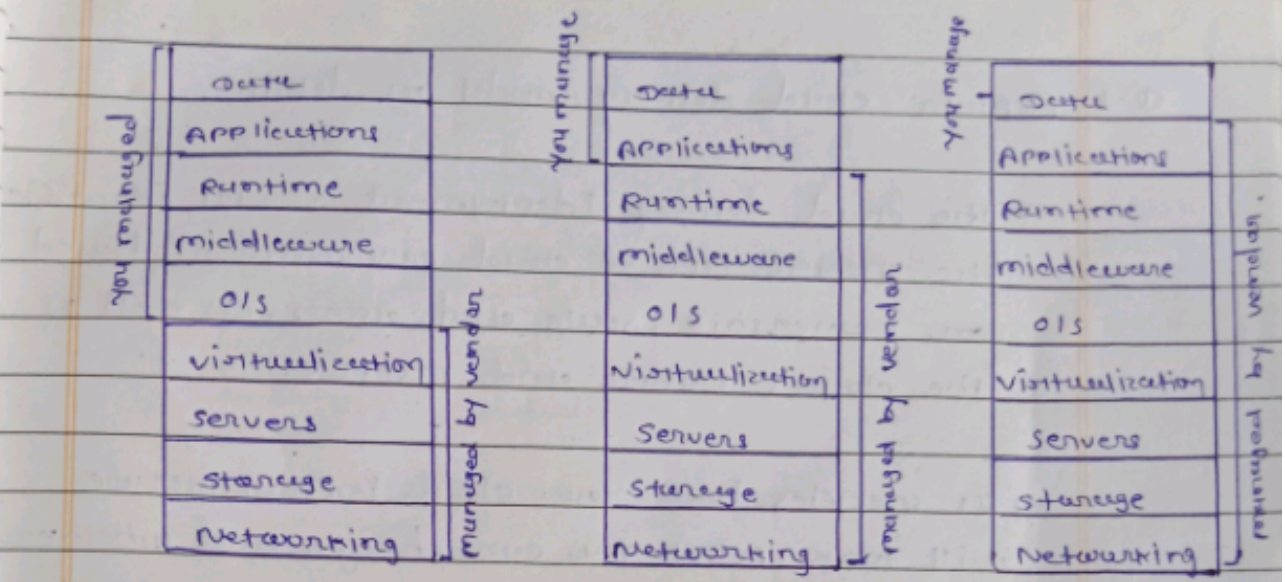
- Since SaaS solutions are usually cloud-based a steady Internet connection is necessary for them to operate as intended.
- Users who need to access the software offlin may find this troublesome.

- Security issues :

- Although SaaS providers are in charge of ensuring the security of the information kept on their servers, security incidents and data breaches are still a possibility.

- Limited control over data :

- SaaS providers may have access to a user's data, which can be a concern for organizat that need to maintain strict control over thei data for regulatory or other reasons.



IaaS PaaS SaaS

* difference beetween IaaS, PaaS and SaaS.

features	IaaS	PaaS	SaaS
what is offers	virtualized infrastructure	A platform for app development	full software access
User Role	manage OS, apps, and data	manage apps and data	use software
Key features	full control, Scalable Pay-as-you-go	pre-configured dev tools	No install, subscription-based
use case	Hosting, VMs, big data	App development, testing	Email, CRM, collaboration
providers	AWS, Azure, Google cloud	Heroku, Google App Engine	Google workspace, microsoft 365

Q:2 Explain cloud delivery model in detail.

→ The cloud delivery / deployment model identifies the specific type of cloud environment based on ownership, scale and access, as well as the cloud's nature and purpose.

→ It specifies how your cloud infrastructure will look, what you can change and whether you will be given services or will have to create everything yourself.

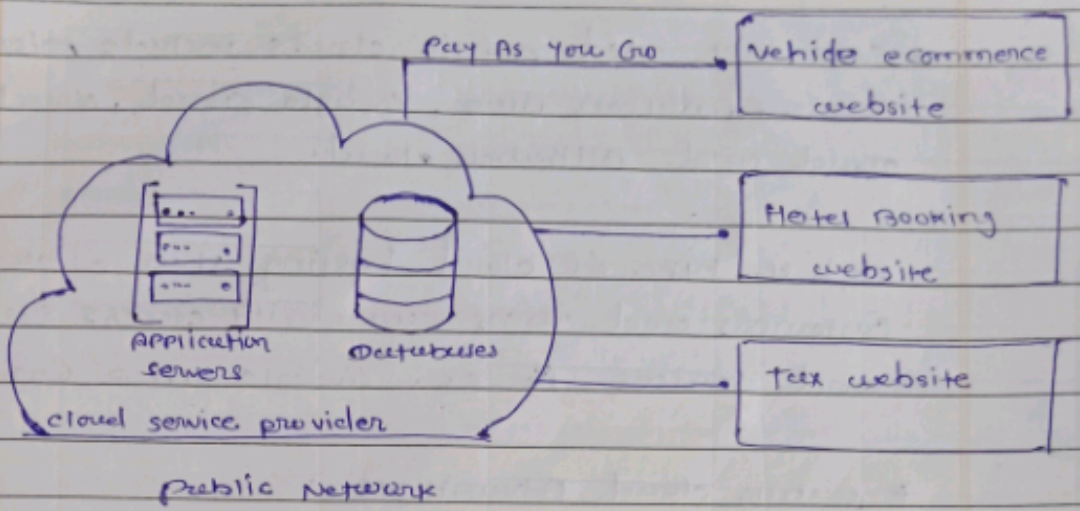
→ It works as your virtual computing environment with a choice of deployment model depending on how much data you want to store and who has access to the Infrastructure.

