**Cloud computing**

1. **Introduction:** Cloud Computing is the use of hardware and software to deliver a service over a network (typically the Internet). With cloud computing, users can access files and use applications from any device that can access the Internet. An example of a Cloud Computing provider is Google's Gmail.

# The Evolution of Cloud Computing

Cloud computing has its roots as far back in 1950s when mainframe computers came into existence. At that time, several users accessed the central computer via dummy terminals. The only task these dummy terminals could perform was to enable users access the mainframe computer. The prohibitive costs of this mainframe devices did not make them economically feasible for organizations to buy them. That was the time when the idea of provision of shared access to a single computer occurred to the companies to save costs.   
  
In 1970s, IBM came out with an operating system (OS) named VM. This allowed for simultaneous operation of more than one OS. Guest Operating Systems could be run on every VM, with their own memory and other infrastructure, making it possible to share these resources. This caused the concept of virtualization in computing to gain popularity.   
  
The 1990s witnessed telecom operators begin offering virtualized private network connections, whose quality of service was as good as those of point-to-point (dedicated) services at a lesser cost. This paved way for telecom companies' to offer many users shared access to a single physical infrastructure.  
  
The other catalysts were grid computing, which allowed major issues to be addressed via parallel computing; utility computing facilitated computing resources to be offered as a metered service and SaaS allowed subscriptions, which were network-based, to applications. Cloud computing, therefore, owes its emergence to all these factors

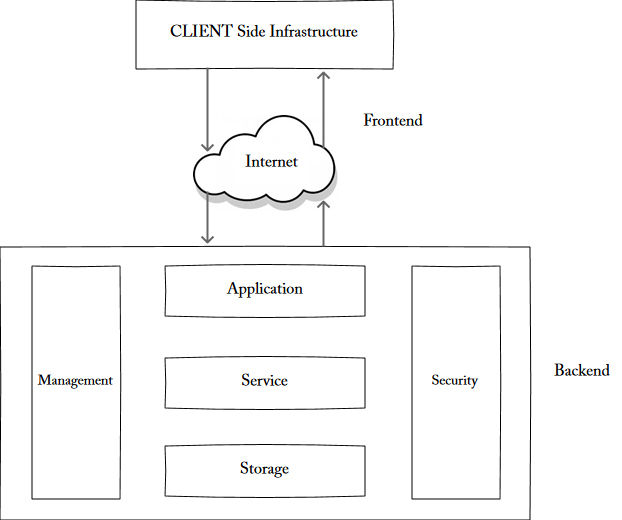
* 1. Cloud Computing Architecture:

The cloud infrastructure is closely related to its architecture & comprises of many cloud component which is loosely connected.  
The broad divisions of cloud architecture are:

* Front-end
* Back-end

It is the responsibility of the **back-end** to provide the security of data for cloud users along with the traffic control mechanism. The server also provides the middleware which helps to connect devices & communicate with each other.

 Cloud Computing Architecture:

  
Businesses used cloud infrastructures to work with these applications. Unlike subscription-based models of pricing, payment structure of the cloud enables the user to subscribe to vendor services & cloud infrastructures are paid on a 'pay-per-use' basis.

The cloud technology architecture also consists of **front-end** platforms (as read in the early chapters) called the cloud client which comprises servers, thin & fat client, tablets & mobile devices. The interaction is done through middleware or via web-browser or virtual sessions. According to Jason Bloomberg of ZapThink, the cloud-oriented architecture can essentially be the building block of IoT (Internet of Things) in which anything can be connected to the internet. The cloud architecture is a combination of both services oriented architecture & event-driven architecture. SO cloud architecture encompasses all elements of the cloud environment.

# Characteristics of Cloud Computing

* On-demand self-service: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
* Broad network access: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., [mobile](https://www.govinfosecurity.com/mobility-c-212)phones, tablets, laptops and workstations).
* Resource pooling: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state or datacenter). Examples of resources include storage, processing, memory and network bandwidth.
* Rapid elasticity: Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
* Measured service: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth and active user accounts). Resource usage can be monitored, controlled and reported, providing transparency for the provider and consumer.

# Benefits of cloud computing

Cloud computing offers your business many benefits. It allows you to set up what is essentially a virtual office to give you the flexibility of connecting to your business anywhere, any time. With the growing number of web-enabled devices used in today's business environment (e.g. smartphones, tablets), access to your data is even easier. There are many benefits to moving your business to the cloud:

## Reduced IT costs

Moving to cloud computing may reduce the cost of managing and maintaining your IT systems. Rather than purchasing expensive systems and equipment for your business, you can reduce your costs by using the resources of your cloud computing service provider. You may be able to reduce your operating costs because:

* the cost of system upgrades, new hardware and software may be included in your contract
* you no longer need to pay wages for expert staff
* your energy consumption costs may be reduced
* there are fewer time delays.

## Scalability

Your business can scale up or scale down your operation and storage needs quickly to suit your situation, allowing flexibility as your needs change. Rather than purchasing and installing expensive upgrades yourself, your cloud computer service provider can handle this for you. Using the cloud frees up your time so you can get on with running your business.

## Business continuity

Protecting your data and systems is an important part of business continuity planning. Whether you experience a natural disaster, power failure or other crisis, having your data stored in the cloud ensures it is backed up and protected in a secure and safe location. Being able to access your data again quickly allows you to conduct business as usual, minimising any downtime and loss of productivity.

## Collaboration efficiency

Collaboration in a cloud environment gives your business the ability to communicate and share more easily outside of the traditional methods. If you are working on a project across different locations, you could use cloud computing to give employees, contractors and third parties access to the same files. You could also choose a cloud computing model that makes it easy for you to share your records with your advisers (e.g. a quick and secure way to share accounting records with your accountant or financial adviser).

## Flexibility of work practices

Cloud computing allows employees to be more flexible in their work practices. For example, you have the ability to access data from home, on holiday, or via the commute to and from work (providing you have an internet connection). If you need access to your data while you are off-site, you can connect to your virtual office, quickly and easily.

## Access to automatic updates

Access to automatic updates for your IT requirements may be included in your service fee. Depending on your cloud computing service provider, your system will regularly be updated with the latest technology. This could include up-to-date versions of software, as well as upgrades to servers and computer processing power.

# Risks of cloud computing

Before considering cloud computing technology, it is important to understand the risks involved when moving your business into the cloud. You should carry out a risk assessment process before any control is handed over to a service provider..

## Cloud Computing Disadvantages

### 1.5.1. Network Connection Dependency

In order to reap the benefits of cloud computing, your business must always have an internet connection. Unfortunately, there is no way to get around this fact. You need a network in order to send files to the cloud and retrieve them.

You need a network to be able to use your virtual machines even if you opt for an IaaS, Infrastructure-as-a-Service. If you lose your network connection because of a storm or an outage, you may experience some downtime. However, a good Hosted Services provider will help you develop a business continuity plan, as well as the promise to deliver an SLA of more than 95% uptime.

### 1.5.2. Limited Features

Not all cloud providers are created equally. When you use cloud computing for storage and backup, you should ideally be working with a provider who offers the value of unlimited bandwidth. You may also experience limited storage space or accessibility. SaaS offerings may usually begin with a free package, but you will be charged for premium offerings and extra space. Can your business afford the costs as your business needs grow?

