UNIT 1
QUESTION BANK

What is cloud computing? What are the component of cc?

•Cloud computing is the on-demand availability of computer system resources, especially data storage and computing power, without direct active management by the user.
Simply cloud computing is the delivery of computing services—including servers, storage, databases, networking, software, analytics, and intelligence—over the Internet ("the cloud") to offer faster innovation, flexible resources, and economies of scale.
Characteristics of Cloud Computing
1. On-demand self-service

2. Broad network access

3. Multi-tenancy and resource pooling

4. Rapid elasticity and scalability

5. Measured service

Components of Cloud Computers are 1) Client Infrastructure, 2) Application, 3) Service, 4) Runtime Cloud, 5) Storage, 6) Infrastructure, 7) Management, 8) Security, and 9) Internet.
1. Client Infrastructure:

Client Infrastructure is a front-end component that provides a GUI. It helps users to interact with the Cloud.
2. Application:

The application can be any software or platform which a client wants to access.
3. Service:

The service component manages which type of service you can access according to the client's requirements.
Three Cloud computing services are:

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

4. Runtime Cloud:

Runtime cloud offers the execution and runtime environment to the virtual machines.

5. Storage:

Storage is another important Cloud computing architecture component. It provides a large amount of storage capacity in the Cloud to store and manage data.

6. Infrastructure:

It offers services on the host level, network level, and application level. Cloud infrastructure includes hardware and software components like servers, storage, network devices, virtualization software, and various other storage resources that are needed to support the cloud computing model.

7. Management:

This component manages components like application, service, runtime cloud, storage, infrastructure, and other security matters in the backend. It also establishes coordination between them.

8. Security:

Security in the backend refers to implementing different security mechanisms for secure Cloud systems, resources, files, and infrastructure to the end-user.

9. Internet:

Internet connection acts as the bridge or medium between frontend and backend. It allows you to establish the interaction and communication between the frontend and backend.

Advantages and disadvantages of cc?

ADVANTAGE-

1) 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.

2) Improved collaboration

Cloud applications improve collaboration by allowing groups of people to quickly and easily share information in the cloud via shared storage.

3) Excellent accessibility

Cloud allows us to quickly and easily access store information anywhere, anytime in the whole world, using an internet connection. An internet cloud infrastructure increases organization productivity and efficiency by ensuring that our data is always accessible.

4) Low maintenance cost

Cloud computing reduces both hardware and software maintenance costs for organizations.

5) Mobility

Cloud computing allows us to easily access all cloud data via mobile.

6) IServices in the pay-per-use model

Cloud computing offers Application Programming Interfaces (APIs) to the users for access services on the cloud and pays the charges as per the usage of service.

7) Unlimited storage capacity

Cloud offers us a huge amount of storing capacity for storing our important data such as documents, images, audio, video, etc. in one place.

8) Data security

Data security is one of the biggest advantages of cloud computing. Cloud offers many advanced features related to security and ensures that data is securely stored and handled.

DISADVANTAGE-

1) Internet Connectivity

As you know, in cloud computing, every data (image, audio, video, etc.) is stored on the cloud, and we access these data through the cloud by using the internet connection. If you do not have good internet connectivity, you cannot access these data. However, we have no any other way to access data from the cloud.

2) Vendor lock-in

Vendor lock-in is the biggest disadvantage of cloud computing. 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.

3) Limited Control

As we know, 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.

4) Security

Although cloud service providers implement the best security standards to store important information. But, before adopting cloud technology, 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 information is hacked by Hackers.

What are the main benefits of migration to the cloud?

Cloud migration is the process of moving a company's digital assets, services, databases, IT resources, and applications either partially, or wholly, into the cloud. Cloud migration is also about moving from one cloud to another.
Benefits of migrating to the cloud include:

- Increased agility and flexibility
- Ability to innovate faster
- Easing of increasing resource demands
- Better managing of increased customer expectations
- Reduction in costs
- Deliver immediate business results
- Simplify IT
- Shift to everything as-a-service
- Better consumption management
- Cloud scalability
- Improved performance

Write a note on the multitenant nature of the SAAS solution?

Multi-tenant SaaS is a business structure where many organizations share the same software to save and store data. Multi-tenant SaaS also implies that a single instance of the software and its supporting information is used by multiple customers.

Each customer shares the same database and application.