* Different types of delivery models are as follow

1. public cloud
2. Hybrid cloud
3. private cloud
4. community cloud.
5. multi cloud.

1) public cloud :

- The public cloud makes it possible for anybody to access systems and services.



- The public cloud may be less secure as it is open to everyone. It is also called the "external cloud".

- The public cloud is one in which cloud infrastructure services are provided over the internet to the general people or major industry groups.

- The infrastructure in this cloud model is owned by the entity that delivers the cloud services, not by the consumer.

- It is a good choice for companies and organizations with low-security concerns.

- public cloud deployments are frequently used to provide web-based email, online office applications, storage and testing and development environments.

- Commonly used public clouds include microsoft Azure, Amazon AWS, Google Cloud, Oracle cloud and Alibaba cloud.

- It is a type of cloud hosting that allows customers and users can easily access system and services. for ex. Google App Engine

* public cloud Advantages :

- It provides hassle-free infrastructure management. There is no need to configure, manage and maintain resources such as hardware and software. cloud service provider does it for you.

- It provides high scalability as you can scale up and down the resources as per the requirement.

- It is a cost-effective way in which you only pay for the resources you use.

- cloud computing providers promise 99.99% availability of your infrastructure.

* Minimal Investment :

Because it is a pay-per-use service, there is no substantial upfront fee making it excellent for enterprises that require immediate access to resources.

- No setup cost :

The entire infrastructure is fully subsidized by the cloud service providers, thus there is no need to set up any hardware.

- Infrastructure management is not required :

Using the public cloud does not necessitate infrastructure management.

- No maintenance : The maintenance work is done by the service provider (not users).

- Dynamic scalability : To fulfill your company's needs, on-demand resources are accessible.

* public cloud disadvantages :

- Data security and privacy concerns :

since it is accessible to all, it does not fully protect against cyber-attacks and could lead to vulnerabilities.

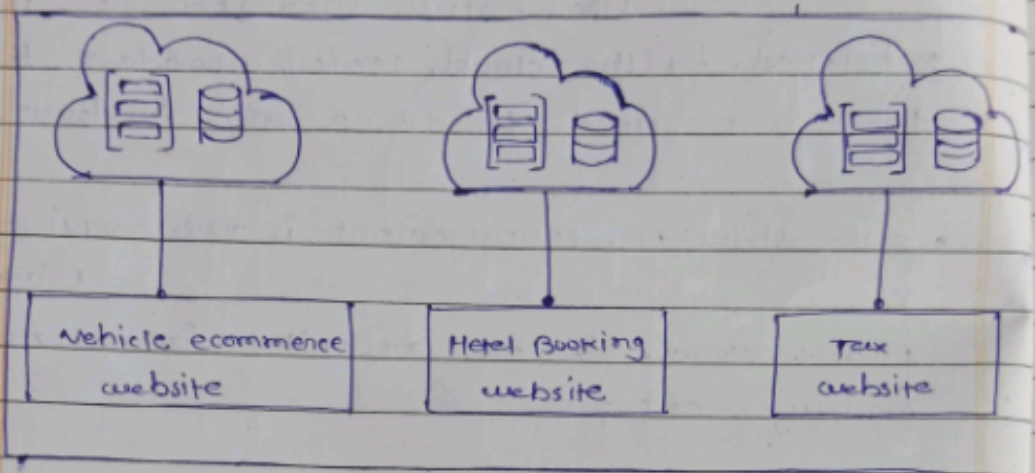
- Reliability issues :

since the same server network is open to a wide range of users, it can lead to malfunction.

- low customization :

It is accessed by many public so it can't be customized according to personal requirements.

2) private cloud



- The private cloud deployment model is the exact opposite of the public cloud deployment model.

- private cloud lets you use the infrastructure and resources for a single organization.

- users and organizations do not share resources with other users.

- That is why it is also called as Internal or Corporate model.

- private clouds are more costly than public clouds due to their costly maintenance.

- It's a one-on-one environment for a single user. (customer).

- There is no need to share your hardware with anyone else. It is also called the "Internal cloud" and it refers to the ability to access systems and services within a given border or organization.

- The cloud platform is implemented in a cloud-based secure environment that is protected by powerful firewalls and, under the supervision of an organization's IT department.

- The private cloud gives greater flexibility of control over cloud resources.

- private clouds are often used by government agencies, financial institutions, any other mid-to large-size organizations with business-critical operations seeking enhanced control over their environment.