The answer to the concern of limited features is to partner with a Hosted Services providerwho can meet your cloud storage, virtualization, and backup needs both now and in the future when your business grows. Ideally, you will want to work with a provider who will offer you a Hosted Services package at the highest value for the features and space your business needs.

### 1.5.3. Loss of Control

You are, essentially, trusting another party to take care of your data. You are trusting that they will maintain their data centers and servers with the same care as you would, if not more. You have to trust that your provider’s data centers are compliant and secured both physically and online. Some find the lack of in-house control of the server unnerving.

If this is one of your concerns, work with a partner with local contacts. Speak one-on-one with a representative who can address your access concerns, and learn about the measures that the Hosted Services company takes to ensure the integrity and safety of their cloud servers.

### 1.5.4. Security

[Cloud hacking cases](http://www.infoworld.com/article/2687089/cloud-security/sum-of-all-cloud-security-fears.html) as recent as the past few months have shown that not all cloud providers are as secure as they claim to be. As a business, you can’t afford to have sensitive information about your company or your clients fall victim to hackers. One of cloud computing’s greatest disadvantages is that you don’t always know which providers you can trust.

This cloud computing disadvantage is more prevalent in SaaS providers than with Hosted providers. Because of the popularity of SaaS providers, they get targeted more frequently, and more easily, than a Hosted provider.

### 1.5.5. Technical Issues

If you experience any technical issues, you have no choice but to call your hosted provider’s technical support for help. You cannot fix your cloud computing problems in-house, and some providers do not offer around-the-clock technical support

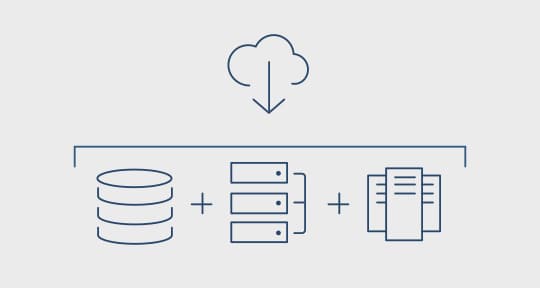
## **Service models of cloud computing**

* 1. Introduction:

In the traditional method of consuming services or resources, the owner of the infrastructure is responsible for managing every piece of hardware and software he or she uses. Normally, it takes some time for a user to access a new resource, but it can be configured exactly as needed.

Traditional infrastructure is often related to legacy core applications (tied to older technologies perhaps) that cannot be easily migrated to cloud paradigms. Elasticity, standardization and other clear cloud advantages are not sufficient reasons to migrate. In other cases, rigid security and country regulations sometimes force users to have data located nearby and/or under total management control.

## Defining IaaS, PaaS and SaaS



#### Infrastructure as a service (IaaS)

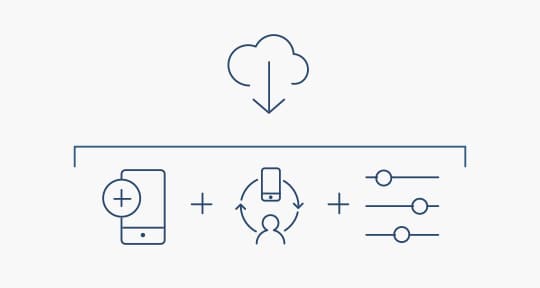
A vendor provides clients pay-as-you-go access to storage, networking, servers and other computing resources in the cloud.

* + 1. Key features
* Instead of purchasing hardware outright, [users pay for IaaS on demand](https://cloud.ibm.com/docs/vsi/vsi_about_transient.html#transient-virtual-servers).
* Infrastructure is scalable depending on processing and storage needs.
* Saves enterprises the costs of buying and maintaining their own hardware.
* Because data is on the cloud, there can be no single point of failure.
* Enables the virtualization of administrative tasks, freeing up time for other work.
  + 1. **Strengths**

• Vendor manages physical infrastructure, plus the operating system, runtime, middleware and possibly other development tooling   
• Developers can focus on writing code rather than managing infrastructure   
• Streamlines and speeds application development and testing   
• Easy creation of dev and test environments that are identical to production environments   
• Easy scaling   
• Cost varies with consumption of resources.

* + 1. **Weaknesses**• Costs may be unpredictable   
       • Customer has less control than with IaaS   
       • Requires more management and configuration than SaaS   
       • Requires skilled personnel   
       Some potential for vendor lock-in.
    2. **Best For**

• Developers creating new cloud-native applications   
• DevOps teams   
• Large organizations with custom in-house applications.



#### Platform as a service (PaaS)

A service provider offers access to a cloud-based environment in which users can build and deliver applications. The provider supplies underlying infrastructure.

2.3.1. Key features

PaaS provides a platform with tools to test, develop and host applications in the same environment. Enables organizations to focus on development without having to worry about underlying infrastructure. Providers manage security, operating systems, server software and backups. Facilitates collaborative work even if teams work remotely.

* + 1. **Strengths**

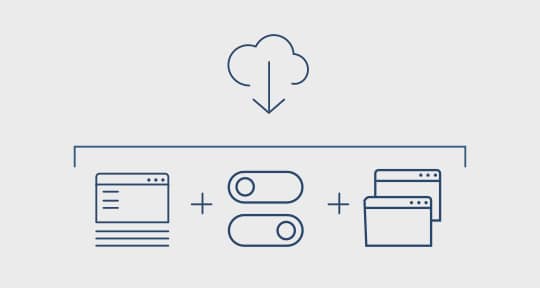
• Vendor manages physical infrastructure, plus the operating system, runtime, middleware and possibly other development tooling   
• Developers can focus on writing code rather than managing infrastructure   
• Streamlines and speeds application development and testing   
• Easy creation of dev and test environments that are identical to production environments   
• Easy scaling   
• Cost varies with consumption of resources.

* + 1. **Weaknesses**

• Costs may be unpredictable   
• Customer has less control than with IaaS   
• Requires more management and configuration than SaaS   
• Requires skilled personnel   
Some potential for vendor lock-in.

* + 1. **Best For**

• Developers creating new cloud-native applications   
• DevOps teams   
• Large organizations with custom in-house applications.



#### Software as a service (SaaS)

A service provider delivers software and applications through the internet. Users subscribe to the software and access it via the web or vendor APIs.

2.4.1. Key features

SaaS vendors provide users with software and applications via a subscription model.

Users do not have to manage, install or upgrade software; SaaS providers manage this.

Data is secure in the cloud; equipment failure does not result in loss of data.

Use of resources can be scaled depending on service needs.

Applications are accessible from almost any internet-connected device, from virtually anywhere in the world.

* + 1. **Strengths**

• Vendor manages all infrastructure and software   
• No need to download, install or upgrade software on PCs and other devices   
• Costs are predictable   
• Fast, easy setup   
Anyone can use it.

* + 1. **Weaknesses**
* Usually fewer customization options
* May be more difficult to access and protect data stored in SaaS applications
* Customer may be charged subscription fees for users who access the service rarely or never
* No control over software or infrastructure
* Integration with other software may be difficult
* Vendor may have access to customer data
* High potential for vendor lock-in.
  + 1. **Best For**

• Small organizations with minimal IT staff   
• Applications that require mobile access   
• Replacing a particular type of business software  
• Small organizations with minimal IT staff   
• Applications that require mobile access   
• Replacing a particular type of business software.

