Cloud Computing (RCS-075)

Unit-3

Layered Cloud Architecture

Architecturally, Cloud can be divided as 4 layers:

Physical layer: Contains physical servers, network etc

Infrastructure layer: Virtualized servers, networking and storage resources. Infrastructure as a Service is the hosted delivery of infrastructure services such as servers, networks and other hardware to consumers. IaaS provides consumers access to on-demand, scalable storage and compute power.

Platform layer: contains components or services like Windows Azure, Google App Engine .A platform for development and deployment. Platform as a Service offers a complete platform and the tools to develop and deploy applications on the platform.

Application Layer: This is the layer end users interact with. This contains software which is delivered as service like Gmail, Salesforce, dropbox etc. Software as a Service is the hosted delivery of Software that consumers can access over the internet. Two features of a SaaS application are scalability and configurability. SaaS applications should be able to quickly scale with demand. In mature SaaS applications, the customer should be able to customize their instance of the software using meta-data.

Cloud architecture is not as simple as it first seems. Cloud is the outcome of several layers of cloud architecture intelligently placed over one another. Before we move towards the various layers, take a look at the more general picture of cloud layers below –

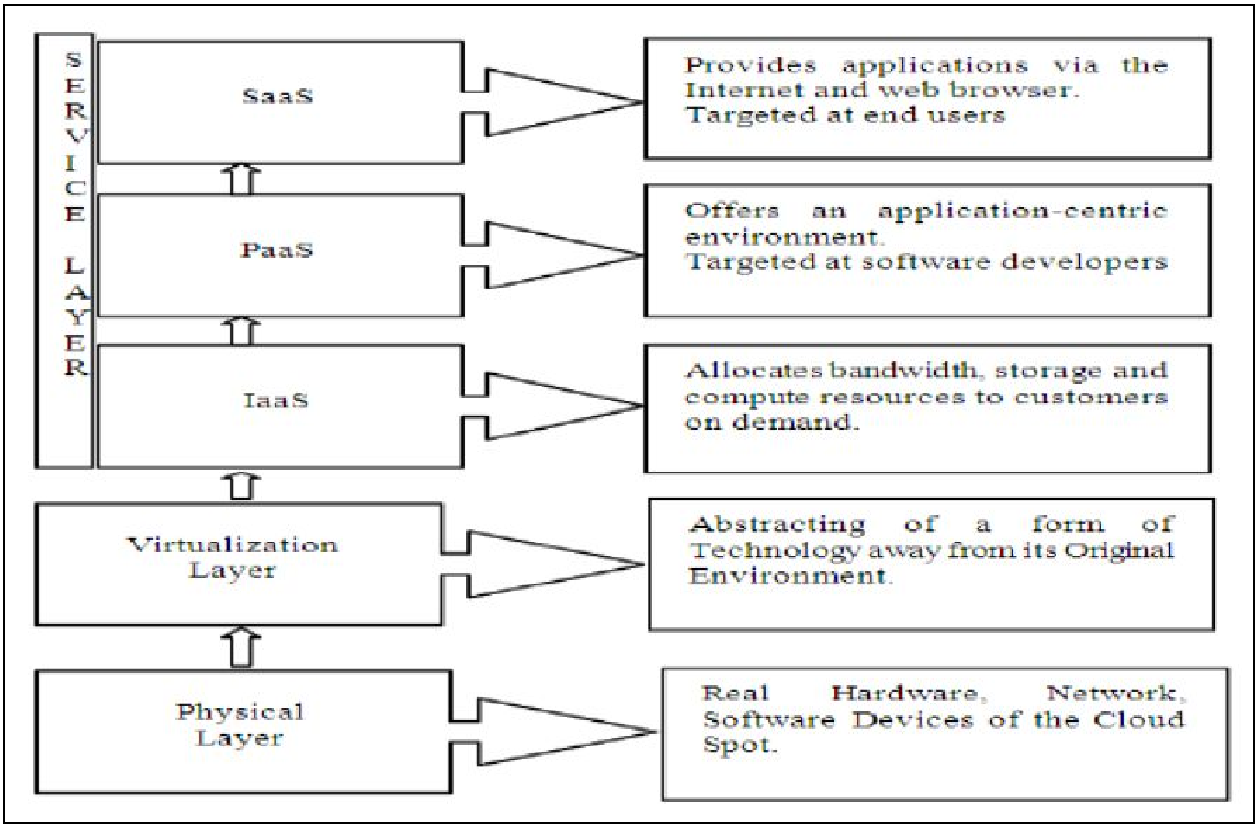
Hardware Layer: This bottom most layer of cloud architecture, the hardware layer, primarily deals with all the hardware powering clouds. The hardware includes but is not restricted to routers, servers, switches, power and cooling systems.