- Examples of top private cloud Deployment model providers: Amazon web services, Microsoft Azure, Google cloud platform, Dell, cisco.

* Advantages of private cloud:

- private cloud provides high security and data privacy since only authorized users can access the resources.

- It offers high scalability and flexibility deployment options that allow companies to customize their infrastructures as per the need.

- private cloud supports a legacy system that cannot access the public cloud.

- Better control :

You are the sole owner of the property. you gain complete command over service integration, IT operations, policies and user behaviour.

- Data security and privacy :

It's suitable for storing corporate information, to which only authorized staff have access. By segmenting resources within the same infrastructure, improved access and security can be achieved

- supports legacy systems :

This approach is designed to work with legacy systems that are unable to access the public cloud.

- customization :

unlike a public cloud deployment a private cloud allows a company to tailor its solution to meet its specific needs.

- Security

Infrastru

higher le

* Disad

- less s

- Costly

- High

3) Hybri

private network

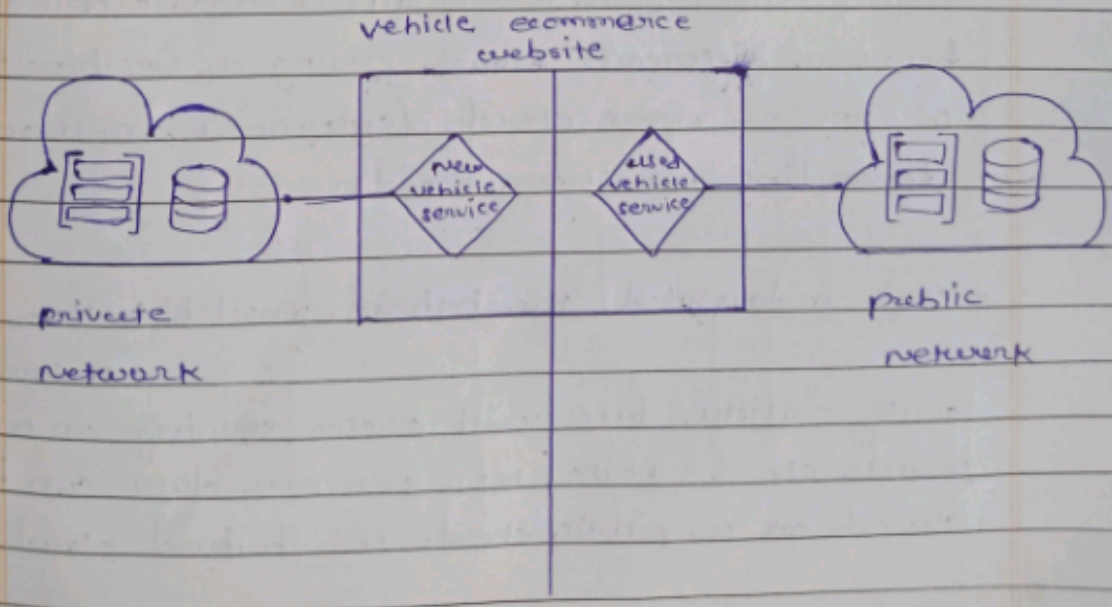
- Security :

segmentation of resources within the same Infrastructure can help with better access and higher levels of security.

* Disadvantages of private cloud :

- less scalable : private clouds are scaled within a certain range as there is less number of clients.
- Costly : private clouds are more costly as they provide personalized facilities.
- High maintenance : since it is managed in-house, the maintenance costs also increase.

3) Hybrid cloud :



- A hybrid cloud is a combination of two or more cloud architectures.

- The Hybrid cloud is a combination of both public and private clouds.

- cloud vendors keep the sensitive data in the private cloud, and non-sensitive data in the public cloud.

- By bridging the public and private worlds with a layer of proprietary software, hybrid cloud computing gives the best of both worlds.

- with a hybrid solution, you may host the app in a safe environment while taking advantage of the public cloud's cost savings.

- Organizations can move data and application between different clouds using a combination of two or more cloud deployment methods, depending on their needs.

- let's understand the hybrid model better:

A company with critical data will prefer storing on a private cloud, while less sensitive data can be stored on a public cloud. The hybrid cloud is

also frequently used for 'cloud bursting'. It means, suppose an organizations runs an application on-premises, but due to heavy load, it can burst into the public cloud.

* Advantages of Hybrid cloud :

- one of the major advantages of a hybrid cloud is that it comes up at a reasonable cost.
- It enhances the scalability and flexibility of resources.
- It offers improved security.
- Cost-Effectiveness :

  The overall cost of a hybrid solution decreases since it majorly uses the public cloud to store data.
- security :

  since data is properly segmented, the chances of data theft from attackers are significantly reduced.
- flexibility :

  with higher levels of flexibility, businesses can create custom solutions that fit their exact requirements.

* Disadvantages of hybrid cloud :

- Complexity : It is complex setting up a hybrid cloud since it needs to integrate two or more cloud architectures.
- specific use case : This model makes more sense for organizations that have multiple use cases or need to seperate critical and sensitive data.
- Difficult to manage : Hybrid clouds are difficu to manage as it is a combinat of both public and private cloud. so, it is complex.