# Deployment models in Cloud computing

As cloud technology is providing users with so many benefits, these benefits must have to be categorized based on users requirement. Cloud deployment model represents the exact category of cloud environment based on proprietorship, size, and access and also describes the nature and purpose of the cloud. Most organizations implement cloud infrastructure to minimize capital expenditure & regulate operating costs.

To know which deployment model matches your requirement and desire it is necessary for users as well as learners to understand the four sub-categories of models for deployment.

These are:

* [Public Cloud Model](https://www.w3schools.in/deployment-models-in-cloud-computing/public-cloud-model/)
* [Private Cloud Model](https://www.w3schools.in/deployment-models-in-cloud-computing/private-cloud-model/)
* [Hybrid Cloud Model](https://www.w3schools.in/deployment-models-in-cloud-computing/hybrid-cloud-model/)
* [Community Cloud Model](https://www.w3schools.in/deployment-models-in-cloud-computing/community-cloud-model/)
  + 1. Public cloud

# **Public Cloud** is a type of cloud hosting that allows the accessibility of systems & its services to its clients/users easily. Some of the examples of those companies which provide public cloud facilities are IBM, Google, Amazon, Microsoft, etc. This cloud service is open for use. This type of cloud computing is a true specimen of cloud hosting where the service providers render services to various clients. From the technical point of view, there is the least difference between private clouds and public clouds along with the structural design. Only the security level depends based on the service providers and the type of cloud clients use. Public cloud is better suited for business purposes for managing the load. This type of cloud is economical due to the decrease in capital overheads.

The advantages of the Public cloud are:

* Flexible
* Reliable
* High Scalable
* Low cost
* Place independence

This type also holds some disadvantages such as:

* Less Secured
* Poor Customizable Services

# 2.5.2. Private cloud

Private Cloud also termed as 'Internal Cloud'; which allows the accessibility of systems and services within a specific boundary or organization. The cloud platform is implemented in a cloud-based secure environment that is guarded by advanced firewalls under the surveillance of the IT department that belongs to a particular organization. Private clouds permit only authorized users, providing the organizations greater control over data and its security. Business organizations that have dynamic, critical, secured, management demand based requirement should adopt Private Cloud.

The advantages of using a private cloud are:

* Highly private and secured: Private cloud resource sharing is highly secured.
* Control Oriented: Private clouds provide more control over its resources than public cloud as it can be accessed within the organization's boundary.

The Private cloud has the following disadvantages:

* Poor scalability: Private type of clouds is scaled within internal limited hosted resources.
* Costly: As it provides secured and more features, so it's more expensive than a public cloud.
* Pricing: is inflexible; i.e., purchasing new hardware for up-gradation is more costly.
* Restriction: It can be accessed locally within an organization and is difficult to expose globally.

# 2.5.3. Hybrid cloud service models

Hybrid Cloud is another cloud computing type, which is integrated, i.e., it can be a combination of two or more cloud servers, i.e., private, public or community combined as one architecture, but remain individual entities. Non-critical tasks such as development and test workloads can be done using public cloud whereas critical tasks that are sensitive such as organization data handling are done using a private cloud. Benefits of both deployment models, as well as a community deployment model, are possible in a hybrid cloud hosting. It can cross isolation and overcome boundaries by the provider; hence, it cannot be simply categorized into any of the three deployments - public, private or community cloud.

Advantages of Hybrid Cloud Computing are:

* Flexible
* Secure
* Cost Effective
* Rich Scalable

Disadvantages of Hybrid Cloud are:

Complex networking problem

2.5.4. Community cloud

Community Cloud is another type of cloud computing in which the setup of the cloud is shared manually among different organizations that belong to the same community or area. Example of such a community is where organizations/firms are there along with the financial institutions/banks. A multi-tenant setup developed using cloud among different organizations that belong to a particular community or group having similar computing concern.

For joint business organizations, ventures, research organizations and tenders community cloud is the appropriate solution. Selection of the right type of cloud hosting is essential in this case. Thus, community-based cloud users need to know and analyze the business demand first.

1. **SLA (Service level agreement)**

**3.1 Overview**: A cloud SLA (cloud service-level agreement) is an agreement between a [cloud service provider](https://searchitchannel.techtarget.com/definition/cloud-service-provider-cloud-provider) and a customer that ensures a minimum level of service is maintained. It guarantees levels of reliability, availability and responsiveness to systems and applications, while also specifying who will govern when there is a service interruption.

A cloud infrastructure can span geographies, networks and systems that are both physical and virtual. While the exact metrics of a cloud SLA can vary by service provider, the areas covered are uniform: volume and quality of work -- including precision and accuracy -- speed, responsiveness and efficiency. The document aims to establish a mutual understanding of the services, prioritized areas, responsibilities, guarantees and warranties provided by the service provider.

Metrics and responsibilities among the parties involved in cloud configurations are clearly outlined, such as the specific amount of response time for reporting or addressing system failures.

Financial penalties a provider must pay for failing to live up to the guaranteed terms are also included. These penalties are often in the form of credits for service time.

## A cloud SLA (cloud service-level agreement) is an agreement between a cloud service provider and a customer that ensures a minimum level of service is maintained.

Most SLAs are negotiated to meet the needs of the customer at the time of signing, but many businesses change dramatically in size over time. A solid cloud service-level agreement outlines intervals for reviewing a contract so that it meets the changing needs of an organization.

Some vendors even build in notification workflows that indicate when a cloud service-level agreement is close to being breached so new negotiations can be initiated based on the changes in scale. When entering any cloud SLA negotiation, it's important to protect the business by clarifying uptimes. A good SLA protects both the customer and supplier from missed expectations.

## 3.2. How do you Design SLA Structures?

There are several ways in Service Level Management in which you can structure your SLAs. To do that, here are a few important factors to consider:

* Will the SLA structure allows flexibility in the levels of service to be delivered for various customers?
* Will the SLA structure require much duplication of effort?
* Who are the stakeholders who will sign the SLAs?

There are three types of options for structuring SLA: Service-based, Customer-based, and Multi-level or Hierarchical SLAs. Many different factors will need to be considered when deciding which SLA structure is most appropriate for an organization to use.

### 3.3. Commonly known Multi-level SLA structure components include:

#### 3.3.1. Corporate level:

All of the general issues relevant to the organization are covered, and they are the same throughout the entire organization.  
For example, with security SLA at the organization level, every employee needs to create passwords of 8 characters and must change it every thirty days—or every employee needs to have an access card with an imprinted photograph.

#### 3.3.2. Customer level:

Those issues specific to a customer can be dealt with.  
Security requirements of one or more departments within the organization are higher. For example, the financial department needs more top security measures by virtue of its crucial role and handling of financial resources.

#### 3.3.3. Service Level:

All issues relevant to a specific service (in relation to the customer) can be covered.  
Applies to all customers that contract the same service — for example, contracting IT support services for everyone who uses a particular IP telephony provider.

Using a multi-level structure for a large organization reduces the duplication of effort while still providing customization for customers and services. Therefore, corporate-level SLAs apply to everybody and every department in that organization; customer level SLAs apply to the department, and so on.

Let’s use another example. Say we are a beverages provider, with tea, coffee, and juices in our service portfolio. If customer A wants the tea to be provided every morning and evening, coffee before and after lunch, and juices during lunch hours, that’s the customer-specific SLA we have signed with that particular customer, and that’s how we price the offering.