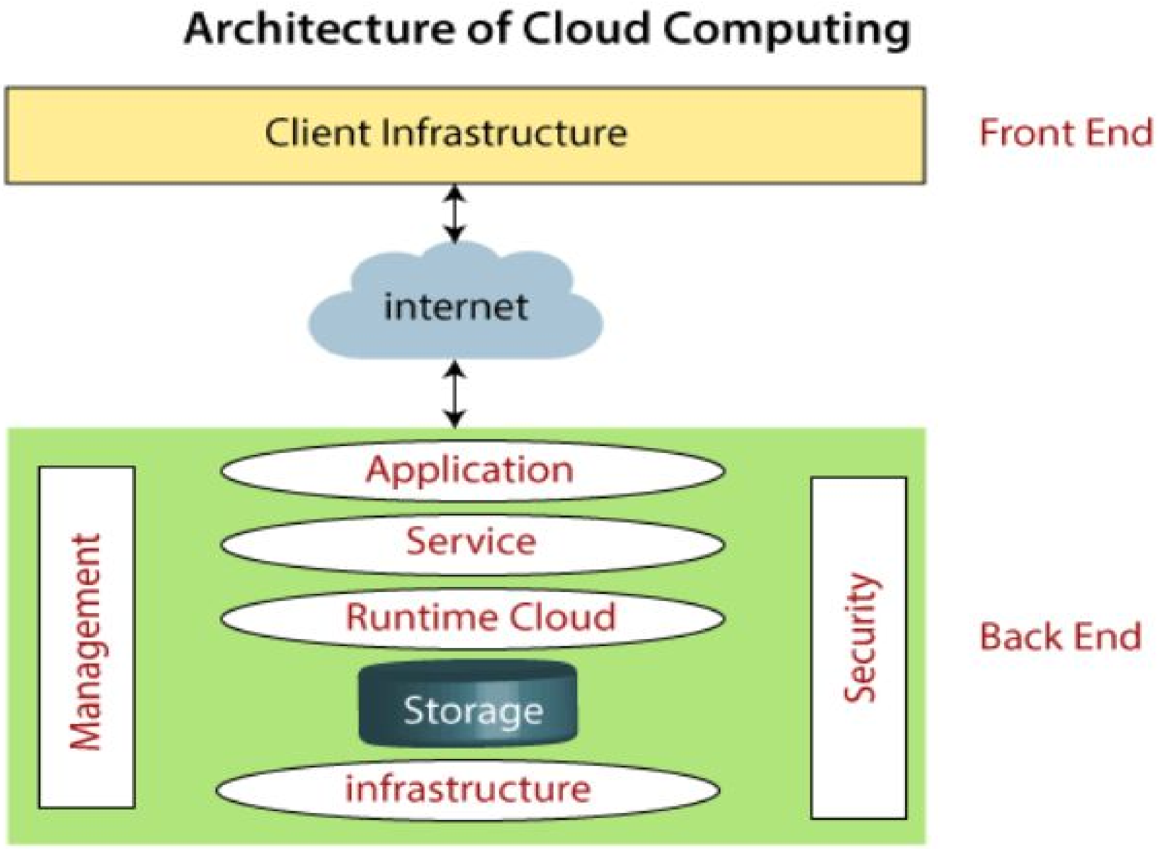
Infrastructure Layer: Also called the virtualization layer, the infrastructure layer is where all the servers are pooled together into one.