* Cloud computing Deployment models Comparison

public	private	Community	Hybrid
used by small Enterprises	used by large Enterprises	used by small & large Enterprises	used by large Enterprise
supports multiple cust. (multi-Tenant)	supports dedicated cust. (single-Tenant)	supports multiple cust. (multi-Tenant)	supports multiple cu (multi-Ten

Connectivity over Internet	Connectivity over Internet, private network.	Connectivity over Internet, private network.	Connectivity over Internet, private network
Insecure. used for non-confidential data	Very secure. used for confidential data	Secure towards outside the community	medium secure.
Cost-effective	costly	Cost-effective	Cost-effective.
High-scalable	low-scalable	High scalable	High scaleable
non-guaranteed solution	Guaranteed solution	Guaranteed solution	partly guaranteed solution
shared servers	Dedicated servers	shared servers between community members	shared and Dedicated servers
provide low performance	provide. High performance	provide High Performance	provide High performance
flexible	Inflexible. There can be unused resources	flexible	Inflexible. There can be unused resources.

Q:3 Explain cloud data center Architecture.

→ A data center is a physical location that sto computing machines and their related hardware equipment.

→ It contains the computing infrastructure that IT systems require, such as servers, data stor drivers and network equipment.

→ It is the physical facility that stores every company's digital data.

→ simple datacenter definition then it is the brain of any organization where all the complex and critical operations are performed on powerful server machines.

* Main Components of a Data Center:

- Every data center is designed according to the needs and requirements of a particulare organization, in a well-constructed and safe building having the following Components:

- servers
- Networking
- storage
- software
- Environment monitoring.
- cabling
- Infrastructure
- Cooling
- Backup power.

- Servers :

Servers are powerful computers that process and store data.

- Servers run applications, manage network traffic and respond to user or system requests.

- Storage systems :

Data centers utilize different types of storage systems, including hard disk drives (HDDs) and solid-state drives (SSDs), to store and access data.

- Networking Equipment :

Networking equipment, including routers, switches and firewalls, facilitates communication between servers within the data center & with external networks.

- Cooling system :

Data centers produce a considerable amount of heat due to the operation of servers and other hardware components.

- Power Infrastructure :

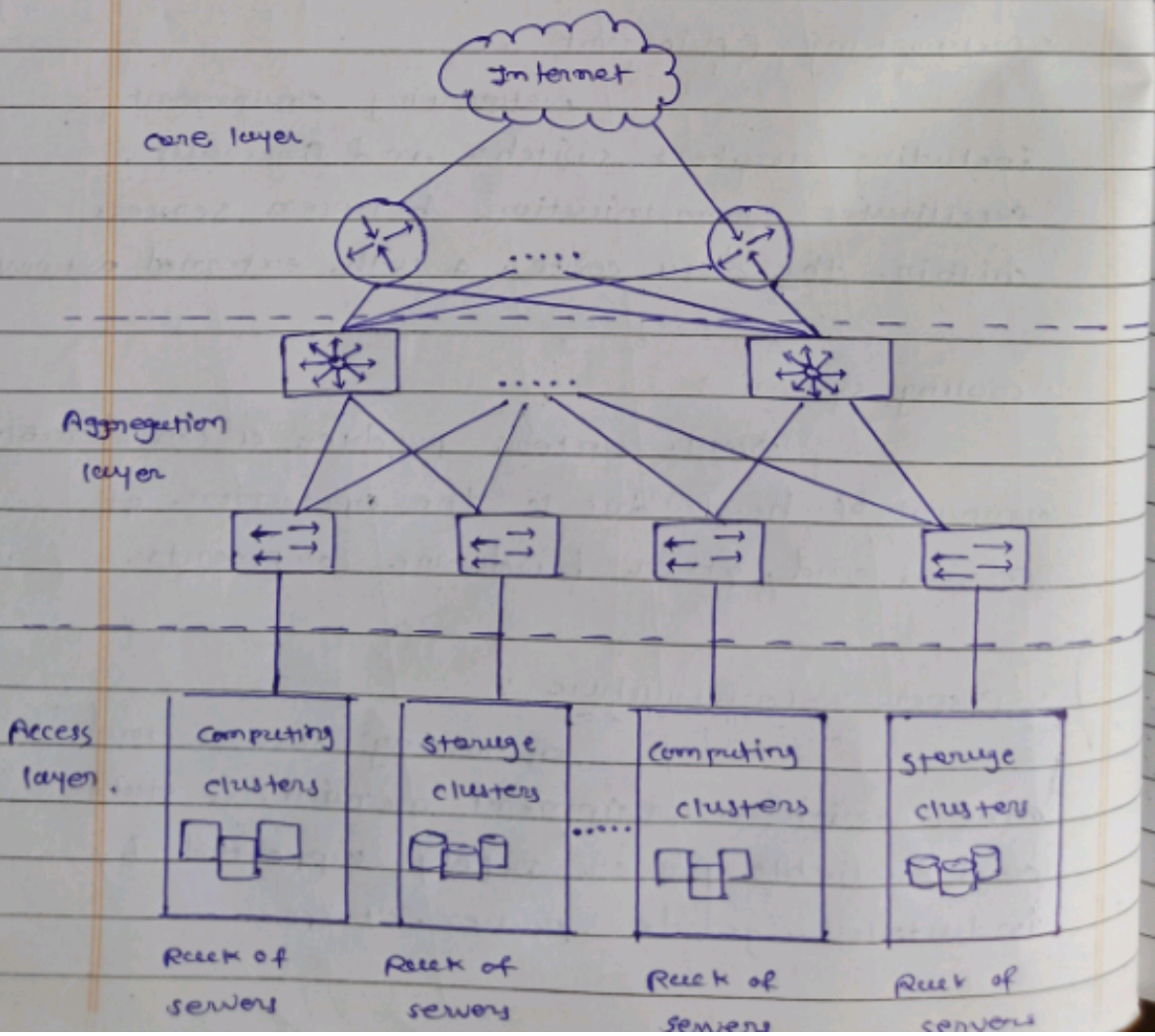
Operating servers and other critical equipment require a stable and reliable power supply supported by industrial-grade power-strips.