On the other hand, if we also have a stand where we offer juices throughout the day but at fixed prices and where customers B and C can source their needs, this is a service-based SLA.

So what does an SLA document typically consist of? Aspects of the service, including responsibilities, quality, and availability, are agreed on between the service provider and service user. Therefore, you should make sure that you can deliver the promised product at the promised time.

3.4. An SLA document typically consists of:

* An introduction to the SLA, what does this agreement propose
* A Service description, what service this SLA supports and details of the service
* Mutual responsibilities, who’s responsible for what part of the service
* Scope of SLA
* Applicable service hours, from what time till what time is the service available according to the agreement
* Service availability, how much is the service available during the service window and outside of the service window
* Reliability
* Customer support arrangements
* Contact points and escalation; a communication matrix
* Service performance
* Security
* Costs and charging method used

3.5. SLA  key items are:

3.5.1. Specify roles and responsibilities of all parties with respect to the SLA, and, at a minimum, include agency and cloud providers. These definitions would include, for example, the persons responsible for oversight of the contract, audit, performance management, maintenance, and security.  Define key terms, including activation date, performance, and identify any ambiguities in the definitions of cloud computing terms.

3.5.2. Define key terms, such as dates and performance. Define the performance measures of the cloud service, including who is responsible for measuring performance. These measures would include, among other things, the availability of the cloud service; the number of users that can access the cloud at any given time; and the response time for processing a customer transaction.

3.5.3. Define clear measures for performance by the contractor. Include which party is responsible for measuring performance. Examples of such measures would include:

•Level of service (e.g., service availability—duration the service is to be available to the agency).

•Capacity and capability of cloud service (e.g., maximum number of users that can access the cloud at one time and ability of provider to expand services to more users).

•Response time (e.g., how quickly cloud service provider systems process a transaction entered by the customer, response time for responding to service outages).

3.5.4. Specify how and when the agency has access to its own data and networks. This includes how data and networks are to be managed and maintained throughout the duration of the SLA and transitioned back to the agency in case of exit/termination of service.

3.5.5.Specify the following service management requirements:

•How the cloud service provider will monitor performance and report results to the agency.

•When and how the agency, via an audit, is to confirm performance of the cloud service provider.

3.5.6. Provide for disaster recovery and continuity of operations planning and testing, including how and when the cloud service provider is to report such failures and outages to the agency. In addition, how the provider will remediate such situations and mitigate the risks of such problems from recurring.

3.5.7. Describe any applicable exception criteria when the cloud provider’s performance measures do not apply (e.g., during scheduled maintenance or updates).

3.5.8. Specify metrics the cloud provider must meet in order to show it is meeting the agency’s security performance requirements for protecting data (e.g., clearly define who has access to the data and the protections in place to protect the agency’s data). Specify the security performance requirements that the service provider is to meet. This would include describing security performance metrics for protecting data, such as data reliability, data preservation, and data privacy. Cleary define the access rights of the cloud service provider and the agency as well as their respective responsibilities for securing the data, applications, and processes to meet all federal requirements. Describe what would constitute a breach of security and how and when the service provider is to notify the agency when the requirements are not being met.

3.5.9. Specifies performance requirements and attributes defining how and when the cloud service provider is to notify the agency when security requirements are not being met (e.g., when there is a data breach).

3.5.10. Specify a range of enforceable consequences, such as penalties, for non-compliance with SLA performance measures. Identify how such enforcement mechanisms would be imposed or exercised by the agency.Without penalties and remedies, the agency may lack leverage to enforce compliance with contract terms when situations arise.

## **Virtualization concepts**

4.1. Overview:

Virtualization in Cloud Computing is making a virtual platform of server operating system and storage devices. This will help the user by providing multiple machines at the same time it also allows sharing a single physical instance of resource or an application to multiple users. Cloud Virtualizations also manage the workload by transforming traditional computing and make it more scalable, economical and efficient.

Virtualizations in Cloud Computing rapidly integrating the fundamental way of computing. One of the important features of virtualization is that it allows sharing of applications to multiple customers and companies.

Cloud Computing can also be known as services and application delivered to help the virtualized environment. This environment can be either public or private. With the help of virtualization, the customer can maximize the resources and reduces the physical system which is in need.

## 4.2. Types of Virtualization in Cloud Computing

* Operating System Virtualization
* Hardware Virtualization
* Server Virtualization
* Storage Virtualization

4.2.1 . Operating System Virtualization

In operating system virtualization in Cloud Computing, the virtual machine software installs in the operating system of the host rather than directly on the hardware system. The most important use of operating system virtualization is for testing the application on different platforms or operating system. Here, the software is present in the hardware, which allows different applications to run.

### 4.2.2. Server Virtualization

In server virtualization in Cloud Computing, the software directly installs on the server system and use for a single physical server can divide into many servers on the demand basis and balance the load. It can be also stated that the server virtualization is masking of the server resources which consists of number and identity. With the help of software, the server administrator divides one physical server into multiple servers.

### 4.2.3. Hardware Virtualization

Hardware virtualization in Cloud Computing, used in server platform as it is flexible to use Virtual Machine rather than physical machines. In hardware virtualizations, virtual machine software installs in the hardware system and then it is known as hardware virtualization. It consists of a hypervisor which use to control and monitor the process, memory, and other hardware resources. After the completion of hardware virtualization process, the user can install the different operating system in it and with this platform different application can use.

### 4.2.4. Storage Virtualization

In storage virtualization in Cloud Computing, a grouping is done of physical storage which is from multiple network storage devices this is done so it looks like a single storage device. It can implement with the help of software applications and storage virtualization is done for the backup and recovery process. It is a sharing of the physical storage from multiple storage devices.

## 4.3. How Virtualization Works

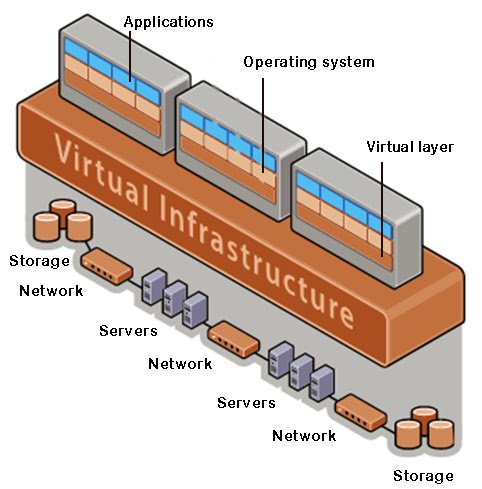
Virtualization in Cloud Computing is a process in which the user of cloud shares the data present in the cloud which can be application software etc. It provides a virtual environment in the cloud which can be software hardware or any other thing. In virtualization, the server and the software application which are required by the**dcloud providers** maintain by the third party and in this, the cloud provider please some amount to the third party. It is done because it will be costly if a new version of an application is released and it has to be introduced to the customers.

4.4. HYPERVISITOR

It can be also explained in a way that with the help of Hypervisor which is software the cloud customer can access server. A hypervisor is connectivity between the server and the virtual environment and distributes the resources between different virtual environments.

