CLOUD COMPUTING
Unit 1

With changing times, the demands on technology have changed. In response different computing models have evolved since the past decade, starting with Cluster Computing to Grid Computing and finally to Cloud Computing. Cloud Computing has emerged as an important technique in the field of computer applications and information technology. It involves services for the storage, processing and transmission of data through shared resources, over the internet. Resources utilized for these services can be metered and the clients can be charged for the resources they utilize.

Cloud computing refers to the delivery of computing services over the internet, or "the cloud," to enable faster innovation, flexible resources, and economies of scale. These services include servers, storage, databases, networking, software, analytics, and intelligence. Rather than owning and maintaining physical hardware or software, users access and pay for services on an as-needed basis.

Cloud computing is a key technological development in the information technology industry. It is one of the best techniques for managing and allocating a lot of information and resources across the entire internet. Technically speaking, cloud computing refers to accessing IT infrastructure through a computer network without having to install anything on your personal computer. Businesses can modify their resource levels to match their operational needs by utilizing cloud computing. Organizations and corporations can cut infrastructural costs with the use of cloud computing. Organizations can test their applications more quickly, with better management, and with less upkeep. The IT team can adapt resources to changing and erratic requirements thanks to cloud computing. There is proof that cloud computing has a role in everyday life thanks to various applications in various contexts. This essay will cover every aspect of cloud computing, including its architecture, traits, types, service models, advantages, and challenges.

Cloud computing is a transformative technology that delivers computing services—including servers, storage, databases, networking, software, analytics, and intelligence—over the internet.[1] By leveraging the power of the cloud, organizations can access and utilize these resources on-demand, without the need for significant upfront investments in hardware or infrastructure.

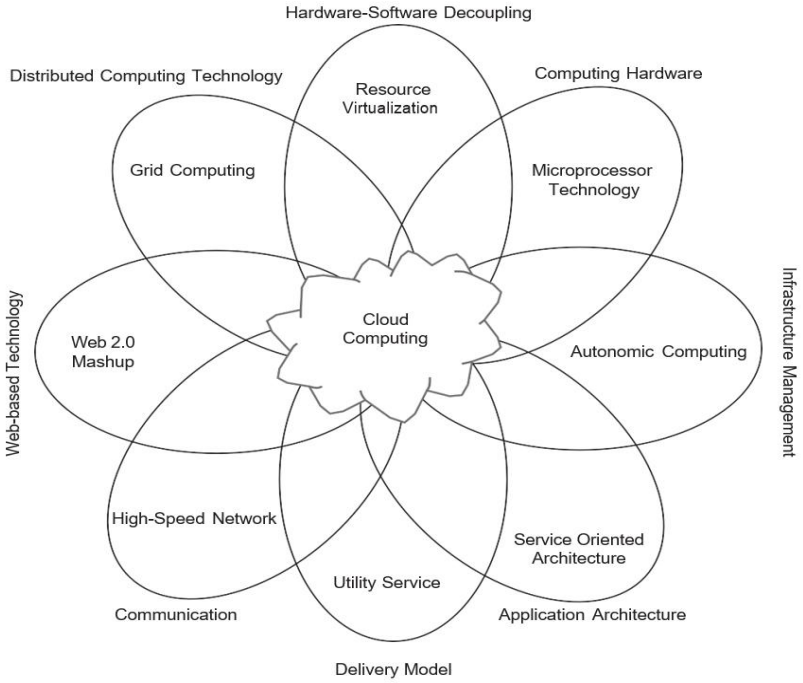


FIG 2.7: Convergence of technologies for evolution of cloud computing

LIMITATIONS OF THE TRADITIONAL COMPUTING APPROACHES

Every new technology emerges with the promise to resolve the shortcomings of the existing ones. Traditional computing has played a pivotal role in the field of computing and communication over the past few decades. Since cloud computing is being considered as the successor of the traditional computing system, therefore, it would be wise to recognize the limitations of the traditional computing approaches before studying the contents of cloud computing. Computing and information technology (IT) has changed the nature and scope of the human civilization in last few decades. There was a time, nearly half-of-the-decade back, when enterprises used to execute their businesses merely by the aid of the pen, paper, telephone and fax machine. Gradually, computer systems intruded manual processes and started automating them. The pen and paper were replaced by digital communication, and even the phone and faxing services started being managed by computers. At present, businesses from local to global, are dependent on the computing systems for almost everything they do. Even individuals depend heavily on computing systems for their day-to-day activities. IT and computing are critical factors now, and life cannot be imagined without easy and all-time access to computing systems. Easy and cheap access to computing facilities has become essential for everyone. But, a little investigation raises concerns about several issues regarding the conventional uses of computing technology. Following section focuses on problems associated with traditional computing approaches.

Difficulties faced by enterprises in traditional computing

Traditional Computing Scenario	***Problematic facts and related questions***
Business without help of computing services is beyond imagination, and the customized software packages manage business activities. Most organizations use ERP packages (implemented by some IT enterprise) to get maximum benefits from regular business operations.	To run enterprise resource planning applications, business organizations need to invest huge volumes of capital to setup the required IT infrastructure. Servers, client terminals, network infrastructure are required, and they to be put together in a proper manner. Moreover, arranging adequate power supply, cooling system and provisioning space also consume a major part of the IT budget. Are there ways to avoid this huge initial investment for computing infrastructural setup?
Business application package implementation also over-burdens the IT enterprises with many other costs. Setting up infrastructure, installation of OS, device drivers, management of routers, firewalls, proxy servers etc. are all responsibilities of the enterprise in traditional computing approach.	Enterprises (or IT service firms) need to maintain a team of experts (system maintenance team) in order to manage the whole thing. This is a burden for HR management and incurs recurring capital investment (for salaries). Can enterprises get relief from these responsibilities and difficulties? It would help them concentrate fully on the functioning of business applications.

Even those IT enterprises whose sole business interest is developing applications are bound to setup computing infrastructure before they start any development work.	This is an extra burden for enterprises who are only interested in application development. They can outsource the management of infrastructure to some third party, but the cost and quality of such services varies quite a bit. Can IT enterprises avert such difficulties?
Computing infrastructure requires adequate hardware procurement. This procurement is costly, but it is not a one-time investment. After every few years, existing devices become outdated as more powerful devices appear.	It becomes difficult to compete in the market with outdated hardware infrastructure. Advanced software applications also require upgraded hardware in order to maximize business output. Can this process of upgrading hardware on a regular basis be eliminated from an enterprise's responsibility?
It is not unusual to find an updated version of application with new releases that is more advanced and apt to keep up with changing business scenario.	Adopting an updated version of an application requires necessary efforts from subscriber's end. Fresh installation and integration of components need to be done. Can subscribers be relieved of this difficulty of periodically upgrading the applications?
Capacity planning of computing resources is a critical task for any organization. Appropriate planning needs time, expertise and budgetary allocation since low resource volume hampers the pace of the performance of applications.	Enterprises generally plan and procure to support the maximum business load that they have anticipated. But average resource demand remains far less, most of the time. This causes resource wastage and increases the recurring cost of business. If this capacity planning task could be made less critical and resource procurement strategy more cost effective?
Resource requirements of a system may increase or decrease from time to time.	Individual enterprises cannot manage system contraction in a way that unutilized resources of a system can be utilized in some other system so that the cost of the business could be reduced. If this were somehow possible?
Many enterprise computing systems run forever without stopping. Such systems host applications which require round-the-clock availability to fulfill business demand.	When resource capacity expansion of such system becomes an absolute requirement for the respective business, an system shutdown (hence service disruption) becomes unavoidable which may cause loss in the business. If a system could be expanded without shutting it down?

Essential Characteristics:

There are many characteristics of Cloud Computing here are few of them :

1. **On-demand self-services:** The Cloud computing services does not require any human administrators, user themselves are able to provision, monitor and manage computing resources as needed.

2. **Broad network access:** The Computing services are generally provided over standard networks and heterogeneous devices.
3. **Rapid elasticity**: The Computing services should have IT resources that are able to scale out and in quickly and on a need basis. Whenever the user require services it is provided to him and it is scale out as soon as its requirement gets over.
4. **Resource pooling**: The IT resource (e.g., networks, servers, storage, applications, and services) present are shared across multiple applications and occupant in an uncommitted manner. Multiple clients are provided service from a same physical resource.
5. **Measured service:** The resource utilization is tracked for each application and occupant, it will provide both the user and the resource provider with an account of what has been used. This is done for various reasons like monitoring billing and effective use of resource.
6. **Multi-tenancy**: Cloud computing providers can support multiple tenants (users or organizations) on a single set of shared resources.
7. **Virtualization**: Cloud computing providers use virtualization technology to abstract underlying hardware resources and present them as logical resources to users.
8. **Resilient computing**: Cloud computing services are typically designed with redundancy and fault tolerance in mind, which ensures high availability and reliability.
9. **Flexible pricing models**: Cloud providers offer a variety of pricing models, including pay-per-use, subscription-based, and spot pricing, allowing users to choose the option that best suits their needs.
10. **Security:** Cloud providers invest heavily in security measures to protect their users' data and ensure the privacy of sensitive information.
11. **Automation**: Cloud computing services are often highly automated, allowing users to deploy and manage resources with minimal manual intervention.
12. **Sustainability**: Cloud providers are increasingly focused on sustainable practices, such as energy-efficient data centers and the use of renewable energy sources, to reduce their environmental impact.

Key Principles:

These essential characteristics underpin the following key principles of cloud computing:

A. ***Federation:*** A cloud computing environment must be capable of providing federated service providers which means that, these providers, must be capable of collaborating and resource sharing at any point irrespective of their type. This is usually needed when an organization extends its computing paradigm from the private to the public cloud. Moreover, This federation must be kept transparent so that the virtual application can be used on all the sites. This makes the application be handled remotely and allows it to migrate from one site to another. Apart from this, the federation must be carried out in a secure and independent way.

B. **Independence:** The user of cloud computing services must be independent of the provider's specific tool and the type of service. According to this principle, a user must be allowed the required virtual resource irrespective of the type of provider. Moreover, it is the responsibility of service providers to handle infrastructure while hiding confidential information.

C. **Isolation:** According to this principle, a service provider must ensure the user with respect to the isolation of their data from others. Even the data in the same cloud must be separated from different users and therefore should not be accessed.

D. **Elasticity:** The user of cloud computing must be provided with ease of accessing and releasing the resources as required. This is typically referred to as elasticity. The rules associated with elasticity must be included within the contract made between consumers and services providers.

E. **Business Orientation:** To develop a more efficient computing environment, an efficient platform must be developed before the applications are included in the cloud. This typically ensures the quality of services and assist SLA (Service-Level-Agreement).