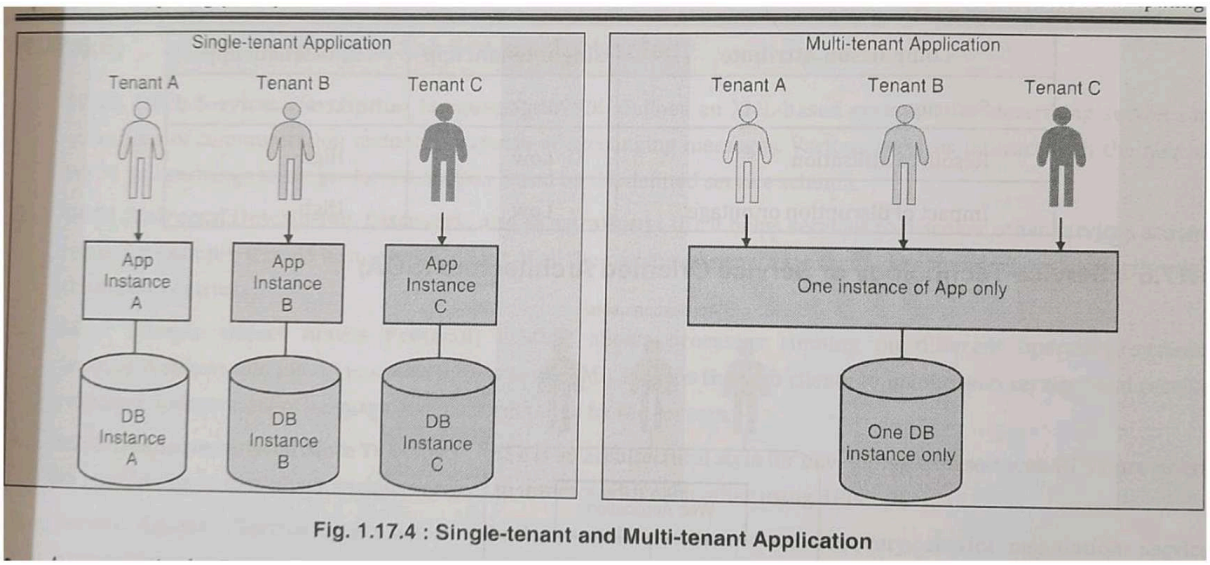


Fig. 1.17.4 : Single-tenant and Multi-tenant Application

As you see in Fig. 1.17.4, single-tenant applications can only serve one tenant at a time whereas the multi-tenant applications require just one instance (one installation only) and can serve multiple users simultaneously.

So, in a nutshell, to build a multi-tenant application, you need to separate the user data and provide a mechanism to use the application without disrupting the usage by other tenants of the applications. Various cloud services such as Google App Engine and Amazon S3 support multi-tenancy.

Benefits of Multi-Tenant SaaS Architecture

1. Lower Costs

Since multi-tenant architecture enables the exchange of services, databases, resources, and applications, it can cost less than a single-tenant structure. Scaling has fewer implications because new users can access the same software as the original buyers.

2. Efficient Resources

Because all resources are shared, multi-tenant architecture uses resources that offer optimum efficiency. Since it's a changing environment where resources are accessed simultaneously, multi-tenant SaaS software needs to have the capacity for powering multiple customers at once.

3. Fewer Maintenance Costs

Customers don't have to pay expensive fees to keep the software up to date. Maintenance costs are usually associated with a SaaS subscription and aren't charge per case like with a single-tenant structure.

4. Shared Data Centers

Similar to a single-tenant environment, a vendor doesn't have to create a new data center for every new user. Customers have to use a common infrastructure that removes the need to increase the number of data centers for each tenant.

5. Larger Computing Capacity

The multi-tenant architecture provides organizations with the ability to stay in the same data center and infrastructure. Therefore, customers won't have to think about adding more server or computing capacity.

Now that we understand the differences between single- and multi-tenant SaaS, let's compare the drawbacks of each one.

Single-Tenant vs Multi-Tenant Pros and Cons

- Single-tenant SaaS typically costs more than multi-tenant SaaS.
- Single-tenant SaaS requires more maintenance than multi-tenant SaaS.
- Single-tenant SaaS can be more inefficient than multi-tenant SaaS.
- Multi-tenant SaaS can experience more downtime than single-tenant SaaS.
- Multi-tenant SaaS has more in-app disturbances than single-tenant SaaS.
- Multi-tenant SaaS can't be customized like single-tenant SaaS.

write a short note on identity management as a service?

Identity-as-a-Service, or IDaaS, refers to a wide variety of cloud-hosted services for identity and access management (IAM). Essentially, IDaaS is a category of technological functions that have to do with user identity and are hosted in the cloud. IDaaS providers help ensure that users are who they claim to be, ultimately blocking cybercriminals and other unauthorized users from accessing sensitive data.

IDaaS providers can offer a number of user authentication services, such as:

Multi-factor authentication (MFA): MFA is the use of multiple authentication factors to verify a user's identity. One example would be requiring users to insert a USB device into their laptop, in addition to entering their password. MFA is more secure than username and password combinations alone. Cloud MFA providers enable organizations to quickly implement MFA. (See also: What is two-factor authentication?)

Single sign-on (SSO): SSO allows users to sign in once to a single portal in order to access all of their SaaS applications, and it also provides a centralized place for companies to manage the applications each user has access to. Most SSO services are cloud-hosted and allow users to access their SSO login pages through a web browser.

Identity management: An identity provider (IdP) stores and manages user identities. An IdP may check user identities via username-password combinations and other factors, or it may simply provide a list of user identities that another service provider checks. Cloud-hosted IdPs fit under the IDaaS umbrella.

what are the benefits of cloud storage?

1. **Backup Your Data to the Cloud**

If you've ever had a hard drive die on you, you're familiar with the pandemonium it can cause, especially if you're an at-home worker. Not only do you have to get it replaced, but your data might be gone for good.

Some data might be salvageable via a very pricey restoration service, although those aren't always capable of recovering your data, and usually at least some of it will be gone for good. Or an even worse scenario: you lose your phone or laptop. Now there's no way of getting your data back at all.

A cloud backup can save your data even in the worst cases.

That's where cloud storage comes in. Keeping your data backed up to the cloud is the only way you can make sure it stays safe and easily accessible. Even better, cloud storage providers that keep multiple versions of your files stored in the cloud are the best suited for disaster recovery.

2. **No More External Hard Drives**

Like the laptop before it, the cloud brings a new level of portability for your data. However, with cloud storage, you don't have to lug around a laptop, USB stick or external hard drive. Portability is built into the cloud, with all your data available to you wherever you can log in to your cloud account.