Platform Layer: The platform layer comprises the operating system and other requisition structures and is based over the infrastructure layer.

Application Layer: As the name suggests, the application layer - the topmost layer - contains applications that directly interact with the end-user.

Cloud computing architecture is made of several layers for better operational efficiency. Cloud controller or CLC is at the top and is used to manage virtualized resources like servers, network and storage. Walrus is the next layer and used as a storage controller to manage the demands of the users. Cluster Controller or CC manages the virtual networking between Virtual machines and external users. Storage Controller or SC is a block-form **storage device**, dynamically attached by **Virtual machines**. The next layer is NC or Node Controller. It acts as a hypervisor and controls the Virtual machines activities such as execution, management and termination of many instances.


SERVICE LAYER
SaaS
Provides applications via the Internet and web browser. Targeted at end users
PaaS
Offers an application-centric environment. Targeted at software developers
IaaS
Allocates bandwidth, storage and compute resources to customers on demand.
Virtualization Layer
Abstracting of a form of Technology away from its Original Environment.
Physical Layer
Real Hardware, Network, Software Devices of the Cloud Spot.



Main Characteristics of a Cloud

1. On-demand self-service Cloud computing resources can be provisioned without human interaction from the service provider. In other words, a manufacturing organization can provision additional computing resources as needed without going through the cloud service provider. This can be a storage space, virtual machine instances, database instances, and so on.

Manufacturing organizations can use a web self-service portal as an interface to access their cloud accounts to see their cloud services, their usage, and also to provision and de-provision services as they need to.

2. Broad network access

Cloud computing resources are available over the network and can be accessed by diverse customer platforms. It other words, cloud services are available over a network—ideally high broadband communication link—such as the internet, or in the case of a private clouds it could be a local area network (LAN).

Network bandwidth and latency are very important aspects of cloud computing and broad network access, because they relate to the quality of service (QoS) on the network. This is particularly important for serving time sensitive manufacturing applications.

3. Multi-tenancy and resource pooling

Cloud computing resources are designed to support a multi-tenant model. Multi-tenancy allows multiple customers to share the same applications or the same physical infrastructure while retaining privacy and security over their information. It's similar to people living in an apartment building, sharing the same building infrastructure but they still have their own apartments and privacy within that infrastructure. That is how cloud multi-tenancy works.

Resource pooling means that multiple customers are serviced from the same physical resources. Providers' resource pool should be very large and flexible enough to service multiple client requirements and to provide for economy of scale. When it comes to resource pooling, resource allocation must not impact performances of critical manufacturing applications.

4. Rapid elasticity and scalability

One of the great things about cloud computing is the ability to quickly provision resources in the cloud as manufacturing organizations needing them. And then to remove them when they don't need them. Cloud computing resources can scale up or down rapidly and, in some cases, automatically, in response to business demands. It is a key feature of cloud computing. The usage, capacity, and therefore cost, can be scaled up or down with no additional contract or penalties.

Elasticity is a landmark of cloud computing and it implies that manufacturing organizations can rapidly provision and de-provision any of the cloud computing resources. Rapid provisioning and de-provisioning might apply to storage or virtual machines or customer applications.

With cloud computing scalability, there is less capital expenditure on the cloud customer side. This is because as the cloud customer needs additional computing resources, they can simply provision them as needed, and they are available right away. Scalability is more planned and gradual. For instance, scalability means that manufacturing organizations are gradually planning for more capacity and of course the cloud can handle that scaling up or scaling down.