F. **Trust:** To build a successful cloud computing environment, one of the major factors is trust between consumers and service providers. Therefore, effective mechanisms must be included to develop a trustworthy computing environment.

Cloud Deployment Model:-

As the name suggests, the cloud deployment model refers to how computing resources are acquired on location and provided to the customers. Cloud computing deployments can be classified into four different forms as below:

1) ***Private Cloud***

A cloud environment deployed for the exclusive use of a single organization is a private cloud. An organization can have multiple cloud users belonging to different business units of the same organization.

Private cloud infrastructure can be either on or off, depending on the organization. The organization may unilaterally own and manage the private cloud. It may assign this responsibility to a third party, i.e., cloud providers, or a combination of both.

2) ***Public Cloud***

The cloud infrastructure deployed for the use of the general public is the public cloud. This public cloud model is deployed by cloud vendors, Govt. organizations, or both.

The public cloud is typically deployed at the cloud vendor's premises.

3) ***Community Cloud***

A cloud infrastructure shared by multiple organizations that form a community and share common interests is a community cloud. Community Cloud is owned, managed, and operated by organizations or cloud vendors, i.e., third parties.

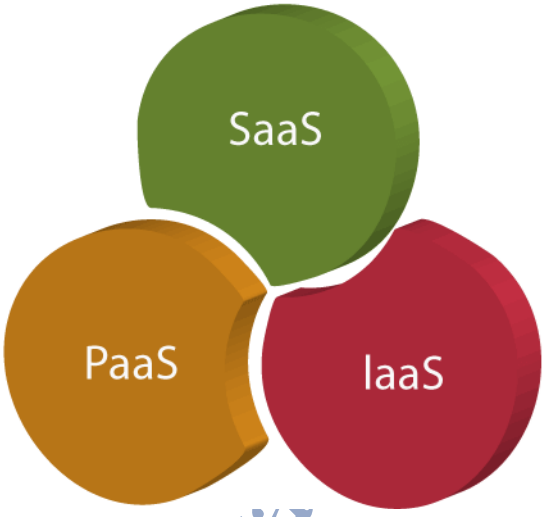
4) ***Hybrid Cloud***

Cloud infrastructure includes two or more distinct cloud models such as private, public, and community, so that cloud infrastructure is a hybrid cloud.While these distinct cloud structures remain unique entities, they can be bound together by specialized technology enabling data and application portability.

Cloud Service Models:-

There are the following three types of cloud service models -

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



Infrastructure as a Service (IaaS)

IaaS is also known as **Hardware as a Service (HaaS)**. It is a computing infrastructure managed over the internet. The main advantage of using IaaS is that it helps users to avoid the cost and complexity of purchasing and managing the physical servers.

Characteristics of IaaS

There are the following characteristics of IaaS -

Resources are available as a service
Services are highly scalable
Dynamic and flexible
GUI and API-based access
Automated administrative tasks

Example: DigitalOcean, Linode, Amazon Web Services (AWS), Microsoft Azure, Google Compute Engine (GCE), Rackspace, and Cisco Metacloud.

To know more about the IaaS, click here.

Platform as a Service (PaaS)

PaaS cloud computing platform is created for the programmer to develop, test, run, and manage the applications.

Characteristics of PaaS

There are the following characteristics of PaaS -

Accessible to various users via the same development application.

Integrates with web services and databases.

Builds on virtualization technology, so resources can easily be scaled up or down as per the organization's need.

Support multiple languages and frameworks.

Provides an ability to "**Auto-scale**".

Example: AWS Elastic Beanstalk, Windows Azure, Heroku, Force.com, Google App Engine, Apache Stratos, Magento Commerce Cloud, and OpenShift.

To know more about PaaS, click here.

Software as a Service (SaaS)

SaaS is also known as "**on-demand software**". It is a software in which the applications are hosted by a cloud service provider. Users can access these applications with the help of internet connection and web browser.

Characteristics of SaaS

There are the following characteristics of SaaS -

Managed from a central location

Hosted on a remote server

Accessible over the internet

Users are not responsible for hardware and software updates. Updates are applied automatically.

The services are purchased on the pay-as-per-use basis

Example: BigCommerce, Google Apps, Salesforce, Dropbox, ZenDesk, Cisco WebEx, ZenDesk, Slack, and GoToMeeting.

To know more about the SaaS, click here.

Difference between IaaS, PaaS, and SaaS

The below table shows the difference between IaaS, PaaS, and SaaS -

IaaS	PaaS	SaaS
It provides a virtual data center to store information and create platforms for app development, testing, and deployment.	It provides virtual platforms and tools to create, test, and deploy apps.	It provides web software and apps to complete business tasks.
It provides access to resources such as virtual machines, virtual storage, etc.	It provides runtime environments and deployment tools for applications.	It provides software as a service to the end-users.
It is used by network architects.	It is used by developers.	It is used by end users.
IaaS provides only Infrastructure.	PaaS provides Infrastructure +Platform.	SaaS provides Infrastructure +Platform +Software.

Advantages of Cloud Service Models

Cost Efficiency: Cloud providers provide a pricing model that permits customers to pay only for the sources they consume. This gets rid of the need for advanced infrastructure investments and allows price efficiency as businesses scale resources based totally on need.

Scalability: Cloud services provide the potential to scale sources up or down speedily and respond to changing workloads and commercial organization requirements. This flexibility ensures that agencies can correctly manipulate fluctuating needs without over-provisioning.

Accessibility and Flexibility: Cloud computing allows one to get access to applications and facts remotely from everywhere with an internet connection. This fosters collaboration among geographically dispersed groups and allows users to work flexibly.

Rapid Deployment: Cloud provider models facilitate rapid deployment of programs. Users can provision sources and deploy programs quickly, decreasing time-to-market and allowing faster innovation.

Managed Services: Cloud providers offer more than a few managed offerings, managing duties together with safety, tracking, and safety. This helps agencies dump operational obligations, pay attention to relevant skills, and experience the records of cloud carriers.

Automatic Updates and Patch Management: Cloud providers manipulate software application updates, patches, and protection functions robotically. This ensures that clients always have to get proper entry to the required abilities and protection upgrades without the need for guide intervention.

Disadvantages of Cloud Service Models

Security Concerns: Security remains a top concern for companies moving to the cloud. Storing information and programs on out-of-door servers will increase questions on statistics' privateness, regulatory compliance, and the functionality of unauthorized access.

Dependency on Internet Connectivity: Cloud services require a reliable internet connection. Downtime or disruptions in internet connectivity can impact the right to access essential applications and information, affecting business operations.

Limited Customization in SaaS: While SaaS offers convenience, it is able to lack the extent of customization that a few organizations require. Users depend on the capabilities and configurations supplied by the useful resources of the SaaS company, restricting flexibility.

Data Transfer Costs: Moving huge volumes of records from the cloud can require extra charges. Organizations need to cautiously recollect and manipulate facts and switch fees, in particular at the same time as dealing with enormous amounts of records.

Vendor Lock-In: Adopting certain cloud providers can also result in provider lock-in, wherein it becomes hard to migrate packages and statistics to a different employer or again to on-premises surroundings. This can limit flexibility and cause lengthy periods of dependence on a specific cloud organization.

Potential for Downtime: Cloud company companies may also experience outages or downtime, impacting the supply of services. While respectable businesses try for immoderate availability, occasional disruptions can occur, affecting users who get proper entry to agency continuity.

Cluster Computing	*Grid Computing*	*Cloud Computing*
A cluster is normally formed with computers of a single location, otherwise the system becomes complex.	Grid is inherently more distributed by its nature. The computers need not to be in the same geographical location.	It allows total distribution of resources like the grids. Hardware resources are maintained in multiple data centers spread across the globe.
Computation job takes place in one administrative domain owned by a single party.	Computation could occur over many administrative domains owned by multiple parties as connected together.	Computing resources of a cloud is usually owned by a single party. But multiple administrative domains can be combined together to perform the job.
In a cluster, all computing nodes should have similar hardware systems. That is, the system should be homogeneous in nature.	It can be heterogeneous in nature. The computers that are part of a grid can be made of different hardware architectures.	It can use heterogeneous collection of commodity hardware.
It features the centralized task management and scheduling system.	It features the distributed task management and decentralized scheduling.	It features the decentralized task management with more dynamic computing infrastructure.
Resources are generally pre-reserved for specific type of task.	Resources are generally pre-reserved for specific type of task.	Resources are not pre-reserved for specific task. Resource utilization is mainly demand-driven.
System is not dynamic in nature. Application mobility is not possible.	System is not dynamic in nature. Application mobility is not possible.	It is a dynamic system. Mobility of application is an inherent feature in this system.
One whole cluster behaves like a single system. As resources are managed by centralized resource manager, the individual computers can not be operated as separate computers.	Every node is autonomous that is, it has its own resource manager and behaves like an independent entity. So, each computer can be operated independently as distinct computer.	There is no concept of directly accessing any particular physical computing nodes. Underlying computing infrastructure remains hidden from the users.

II. BENEFITS OF CLOUD COMPUTING

Cloud computing has introduced a real paradigm shift in the scope of computing. Unlike the conventional uses of computer technology, it facilitates computing as a utility service which is delivered on demand. The computing facility is managed by providers and can be measured in usage volume or usage time.

All these features of cloud computing provide several benefits. It has the

flexibility where users can have as much or as little of it as they want at any given time. The advantages influence the adoption of cloud computing over the traditional computing process. Following section discusses different benefits that subscribers of cloud computing can enjoy.

1) Less Acquisition/Purchase Cost

In traditional computing, users have to purchase or procure computing resources in significantamount at very beginning. Cloud computing is delivered following the utility service model. Since vendor arranges all necessary resources in this model, subscribers' initial investment for acquiring hardware or software drops down drastically. They need not to arrange anything apart from client systems to access cloud services. Thus, initial capital expenditure of user gets reduced considerably.

The initial investment of users adopting cloud computing is very low.

2) Reduced Operational Cost

With the outsourcing model of utility computing the cost of running any systems round the clock moves towards the provider's end. Subscribers get rid of the responsibility of system administration, maintenance, and 24 × 7 energy support as well as its cooling support. This is a basis for cost savings because subscribers can use the service by paying very nominal. The provider on the other hand can offer the service at nominal fee to subscribers because of their volume of business (due to large customer base).

Subscribers of cloud computing service need to bear nominal operational cost.

3) Reduced System Management Responsibility

Be it a data center for enterprises or single standalone machine (PC, laptop etc.) for normal users, management of the computing setup (both hardware and software) is an extra headache for consumers of traditional computing. Cloud computing model shifts majority of the infrastructure and other system management tasks towards cloud vendors. Dedicated teams at the vendor's end takes care of all of these activities. Thus, the users can enjoy a sense of relief and can concentrate only on their area (layer) of computing interest without bothering about the management of the underlying computing layers.