3. **Remotely Update and Sync Your Files**

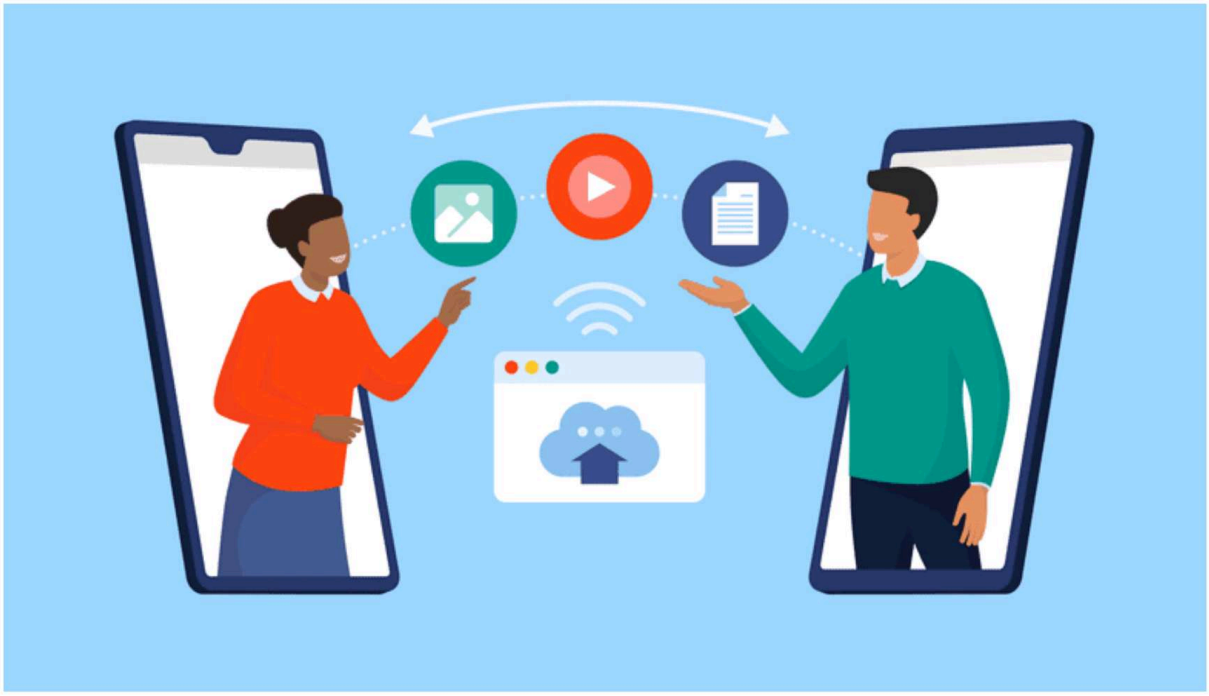
If you make a change to a file that's on your computer and want to update the file on another computer, you'll have to manually copy the file over to that device. On the other hand, updating a cloud file means the file now looks the same to everyone accessing it on every device.

Plus, most cloud services have a feature called "synchronization," or just "sync." To use sync, you usually need to download a cloud app called a "sync client" and log in. If you have the sync client installed on multiple devices, it will sync your files instantly across every device, which means you don't have to manually upload or download anything.

Some services, like pCloud and Icedrive, even offer so-called "network drives" that allow you to access your files without syncing them, saving you precious hard drive space.

4. **Share Files Easily**

One of the best things about cloud storage is just how easy file sharing is. If your files are already in the cloud, you don't need to upload them to a file transfer service or even send an email. You can just find the file in your cloud account and hit "share." Usually you'll get a link that you can paste wherever you want, and the recipient will be able to download or view your file.



Sharing files is easy when all your files are in the cloud.

If easy file sharing is what you need, you can check out our list of the best cloud storage services for sharing, where Sync.com comes out on top (take a look at our Sync.com review, too).

5. **Remote Work Made Easy**

Cloud technology is essentially what makes remote work possible in the first place. Without remote access to your work files, you're stuck moving back and forth between the office, which defeats the purpose of remote working.

However, since the cloud leaves all your cloud files at your disposal wherever you are, it's easy to pick up where you left off when you get back home. Just open your cloud account, and all the files you worked on in the office are right there. Head over to our best cloud storage for collaboration list if you need a cloud service for remote work.

The cloud lets you access your work files remotely to work from home.

6. **Keep Your Files Encrypted**

A lot of people are scared of the internet and think their files are safer just staying offline. However, that's not the case. If your files are only stored locally on your device, it makes them susceptible to hackers who can get into your computer and hold your data for ransom. Not to mention all the various hardware issues that could cause you to lose your data permanently.

Keeping your files in the cloud is simply the smarter thing to do. Luckily most cloud services offer encryption for your files. Encryption is a process that scrambles your files into a string of unreadable code, which is only readable using an encryption key. One flaw is that if you store your files with an untrustworthy operator, the operator can decrypt and access your files.

However, that's not the case if you use a zero-knowledge cloud service. Zero-knowledge encryption is a type of encryption where you're the only person holding the encryption key. The encryption happens on your device before the files are even sent to the cloud service, which means you're the only one who'll ever be able to view them.

7. **Storage for a Lifetime**

When you use an online service, making a long-term commitment always pays off. That's especially true with something you don't want to change frequently, like cloud storage.

Thankfully several cloud solutions offer lifetime plans. A lifetime plan lets you make a one-time purchase for a certain amount of storage and use that storage forever. The cost savings are usually greater than monthly or even yearly plans.

Unfortunately lifetime plans are few and far between. Icedrive and pCloud — two services we already mentioned — are the only services whose lifetime plans we'd recommend. You can see our pCloud review and Icedrive review for more details.

explain the cloud deployment model as per and nist guidelines?

Deployment Models

Cloud deployment models represent a specific type of cloud environment that is distinguished by ownership, size, and access. NIST offers guidance via its definitions of each of the four deployment cloud models (Private, Community, Public, and Hybrid).

private cloud

Definition: The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units).

A private cloud is created for the self-use of any organization. The organization itself creates a private cloud or it can let a third-party vendor set it up and manage it on its behalf of it. The resources in the private cloud are for the exclusive use of the organization for which the private cloud is created. The organization can choose to have its private cloud deployed within its physical perimeter (on-premises or on-site) or outside the company boundaries (off-premises or off-site).

Drawing from our taxi service example, private cloud is like you buying or renting a bus for your employees on a long-term basis. Only the employees of the company can use the bus and no one else even if the bus is lying idle during office hours.

Public Cloud

The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

The public cloud is the cloud deployment environment that is open to public use. It is not tied to a particular organization's usage exclusively. This is the most prevalent form of cloud deployment option today. Public cloud providers serve multiple tenants by sharing and isolating the computing resources.