· Back up power systems :

Backup power systems like generators & batteries provide uninterrupted electricity during power outages, ensuring continuous data center operations.

· security system :

It implements various security measures, including access control systems, surveillance cameras and biometric authentication, to safeguard against unauthorized access, theft and physical threa



* Three-Tier Data Center Network Architecture :

- The three-tier data center network architecture is a traditional network topology that has been widely adopted in many older data centers and is often referred to as the 'core-aggregation-access' model or the 'core-distribution-access' model.

- Redundancy is a key part of this design, with multiple paths from the access layer to the core, in addition to helping networks achieve high availability and efficient resource allocation.

→ Here's an overview of each tier in the three-tier data center Network architecture :

• Access layer :

As the lowest tier in the three-tier data center Network Architecture, it functions as the entry point for servers, storage systems, and other devices into the network, providing connectivity through switches and cables.

- Access layer switches, often arranged in a top-of-rack (TOR) configuration, enforce policies such as security settings and VLAN (Virtual local Area Network) assignments.

• Aggregation layer :

- Also known as the distribution layer.
- it consolidates data traffic from the access layer's top-of-rack switches before transmitting it to the core layer for routing to its ultimate destination.
- This layer enhances the data center network's resilience and availability through redundant switches, eliminating single points of failure, and controlling network traffic through policies like load balancing, quality of service (QoS) packet filtering, queuing and inter-VLAN routing.

• Core layer :

- Also known as the backbone.
- it is the high-capacity, central part of the network designed for redundancy and resilience, interlinking aggregation layer switches and connecting to external networks.

- Operating at level 3, the core layer prioritizes speed, minimal latency and connectivity using high-end switches, high-speed cables and routing protocols with lower convergence

* How do data centers work ?

- A data center facility enables an organization to assemble its resources and infrastructure for data processing, storage and communication, including :

- Data centers contain physical or virtual servers that are connected internally and externally through networking and communication equipment to store, transfer and access digital information.

- Each server has a processor, storage space and memory, similar to a personal computer but with more power.

- Data centers use software to cluster the servers and distribute the workload among them.

* What is inside a data center :

- Most enterprise data center infrastructure falls into three broad categories :

  - Compute
  - storage
  - Network

- Also data center equipment includes support infrastructure like power systems which help the main equipment function effectively.

- Computing infrastructure :

Computing resources include several types of servers with varying internal memory, processing power and other specifications.

- We give some examples below.

1 Rack servers :

Rack servers have a flat, rectangular design and you can stack them in racks or shelves in a server cabinet.

- The cabinet has special features like mesh doors, sliding shelves and space for other data center resources like cables and fans.

2 Blade servers :

A blade server is a modular device & you can stack multiple servers in a smaller area.

- The server itself is physically thin and typically only has memory, CPUs, integrated network controllers and some built-in storage drivers.

- You can slide multiple servers into a storage unit called a chassis.

- The chassis facilitates any additional components that the servers inside it require.
- Blade servers take up less space than rack servers and offer higher processing speed, minimal wiring and lower power consumption.

• storage infrastructure :

- The following are two types of data center storage systems:

1. Block storage devices:

Block storage device like hard drives and solid-state drives store data in blocks and provide many terabytes of data capacity.

- storage area networks (SANs) are storage units that contain several internal drives and act as large block storage systems.

2. File storage devices :

File storage devices, like Network-attached storage (NAS), can store a large volume of files.

- You can use them to create image and video archives.

• Network infrastructure :

- A large number of Networking devices, such as cable

switches, routers and firewalls connect other data center components to each other and end-user locations.
- They provide flawless data movement and connectivity across the system.

• Support infrastructure :

- Data centers also contain these components
  - power subsystems
  - uninterruptible power supplies (UPS)
  - Backup generators
  - Ventilation and cooling equipment
  - Fire suppression systems
  - Building security systems.

* what are the types of data center services ?