[](https://d2h0cx97tjks2p.cloudfront.net/blogs/wp-content/uploads/sites/2/2018/12/traditional.png)

Traditional

[](https://d2h0cx97tjks2p.cloudfront.net/blogs/wp-content/uploads/sites/2/2018/12/vmware_infrastructure.jpg)

Traditional Architecture Vs Virtual Architecture

## Benefits of Virtualization

#### 4.5.1. Security

During the process of virtualization security is one of the important concerns. The security can be provided with the help of firewalls, which will help to prevent unauthorized access and will keep the data confidential. Moreover, with the help of firewall and security, the data can protect from harmful viruses malware and other cyber threats. Encryption process also takes place with protocols which will protect the data from other threads. So, the customer can virtualize all the data store and can create a backup on a server in which the data can store.

#### 4.5.2. Flexible operations

With the help of a virtual network, the work of it professional is becoming more efficient and agile. The network switch implement today is very easy to use, flexible and saves time. With the help of virtualization in Cloud Computing, technical problems can solve in physical systems. It eliminates the problem of recovering the data from crashed or corrupted devices and hence saves time.

4.5.3. Economical

Virtualization in Cloud Computing, save the cost for a physical system such as hardware and servers. It stores all the data in the virtual server, which are quite economical. It reduces the wastage, decreases the electricity bills along with the maintenance cost. Due to this, the business can run multiple operating system and apps in a particular server.

#### 4.5.4. Eliminates the risk of system failure

While performing some task there are chances that the system might crash down at the wrong time. This failure can cause damage to the company but the virtualizations help you to perform the same task in multiple devices at the same time. The data can store in the cloud it can retrieve anytime and with the help of any device. Moreover, there is two working server side by side which makes the data accessible every time. Even if a server crashes with the help of the second server the customer can access the data.

4.5.5. Flexible transfer of data

The data can transfer to the virtual server and retrieve anytime. The customers or cloud provider don’t have to waste time finding out hard drives to find data. With the help of virtualization, it will very easy to locate the required data and transfer them to the allotted authorities. This transfer of data has no limit and can transfer to a long distance with the minimum charge possible. Additional storage can also provide and the cost will be as low as possible.

## **Cloud Security**

5.1. Introduction:

Cloud security, also known as cloud computing security, consists of a set of policies, controls, procedures and technologies that work together to protect cloud-based systems, data and infrastructure. These security measures are configured to protect data, support regulatory compliance and protect customers' privacy as well as setting authentication rules for individual users and devices. From authenticating access to filtering traffic, cloud security can be configured to the exact needs of the business. And because these rules can be configured and managed in one place, administration overheads are reduced and IT teams empowered to focus on other areas of the business.

The way cloud security is delivered will depend on the individual cloud provider or the cloud security solutions in place. However, implementation of cloud security processes should be a joint responsibility between the business owner and solution provider.

## 5.2. Benefits of Cloud Security

For businesses making the transition to the cloud, robust cloud security is imperative. Security threats are constantly evolving and becoming more sophisticated, and cloud computing is no less at risk than an on-premise environment. For this reason, it is essential to work with a cloud provider that offers best-in-class security that has been customized for your infrastructure.

5.2.1. Centralized security: Just as cloud computing centralizes applications and data, cloud security centralizes protection. Cloud-based business networks consist of numerous devices and endpoints. Managing these entities centrally enhances traffic analysis and filtering, streamlines the monitoring of network events and results in fewer software and policy updates. Disaster recovery plans can also be implemented and actioned easily when they are managed in one place.

5.2.2. Reduced costs: One of the benefits of utilizing cloud storage and security is that it eliminates the need to invest in dedicated hardware. Not only does this reduce capital expenditure, but it also reduces administrative overheads. Where once IT teams were firefighting security issues reactively, cloud security delivers proactive security features that offer protection 24/7 with little or no human intervention.

5.2.3. Reduced Administration: When you choose a reputable cloud services provider or cloud security platform, you can kiss goodbye to manual security configurations and almost constant security updates. These tasks can have a massive drain on resources, but when you move them to the cloud, all security administration happens in one place and is fully managed on your behalf.

5.2.4. Reliability: Cloud computing services offer the ultimate in dependability. With the right cloud security measures in place, users can safely access data and applications within the cloud no matter where they are or what device they are using.

More and more organizations are realizing the many business benefits of moving their systems to the cloud. Cloud computing allows organizations to operate at scale, reduce technology costs and use agile systems that give them the competitive edge. However, it is essential that organizations have complete confidence in their cloud computing security and that all data, systems and applications are protected from data theft, leakage, corruption and deletion.

All cloud models are susceptible to threats. IT departments are naturally cautious about moving mission-critical systems to the cloud and it is essential the right security provisions are in place, whether you are running a native cloud, hybrid or on-premise environment. Cloud security offers all the functionality of traditional IT security, and allows businesses to harness the many advantages of cloud computing while remaining secure and also ensure that data privacy and compliance requirements are met.

5.3. Types of cloud security

# 5.3.1. Data Security

Data security refers to protective digital privacy measures that are applied to prevent unauthorized access to computers, databases and websites. Data security also protects data from corruption. Data security is an essential aspect of IT for organizations of every size and type.

Data security is also known as information security (IS) or computer security.

Examples of data security technologies include backups, data masking and data erasure. A key data security technology measure is encryption, where digital data, software/hardware, and hard drives are encrypted and therefore rendered unreadable to unauthorized users and hackers.

One of the most commonly encountered methods of practicing data security is the use of authentication. With authentication, users must provide a password, code, biometric data, or some other form of data to verify identity before access to a system or data is granted.  
Data security is also very important for health care records, so health advocates and medical practitioners in the U.S. and other countries are working toward implementing electronic medical record (EMR) privacy by creating awareness about patient rights related to the release of data to laboratories, physicians, hospitals and other medical facilities.

# 5.3.2. Infrastructure Security

For the past several years, the trend in the enterprise has been to move away from an on-premises computing model to a cloud-based one. Cloud computing offers businesses a number of compelling benefits, such as improved scalability and flexibility, on-demand provisioning, and lower cost. Organizations no longer have to install expensive dedicated appliances behind corporate firewalls to deliver mission-critical applications, and the cloud makes it possible for knowledge workers to remain productive no matter where they are or what device they’re using. But cloud computing also comes with [security risks](http://www.im-techsolutions.com/security/avoid-these-3-cloud-security-issues). Here are two key concepts to keep in mind when your customers approach you with questions about creating a secure cloud experience.

### The secure cloud experience starts at the client connection

Under the traditional information security model, the physical and logical infrastructure that houses corporate data and applications is kept on-premises, behind the corporate perimeter and secured by corporate firewalls and other security appliances. But cloud computing is fast dissolving the perimeter. [A secure cloud experience](http://www.im-techsolutions.com/security/get-to-know-these-3-cloud-security-best-practices) doesn’t depend on physical security devices that protect corporate servers and databases: those are now the responsibility of the third-party cloud services provider. Instead, organizations must focus on making sure that their data reaches the cloud service safely. That means securing the client’s connection to the cloud service so that sensitive information cannot be intercepted in transit, as often happens when information travels over unsecured networks such as public Wi-Fi.

Customers who wish to secure cloud connections for their employees will typically need to implement a Virtual Private Network (VPN) and require its use in order to connect to corporate cloud services. In this use case, VPNs serve two purposes. First, they protect the data in transport between the client and the cloud service, and second, they provide an additional layer of authentication, since the employee must log in to use the VPN.