Several public cloud providers exist in the market today - Amazon Web Services, Microsoft Azure and Google Cloud Platform are the most preferred public cloud providers.

Community Cloud

Definition: The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off-premises.

Community Cloud is similar to a Private Cloud except for one key difference instead of a single organization for which the private cloud is created, a community cloud is created by and for a group of organizations. These organizations are similar in nature in terms of their mission, business, market requirements, policies, legal implications, compliance, and customers. For example, various banks such as ICICI, HDFC, IDFC, etc. can come together and build a community cloud that can serve their respective requirements. These banks have more or less the same business requirements and thus mutually benefit by sharing the infrastructure cost and leveraging community cloud service for their exclusive use. A common example of a community cloud is AWS GovCloud (US) which is created to be used only by the US-based Government agencies and has strict tenant qualification criteria for using its cloud services.

UNIT 2

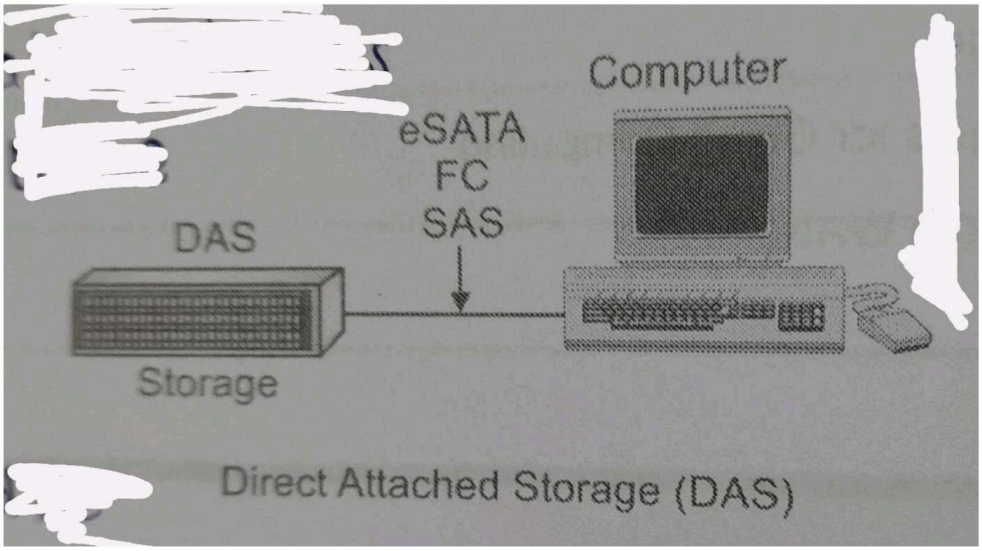
What is DAS?

Direct-attached storage (DAS) is a type of storage that is attached directly to a computer without going through a network. The storage might be connected internally or externally. Only the host computer can access the data directly. Other devices must go through the host computer to work with the data.

Most servers, desktops and laptops contain an internal hard disk drive (HDD) or solid-state drive (SSD). Each of these devices is a form of direct-attached storage. Some computers also use external DAS devices. In some cases, an

enterprise server might connect directly to drives that are shared by other servers.

A direct-attached storage device is not networked. There are no connections through Ethernet or Fibre Channel (FC) switches, as is the case for network-attached storage (NAS) or a storage area network (SAN).



Advantages of DAS:

- It is high availability
- Data security and fault tolerance
- Storage capacity expansion
- Faster for certain applications
- Greater data security
- High access rate due to storage area network absence
- Elimination of network setup complications

Disadvantages of DAS:

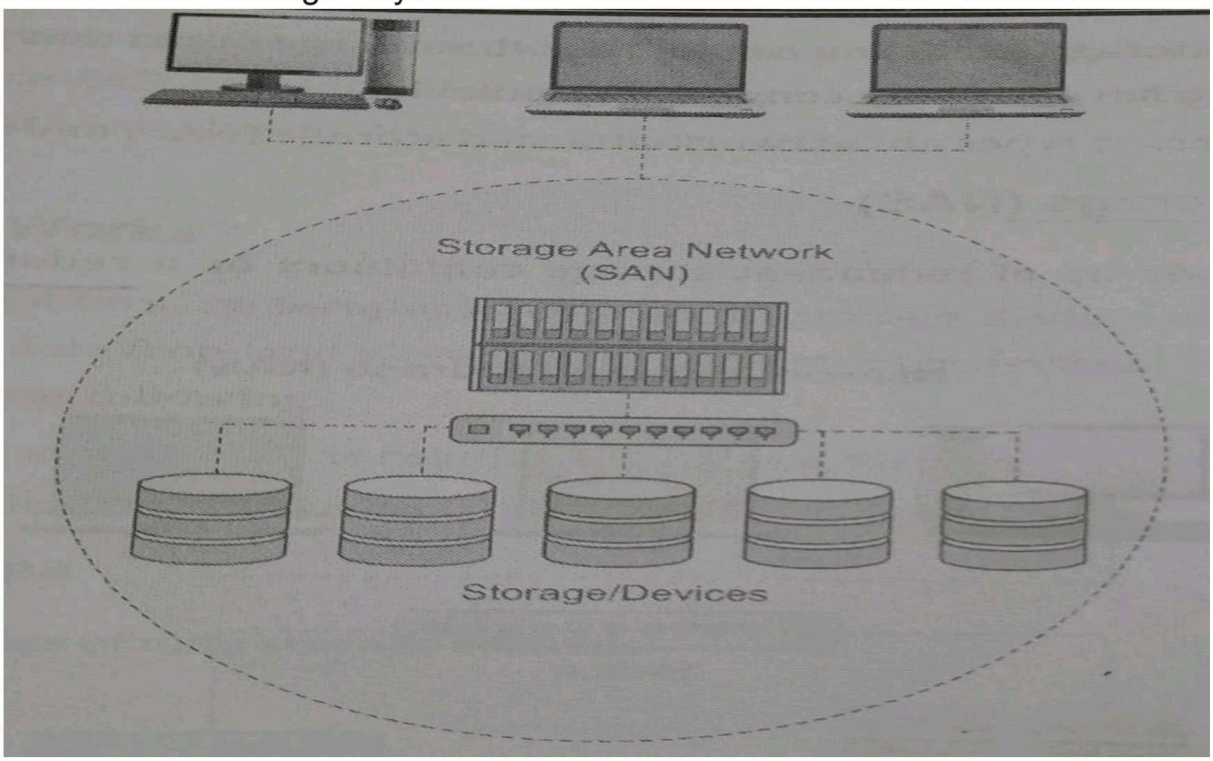
- Data not accessible by diverse user groups
- High administrative costs
- Allows only one user at a time
- Limited sharing
- Mangaribly for IT managers
- Improper capacity utilization