Another feature available for rapid elasticity and scalability in the cloud is related to testing of manufacturing applications. If a manufacturing organization needs, for example, a few virtual machines to test a supervisory control and data acquisition (SCADA) system before they roll it out in production, they can have it up and running in minutes instead of physically ordering and waiting for hardware to be shipped.

5. Measured service

Cloud computing resources usage is metered and manufacturing organizations pay accordingly for what they have used. Resource utilization can be optimized by leveraging charge-per-use capabilities. This means that cloud resource usage—whether virtual server instances that are running or storage in the cloud—gets monitored, measured and reported by the cloud service provider. The cost model is based on “pay for what you use”—the payment is variable based on the actual consumption by the manufacturing organization.

NIST Cloud Computing Reference Architecture

NIST defines cloud computing as-

1. A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
2. This short description is intended to serve as a means for broad comparisons of cloud services and deployment strategies while providing a baseline for discussion on the overall best uses for cloud computing.
3. NISTs definition identified self-service, accessibility from desktops, laptops, and mobile phones, resources that are pooled among multiple users and applications, elastic resources that can be rapidly reapportioned as needed.
4. When these characteristics are combined, they create cloud computing infrastructure that contains both a physical layer and an abstraction layer.
5. The physical layer consists of hardware resources that support the cloud services (i.e. servers, storage and network components).
6. The abstraction layer consists of the software deployed across the physical layer, thereby expressing the essential characteristics of the cloud per NISTs definition.

Deployment Models as per NIST

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

Private Cloud

1. Private cloud computing is a deployment model that is purchased and dedicated to a single client or company in a single-tenant environment where the hardware, storage and network assume the highest levels of security.
2. Data that is stored in the private clouds data center cannot be accessed by anyone other than the client that owns it. This is a great solution for organizations that feel as though their data is too sensitive or valuable to put on a public, community or hybrid cloud.
3. The private cloud also gives administrators the ability to automate their data center thereby minimizing manual provisioning and management which is incredibly important for safe and secure day-to-day operations to flourish.

Community Cloud

1. NIST defines a community cloud deployment model as one that is used exclusively by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations).

2. 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.

3. This multi-tenant platform allows several companies work on the same platform if they share similar needs and concerns. A community cloud allows companies to collaborate on joint projects, applications, or research in a secure setting.

Public Cloud

1. A public cloud is a deployment model that is owned by cloud service providers and made available to the public. Customers can gain new capabilities on demand without investing in new hardware or software by tapping into the public cloud.
2. Customers simply pay their cloud provider a subscription fee or pay for only for the resources they wish to use. The vendor is then responsible for all the administration, maintenance, capacity planning, backups, and troubleshooting.
3. Each public cloud can simultaneously handle massive amounts of storage that allows businesses the ability to handle multiple projects and become more available to their users at a moment's notice.

Hybrid Cloud

1. Hybrid cloud deployment models are a collaboration of private and public cloud models in a single environment. Hybrid clouds are comprised of parallel environments where applications can easily move between private and public clouds.
2. Hybrid clouds are bound together by proprietary technology that enables data and application portability. Hybrid cloud offers more IT teams more flexibility, portability, and scalability than other deployment models.
3. Companies that are constantly transitioning between managing public cloud projects and building applications of a sensitive nature on their private cloud is likely to seek out a hybrid cloud solution.

Analysis of Cloud Service Models (NIST Guided)

1. The NIST Cloud Computing Definition provides three possible cloud services categories (called service models): Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). With respect to the NIST Cloud Computing Reference Architecture (CCRA), cloud services are made available in the Service layer, which is part of the Service Orchestration stack.
2. SaaS, PaaS, and IaaS are best distinguished by two factors: the computing capability that is provisioned and the primary CSCs(common service centre) (end user, developer, or IT operations). The term "platform" in the PaaS context refers to a development platform and/or deployment platform for cloud-enabled applications. The term

"platform" is broadly used in the computing industry. It therefore helps to understand the context of the term with regard to Platform as a Service.