### Data security trumps infrastructure security

As mentioned above, cloud computing makes most physical security infrastructure the responsibility of the third-party cloud services provider. This does not mean that the enterprise should blindly trust every provider’s assurances of security and compliance, however. And it does not mean that the enterprise is off the hook legally in the event of a data breach. Data privacy and security regulations invariably make the owner of the data—the enterprise—liable and responsible for its protection, and that means that enterprises should look for ways to supplement their [cloud providers’ security](http://www.im-techsolutions.com/security/the-4-most-secure-cloud-storage-solutions)with additional security measure of their own.

In most cases, that will mean taking steps to secure the data itself, rather than the infrastructure on which it is housed. Technologies such as encryption can ensure that data remains unreadable to unauthorized parties, even if it is intercepted in transit or stolen from the cloud provider’s servers; tokenization provides mathematically generated substitute values for some types of data too sensitive to leave the corporate premises. A number of appliances and services now exist to provide data security to enterprises looking at adopting cloud computing for mission-critical operations.

Creating a secure cloud experience requires a rethinking of the security paradigm and can seem daunting to those more used to the traditional approach. But it is necessary for any business that wants to leverage the many benefits of the cloud, without endangering their data security or regulatory compliance.

# 5.4. Legal Issues For The Cloud

Cloud computing is bringing amazing advantages and benefits companies. But it also brings some challenges. There are several legal issues that must be taken into consideration when moving into the cloud. Let’s see which are the most challenging legal issues around cloud computing and how to overcome them.

## 5.4.1. Security procedures

The majority of companies which implemented cloud solutions and services do not have security procedures in place. Also, they lack measures to approve or evaluate cloud applications. When adopting the BYOD trend for example, organizations needed these security procedures more than ever. General data security trainings, multiple levels of security, rigorous procedures to use one’s own device and to transfer or copy data are some of the options available to protect data in organizations. The bottom line is that security procedures must be established according to every company’s objectives and work flow.

## 5.4.2. Third party access issues

Third-party involvement could be a risk. All third parties using a multi-tenant shared cloud are using the same administration interface, so make sure multi-factor authentication and enhanced security is present.  Also, look for [HIPAA](https://www.rickscloud.com/how-to-build-hipaa-compliant-cloud-applications/)compliant providers – a business associate agreement (BAA) with third-party vendor who access Protected Health Information (PHI) is necessary to ensure privacy and security requirements. A partnership with a HIPAA solutions provider that signs a BAA is an efficient method to make sure this this goes smoothly and everything is secure. And don’t forget to read carefully the terms and conditions before signing up for a cloud based services.

## 5.4.3. Intellectual Property Rights

Intellectual Property Rights differ from one country to another, so it is not very clear what intellectual property laws will apply in the cloud computing environment. Make sure you are aware of the regulations and rights from the country you store your intellectual work. The provider you choose should know how to protect intellectual property it stores and how to avoid potential infringement pitfalls.

## 5.4.4. Confidential data theft attacks

Data stored in the cloud might be compromised or breached. Therefore, most cloud computing providers also offer the customer different [levels](https://www.rickscloud.com/top-myths-about-cloud-computing/)of security protection, which allows for more enhanced security. Encryption might seem to have failed in protecting data from theft attacks, but other methods have been discovered and implemented, including monitoring data access in the cloud to detect abnormal data access patterns. The customer has to understand the cloud provider’s disclosure policy and how quickly the breach would be disclosed to them. Most of the U.S. states have security breach disclosure laws requiring the provider to inform the customers when their data has been compromised.

Many of these legal issues and the methods to inform about them or to solve them should be mentioned in the [Service Level Agreement](https://www.rickscloud.com/working-on-a-cloud-software-service-level-agreement/). It is essential to understand all the terms of the cloud’s provider and to consider the needs and objectives of the enterprise before signing an agreement

# Cloud Storage

## 6.1 Overview:

## Cloud storage is a service model in which data is maintained, managed, backed up remotely and made available to users over a network (typically the Internet). Users generally pay for their cloud data storage on a per-consumption, monthly rate.

6.2. Storage as a service (SaaS)

Storage as a service (SaaS) is a business model in which a company leases or rents its storage infrastructure to another company or individuals to store data. Small companies and individuals often find this to be a convenient methodology for managing backups, and providing cost savings in personnel, hardware and physical space.

A company providing SaaS may be called a storage service provider (SSP). Storage as a service can also be referred to as hosted storage.

As an alternative to storing magnetic tapes offsite in a vault, IT administrators are meeting their storage and backup needs by service level agreements (SLAs) with an SaaS provider, usually on a cost-per-gigabyte-stored and cost-per-data-transferred basis. The client transfers the data meant for storage to the service provider on a set schedule over the SaaS provider’s wide area network or over the Internet. The storage provider provides the client with the software required to access their stored data. Clients use the software to perform standard tasks associated with storage, including data transfers and data backups. Corrupted or lost company data can easily be restored.

Storage as a service is prevalent among small to mid-sized businesses, as no initial budget is required to set up hard drives, servers and IT staff. SaaS is also marketed as an excellent technique to mitigate risks in disaster recovery by providing long-term data storage and enhancing business stability.

# 6.3. Advantages of Storage as a service

6.3.1. Cost- factually speaking, backing up data isn’t always cheap, especially when take the cost of equipment into account. Additionally, there is the cost of the time it takes to manually complete routine backups. Storage as a service reduces much of the cost associated with traditional backup methods, providing ample storage space in the cloud for a low monthly fee.

6.3.2. Invisibility- Storage as a service is invisible, as no physical presence of it is seen in its deployment and so it doesn’t take up valuable office space.

6.3.3. Security- In this service type, data is encrypted both during transmission and while at rest, ensuring no unauthorized user access to files.

6.3.4. Automation- Storage as a service makes the tedious process of backing up easy to accomplish through automation. Users can simply select what and when they want to backup, and the service does all the rest.

6.3.5. Accessibility- By going for storage as a service, users can access data from smart phones, netbooks to desktops and so on.

6.3.6. Syncing- Syncing ensures your files are automatically updated across all of your devices. This way, the latest version of a file a user saved on their desktop is available on your smart phone.

6.3.7. Sharing- Online storage services allow the users to easily share data with just a few clicks

6.3.8. Collaboration- Cloud storage services are also ideal for collaboration purposes. They allow multiple people to edit and collaborate on a single file or document. Thus, with this feature users need not worry about tracking the latest version or who has made what changes.

6.3.9. Data Protection- By storing data on cloud storage services, data is well protected by all kind of catastrophes such as floods, earthquakes and human errors.

6.3.10. Disaster Recovery- as said earlier, data stored in cloud is not only protected from catastrophes by having the same copy at several places, but can also favour disaster recovery to ensure business continuity

6.4. Storage area network (SAN)

A storage area network (SAN) is a secure high-speed data transfer network that provides access to consolidated block-level storage. An SAN makes a network of storage devices accessible to multiple servers. SAN devices appear to servers as attached drives, eliminating traditional network bottlenecks.

SANs are sometimes also referred to (albeit redundantly) as SAN storage, SAN network, network SAN, etc.

## 6.4.1. Storage Area Networks And The Cloud

An increasing number of companies are utilizing cloud-based services to store their data. Using virtual servers, cloud computing expands a company’s storage capacities beyond its existing infrastructural capabilities. Due to its ability to connect large numbers of servers to storage devices, SAN technology is used heavily by cloud technology creators.