Explain SAN?

A SAN (storage area network) is a network of storage devices that can be accessed by multiple servers or computers, providing a shared pool of storage

space. Each computer on the network can access storage on the SAN as though they were local disks connected directly to the computer.

A storage area network (SAN) is a dedicated, independent high-speed network that interconnects and delivers shared pools of storage devices to multiple servers. Each server can access shared storage as if it were a drive directly attached to the server. A SAN is typically assembled with cabling, host bus adapters, and SAN switches attached to storage arrays and servers. Each switch and storage system on the SAN must be interconnected.



Advantages of Storage area network:

- Simplified storage administration
- Disk mirroring
- Low cost of storage management
- Instant and real-time information
- Ability to boot itself and expand the storage capacity
- Hundreds of terabytes of data can be stored using any number of storage devices.
- SAN is not directly attached to any particular server or network, SAN can be shared by all

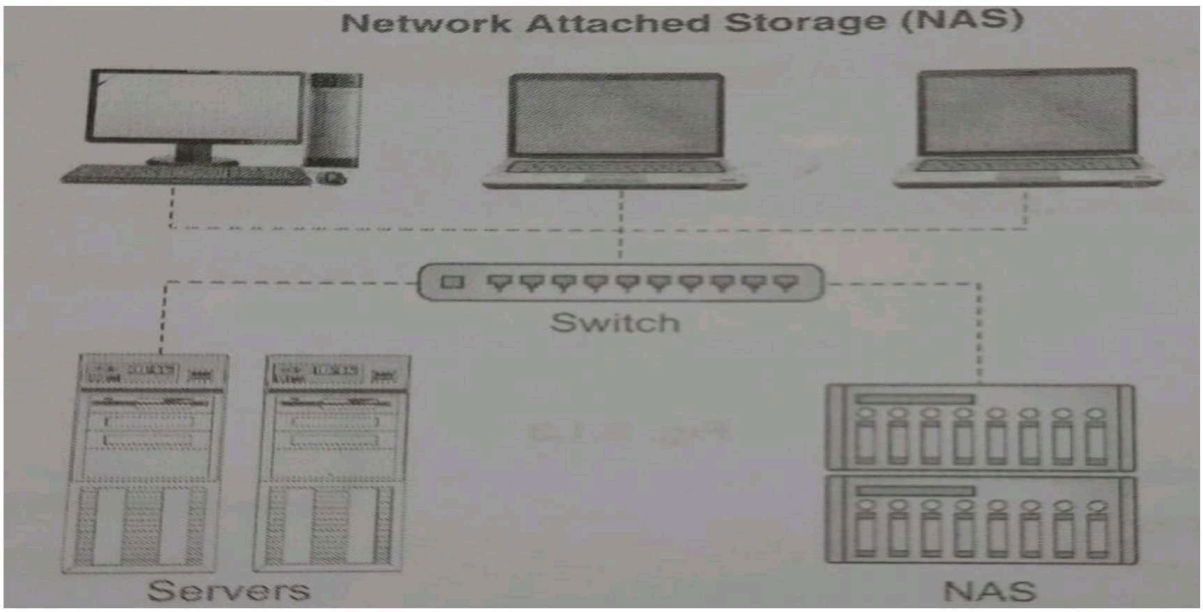
Disadvantages of storage area network:

- If client computers need intensive data transfer then SAN is not the right choice. SAN is good for low data traffic
- More expensive
- It is very hard to maintain
- As all client computers share the same set of storage devices so sensitive data can be leaked. It is preferable not to store confidential information on this network.
- Poor implementation results in a performance bottleneck
- It's difficult to keep a data backup in case of a system failure.
- Not affordable for small business
- Require a high-level technical person

Explain NAS?

Network-attached storage (NAS) is dedicated file storage that enables multiple users and heterogeneous client devices to retrieve data from centralized disk capacity. Users on a local area network (LAN) access the shared storage via a standard Ethernet connection.

NAS devices typically do not have a keyboard or display and are configured and managed with a browser-based utility. Each NAS resides on the LAN as an independent network node, defined by its own unique Internet Protocol (IP) address.



Advantages of NAS:

- Relatively inexpensive
- A self-contained solution
- Ease of administration
- It is multi-protocol
- A wide array of system and size to choose from
- Drive failure tolerant storage volumes
- Automatic backup to other devices and the cloud.
- Easy to install and configure
- 24/7 and remote data availability
- More flexible than DAS
- It requires some knowledge of computer network to use them efficiently
- Universal client access
- With NAS you will get the same speed of data transfer as DAS that is faster
- The user who wants their data processed directly because will need to do it through installed OS

Disadvantages of NAS:

- Performance depends on the protocol
- Slow down for video application or multiple large files

- It is file oriented
- Increased LAN traffic
- The file transfer speed is not as fast as DAS
- Limited scalability
- Additional Input-output processing
- System available features depend upon the NAS chip and firmware
- For using NAS device people should know some basic knowledge about computer networking

Q12) How to improve Performance in cloud through Load balancing ?