Cloud computing releases users from the task of managing underlying computing system.

4) Use-basis Payment Facility

Cloud computing does not charge its subscribers when they do not use it. Even the charge is not fixed; it depends on the duration of usage. Rather, any use is metered and users are charged a reasonable fee according to their consumption. This reduces the cost of computing.

5) *Unlimited Computing Power and Storage*

In cloud computing, users can easily access supercomputer like computing power at reasonable cost, if necessary. Earlier in traditional approach, only big corporate could afford high-end computing. Storage is another important issue for users. Cloud provides as much storage as required. It is virtually unlimited which is viewed as a big benefit for users.

6) *Quality of Service*

In traditional computing, enterprises often used to outsource major portion of computing related jobs to some third party. Thus, service quality was broadly dependent on the expertise of those third parties or the in-house teams managing it. Whereas in cloud computing, high quality of service (QoS) is ensured as it is

When service is provided by reputed vendors, QoS is assured and it becomes a responsibility of the vendor.

provided by renowned computing vendors having well-trained staffs and expertise exclusively in the field of computing.

7) *Reliability*

The ability to deliver the quality service and support load balancing, backup and recovery in cases of failure makes the reputed cloud vendors highly reliable which often emerges as big worry in traditional computing. In cloud computing, subscribers no more need to plan for all of these complex tasks as vendors take care of those issues and they do it better.

8) *Continuous Availability*

Reputed cloud vendors assure almost 24 × 7 service availability. Statistics have shown that service uptime (delivered from reputed vendors) counted for a year generally doesn't go below 99.9%. Such guaranteed continuous availability of cloud service is a big enabler for any business.

9) *Locational Independence/Convenience of Access*

Cloud computing is available everywhere via Internet. Users can access it through any computing device like PCs, or portable computing devices like tablet, laptop or smart phone. Only the thing required to avail cloud computing through those devices is the access to Internet, irrespective of geographic location or time zone.

Convenience of access and low investment make cloud computing the field with low barrier to entry.

10) *High Resiliency*

Resiliency is the ability of reducing the magnitude and/or period of disruptions caused by undesirable circumstances. Higher level of resiliency has great value in computing environment. Cloud computing is developed based on

resilient computing infrastructure, and thus cloud services are more resilient to attacks and faults. Infrastructure resiliency is achieved through infrastructure redundancy combined with effective mechanism to anticipate, absorb and adapt. The cloud consumers can increase the reliability of their businesses by leveraging the resiliency of cloud-based IT resources.

11) *Quick Deployment*

Deployment time in cloud environment has significantly reduced than what is was in traditional computing environment. This is possible since resource provisioning is rapid and automatic in cloud environment. In a highly competitive market, the ability of quicker deployment gains significant business advantages.

Quicker system or application deployment attains business advantage in competitive market.

12) *Automatic Software Updates*

The issue of software upgrade incurs a lot of headache in traditional computing environment. New patches are released every now and then and users need to run those patches periodically. In cloud computing environment, this upgrade happens automatically. Cloud vendors always deliver the latest available version of any software (if not asked for otherwise). Upgraded environment gets available to users almost immediately after it releases, and whenever user logs in next time.

13) *No License Procurement*

Application license procurement needed separate budgetary arrangements in traditional computing. Moreover, unnecessary applications used to be provided with licensed packages. Cloud computing has eliminated that problem too. Here, users need not procure any periodic license for using applications; rather, they are allowed to pay (post-payment) according to their use of any software.

Software licensing is no more a concern for users in cloud computing.

14) *Safety against Disaster*

Breakdown of systems due to sudden technical failure or natural disaster is a major concern for users. Specially, any damage to physical storage devices may cause huge commercial loss. Cloud computing delivered by reputed vendors have robust recovery systems incorporated in their set up. Thus, systems and data remain more protected in cloud computing in terms of safety and security than previous ones.

15) *Environment Friendly*

Cloud computing promotes green computing. Proper utilization of resources minimizes overall electronic resource requirement, hence reduces generation of e-waste too. This is beneficial for environment as e-wastes are harmful for eco-system if not being processed properly. Apart from this, the reduced resource

Cloud computing is an eco-friendly computing approach.

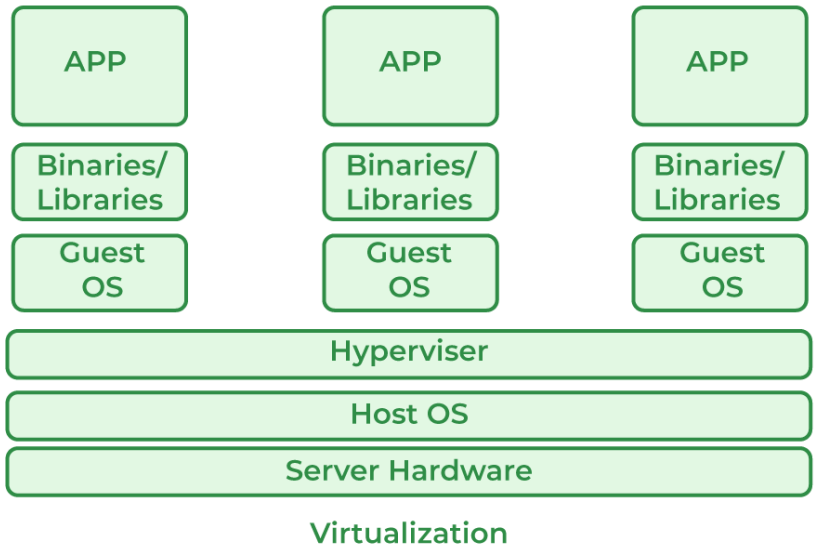
requirement results in lesser demand, hence production of computing resources. This decrease in e-production reduces carbon emissions and helps to decrease the overall carbon footprint.

III. What Is Virtualization in Cloud Computing?

Cloud virtualization refers to the use of virtualization within a cloud-based environment. Cloud providers use this technology to create virtual instances of computing resources and deliver them to end-users over the Internet.

Virtualization is used to create a virtual version of an underlying service With the help of Virtualization, multiple operating systems and applications can run on the same machine and its same hardware at the same time, increasing the utilization and flexibility of hardware. It was initially developed during the mainframe era.

It is one of the main cost-effective, hardware-reducing, and energy-saving techniques used by cloud providers. Virtualization allows sharing of a single physical instance of a resource or an application among multiple customers and organizations at one time. It does this by assigning a logical name to physical storage and providing a pointer to that physical resource on demand. The term virtualization is often synonymous with hardware virtualization, which plays a fundamental role in efficiently delivering Infrastructure-as-a-Service (IaaS) solutions for cloud computing. Moreover, virtualization technologies provide a virtual environment for not only executing applications but also for storage, memory, and networking.



Virtualization
Host Machine: The machine on which the virtual machine is going to be built is known as Host Machine.
Guest Machine: The virtual machine is referred to as a Guest Machine.

Work of Virtualization in Cloud Computing
Virtualization has a prominent impact on Cloud Computing. In the case of cloud computing, users store data in the cloud, but with the help of Virtualization, users have the extra benefit of sharing the infrastructure. Cloud Vendors take care of the required physical resources, but these cloud providers charge a huge amount for these services which impacts every user or organization. Virtualization helps Users or Organisations in maintaining those services which are required by a company through external (third-party) people, which helps in reducing

costs to the company. This is the way through which Virtualization works in Cloud Computing.

A. ***Benefits of Virtualization***

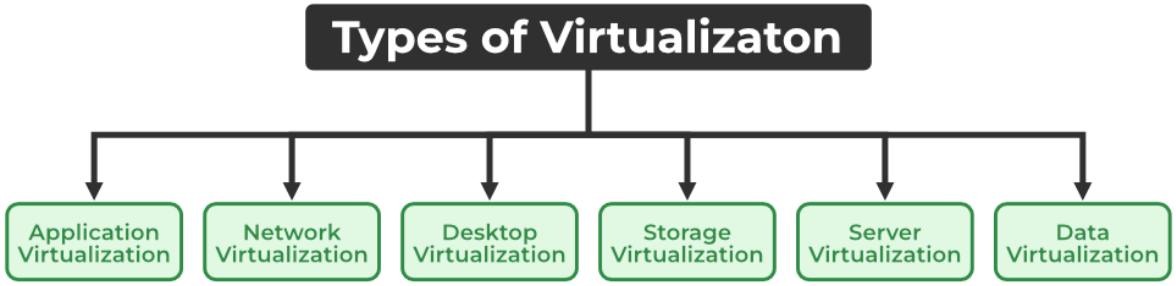
- More flexible and efficient allocation of resources.
- Enhance development productivity.
- It lowers the cost of IT infrastructure.
- Remote access and rapid scalability.
- High availability and disaster recovery.
- Pay peruse of the IT infrastructure on demand.
- Enables running multiple operating systems.

B. ***Drawback of Virtualization***

High Initial Investment: Clouds have a very high initial investment, but it is also true that it will help in reducing the cost of companies.
Learning New Infrastructure: As the companies shifted from Servers to Cloud, it requires highly skilled staff who have skills to work with the cloud easily, and for this, you have to hire new staff or provide training to current staff.
Risk of Data: Hosting data on third-party resources can lead to putting the data at risk, it has the chance of getting attacked by any hacker or cracker very easily.
For more benefits and drawbacks, you can refer to the Pros and Cons of Virtualization.
Characteristics of Virtualization
Increased Security: The ability to control the execution of a guest program in a completely transparent manner opens new possibilities for delivering a secure, controlled execution environment. All the operations of the guest programs are generally performed against the virtual machine, which then translates and applies them to the host programs.
Managed Execution: In particular, sharing, aggregation, emulation, and isolation are the most relevant features.
Sharing: Virtualization allows the creation of a separate computing environment within the same host.
Aggregation: It is possible to share physical resources among several guests, but virtualization also allows aggregation, which is the opposite process.
For more characteristics, you can refer to Characteristics of Virtualization.