- you can choose from many types of data center services, depending on your requirement

• On-premises data centers :

- On-premises data centers are fully owned company data centers that store sensitive data and critical applications for that company.
- you set up the data center, manage its ongoing operations and purchase and maintain the equipment.

* Benefits : An enterprise data center can give better security because you manage risks internally.
- you can customize the data center to meet your requirements.

* limitations : It is costly to set up your own data center and manage ongoing staffing and running costs.
- you also need multiple data centers because just one can become a single high-risk point of failure.

• Collection data centers :

- Colocation facilities are large data center facilities in which you can rent space to store your servers, racks and other computing hardware.
- The colocation center typically provides security and support infrastructure such as cooling and network bandwidth.

- Benefits : Colocation facilities reduce ongoing maintenance costs and provide fixed monthly costs to house your hardware.
- you can also geographically distribute hardware to minimize latency and to be closer to your end users.

- limitations : It can be challenging to source colocation facilities across the globe and in different geographical areas you target.
  - costs could also add up quickly as you expand.

- Cloud Data Centers :

- In a cloud data center, you can rent both space and infrastructure.
- cloud providers maintain large data centers with full security and compliance.
- You can access this infrastructure by using different services that give you more flexibility in usage and payment.
- Benefits : A cloud data center reduces both hardware investment and the ongoing maintenance cost of any infrastructure.
  - It gives greater flexibility in terms of usage options, resource sharing, availability and redundancy.

Q:4 Explain following terms :

1. Region
2. availability zone
3. Point of presence.

(i) Region :

→ In the context of cloud computing, a region refers to a geographical area where a cloud service provider, such as Amazon web services (AWS), Microsoft Azure, or Google cloud platform (GCP), has established data centers and infrastructure to offer its services.

→ Each region comprises multiple availability zones or data centers that are strategically located to provide redundancy, high availability, and disaster recovery capabilities.

→ Customers can deploy their applications and data in specific regions to optimize performance, compliance and data residency requirements.

→ Cloud regions are distinct geographical areas where cloud providers operate data centers.

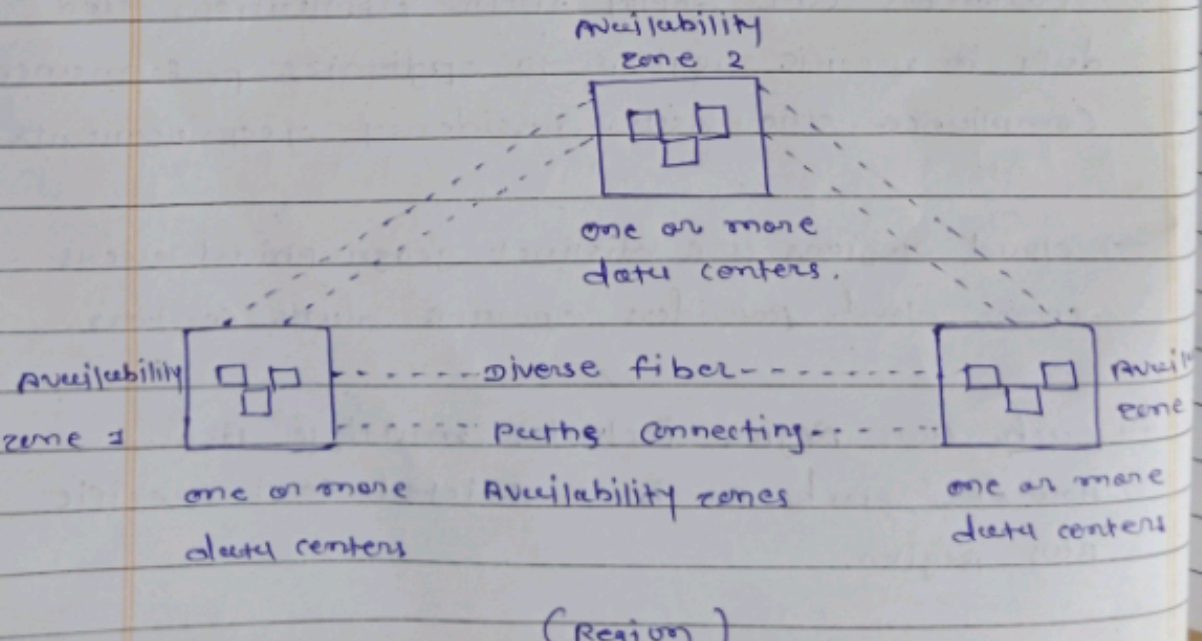
→ Each AWS Region includes multiple AZs. However, each AZ is restricted to a specific AWS Region.

→ you can use multiple AZs within one Region, but you can't use the same AZ across multiple Regions.

→ cloud regions usually have multiple isolated AZ's (Availability zones), with each AZ comprising one or more data centers located in close proximity.

→ To make their services readily accessible worldwide, CSPs (cloud service providers) usually organize their cloud infrastructure into different geographical regions, known as cloud regions.

→ cloud regions are essentially arbitrary geographical areas, which means each vendor may have distinct regions with varying names and boundaries.



(Region)

(ii) Availability zone :

→ Availability zones are physically separate data centers within an Azure region.