The difference between storage area networks and cloud storage is that SAN systems are hosted through a company’s own servers, while the cloud stores it virtually via internet servers. Additionally, cloud hosting services can be more cost-effective than purchasing hardware to accommodate more storage. Businesses that are unwilling or unable to invest in additional infrastructure are more frequently turning to the cloud.

Some companies also use a hybrid approach to storage, using the cloud for archives or lower-priority items and SANs for materials that need to be quickly and readily available. This allows them to customize their storage solution to meet their practical and budgetary needs.

## How Storage Area Networks Can Improve Your Performance

6.4.2. Storage area networks can help your company in a number of ways, including:

6.4.2.1. Improved disk utilization. When your storage is centralized through a SAN, it makes for more effective and efficient use of resources.

6.4.2.2. Disaster recovery (DR). In case of catastrophe, a SAN lets you recover data from multiple applications.

6.4.2.3. Application availability. SAN storage arrays use data protection algorithms to keep data consistent and accessible.

6.4.2.4. Increased backup speed. SAN storage devices create exact, hardware-based copies of data almost instantaneously. This makes them an easy way to back up large amounts of data in less time.

Although setting up a SAN can require a significant upfront investment, the payoff is a more secure, organized, and accessible network. When used on their own or in conjunction with cloud technology, storage area networks allow businesses to streamline their storage, freeing owners and employees to focus on the work that makes their companies successful.

7. Scheduling in cloud

7.1. Overview:

Cloud computing is known as a provider of dynamic services using very large scalable and virtualized resources over the Internet. Various definitions and interpretations of “clouds” and / or “cloud computing” exist. With particular respect to the various usage scopes the term is employed to, we will try to give a representative (as opposed to complete) set of definitions as recommendation towards future usage in the cloud computing related research space. We try to capture an abstract term in a way that best represents the technological aspects and issues related to it. In its broadest form, we can define a 'cloud' is an elastic execution environment of resources involving multiple stakeholders and providing a metered service at multiple granularities for a specified level of quality of service. To be more specific, a cloud is a platform or infrastructure that enables execution of code (services, applications etc.), in a managed and elastic fashion, whereas “managed” means that reliability according to pre defined quality parameters is automatically ensured and “elastic” implies that the resources are put to use according to actual current requirements observing overarching requirement definitions – implicitly, elasticity includes both up- and downward scalability of resources and data, but also load-balancing of data throughput.

Job scheduling is one of the major activities performed in all the computing environments. Cloud computing is one the upcoming latest technology which is developing drastically. To efficiently increase the working of cloud computing environments, job scheduling is one the tasks performed in order to gain maximum profit. The goal of scheduling algorithms in distributed systems is spreading the load on processors and maximizing their utilization while minimizing the total task execution time Job scheduling, one of the most famous optimization problems, plays a key role to improve flexible and reliable systems. The main purpose is to schedule jobs to the adaptable resources in accordance with adaptable time, which involves finding out a proper sequence in which jobs can be executed under transaction logic constraints. There are main two categories of scheduling algorithm. 1) Static scheduling algorithm and 2) Dynamic scheduling algorithm. Both have their own advantage and limitation. Dynamic scheduling algorithm has higher performance than static algorithm but has a lot of overhead compare to it.

7.2. Types of scheduling

Task Scheduling is considered under two main categories

7.2.1. Static Scheduling In Static Scheduling, for each and every task, communication cost and computation cost is considered beforehand. Static Scheduling further comprise Heuristic and Guided Random algorithms. Heuristics involves 3 subcategories namely clustering, list and duplication algorithms. In Clustering based algorithms such as Clustering for Heterogeneous Processors clusters of tasks are assigned to appropriate processors. On the other hand, duplication algorithms try to duplicate tasks to minimize makespan. Algorithms such as Contention aware duplication algorithms eliminates the communication cost by placing tasks on same processor. A large time complexity and more processor usage limit the use of duplication based algorithms in cloud environment. List Scheduling algorithms such as Critical Path on Processor give minimum makespan along with efficient time complexity. The list Scheduling Algorithms are most practical.

* + A novel approach which used concept of constrained critical paths to provide better schedule for task to be assigned to resources in cloud environment.
  + The clusters of tasks were created and these clusters mapped to fixed number of available processors
  + This algorithm eliminated communication cost after placing tasks upon same processor
  + Tasks were grouped as per processing power of resources. Cost varied based on complexity of tasks. The method reduced processing cost as tasks are scheduled based on their respective cost for different resources.
  + The algorithm computed earliest finish time for child tasks on every processor

7.2.2. Dynamic Scheduling In Dynamic one, decisions are taken beforehand at run time and no cost information is available earlier

* + Proposed Dynamic Level Scheduling that computed availability of each processor and then scheduled task to current busy processor.
  + Two novel slack sharing scheduling algorithms for set of tasks. The technique used slack time that was unused by task. Hence, there was reduction in total energy consumption
  + An algorithm that calculated slack time and generated frequency that task need to be executed. The algorithm was applied only for non-critical tasks and no further communication cost was taken into consideration

There has been various types of scheduling algorithm exist in distributed computing system. Most of them can be applied in the cloud environment with suitable verifications. The main advantage of job scheduling algorithm is to achieve a high performance computing and the best system throughput. Traditional job scheduling algorithms are not able to provide scheduling in the cloud environments. According to a simple classification, job scheduling algorithms in cloud computing can be categorized into two main groups; Batch Mode Heuristic scheduling Algorithms (BMHA) and online mode heuristic algorithms. In BMHA, Jobs are queued and collected into a set when they arrive in the system. The scheduling algorithm will start after a fixed period of time. The main examples of BMHA based algorithms are; First Come First Served scheduling algorithm (FCFS), Round Robin scheduling algorithm (RR), Min–Min algorithm and Max–Min algorithm.

7.3. Heuristic scheduling algorithm

By On-line mode heuristic scheduling algorithm, Jobs are scheduled when they arrive in the system. Since the cloud environment is a heterogeneous system and the speed of each processor varies quickly, the on-line mode heuristic scheduling algorithms are more appropriate for a cloud environment. Most Fit Task scheduling algorithm is suitable example of On-line mode heuristic scheduling algorithm.

7.3.1. First Come First Serve Algorithm:

Job in the queue which comes first is served. This algorithm is simple and fast.

7.3.2. Round Robin Algorithm:

In the round robin scheduling, processes are dispatched in a FIFO manner but are given a limited amount of CPU time called a time-slice or a quantum. If a process does not complete before its CPU-time expires, the CPU is preempted and given to the next process waiting in a queue. The pre-empted process is then placed at the back of the ready list.

7.3.3. Min–Min Algorithm:

This algorithm chooses small tasks to be executed first, which in turn delays large tasks for long time.

7.3.4. Max–Min Algorithm:

This algorithm chooses large tasks to be executed first, which in turn delays small tasks for long time.

7.3.5. Most Fit Task Scheduling Algorithm:

In this algorithm task which fit best in queue are executed first. This algorithm has high failure ratio.

7.3.6. Priority Scheduling Algorithm:

The basic idea is straightforward: each process is assigned a priority, and priority is allowed to run. Equal-Priority processes are scheduled in FCFS order. The Shortest-Job-First (SJF) algorithm is a special case of general priority scheduling algorithm. An SJF algorithm is simply a priority algorithm where the priority is the inverse of the (predicted) next CPU burst. That is, the longer the CPU burst, the lower the priority and vice versa. Priority can be defined either internally or externally. Internally defined priorities use some measurable quantities or qualities to compute priority of a process.