SaaS (Software as a service)

1. The capability provided to the CSC is to use the CSP's applications running on a cloud infrastructure.

2. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface.

3. The CSC does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

4. The term "applications" in the SaaS context refers to cloud enabled applications (e.g., web or mobile) by nature of supporting essential characteristic – broad network access.

5. This differs from VM/desktop applications that may be installed on a virtual machine.

6. SaaS applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or application programming interface (API).

7. SaaS applications may be extensible by way of an API. A web application is not necessarily considered SaaS, unless the application itself qualifies as a cloud service.

8. The SaaS provider is typically responsible for all aspects of making the software service available, including the availability of any PaaS and IaaS dependencies.

9. The NIST Reference Architecture for Cloud Computing clarifies that the SaaS provider is responsible for deploying, configuring, maintaining, and updating the operation of the software applications on a cloud infrastructure.

10. The term "provider" refers to the entity responsible for making the service available and may therefore be different than the SaaS application developer.

PaaS (Platform as a Service)

1. The capability provided to the CSC is to deploy onto the cloud infrastructure CSC-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider.

2. The CSC does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

3. The term “platform” in the PaaS context refers to a development and/or deployment platform for cloud-enabled applications.

4. The term “platform” in the PaaS context refers to a development and/or deployment platform for cloud-enabled applications.

5. The term “applications” in the PaaS context refers to cloud enabled applications (e.g., web or mobile) by nature of supporting essential characteristic – broad network access. This differs from VM/desktop applications that may be installed on a virtual machine.

6. PaaS is distinguished from an extensible SaaS or web application by its primary CSCs: developers versus end users. The applications can be CSC-created or acquired.

7. The applications can be created using programming languages, libraries, services, and tools supported by the provider. This does not necessarily preclude the use of compatible programming languages, libraries, services, and tools from other sources.

8. A PaaS provider may be responsible for making the platform service available, including any IaaS dependencies. These typical terms may be negotiated as a shared responsibility model.

IaaS (Infrastructure as a Service)

1. The capability provided to the CSC to provision processing, storage, networks, and other fundamental computing resources where the CSC can deploy and run arbitrary software, which can include operating systems and applications.

2. The CSC does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

3. The infrastructure service is typically software-defined.

4. Infrastructure as a Service is distinctly different from cloud infrastructure (see definition) and also different from the underlying physical infrastructure.

5. The terms “software” and “application” in the IaaS context refers to VM/desktop software and applications, rather than referring to cloud-enabled SaaS or web applications.

6. The infrastructure service may optionally include a pre-installed operating system and other support VM/desktop software and applications, such as web server.

7. The term “arbitrary software” in this context means that the CSC can deploy and run many types of VM/desktop software.

Architectural Design Challenges

1. **Cost**

   Cloud computing itself is affordable, but tuning the platform according to the company’s needs can be expensive. Furthermore, the expense of transferring the data to public clouds can prove to be a problem for short-lived and small-scale projects.

   Companies can save some money on system maintenance, management, and acquisitions. But they also have to invest in additional bandwidth, and the absence of routine control in an infinitely scalable computing platform can increase costs.

2. **Service Provider Reliability**

   The capacity and capability of a technical service provider are as important as price. The service provider must be available when you need them. The main concern should be the service provider’s sustainability and reputation. Make sure you comprehend the techniques via which a provider observes its services and defends dependability claims.

3. **Downtime**

   Downtime is a significant shortcoming of cloud technology. No seller can promise a platform that is free of possible downtime. Cloud technology makes small companies reliant on their connectivity, so companies with an untrustworthy internet connection probably want to think twice before adopting cloud computing.

4. **Password Security**

   Industrious password supervision plays a vital role in cloud security. However, the more people you have accessing your cloud account, the less secure it is. Anybody aware of your passwords will be able to access the information you store there.