C. ***Types of Virtualization***

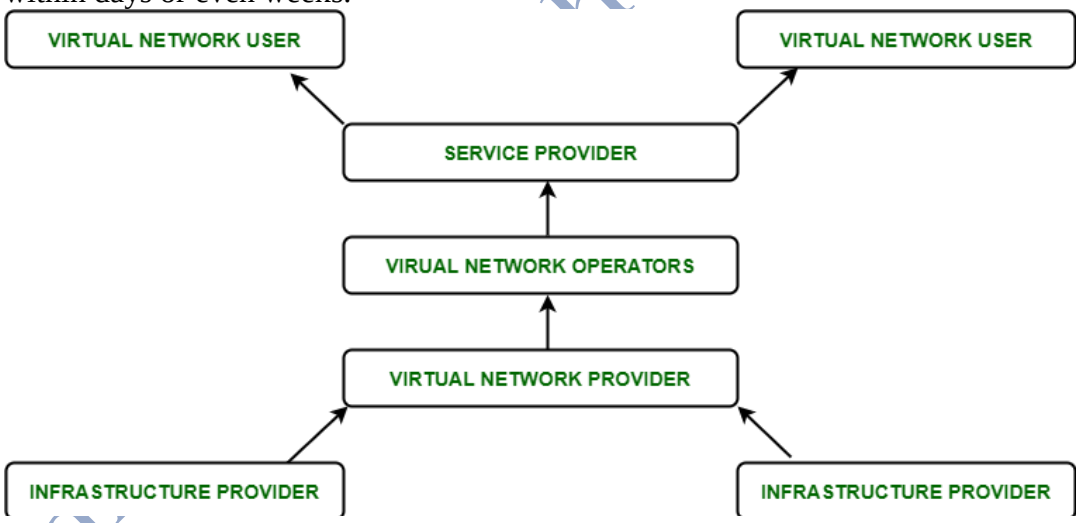
- Application Virtualization
- Network Virtualization
- Desktop Virtualization
- Storage Virtualization
- Server Virtualization
- Data virtualization



Types of Virtualization

1. Application Virtualization: Application virtualization helps a user to have remote access to an application from a server. The server stores all personal information and other characteristics of the application but can still run on a local workstation through the internet. An example of this would be a user who needs to run two different versions of the same software. Technologies that use application virtualization are hosted applications and packaged applications.

2. Network Virtualization: The ability to run multiple virtual networks with each having a separate control and data plan. It co-exists together on top of one physical network. It can be managed by individual parties that are potentially confidential to each other. Network virtualization provides a facility to create and provision virtual networks, logical switches, routers, firewalls, load balancers, Virtual Private Networks (VPN), and workload security within days or even weeks.

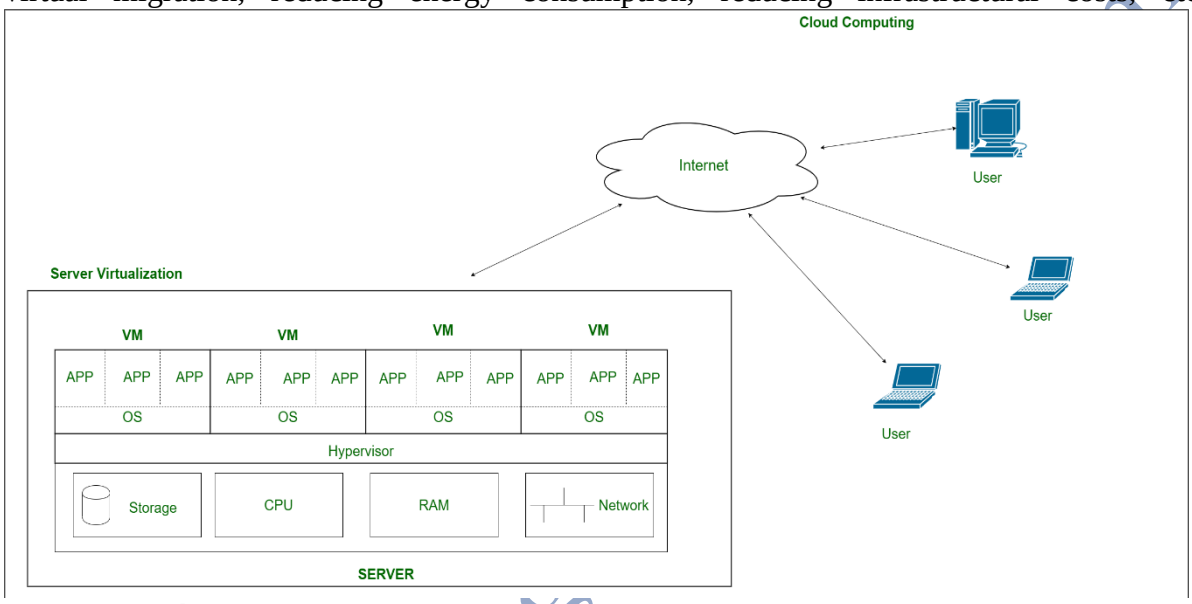


3. Desktop Virtualization: Desktop virtualization allows the users' OS to be remotely stored on a server in the data center. It allows the user to access their desktop virtually, from any location by a different machine. Users who want specific operating systems other than Windows Server will need to have a virtual desktop. The main benefits of desktop virtualization are user mobility, portability, and easy management of software installation, updates, and patches.

4. Storage Virtualization: Storage virtualization is an array of servers that are managed by a virtual storage system. The servers aren't aware of exactly where their data is stored and instead function more like worker bees in a hive. It makes managing storage from multiple

sources be managed and utilized as a single repository. storage virtualization software maintains smooth operations, consistent performance, and a continuous suite of advanced functions despite changes, breaks down, and differences in the underlying equipment.

5. Server Virtualization: This is a kind of virtualization in which the masking of server resources takes place. Here, the central server (physical server) is divided into multiple different virtual servers by changing the identity number, and processors. So, each system can operate its operating systems in an isolated manner. Where each sub-server knows the identity of the central server. It causes an increase in performance and reduces the operating cost by the deployment of main server resources into a sub-server resource. It's beneficial in virtual migration, reducing energy consumption, reducing infrastructural costs, etc.



Server Virtualization

6. Data Virtualization: This is the kind of virtualization in which the data is collected from various sources and managed at a single place without knowing more about the technical information like how data is collected, stored & formatted then arranged that data logically so that its virtual view can be accessed by its interested people and stakeholders, and users through the various cloud services remotely. Many big giant companies are providing their services like Oracle, IBM, At scale, Cdata, etc.

Uses of Virtualization:-
Data-integration
Business-integration
Service-oriented architecture data-services
Searching organizational data

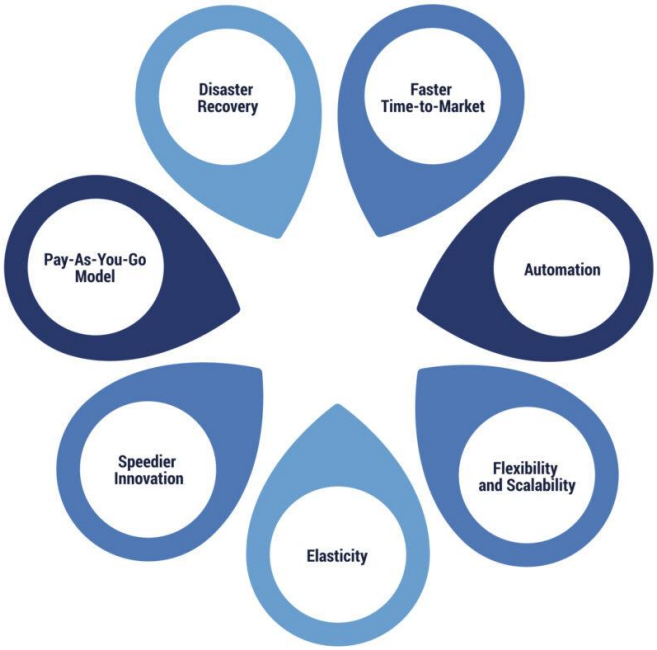
IV. What is Cloud Agility?

Cloud agility allows businesses to create, launch, and test their applications quickly in a cloud-based environment. When an organization is agile, it's able to respond rapidly and effectively to new business challenges or changing technological environments. Agility is a key component of cloud computing and enables organizations to respond

appropriately to user demands.

Why is Cloud Agility Important for Businesses?
Companies that remain stagnant run the risk of losing business over time to competitors that are offering products and services that customers have grown to want. Cloud agility is important for business because of what's provided in a cloud environment.
Organizations are able to iterate and progress more quickly in a cloud environment, improving the chances of relevancy and profitability, than in a traditional on-premises environment.

Benefits of Achieving Cloud Agility
Achieving cloud agility comes with several business-friendly benefits, including speeding up the time to market, allowing for more flexibility, and adding value to the organization.



Faster Time-to-Market
The iterative nature of cloud computing gives businesses the chance to develop and launch an application and bring it to market, improving it over time. This cuts down on the delay between development and launch that may be present in an on-premises environment, where bringing something to market can require more lift from a business. Instead of taking weeks to procure and provision IT infrastructure, for example, cloud servers can accomplish this in minutes.

Automation
Automating routine tasks in a cloud environment can free up time on IT teams for other, more important tasks. Through automation, businesses are also able to reduce the number of errors from manual entry and oftentimes reduce the cost of labor associated with mundane, repetitive tasks, such as provisioning, scaling, and managing of resources.

Flexibility and Scalability

Whether it's automated or not, businesses can easily scale their IT resources up or down to respond appropriately to demands. The flexibility of paying for what you use is not possible in an on-premises environment.

Elasticity

Cloud platforms offer elasticity, which means resources can be automatically adjusted to match demand. Businesses can put rules in place to trigger an increase or decrease that react to changes in demands on the system.

For example, if a website has an unexpected surge in traffic, the cloud infrastructure can automatically allocate more resources to handle the increased load to prevent the site from crashing.

Speedier Innovation

Cloud services offer access to various tools and technologies, like machine learning, big data analytics, and IoT platforms.This allows for innovation by letting organizations experiment with new technologies without substantial costs initially; it also accelerates their time-to-market and helps product improvements to be launched more quickly.

Pay-As-You-Go Model

Cloud services operate according to an OpEx model rather than CapEx. This pay-as-you-go or pay-per-use model, enables organizations to pay solely for the resources they utilize. This cost-efficient approach eliminates the necessity for substantial upfront investments in hardware and software, which gives IT leaders the opportunity to invest their former CapEx budget into other areas.

Disaster Recovery

Cloud agility includes the ability to establish resilient disaster recovery and backup solutions that safeguard critical data and operations. Through the cloud's infrastructure, data can be efficiently replicated across multiple geographical regions and availability zones. This strategic redundancy ensures the continuity of essential business functions even in the face of unexpected failures, disasters, or disruptions. Cloud computing's flexibility empowers organizations to customize disaster recovery plans, fine-tuning them to meet specific recovery time and recovery point objectives, thus enhancing overall business resilience.

What Are the Challenges with Cloud Agility?

When organizations are new to cloud computing, one of the main challenges can result from the culture and process shift to a new type of environment. Enhancing agility in the cloud also calls for an increased need for businesses to be agile in turn.

Depending on your in-house skills, you may also need to upskill current staff or bring in new cloud experts to fill cloud skills gaps, manage the cloud environment, and advance new and innovative capabilities, as well as make the most of cloud agility. Businesses also have to address new security and compliance challenges that can arise from moving to cloud.