#### 7.4. Scheduling Process

Scheduling process in cloud can be generalized into three stages namely:

7.4.1. Resource discovering and filtering: Data center Broker discovers the resources present in the network system and collects status information related to them.

7.4.2. Resource selection: Target resource is selected based on certain parameters of task and resource. This is deciding stage.

7.4.3. Task submission: Task is submitted to resource selected.

7.5. Scheduling Algorithm

#### 7.5.1. Resource-Aware-Scheduling Algorithm (RASA)

It is composed of two traditional scheduling algorithms; Max-min and Min-min. RASA uses the advantages of Max-min and Min-min algorithms and covers their disadvantages. Though the deadline of each task, arriving rate of the tasks, cost of the task execution on each of the resource, cost of the communication are not considered. The experimental results show that RASA is outperforms the existing scheduling algorithms in large scale distributed systems.

#### 7.5.2. An Optimal Model for Priority based Service Scheduling Policy for Cloud Computing Environment

In this algorithm priority is assigned to each admitted queue. Admission of each queue is decided by calculating tolerable delay and service cost. Advantage of this algorithm is that this policy with the proposed cloud architecture has achieved very high (99%) service completion rate with guaranteed QoS. As this policy provides the highest precedence for highly paid user service-requests, overall servicing cost for the cloud also increases.

#### 7.5.3. Extended Max-Min Scheduling Using Petri Net and Load Balancing

Improved Max-min algorithm is based on the expected execution time instead of complete time as a selection basis. Petri nets are used to model the concurrent behaviour of distributed systems. Max-min demonstrates achieving schedules with comparable lower makespan rather than RASA and original Max-min.

#### 7.5.4. Reliable Scheduling Distributed in Cloud computing (RSDC)

In this algorithm, major job is divided to sub jobs. In order to balance the jobs the request and acknowledge time are calculated separately. The scheduling of each job is done by calculating the request and acknowledges time in the form of a shared job. So that efficiency of the system is increased.

#### 7.5.5. Improved Cost-Based Algorithm for Task Scheduling

The improvisation of traditional activity based costing is proposed by new task scheduling strategy for cloud environment where there may be no relation between the overhead application base and the way that different tasks cause overhead cost of resources in cloud. This scheduling algorithm divides all user tasks depending on priority of each task into three different lists. This scheduling algorithm measures both resource cost and computation performance, it also Improves the computation/communication ratio.

#### 7.5.6. An Optimistic Differentiated Job Scheduling System for Cloud Computing

In this approach one web application is created to do some activity like one of the file uploading and downloading then there is need of efficient job scheduling algorithm. The Qos requirements of the cloud computing user and the maximum profits of the cloud computing service provider are achieved with this algorithm.

#### 7.5.7. A Priority based Job Scheduling Algorithm in Cloud Computing

This scheduling algorithm consist of three level of scheduling: object level, attribute level and alternate level. In this algorithm priority can be set by job resource ratio. Then priority vector can be compared with each queue. This algorithm has higher throughput and less finish time.

#### 7.5.8. Performance and Cost Evaluation of Gang Scheduling in a Cloud Computing System with Job Migrations and Starvation Handling

Scheduling is considered as one of the most important tasks in cloud computing environment A number of scheduling algorithms and also tabulated the associated parameters. It has been noticed that disk space management is critical issue in virtual environment. Existing scheduling algorithms give high throughput and are cost effective but they do not consider reliability and availability. So there is a need for algorithms those improve availability and reliability in cloud computing environment.

7.6. Scheduling Parameters

A good scheduling algorithm always considers benefits of both the parties the cloud users and the service providers. The algorithms should try to reduce both the cost and power consumption as well as provide better performance. Scheduling algorithms must consider Load balancing and energy consumption as there two main parameters. Moreover, it should provide the user's fairness and security while providing services. A future enhancement in developing a suitable algorithm is by considering the combination of some important parameters together which can be deployed in a cloud environment for providing better cloud services to the users.The main scheduling parameters considered in the previously mentioned methods are listed below:

7.6.1. Makespan: It is the aggregate consummation time of all tasks in the job queue. A good scheduling algorithm dependably tries to diminish the makespan.

7.6.2. Deadline : It is characterized as the timeframe from presenting a task to the time by which it must be finished. A good scheduling algorithm dependably tries to keep the tasks executed with in the deadline constraint.

7.6.3. Execution Time: This is the exact time taken to execute the given tasks. A good scheduling algorithm ultimately aims to minimize execution time.

7.6.4. Completion Time: Completion time is the time taken to finish the whole execution of work. It incorporates the execution time and delay caused by the cloud system. A number of existing scheduling algorithms consider minimizing completion time of tasks.

7.6.5. Energy Consumption: Energy utilization in cloud data centers is a present issue that ought to be considered with more care nowadays. Numerous scheduling algorithms were developed for diminishing power consumption and enhancing execution and consequently making the cloud services green.

7.6.6. Performance: Performance shows the by and large productivity given by the scheduling algorithm all together to give good services to the clients according to their necessities. A good scheduling algorithm ought to consider the execution at the client end and in addition the cloud service provider end.

7.6.7. Quality of Service: SLAs is defined as a contract document defined between the cloud user and cloud service provider. Input constraints such as meeting execution cost, deadline, performance, cost, makespan, etc enhances quality of service.

7.6.8. Load balancing: It is the strategy for dis ssemination of the whole load in a cloud network crosswise over various nodes furthermore, connects so that at once no nodes and connections remain under loaded while a few nodes or connections are over-loaded. Most of the scheduling algorithms try to keep the load balanced in a cloud network in order to increase the efficiency of the system.

## **Cloud Computing Questions**

1. What is cloud computing?
2. What are the benefits of cloud computing?
3. What is a cloud?
4. Mention platforms which are used for large-scale cloud computing?
5. What are the Layers of PaaS Architecture?
6. What is Saas?
7. What is Iaas?
8. What is Caas?
9. What Are the Top Cloud The Basic Characteristics Of Cloud Computing?
10. What are the essential things that must be followed before going to cloud computing platform?
11. List out different layers which define cloud architecture?
12. Mention About Applications Now A Days?
13. What are the types of data used in cloud computing?
14. How can a company benefit from cloud computing?
15. For transporting data in the cloud, how you can you best secure data?
16. Explain the Security management in terms of Cloud Computing.
17. Mention what is the difference between elasticity and scalability in cloud computing?
18. What are hybrid clouds?
19. Explain four deployment models of cloud computing
20. Differentiate between public private and hybrid cloud
21. What is community cloud
22. What is SLA. Expand and explain.
23. What types of SLAs are there in cloud computing
24. Explain the process of SLA management.
25. What is the difference between cloud computing and mobile computing?
26. What is virtualization? Explain its types and benefits
27. Write short note on Hypervisors
28. What is cloud security? Discuss about infrastructureand data security.
29. What are the privacy and legal issues of cloud computin
30. Explain cloud storage with its benefits and challenges.
31. Expand the term SAN.
32. Write short note on SANs.
33. What do you mean by scheduling problem?
34. What are the different types of scheduling for dependent and independent tasks?
35. Write difference between static and dynamic scheduling.