   Businesses should employ multi-factor authentication and make sure that passwords are protected and altered regularly, particularly when staff members leave. Access rights related to passwords and usernames should only be allocated to those who require them.

5. **Data privacy**

   Sensitive and personal information that is kept in the cloud should be defined as being for internal use only, not to be shared with third parties. Businesses must have a plan to securely and efficiently manage the data they gather.

6. **Vendor lock-in**

   Entering a cloud computing agreement is easier than leaving it. “Vendor lock-in” happens when altering providers is either excessively expensive or just not possible. It could be that the service is nonstandard or that there is no viable vendor substitute.

   It comes down to buyer carefulness. Guarantee the services you involve are typical and transportable to other providers, and above all, understand the requirements.

   Cloud computing is a good solution for many businesses, but it’s important to know what you’re getting into. Having plans to address these six prominent challenges first will help ensure a successful experience.

What is Cloud Storage?

Cloud storage is a cloud computing model that stores data on the Internet through a cloud computing provider who manages and operates data storage as a service. It’s delivered on demand with just-in-time capacity and costs, and eliminates buying and managing your own data storage infrastructure. This gives you agility, global scale and durability, with “anytime, anywhere” data access.

How Does Cloud Storage Work?

Cloud storage is purchased from a third party cloud vendor who owns and operates data storage capacity and delivers it over the Internet in a pay-as-you-go model. These cloud storage vendors manage capacity, security and durability to make data accessible to your applications all around the world.

Applications access cloud storage through traditional storage protocols or directly via an API. Many vendors offer complementary services designed to help collect, manage, secure and analyze data at massive scale.

Benefits of Cloud Storage

Storing data in the cloud lets IT departments transform three areas:

1. Total Cost of Ownership. With cloud storage, there is no hardware to purchase, storage to provision, or capital being used for "someday" scenarios. You can add or remove capacity on demand, quickly change performance and retention characteristics, and only pay for storage that you actually use. Less frequently accessed data can even be automatically moved to lower cost tiers in accordance with auditable rules, driving economies of scale.

2. Time to Deployment. When development teams are ready to execute, infrastructure should never slow them down. Cloud storage allows IT to quickly deliver the exact amount of storage needed, right when it's needed. This allows IT to focus on solving complex application problems instead of having to manage storage systems.

3. Information Management. Centralizing storage in the cloud creates a tremendous leverage point for new use cases. By using cloud storage lifecycle management policies, you can perform powerful information management tasks including automated tiering or locking down data in support of compliance requirements.

Cloud Storage Requirements

1. Durability. Data should be redundantly stored, ideally across multiple facilities and multiple devices in each facility. Natural disasters, human error, or mechanical faults should not result in data loss.

2. Availability. All data should be available when needed, but there is a difference between production data and archives. The ideal cloud storage will deliver the right balance of retrieval times and cost.

3. Security. All data is ideally encrypted, both at rest and in transit. Permissions and access controls should work just as well in the cloud as they do for on premises storage.

Types of Cloud Storage

There are three types of cloud data storage: object storage, file storage, and block storage. Each offers their own advantages and has their own use cases:

1. **Object Storage** - Applications developed in the cloud often take advantage of object storage's vast scalability and metadata characteristics. Object storage solutions like Amazon Simple Storage Service (S3) are ideal for building modern applications from scratch that require scale and flexibility, and can also be used to import existing data stores for analytics, backup, or archive.

2. **File Storage** - Some applications need to access shared files and require a file system. This type of storage is often supported with a Network Attached Storage (NAS) server. File storage solutions like Amazon Elastic File System (EFS) are ideal for use cases like large content repositories, development environments, media stores, or user home directories.

3. **Block Storage** - Other enterprise applications like databases or ERP systems often require dedicated, low latency storage for each host. This is analogous to direct-attached storage (DAS) or a Storage Area Network (SAN). Block-based cloud storage solutions like Amazon Elastic Block Store (EBS) are provisioned with each virtual server and offer the ultra low latency required for high performance workloads.