→ Each availability zone is made up of your one data or more data centers equipped with independent power, cooling and networking.

→ It is set up to be an isolation boundary.

→ Azure creates a duplicates of your data and resources so that the information is safe, in case of failure. If one zone goes down, the other continues working.

→ Resources are highly available through Availability Zones.

→ An AZ is a standalone data center or set of data centers within a Region.

→ Each AZ operates independently, so a failure in one won't affect others.

→ In disaster recovery plans, enterprises use multiple AZs to increase redundancy and reliability.

→ An availability zone (AZ) consists of one

or more discrete but closely located data centers.

- Each data center in a single availability zone is designed to remain operational even in the event of a failure at any other data center within that same zone.

→ Still, multiple data centers or buildings within a single availability zone are considered a single logical entity.

→ They are treated as a single failure domain because all the data centers in an availability zone face the same local physical risks, such as natural disasters or power failures.

→ Major cloud providers divide their operations into regions for fault tolerance and localized performance benefits.

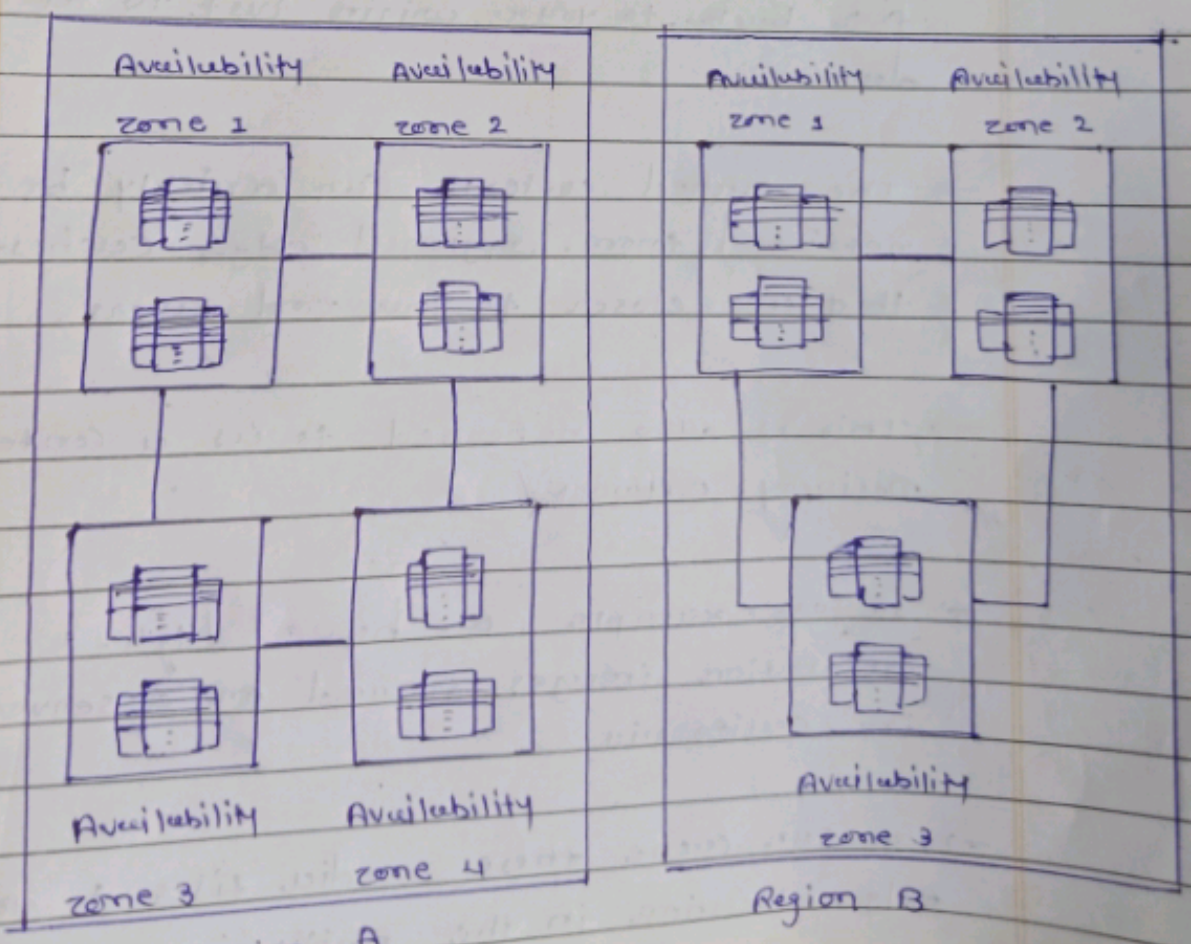
→ A region is not a single, monolithic data center; instead, it is an arbitrary geographical area where the cloud provider has a physical presence and hosts one or more clusters of data centers called availability zones (AZs).

→ All regions are isolated for fault tolerance but interconnected to each other and the internet via high-speed fiber optic networks.

→ It is common to select regions and AZs closest to business operations to achieve the highest performance possible.

→ However, not all regions or AZs are equal, and some services may only be available in specific regions or AZs.