⇒ improve your cloud application Presentation using load balancer.

- Random spikes in online traffic can cause trouble for the best websites and requests.
- During online sales event such as Amazon Prime day, even a brief outage of few seconds can cost you millions in revenue
- Cloud load balancers and traffic managers can save your day by allocating workloads across multiple servers and cloud resources.
- They maximize your Performance and helps in avoiding overload. for a seamless user experience. firstly applying cloud makes a lot of changes in your application architecture.
- Its a misinterpretation that moving your applications and backend on the Internet is adopting cloud. Its way beyond Ping Power and Pipe Strategy and hosting your applications in someone else's server.
- Apart from co-location benefits and designers can use API's load balancers and automation to improve the system Performance.

- Load Balancer :- Load balancer is a device wich allocates network or application traffic across a number of servers. It enables the systems to fulfill requests in a manner that exploits speed and capacity.

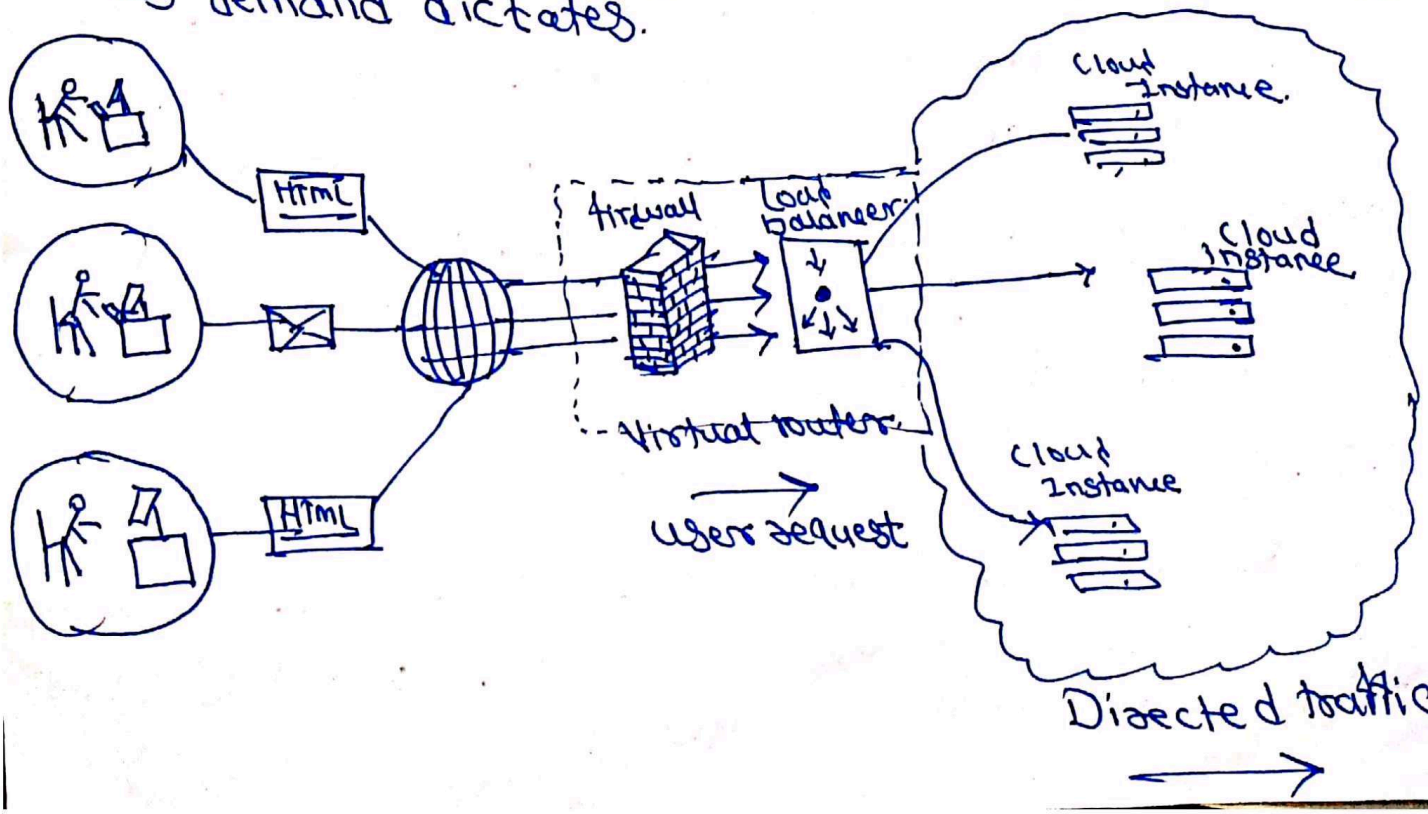
Utilization. The load balancer prevents presentation degradation and ensures none of the servers is overworked.

- The load balancer mechanically redirects traffic to the ~~server~~ remaining running servers if a single server goes down. Correspondingly, when a new server is added to the network the load balancer start sending requests to it. Load balancing feature is providing by all the major cloud providers, eg. AWS Elastic load balancing, Azure load balancer, Rackspace load balancer etc.
- In this manner a load balancer performs the following functions:

i. Allocates client request or network load competently across multiple servers.

ii. Ensures high obtainability and dependability by sending requests only to servers that are online.

iii. Provide the elasticity to add or subtract servers as demand dictates.



Q) Write a note on Cloud File System with architecture.

→ File System is an approach to manage and operates files and data on Storage System. These are various file System. Such as NTFS, FAT32, EXT4, etc that are commonly used today in operating Systems. File Systems typically Provide mechanisms for reading, writing, modifying, deleting or organising files in folders and directories. Similarly.