Advantages of Cloud Storage

1. Usability and accessibility

Most of the cloud services come with an easy-to-use user interface and provide a feature of drag and drop. For instance, you can think of Google drive from Google or iDrive from Apple. They both have a simple interface, and you can easily upload your file on your online drive without any expert knowledge. For example, if you have saved a file in drive using a mobile device, you can retrieve that file using a computer or any other device with internet connectivity. It doesn’t matter where you are right now. If you have a good internet connection, you can access your files, which is saved online somewhere on the data centers.

2. Security

If anything is associated with the internet, then safety becomes our primary concern, and mostly the big and small businesses use cloud storage services, so before they choose a cloud service for their business, they make sure that service provided giving them better security.

The cloud storage saves your data across the redundant servers, so even if one of the data centers gets collapsed, your data will be managed by the other data centers, which make your data safe and supervised. If all the data centers of the storage provider get collapse or destroyed, then only your data could be lost, and this is entirely impossible phenomena because a cloud storage service is formed of thousands of data centers.

Some of the cloud storage vendors keep the copies of your data at the different data centers, so even if the data get lost or corrupted at the server, the backup must be there.

3. Cost-efficient

By only using the cloud storage service, the business outsources the storage problem. By using online data storage, the enterprise reduces the expenses of internal resources. With this technology, the company itself does not need any inner power and support to manage and store their data; the cloud storage vendor handles all. There are some cloud storage services provided which give cloud storage for a lifetime at an affordable price, which is a win-win offer for small business and individual users.

4. Convenient sharing of files

Every cloud storage service provides the file-sharing features, which helps you to share your file with other users. You can either send a file to another user or invite multiple users to view your data. Mostly all the vendors provide a cloud environment in which two users using the same cloud service can share their data, though there are only a few service vendors that offer the cross-platform file sharing features.

5. Automation

Cloud storage works like a hard disk on your system, and if you want to store any file in the cloud, it will not temper any ongoing task. There may be more than one user using a cloud storage service, and the current responsibility of one user would not affect the task of another since it is all is managed and automated by the cloud vendor.

6. Multiple users

The same cloud environment can have more than one use associated with it. With cloud storage, multiple users can collaborate with the common file. For instance, you can give access to your files to multiple users so they can access and edit your file. The authorized person can access your file from any part of the world in real-time.

7. Synchronization

Every storage vendor gives the sync feature. With synchronization, you can sync the cloud storage data with any device you want. As we have discussed, we can access our data from any device and any part of the world, but this accessibility is done with the help of synchronization. With proper credentials, you can log in to your subscribed storage service with any device, and you will be able to access your all data that have been stored in that cloud storage. There is no need to copy data from one device to another, but you need a good internet connection to have access to all of your files.

8. Convenient

You do not need any hard disk or flash drive to access or view your data — all is done online. However, if you want to download any file or data, you may require a storage device or you can download that data in your device. But if you want to surf your data, then it would not occupy any space on your device. Even if you make any changes to the data, all the changes will reflect on every device which is synced with that storage service. You do not require any expert or technical knowledge to use the cloud storage service. All the heavy lifting is managed by the vendor itself.

9. Scalable

Cloud storage is scalable and flexible. If the current plan of storage is not enough, you can upgrade the service plan. And you do not need to move any data from one location to another, the extra space will be added to your storage environment with some extra features.

10. Disaster recovery

Every business has a backup storage plan where they store all the copies of their data. If they encounter any collapse or loss of data problem, they can retrieve data from their backup plan, and that is why cloud storage is the best method to deal with this problem. Cloud storage service provides the best platform for disaster recovery data. Any business can use cloud storage as a data backup storage, so if there is a data loss, the company can retrieve backup data from the cloud.