How to Build Cloud Agility in Your Cloud Environment

You can incorporate cloud agility into your environment by utilizing the following:

Infrastructure as Code (IaC)

Embrace IaC techniques for automating infrastructure provisioning and management through code. Utilize tools like Terraform and AWS CloudFormation to streamline and simplify resource creation and modification as per your requirements.

Continuous Integration/Continuous Deployment (CI/CD)

Set up CI/CD pipelines to automate the software development, testing, and deployment processes. This accelerates the release cycle and guarantees quick, dependable deployment of changes pushed to the production environment.

Multi-Cloud Strategy

Prevent vendor lock-in and enhance flexibility by embracing a multi-cloud approach. This strategy involves leveraging various cloud providers or services to avoid reliance on a single vendor and to capitalize on diverse features and pricing structures.

Cloud Cost Optimization

Ensure ongoing monitoring and cost-efficiency in the cloud through resource optimization, identifying idle resources, and the utilization of cloud cost management tools.

Cloud Native Architecture

Create cloud native applications and services from the ground up. This involves harnessing cloud services and embracing a microservices architecture to develop systems that are:

Modular

Scalable

Exceptionally available

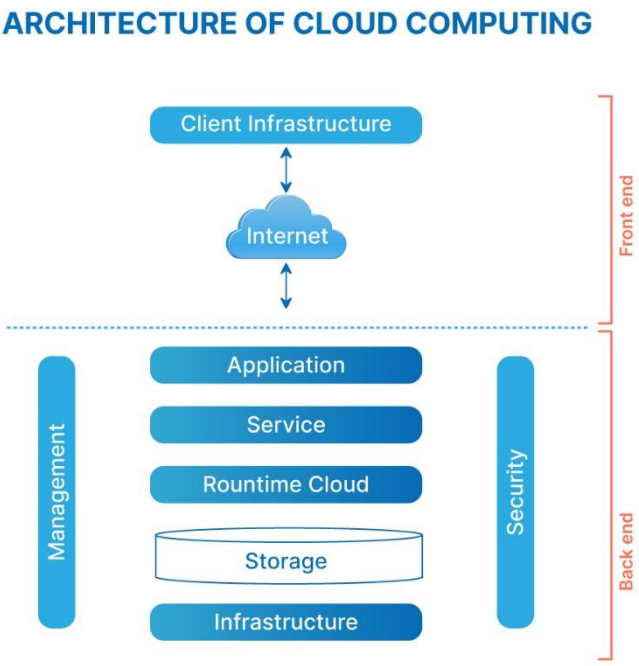
Serverless Computing
Opt for serverless computing platforms like AWS Lambda or Azure Functions to execute code without the need for server provisioning or management. This approach enables automatic scaling and further cost optimization.

Containerization
Employ containerization technologies like Docker and container orchestration platforms such as Kubernetes to package applications and services into portable, isolated units. This ensures uniform deployment across cloud environments.

Security and Compliance Automation
Integrate automated security protocols and compliance assessments. Tools like AWS Security Hub and Azure Security Center prove invaluable for pinpointing and remedying security vulnerabilities while ensuring adherence to compliance standards.

V. WHAT IS CLOUD ARCHITECTURE?

Cloud architecture is a key element of building in the cloud. It refers to the layout and connects all the necessary components and technologies required for cloud computing.
Migrating to the cloud can offer many business benefits compared to on-premises environments, from improved agility and scalability to cost efficiency. While many organizations may start with a "lift-and-shift" approach, where on-premises applications are moved over with minimal modifications, ultimately it will be necessary to construct and deploy applications according to the needs and requirements of cloud environments.
Cloud architecture dictates how components are integrated so that you can pool, share, and scale resources over a network. Think of it as a building blueprint for running and deploying applications in cloud environments.
Explore how Google Cloud helps you design cloud architecture to match your business needs. Use our Architecture Framework for guidance, recommendations, and best practices to build and migrate your workloads to the cloud. Use our Architecture Diagramming Tool for pre-built reference architectures and customizing them to your use cases.



Cloud architecture defined
Cloud architecture refers to how various cloud technology components, such as hardware, virtual resources, software capabilities, and virtual network systems interact and connect to create cloud computing environments. It acts as a blueprint that defines the best way to strategically combine resources to build a cloud environment for a specific business need.

Cloud architecture components

Cloud architecture components include:
A frontend platform
A backend platform
A cloud-based delivery model
A network (internet, intranet, or intercloud)

In cloud computing, frontend platforms contain the client infrastructure—user interfaces, client-side applications, and the client device or network that enables users to interact with and access cloud computing services. For example, you can open the web browser on your mobile phone and edit a Google Doc. All three of these things describe frontend cloud architecture components.

On the other hand, the back end refers to the cloud architecture components that make up the cloud itself, including computing resources, storage, security mechanisms, management, and more.

Below is a list of the main backend components:
Application: The backend software or application the client is accessing from the front end to coordinate or fulfill client requests and requirements.

Service: The service is the heart of cloud architecture, taking care of all the tasks being run

on a cloud computing system. It manages which resources you can access, including storage, application development environments, and web applications.

Runtime cloud: Runtime cloud provides the environment where services are run, acting as an operating system that handles the execution of service tasks and management. Runtimes use virtualization technology to create hypervisors that represent all your services, including apps, servers, storage, and networking.

Storage: The storage component in the back end is where data to operate applications is stored. While cloud storage options vary by provider, most cloud service providers offer flexible scalable storage services that are designed to store and manage vast amounts of data in the cloud. Storage may include hard drives, solid-state drives, or persistent disks in server bays.

Infrastructure: Infrastructure is probably the most commonly known component of cloud architecture. In fact, you might have thought that cloud infrastructure *is* cloud architecture. However, cloud infrastructure comprises all the major hardware components that power cloud services, including the CPU, graphics processing unit (GPU), network devices, and other hardware components needed for systems to run smoothly. Infrastructure also refers to all the software needed to run and manage everything.

Cloud architecture, on the other hand, is the plan that dictates how cloud resources and infrastructure are organized.

Management: Cloud service models require that resources be managed in real time according to user requirements. It is essential to use management software, also known as middleware, to coordinate communication between the backend and frontend cloud architecture components and allocate resources for specific tasks. Beyond middleware, management software will also include capabilities for usage monitoring, data integration, application deployment, and disaster recovery.

Security: As more organizations continue to adopt cloud computing, implementing cloud security features and tools is critical to securing data, applications, and platforms. It's essential to plan and design data security and network security to provide visibility, prevent data loss and downtime, and ensure redundancy. This may include regular backups, debugging, and virtual firewalls.

How does cloud architecture work?

In cloud architecture, each of the components works together to create a cloud computing platform that provides users with on-demand access to resources and services.
The back end contains all the cloud computing resources, services, data storage, and applications offered by a cloud service provider. A network is used to connect the frontend and backend cloud architecture components, enabling data to be sent back and forth between them. When users interact with the front end (or client-side interface), it sends queries to the back end using middleware where the service model carries out the specific task or request.
The types of services available to use vary depending on the cloud-based delivery model or service model you have chosen. There are three main cloud computing service models:

Infrastructure as a service (IaaS): This model provides on-demand access to cloud

infrastructure, such as servers, storage, and networking. This eliminates the need to procure, manage, and maintain on-premises infrastructure.

Platform as a service (PaaS): This model offers a computing platform with all the underlying infrastructure and software tools needed to develop, run, and manage applications.

Software as a service (SaaS): This model offers cloud-based applications that are delivered and maintained by the service provider, eliminating the need for end users to deploy software locally.

Cloud architecture layers

A simpler way of understanding how cloud architecture works is to think of all these components as various layers placed on top of each other to create a cloud platform.

Here are the basic cloud architecture layers:

Hardware: The servers, storage, network devices, and other hardware that power the cloud.

Virtualization: An abstraction layer that creates a virtual representation of physical computing and storage resources. This allows multiple applications to use the same resources.

Application and service: This layer coordinates and supports requests from the frontend user interface, offering different services based on the cloud service model, from resource allocation to application development tools to web-based applications.

Types of cloud architecture

Cloud adoption is not one-size-fits-all. You'll need to consider what type of cloud you want to build based on your existing technology investments, your specific business requirements, and the overall goals you hope to achieve.

There are three main types of cloud architecture you can choose from:
public, private, and hybrid.

Public cloud architecture uses cloud computing resources and physical infrastructure that is owned and operated by a third-party cloud service provider. Public clouds enable you to scale resources easily without having to invest in your own hardware or software, but use multi-tenant architectures that serve other customers at the same time.

Private cloud architecture refers to a dedicated cloud that is owned and managed by your organization. It is privately hosted on-premises in your own data center, providing more control over resources and more security over data and infrastructure. However, this architecture is considerably more expensive and requires more IT expertise to maintain.

Hybrid cloud architecture uses both public and private cloud architecture to deliver a flexible mix of cloud services. A hybrid cloud allows you to migrate workloads between environments, allowing you to use the services that best suit your business demands and the

workload. Hybrid cloud architectures are often the solution of choice for businesses that need control over their data but also want to take advantage of public cloud offerings.
In recent years, **multicloud architecture** is also emerging as more organizations look to use cloud services from multiple cloud providers. Multicloud environments are gaining popularity for their flexibility and ability to better match use cases to specific offerings, regardless of vendor.

What does a cloud architect do?
A cloud architect is an IT expert responsible for developing, implementing, and managing an organization's cloud architecture. As cloud strategies continue to become more complex, the skills and expertise of cloud architects are becoming more vital for helping companies navigate the complexities of cloud environments, implement successful strategies, and keep cloud systems running smoothly.

Benefits of cloud architecture
There are many benefits of cloud architecture for organizations, including:

Cost-effective Instead of investing upfront costs for servers, you can opt to use the infrastructure of a cloud service provider. Dynamic provisioning allows you to further optimize spending by paying only for the computing resources you use.
Accelerated transformation Cloud-native architectures like Kubernetes let you make the most of cloud services and automated environments to speed up modernization and drive digital transformation.
Strong security Cloud service providers consistently upgrade and improve their security mechanisms with expert professionals and the latest technologies to help secure your data, systems, and workloads.
Faster time to market You no longer need to wait to procure, set up, and configure computing infrastructure. Cloud architectures enable you to get up and running fast, so you spend more time focusing on developing and delivering new products.
More innovation Cloud architectures allow you to leverage the latest technologies for storage, security, analytics, and AI like machine learning.
Scalability Cloud architectures give you more flexibility to scale computing resources up (or down) based on your infrastructure requirements. You can easily scale to meet higher demand, whether from growth or seasonal spikes in traffic.
High availability Applications run and managed on cloud architectures benefit from high-performance computing resources that ensure continuous availability, regardless of fluctuating loads.