Availability zones vs. Regions.



(iii) point of presence (PoP) / Edge locations / Content delivery Network.

→ It consists of Edge locations and Regional Edge caches, which enables us to distribute our content with low latency to our global users.

→ Basically, a PoP serves as an access point that allows two different networks to communicate with each other.

→ By using these global edge Networks, a user request doesn't need to travel far back to your origin just to fetch data.

→ The cached contents can quickly be retrieved from regional edge caches that are closer to your end users.

→ This is also referred to as a Content Delivery Network.

→ so for example, we have high-resolution images stored on a server in California.

→ we can cache these media files to an edge location in the philippines, India,

or singapore to allow our customers in Asia to retrieve these photos faster.

→ The images will be loaded quickly because it is fetched to an edge server near our users, instead of retrieving it from the origin server in California.

Q.5 Explain virtual private cloud & SLAC service level

* Virtual private cloud (VPC):

→ Dedicated cloud computing environment within a public cloud that provides a high level of isolation and security for resources.

→ Think of it as having your own private data center within a larger shared cloud infrastructure.

• Key features:

• Isolation: Network isolation is provided using private IP addresses, subnets and virtual local Area Networks (VLANs)

• Control: users have control over their virtual networking environment, including the

selection of IP address ranges, creation of subnets and configuration of route tables and network gateways.

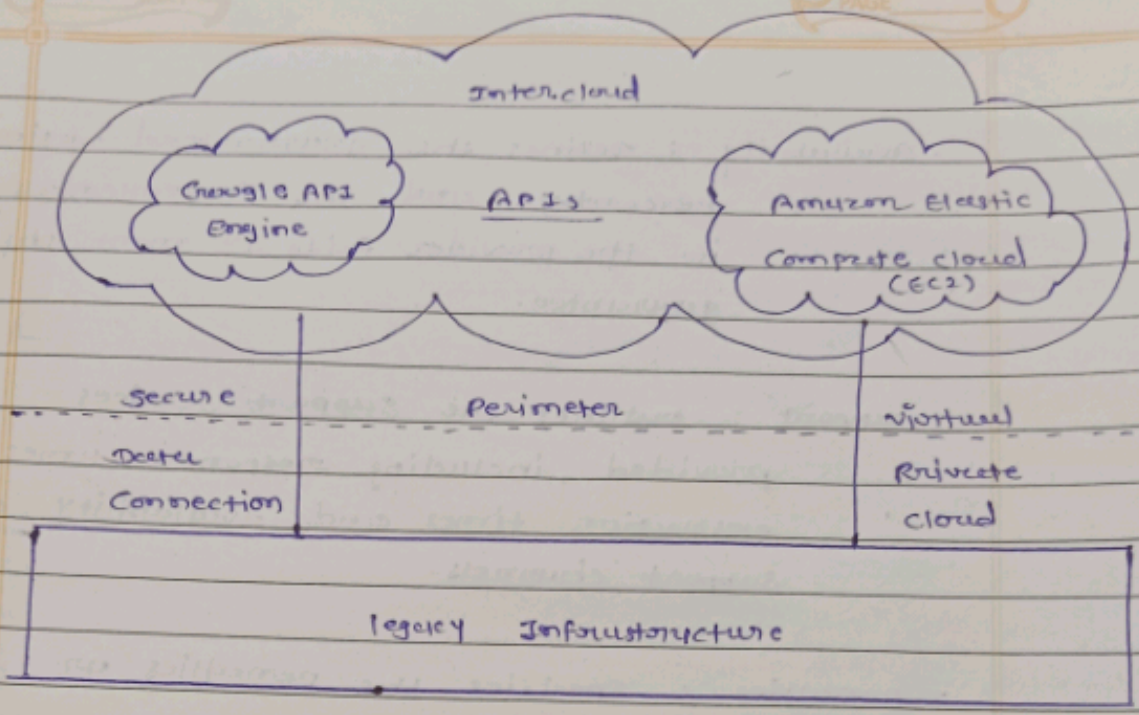
- security : VPCs are typically include features like network firewalls, security groups and network Access Control lists (NACLs) to manage inbound and outbound traffic.

- Advantages of VPC :

- Enhanced security
- customizable Network Configuration
- Scalability
- Reliability
- cost-effective.

- Disadvantages of VPC :

- Complexity
- Resource management
- vendor lock-in
- Cost variability
- Dependency on Internet Connectivity.



Virtual private cloud (VPC)

* Service level Agreement (SLA) :

→ It is a contract between a service provider and a customer that defines the level of service expected from the service provider.

→ In cloud computing, an SLA is crucial for setting expectations and responsibilities for both parties.

• Key point components :

- performance metrics : specifies the minimum performance standards, such as uptime, response time and throughput.

- Availability : Defines the guaranteed uptime percentage and the consequences if the provider fails to meet this guarantee.

- Support : outlines the support services provided, including response times, resolution times and, availability of support channels.

- penalties : Specifies the penalties or compensation if the service provider fails to meet the agreed-upon service levels.

- Data management : Covers data security, backup and recovery protocols.