Def^n :- cloud file System are specifically designed to be distributed and operated in the cloud based environment

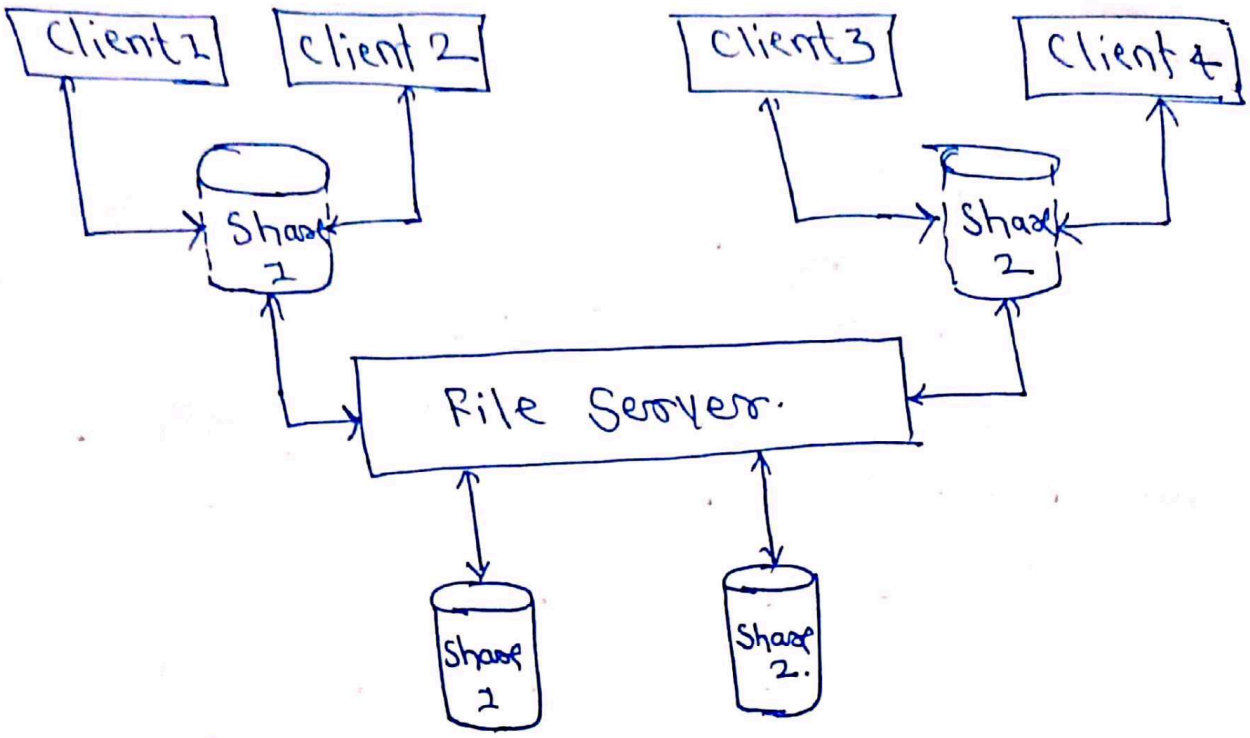
● General Architecture of Cloud file System.

Typically architecture for cloud Systems fall into two categories. A) Client Server architecture.
B) Cluster based architecture.

A) Client Server architecture :- In a client-Server architecture, the file Server hosts the file system that can be mounted (attached) by the clients. one file Server can host multiple file shares and each file share can be mounted and operated by multiple clients. All the file operations are then synchronised back to the file server so that the other clients that have mounted the Same file share can get the updat as well.

- one example of Such file system is Network file System (NFS). Client Server based file system architecture could be limited due to dependency on the availability of the file Server and the need to synchronise the file operations periodically.

- Fig shows block diagram that depicts the client Server architecture at a high-level.



a) Client - Server architecture.

B) Cluster Based architecture :- In a cluster based architecture. the File is broken into Smaller Parts called chunks and each chunks is stored on the Storage Server or (devices). The chunks are redundantly stored on Several Servers to withstand any fault and have high availability.

This architecture does not depends upon a single server for hosting the file system. The File System is distributed and Provides Parallelism that significantly improves the scale and Performance. This architecture is commonly used today in the cloud environment. Google file System, Amazon S3, etc are example of this.

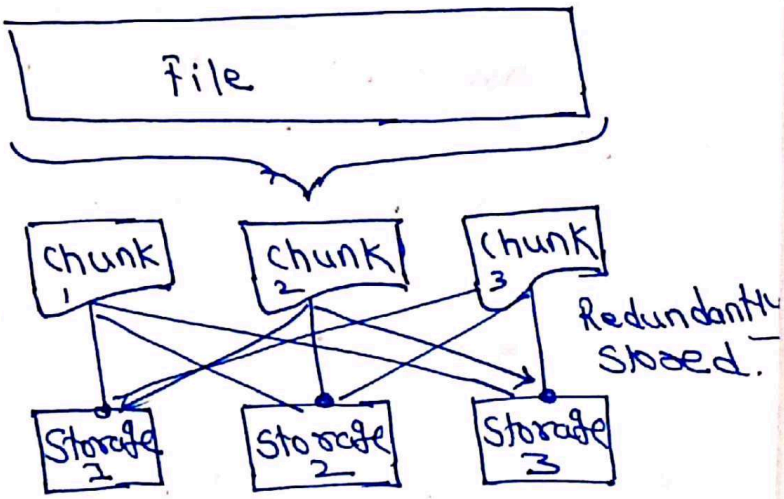


fig. cluster based architecture.

Q14 (4) (3)

Working of Google Data Store :-

Q) Explain the working of Google data store ?

⇒ Google Cloud Data Store (Cloud Data Store) is a highly Scalable fully archieved NOSQL database Service offered by Google on the Google Cloud Platform

- Cloud Storage is Somewhat that "allows you to Save data and file in an off site location that you access either complete the Public internet or a faithful Private network Connection.
- This is very cost operative for businesses since Physical files can replaced with Cloud Storage records.
- Cloud data Store is built upon Google's big table & megastore technology.
- ~~Cloud~~ Google cloud data Store allows the user to create folders either in Native or Data Store mode.
- Native mode is calculated for mobile and Web apps, while Data Store mode is calculated for new Server Projects.