VI. AVAILABILITY MANAGEMENT IN CLOUD COMPUTING

Pre-requisite: **Cloud Computing** and **Cloud Based Services**
Cloud Services are not immune to outages (failure/interruption) and the severity and the scope of impact on the customer can vary based on the situation. As it will depend on the criticality of the cloud application and its relationship to internal business processes.

1. **Impact on business:** In the case of business-critical applications where businesses rely on the continuous availability of service, even a few minutes of service failure can have a serious impact on the organization's productivity, revenue, customer satisfaction, and service-level compliance.

2. **Impact on customers:** During a cloud service disruption, affected customers will not be able to access the cloud service and in some cases may suffer degraded performance or user experience. For Example:- when a storage service is disrupted, it will affect the availability and performance of a computing service that depends on the storage service.

For example, on December 20, 2005, Salesforce.com (the on-demand customer relationship management service) said it suffered from a system outage that prevented users from accessing the system during business hours. Users "experienced intermittent access" because of a database cluster error in one of the company's four global network nodes, company officials said in a statement the day following the outage.

1) ***Factors Affecting Availability****:*

The cloud service's ability to recover from an outage situation and availability depends on a few factors, including the cloud service provider's data center architecture, application architecture, hosting location redundancy, diversity of Internet service providers (ISPs), and data storage architecture.

Following is a list of the major factors:

- The redundant design of System as a Service and Platform as a Service application.
- The architecture of the Cloud service data center should be fault-tolerant.
- Having better Network connectivity and geography can resist disaster in most cases.
- Customers of the cloud service should quickly respond to outages with the support team of the Cloud Service Provider.
- Sometimes the outage affects only a specific region or area of cloud services, so it is difficult in those cases to troubleshoot the situation.
- There should be reliability in the software and hardware used in delivering cloud services.
- The infrastructure of the network should be efficient and should be able to cope-up with DDoS(distributed denial of service) attacks on the cloud service.
- Not having proper security against internal and external threats, e.g., privileged users abusing privileges.
- Regular testing and maintenance of the cloud infrastructure and applications can help identify and fix issues before they cause downtime.
- Proper capacity planning is essential to ensure that the cloud service can handle peak traffic and usage without becoming overloaded.
- Adequate backups and disaster recovery plans can help minimize the impact of outages or data loss incidents.
- Monitoring tools and alerts can help detect and respond to issues quickly, reducing downtime and improving overall availability.
- Ensuring compliance with industry standards and regulations can help minimize the risk of security breaches and downtime due to compliance issues.
- Continuous updates and patches to the cloud infrastructure and applications can help address vulnerabilities and improve overall security and availability.
- Transparency and communication with customers during outages can help manage expectations and maintain trust in the cloud service provider.

2) ***System as a Service Customer's Responsibility:***

- Customers should understand the Service Level Agreement(SLA) and communication methods so that they will be informed on service outages or maintenance.
- Customers should be aware of options to support availability management that is they should understand the factors affecting availability management.
- The customer of System as a service should be aware that the cloud service is multitenant which means Cloud Service Providers typically offer a Standard Service Level Agreement(SLA) for all customers. Thus, Cloud Service Providers may not be able to provide their services to the customers if the standard Service level-Agreement(SLA) does not meet the service requirements. However, if you are a medium or large enterprise with a big budget, a custom SLA can be made available.
- The customers should be aware of how resource democratization occurs within the Cloud Service Providers to best predict the likelihood of system availability and performance during business fluctuations.
- Customers should ensure that their applications are designed and deployed in a way that maximizes availability and resilience. This may include using load balancing, redundancy, and failover mechanisms.
- It's important for customers to monitor their own applications and infrastructure to detect and respond to issues quickly, rather than relying solely on the cloud service provider to do so.
- Customers should understand the security and compliance implications of using a cloud service and take appropriate measures to protect their data and systems.
- It's important for customers to have a disaster recovery plan in place, including backups and a procedure for restoring service in the event of an outage.
- Customers should understand the cost implications of using a cloud service, including any charges for exceeding usage limits or for premium support options.
- It's important for customers to provide feedback to the cloud service provider on their experience using the service, including any issues or suggestions for improvement.
- Customers should understand the limitations and restrictions of their cloud service subscription, such as the maximum number of users or the amount of data that can be stored, and plan accordingly.

3) System as a Service Health Monitoring:

The following options are available to customers to stay informed on the health of their service:

- Service dashboards should be published by the Cloud Service Providers So that they can publish the current state of services and can also inform the outage or any kind of maintenance of the cloud.
- Customer should check their mailing list as the service provider might have notified them about recently occurring outrages.
- Use third-party tools to check the health of the application.

4) Platform as a Services Customer's Responsibilities:

The following considerations are for Platform as a Services Customers:

- **PaaS platform service levels:** Customers should read and understand the terms and conditions of the Cloud Service Provider's Service Level Agreements.

- **Third-party web services provider service levels:** When your Platform as a Services application depends on a third-party service it is critical to understand the Service Level Agreements of that service. Network connectivity parameters with third-party service providers. Example: Bandwidth and latency factors.
- **Platform as a Service Health Monitoring:** The following options are available to customers to monitor the health of their service:
    - Service health dashboard published by the Cloud Service Provider.
    - Cloud Service Providers customer mailing list that notifies customers of occurring and recently occurred outages
    - Use third-party tools to check the health of the application
- **Infrastructure as a Service Health Monitoring:** The following options are available to Infrastructure as a Service customer for managing the health of their service:
    - Service health dashboard published by the Cloud Service Providers.
    - Cloud Service Providers customer mailing list that notifies customers of occurring and recently occurred outages.
    - Third-party-based service monitoring tools that periodically check the health of your Infrastructure as a Service virtual server.

VII. CLOUD COMPUTING SECURITY

What is Cloud Computing ?

Cloud computing refers to the on demand delivery of computing services such as applications, computing resources, storage, database, networking resources etc. through internet and on a pay as per use basis. At the present time the demand for cloud computing services are increasing with respect to that demand for cloud computing skills is also increasing. It provides three main types of service models i.e. SaaS (Software as a Service), PaaS (Platform as a Service) and IaaS (Infrastructure as a Service). With this as starting from small to large organizations have started using cloud services so depending upon their requirement they go for the different types of cloud like Public cloud, Private cloud, Hybrid cloud, Community cloud.

Security In Cloud Computing :

Cloud computing which is one of the most demanding technology of the current time, starting from small to large organizations have started using cloud computing services. Where there are different types of cloud deployment models are available and cloud services are provided as per requirement like that internally and externally security is maintained to keep the cloud system safe. Cloud computing security or cloud security is an important concern which refers to the act of protecting cloud environments, data, information and applications against unauthorized access, DDOS attacks, malwares, hackers and other similar attacks. Community Cloud : These allow to a limited set of organizations or employees to access a shared cloud computing service environment.

Planning of security in Cloud Computing :

As security is a major concern in cloud implementation, so an organization have to plan for security based on some factors like below represents the three main factors on which planning of cloud security depends.

- Resources that can be moved to the cloud and test its sensitivity risk are picked.
- The type of cloud is to be considered.

- The risk in the deployment of the cloud depends on the types of cloud and service models.

Types of Cloud Computing Security Controls :
There are 4 types of cloud computing security controls i.e.

1. **Deterrent Controls** : Deterrent controls are designed to block nefarious attacks on a cloud system. These come in handy when there are insider attackers.
2. **Preventive Controls** : Preventive controls make the system resilient to attacks by eliminating vulnerabilities in it.
3. **Detective Controls** : It identifies and reacts to security threats and control. Some examples of detective control software are Intrusion detection software and network security monitoring tools.
4. **Corrective Controls** : In the event of a security attack these controls are activated. They limit the damage caused by the attack.

Importance of cloud security :
For the organizations making their transition to cloud, cloud security is an essential factor while choosing a cloud provider. The attacks are getting stronger day by day and so the security needs to keep up with it. For this purpose it is essential to pick a cloud provider who offers the best security and is customized with the organization's infrastructure. Cloud security has a lot of benefits –

- **Centralized security :** Centralized security results in centralizing protection. As managing all the devices and endpoints is not an easy task cloud security helps in doing so. This results in enhancing traffic analysis and web filtering which means less policy and software updates.
- **Reduced costs :** Investing in cloud computing and cloud security results in less expenditure in hardware and also less manpower in administration
- **Reduced Administration :** It makes it easier to administer the organization and does not have manual security configuration and constant security updates.
- **Reliability :** These are very reliable and the cloud can be accessed from anywhere with any device with proper authorization.

When we are thinking about cloud security it includes various types of security like access control for authorized access, network segmentation for maintaining isolated data, encryption for encoded data transfer, vulnerability check for patching vulnerable areas, security monitoring for keeping eye on various security attacks and disaster recovery for backup and recovery during data loss.

There are different types of security techniques which are implemented to make the cloud computing system more secure such as SSL (Secure Socket Layer) Encryption, Multi Tenancy based Access Control, Intrusion Detection System, firewalls, penetration testing, tokenization, VPN (Virtual Private Networks), and avoiding public internet connections and many more techniques.

But the thing is not so simple how we think, even implementation of number of security techniques there is always security issues are involved for the cloud system. As cloud system is managed and accessed over internet so a lot of challenges arises during maintaining a secure cloud. Some cloud security challenges are

- Control over cloud data

- Misconfiguration
- Ever changing workload
- Access Management
- Disaster recovery

VIII. WHAT IS CLOUD DISASTER RECOVERY?

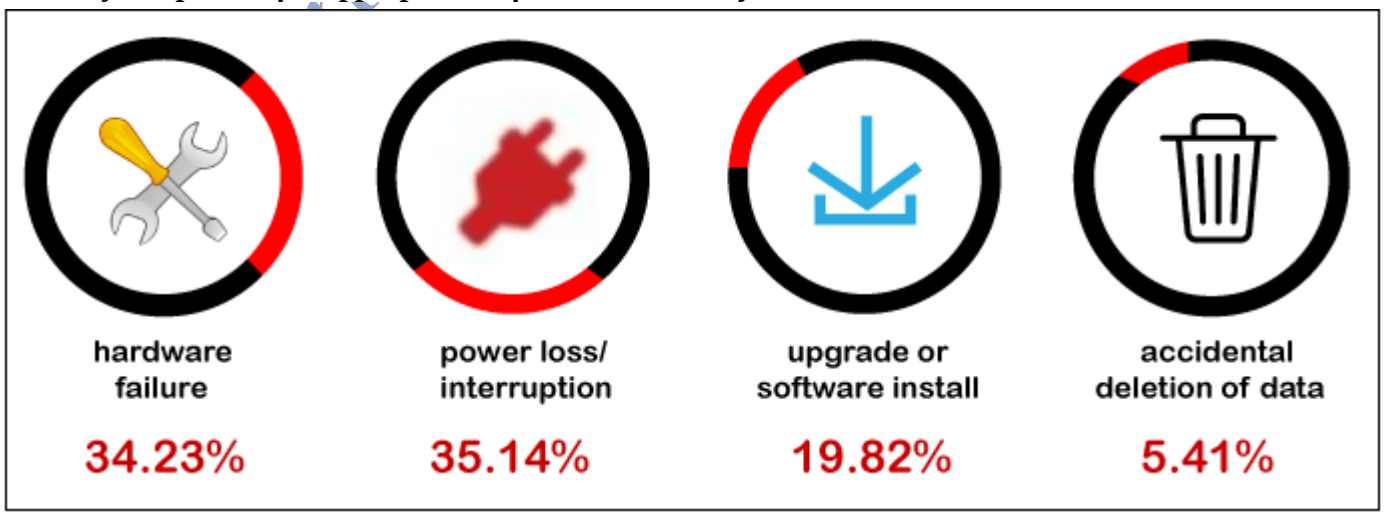
Cloud-based backup and retrieval capabilities help you to back-up and reestablish business-critical directories if they are breached. Thanks to its high adaptability, cloud technologies allow efficient disaster recovery, irrespective of the task's nature or ferocity. Data is kept in a virtual storage environment designed for increased accessibility. The program is accessible on availability, enabling companies of various sizes to customize Disaster Recovery (DR) solutions to their existing requirements.