Google Cloud Platform :- Google Cloud Platform (GCP) offered by Google is a Suit of cloud computing Services that runs on the same infrastructure that Google uses inside for its end user Products Such as. Google Search, Gmail, Google drive, and Youtube.

- alongside a set of organization tools, it Provides a series of modular cloud facilities including Computing, data storage, data analytics and machin learning.
- Registering requires a credit card or bank account details.

- Google Cloud Platform offers infrastructure as a Service, Platform as a Service and Serverless computing situations.
- Google exposed App Engine, a Platform for developing and hosting web applications in google managed data centers, which was the first cloud computing Service from the company.
- Since the Statement of App Engine, Google added multiple cloud Services to the Platform.
- Google Cloud Platform is a Part of Google Cloud, which comprises the Google Cloud Platform Public Cloud infrastructure, as well as Google Workspace (G Suits), enterprise versions of android and chrome OS, and application Programming interfaces (APIs) for machine learning and enterprise mapping Services.

Q) Private Cloud Security Issues :-.

Q) Explain the information Security Concerns associated with data stored in Cloud ?

⇒ Lack of reliable security controls covering over traditional Servers and virtualized Private cloud infrastructures.

- Increasing difficulty of infrastructures resulting in more time/effort for implementation and conservation.
- Lack of Staff with Skills to manage Security for a Software defined data center (e.g virtual compute, network Storage)
- Imperfect visibility over Security for a Software defined data center (eg virtual compute, network, Storage).

- Advanced threats and attacks.
- An important factor in the decision making process to allocate capitals to a Public vs. Private cloud is the fine tuned control available in Private cloud situations.
- In Private clouds, additional levels of control and supplemental Protection can ~~a~~ecompense for others limita-
- tions of Private cloud placements and may contribute to a Practical transition from monolithic Server based data centers.
- At the same time Governmental should consider that upholding fine-tuned control creates complexity at least beyond what the Public cloud has advanced
- Currently cloud Providers take on greatly of the effort into to Preserve infrastructure themselves.
- Cloud users can Simplify Security management and reduce complexity through abstraction of controls.
- This unifies Public and Private cloud Platforms above and across Physical, virtual and hybrid environments.

⑧ **Cloud Storage Providers** :- We are living in a digital age these days. we want everything to be accessible online, and that includes our data. All of our data our Photograph, our Music, our video, our work files.

9/6) Write note on

- cloud Storage also Provides security, efficiency and accessibility to your online data even across multiple devices. It also ensures that your data is backed up and is in safe hands.
- Cloud Storage Services are the best way to store your data safely and securely in the cloud, accessible

from any device. the Problem is there are a lot of cloud Storage Services, and it can be hard to Pick one.

- I have used all the cloud Storage in the list. on the basis of my usage, I will recommend each Storage for different Purposes by seleting Pros-Cons of Storage Provider.

- following list Shows diff^n cloud Storage Providers:-

1. Pcloud - Best Cloud Storage 2022.
2. Sync - Best Secure Cloud Storage.
3. Ice-Drive - Best Budget cloud Storage.
4. Mega - Best in free Cloud Storage.
5. TreSorit - Expensive but Secure.
6. iCloud - for Apple users.
7. One Drive - for office users.
8. DropBox - for collaboration.
9. Google Drive - for Team collaboration.

Some Common Pros of cloud Storage.

1. Syn feature, Fast Speed, File Shearing options, affordable Pricing, Zero knowledge Encryption, Data Center Selection.
2. Sync folders, Seperate Vault Tab, Clean Privacy Policy, Versioning and account rewind, office365, 2FA support.
3. Impressive Speed, Best user Interface, Affordable Pricing, Zero knowledge encryption, Promising roadmap, Decent File Shearing,

4- Swift Speed, Good Sync features, 20 GB free Space, Excellent file Sharing, Decent Interface.

5- Zero knowledge Encryption, Neat Privacy Policy, Exceteonal Security testing, Impressive file Sharing Admirable Sync function, friendly UI, Eropean Servers GAPR and HIPAA Compliant, 2FA Support.

6- Cam Support, Good Privacy Policy.

7.- MS-office Support, Remarkable editing features.

8- Exceptional sync-feature, Fast Speed, Smooth Playback feature, Good integrations.

9- ~~Good Integrations~~ Impressive Speed, best of Collaboration, Smooth Viedo Playback, Good Sync function outstanding Search algorithms.

—o—o— B-81, B-478 868, 8115, A-56, B-100,

Data storage Management -

① Introduction

② Advantage of cloud data Management -
- Gain Accurate visibility
- Forcesast ~~stra~~ saving & data planning
- Archive based on actual data
- radically simplify migration.

③ challenges Faced with enterprise
- Managing data accross common Formate
- Data security concerns to senstive data.
- different users and different objects.
- Handling different file formate & oxptions

④ Feature of cloud data managment ~~tools~~ Platforms
- Data Analytical
- Planning & forcasting
- Policy based data archiving
- Fast reliable & migration.
- Inteligent data archiving

⑤ Working of cloud data maneqment tools :-
- Migration and managing
- EETL (Extraction Transformation & loading
- ipass (intigration Platform as service)
- TOOLS to move & manage enterprise request & DB)

⑥ challenges Feed with cloud data managment security
- Govelmont faces
- some policy & regulation authority

⑦ cloud data manegment service growing

⑧ How enterprise cloud data management different From consumer system

Introduction -

- improve the performance
- NIW virtualization
- Mirroring security
- Data compression
- Data duplication
- Traffic analysis and automation
- storage provisining
- Memory managment
- Prevent data loss
- Data ~~to~~ retension
- Recovery
- Backup of data.