Cloud disaster recovery (CDR) is simple to configure and maintain, as opposed to conventional alternatives. Companies no longer ought to waste a lot of time transmitting data backups from their in-house databases or hard drive to restore after a tragedy. Cloud optimizes these procedures, decisions correctly, and information retrieval.

Cloud Disaster Recovery (CDR) is based on a sustainable program that provides you recover safety functions fully from a catastrophe and offers remote access to a computer device in a protected virtual world.

When it comes to content DRs, maintaining a supplementary data center can be expensive and time taking. CDR (Cloud disaster recovery) has altered it all in the conventional DR (Disaster recovery) by removing the requirement for a centralized system and drastically reducing leisure time. Information technology (IT) departments can now use the cloud's benefits to twist and refuse instantly. This leads to faster recovery periods at a fraction of the price.

A. Always be primed for appropriate information security



As corporations keep adding system and software apps and services to their day-to-day procedures, the associated privacy concerns significantly raise. Crises can happen at any point and maintain a company decimated by huge information loss. When you recognize

what it can charge, it is evident why it makes good sense to establish an information restore and retrieval plan.

Disaster recovery data shows that 98 percent of the surveyed companies signify that a couple of hours of leisure time can charge their corporation more than $100,000. Any quantity of rest time can cost the organization 10 of thousands to hundreds and thousands of person-hour workers expended recovering or redeploying missed productivity.

An 8-hour leisure time screen can pay up to $20k for a small business and tens of millions for large companies in certain instances.Given the estimates, it is apparent why every second of assistance or structure disruption counts data and the real benefit of containing a crisis management plan.

B. ***How is cloud disaster management working?***

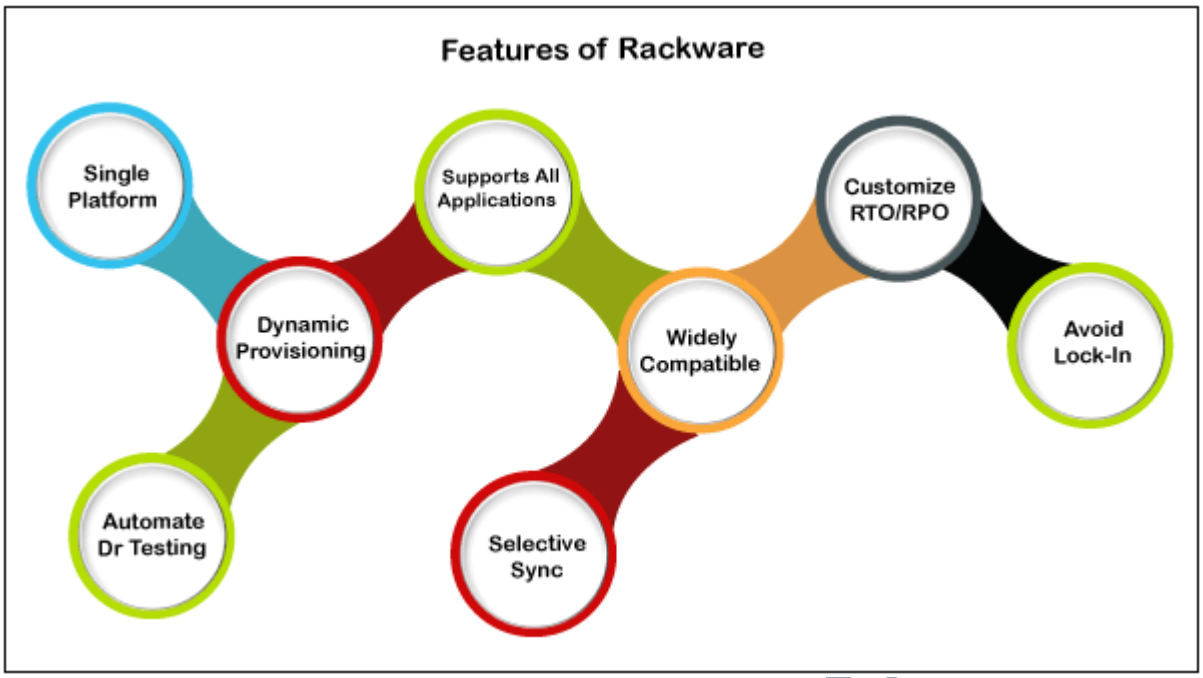
Cloud disaster recovery is taking a very differentiated perspective from classical DR (Disaster recovery). Rather than stacking data centers with Operating system technology and fixing the final configuration used in manufacturing, cloud disaster recovery captures the whole server, including the OS, apps, fixes, and information, into a separate software package or virtual environment.

The virtual server is then replicated or supported to an off-site server farm or rolled to a remote server in mins. While the virtual server is not hardware-dependent, the OS, apps, flaws, and information can be moved from one to another data center much quicker than conventional DR methodologies.

C. ***How could Rackware assist you?***

Rackware evolves cloud management technology that helps businesses relocate implementations, offer additional disaster recovery and fallback, and cloud storage management.

The RackWare Management Module (RMM) offers Information systems adaptability to companies by streamlining disaster recovery and fallback to any server. Several of the features are discussed as follows:



- **Single framework**

It is a single centralized solution that enables replication, sync, integration, cloud-based disaster healing.

- **Widely compatible**

It endorses all physical, digital, and web environments, Hyper-v and cloud atheist load.

- **Endorses all apps**

It promotes all apps, their information, and setup without rewriting any implementations.

- **Prevent lock-in**

Rackware decreases the risk and seller bolt assistance for physical-cloud, data center, and even cloud-physical restore and tragedy retrieval irrespective of supplier.

- **Automatic disaster recovery testing**

Trying down disaster recovery testing helps the company decrease time and labor costs by up to 80 percent from auto DR statistical techniques.

Personalize the RTO/RPO

Provides flexibility to personalize RPO, RTO, and expense priorities as per business requirements through various pre-provisioned or adaptive methods.

- **Dynamic provisioning**

Dynamic procurement considerably reduces the cost of providing Disaster recovery event servers rather than pre-provisioning: this does not use computed assets until failure occurs.

- **Selective synchronization**

Selective sync enables a set of policies, security, and priorities of mission-critical applications and file systems.

D. ***Selecting a Cloud disaster recovery provider***

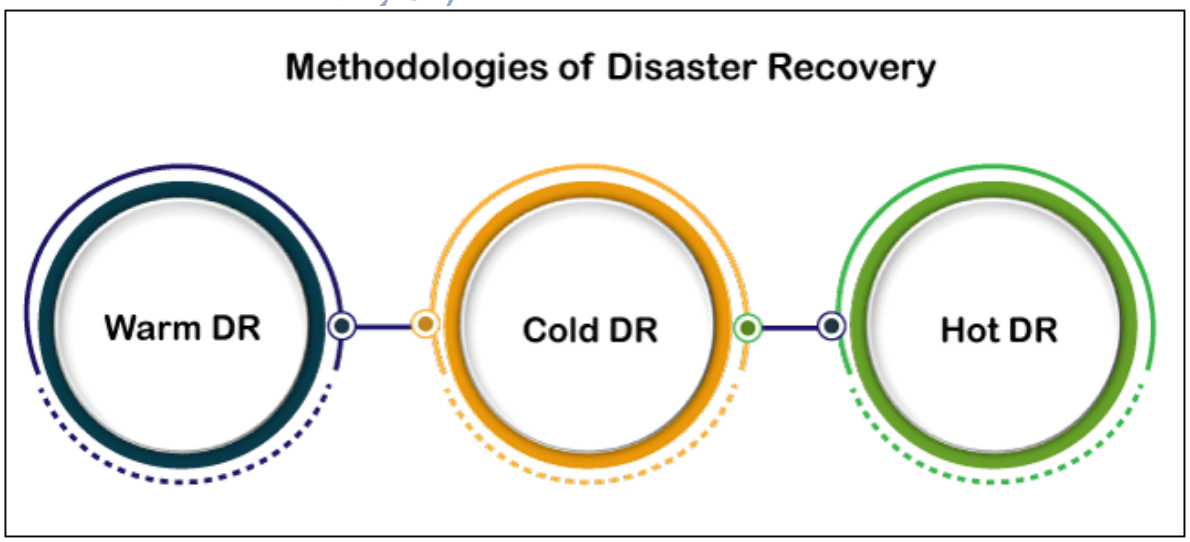
When choosing a cloud disaster recovery provider, six factors must be considered: reliability, location, security, compliance, and scalability.

First, a company must perceive the physical distance and throughput of the CDR vendor; placing the disaster recovery too close raises the risk of a given virtual disaster, but putting the DR too far aside enhances frequency and network traffic, making it more challenging to obtain DR material. When the DR information is available from multiple international business places, the area can be rugged. After that, recognize the dependability of the cloud DR provider. Only the cloud has leisure time, and system failure during rehabilitation can be equivalently devastating for the industry.

E. ***Cloud disaster recovery methodologies***

Recognize the cloud disaster recovery providing scalability. It must be protecting specific information, apps, and other assets while also accommodating added resources as required and providing sufficient efficiency as other international customers utilize the facilities. Recognize the disaster recovery content's security needs and ensure that the vendor can offer authentication, VPNs (virtual private networks), cryptography, and other toolkits are required to protect it's vital resources.

Ultimately, suggest how the DR system should be designed. There are three basic DR strategies: warm, cold, and hot. These concepts are vaguely connected to how easily a structure can be healed.



- **Warm disaster recovery**

Warm disaster recovery is a reserve strategy in which copy data and systems are stored with a cloud DR vendor and regularly updated with services and information in the prior data center. However, the redundant assets aren't doing anything. When a disaster happens, the warm DR can be implemented to capability approach from the DR vendor, which is usually as simple as

beginning a Virtual machine and rerouting Domain names and traffic to the DR assets. Although recovery times might be pretty limited, the secured tasks must still experience some leisure time.

- **Cold disaster recovery**

Cold disaster recovery usually entails storing information or VMware virtual (VM) pictures. These resources are generally inaccessible unless added work is performed, such as retrieving the stored data or filling up the picture into a Virtual machine. Cold DR is typically the easiest (often just memory) and absolute cheapest method. Still, it requires a long time to regain, leaving the organization with the most leisure time in the event of a disaster.

- **Hot disaster recovery**

Hot disaster recovery is traditionally described as a real-time simultaneous implementation of information and tasks that run concurrently. Both the primary and backup data centers execute a specific tasks and information in sync, with both websites communicating a fraction of the entire data packets. When a disaster happens, the residual pages continue to handle things without interruption. Consumers should be unaware of the disturbance. Although there is no time for rest with hot DR, it is the most complex and expensive methodology.

F. Advantages of Cloud disaster recovery

When compared to more conventional disaster recovery strategies, cloud DR offers so many significant advantages. They are defined below.

- **Choices for pay-as-you-go**

Companies that implemented do-it-yourself (DIY) disaster recovery facilities incurred substantial cash expenses, whereas participating maintained colocation vendors for off-site DR systems management entail lengthy licensing agreements. The pay-as-you-go framework of cloud providers allows companies to charge a repeated subscription fee only for the utilized programs and infrastructure. The transactions modify as assets are added or erased.

- **Scalability and adaptability**

Classical disaster recovery methodologies were typically implemented in locally or remotely cloud services, frequently enforced capability and usability constraints. The company had to purchase the servers, storing, networking devices, and productivity tools required for Disaster recovery and layout, measure, and build the system required to manage DR activities - significantly more if the DR was guided to a secondary server farm. It was traditionally a significant capital and repetitive expenditure for the company.

- **High dependability and geographical redundancy**

A global footprint is an essential requirement of a cloud service, guaranteeing multiple systems to support customers across significant international geostrategic areas. Cloud providers use this to accomplish better durability and guarantee duplication. Companies can easily use geo-duplication to position disaster recovery assets in some other place-or even several regions-to enhance accessibility. The classic off-site disaster recovery situation is a natural formation of the cloud.

- **Testing is simple, and restoration is quick**

Cloud workforces frequently run as virtual machines (VMs), making it simple to duplicate Virtual machine picture files to in-house sample data centers to verify workforce accessibility without disrupting production workloads. Furthermore, corporations can choose high bandwidth and rapid disk I/O (input/output) alternatives to maximize transmission speeds is required to address restoration time objective requirements (RTO). Data transfer from cloud services, on the other hand, incur expenses, so tests should be done with those information transfer-cloud data entry and exit-costs in opinion.

G. Traditional disaster recovery vs. Cloud disaster recovery

Cloud-based disaster recovery systems and DRaaS promotions can grant cost savings, adaptability and scalability, geo-duplication, and speedy response. However, cloud disaster recovery may not be relevant for all companies or situations. Recognize some of the scenarios in which more classical DR methodologies may be advantageous, if not critical, to the corporation.

- **Prerequisites for compliance**

Cloud providers are becoming more permissible for innovation use in areas where well-organized regulatory oversight is needed, such as Health Insurance Portability and Accountability Act (HIPAA) and Payment Card Industry Data Security Standard (PCI DSS). After all, some companies may still face restrictions when handling confidential material outside of an instant server farm-or in any asset or facilities that is not directly under the company's control, such as a third-party facility like a public cloud platform.

- **Lack of connectivity**

Cloud resources and services rely on vast area network (WAN) communication worldwide. Even though speedy updating/synchronization and speedy recovery require a dependable, high-bandwidth connection, disaster recovery uses incidents that emphasize on interconnection. Even though credible, high-bandwidth accomplishment is famous in most cities and suburban areas worldwide, it is far from global.

- **Optimum recovery**

Clouds provide powerful benefits, but customers are restricted to the equipment, architectural design, and toolkits that the cloud service provider delivers. The vendor and the service-level agreement (SLA)limit cloud disaster recovery. In many instances, the cloud DR vendor's recovery point objective (RPO) and recovery time objective (RTO) may not be appropriate for the foundation's disaster recovery requirements - or the level of service may not be assured. By purchasing the DR framework, a company can design and implement a customized DR architecture that best meets DR performance standards.

- **Make use of existing investments**

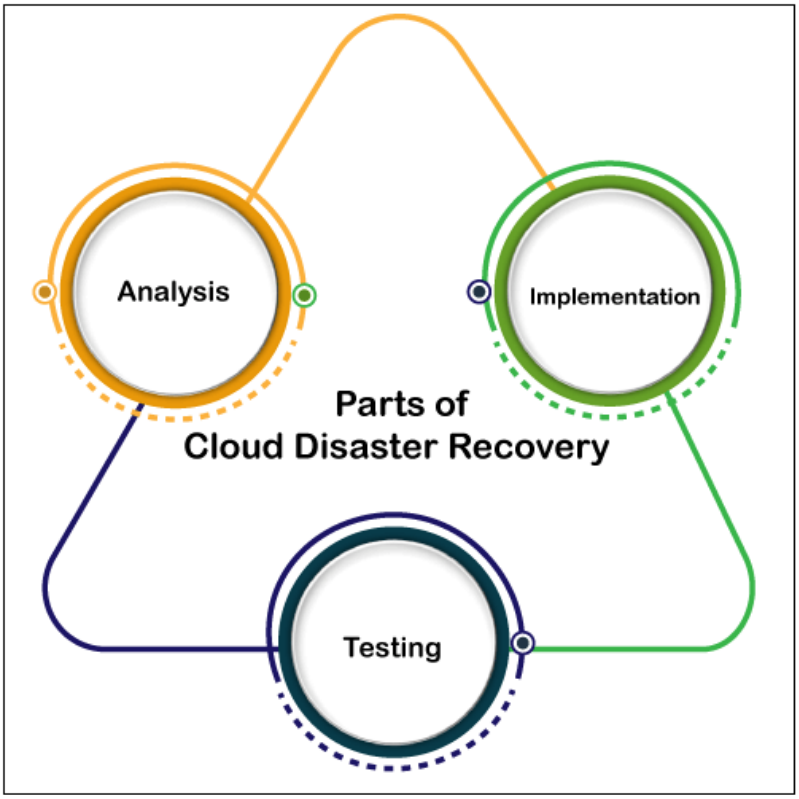
DR requirements have existed much longer than cloud computing, and prestige DR implementations, particularly in larger enterprises or where expenses are still being expensed, may be more difficult to replace by modern cloud disaster recovery offerings. A company that also owns the company, data centers, storage, and other assets may be reluctant to relinquish them. In these situations, the company can move more slowly and carefully to

cloud disaster recovery, methodically attaching workforces to the cloud DR vendor as a means of regular innovation refresh instead of spending the next round of wealth.

H. ***Developing a cloud-based disaster recovery strategy***

Creating a cloud DR plan is extremely similar to creating a more typical cultural or off-site contingency plan. The utilization of cloud services and DRaaS to sustain a practical evaluation distinguishes cloud DR from more conventional DR methodologies. For instance, instead of backing up a major information source to measure the variation in another local computer, cloud-based disaster recovery would store this information set to a cloud network, including an Amazon S3 (Simple Storage Service) container. As a result, cloud disaster recovery does not alter the fundamental requirements for stages to execute DR but instead offers a new sequence of efficient tools and technologies for DR objectives.

There are three main parts: Implementation, analysis, and testing.



- **Analysis**

Any disaster recovery plan must begin with a comprehensive risk evaluation and performance measurement, which analyzes the existing IT facilities and business processes and recognizes the potential disasters that an organization is facing. The purpose is to identify possible security flaws and catastrophes, such as intrusion security flaws and fraud, as well as natural disasters and storms, and then assess whether another IT technology is prepared to meet those obstacles.

An analysis can assist management in achieving the most complicated industry functions and IT aspects and predicting the prospective economic repercussions of a disaster event. RPOs and RTOs for facilities and tasks can also be determined using analysis.

- **Implementation**

Traditionally, the analysis is characterized by a structural requirement that specifics for preparedness, prevention, recovery, and response. The initiative required to reduce potential threats and remove weaknesses is referred to as preventive measures. This could include social manipulation training for employees, and usual operating system (OS) updates to retain stability and security. Readiness entails highlighting the appropriate response - who can do what in the case of a catastrophe. This is primarily a paperwork issue. Response describes the techniques and products to be used in the event of a disaster. This is resiliency combined with the execution of correlating innovations, such as restoring a data set or a Virtual server machine backed up to the cloud. Recovery describes the achievements circumstances for the reaction and moves to help counteract any potential investment destruction.

- **Testing**

Ultimately, any disaster recovery plan must be screened and reviewed regularly to make sure that IT employees are capable of accurately implementing proper recovery efforts and that recovery occurs within an appropriate format for the corporate. Testing has identified discrepancies or inaccuracies in execution, help organizations to accurate and notify their disaster recovery plan well before actual tragedy strikes.

I. Cloud disaster recovery service and vendors

Cloud DR is, at its core, a type of off-site disaster recovery. An off-site model enables companies to protect against occurrences within their local infrastructure (fire, theft, flood, etc.) and either regain the assets to the local infrastructure or keep operating the wide deployment from the DR vendor. As a result, a plethora of vendors have appeared to include off-site DR ability.

The most obvious route for cloud disaster recovery is via significant public cloud providers. Amazon Web Services (AWS) provides the CloudEndure Disaster Recovery facility, Azure offers Azure Site Healing, and GCP (Google Cloud Platform) provides Cloud Storage and Continuous Disk alternatives for safeguarding valuable data.

Entrepreneurship disaster recovery facilities can be designed for all three significant cloud providers.

Aside from public clouds, a plethora of devoted disaster recovery vendors now provide DRaaS goods, effectively getting access to devoted clouds for DR assignments.

Among the top DRaaS venders are:

- Iland
- Expedient
- IBM DRaaS
- Sungard AS
- TierPoint
- Bluelock
- Recovery Point Systems

Furthermore, more generic backup vendors are now providing DRaaS, such as:

- Acronis

- Carbonite
- Zerto
- Databarracks
- Arcserve UDP
- Unitrends
- Datto