SKDAV GOVT. POLYTECHNIC

ROURKELA

CLOUD COMPUTING

PREPARED BY
BIJAYALAXMI PADHIARY
SKDAV GOVT. POLYTECHNIC, ROURKELA

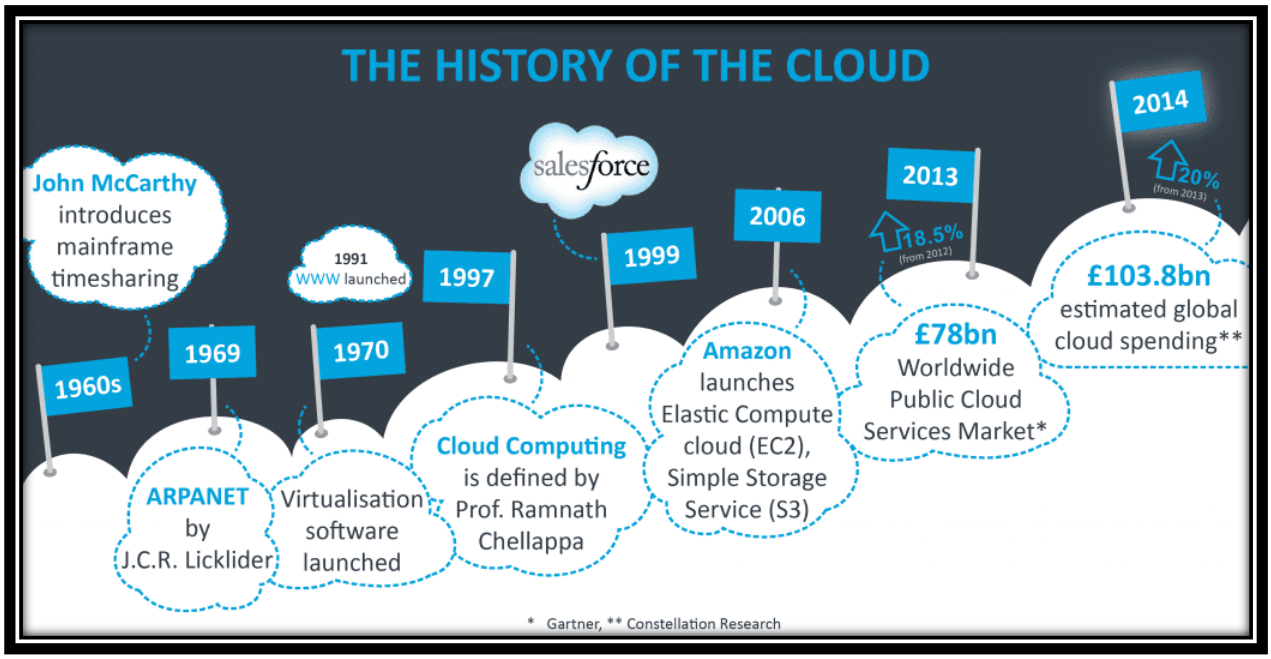
UNIT – 1
INTRODUCTION TO CLOUD COMPUTING

INTRODUCTION OF CLOUD COMPUTING

- Cloud computing is the on demand availability of computer system resources, especially data storage and computing power without direct active management by the user.
- The term is generally used to describe data centers available to many users over the Internet.
- The **National Institute for Standards and Technology (NIST)** offers the definition of cloud computing; Cloud Computing is a model for enabling convenient , on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

HISTORICAL DEVELOPMENT

- The history of cloud computing starts from the 1950's and the work done by AT & T in the area of telephone networking.
- At that time AT & T had already begun to develop an architecture and system where data would be located centrally.
- The IT services progressed over the decades with the adoption of technologies such as Internet Service Providers (ISP) Application service Providers.
- One of the main principles of cloud computing from SAAS (Software as a service) to provide storage on demand, is that the computing capacity varies immediately and transparently with the customer's need.



- **EARLY 1960S**

  Computer scientist **John McCarthy** has a time-sharing concept that allows the organization to use an expensive mainframe at the same time. This machine is described as a major contribution to Internet development, and as a leader in cloud computing.

- **IN 1969**

  J.C.R. Licklider, responsible for the creation of the Advanced Research Projects Agency (ARPANET), proposed the idea of an "Intergalactic Computer Network" or "Galactic Network" (a computer networking term similar to today's Internet). His vision was to connect everyone around the world and access programs and data from anywhere.

- **IN 1970**

  Usage of tools such as VMware for virtualization. More than one operating system can be run in a separate environment simultaneously. In a different operating system it was possible to operate a completely different computer (virtual machine).

- **IN 1997**

  Prof Ramnath Chellappa in Dallas in 1997 seems to be the first known definition of "cloud computing," "a paradigm in which computing boundaries are defined solely on economic rather than technical limits alone."

- **IN 1999**

  Salesforce.com was launched in 1999 as the pioneer of delivering client applications through its simple website. The services firm has been able to provide applications via the Internet for both the specialist and mainstream software companies.

- **IN 2003**

  This first public release of **Xen** ,is a software system that enables multiple virtual guest operating systems to be run simultaneous on a single machine, which also known as the Virtual Machine Monitor (VMM) as a hypervisor.

- **IN 2006**

  The Amazon cloud service was launched in 2006. First, its Elastic Compute Cloud (EC2) allowed people to use their own cloud applications and to access computers. Simple Storage Service (S3) was then released. This incorporated the user-as-you-go model and has become the standard procedure for both users and the industry as a whole.

- **IN 2013**

  A total of £ 78 billion in the world's market for public cloud services was increased by 18.5% in 2012, with IaaS as one of the fastest growing services on the market.

- **IN 2014**

  Global business spending for cloud-related technology and services is estimated to be £ 103.8 billion in 2014, up 20% from 2013 (Constellation Research).

EVOLUTION OF CLOUD TECHNOLOGIES

❖ DISTRIBUTED SYSTEMS

- A distributed system is a collection of independent computers that appears to its users as a single system and also it acts as a single computer.
- The main and primary motive of distributed systems is to share resources and to utilize them better.
- This is absolutely true in case of cloud computing because in cloud computing we are sharing the single resource by paying rent.
- The resource is single because the definition of cloud computing clearly states that in cloud computing the single central copy of a particular software is stored in a sever.

❖ MAINFRAMES AND THIN CLIENT COMPUTING

- It is highly reliable, powerful, centrally located form of computing service. A user of a mainframe system may access applications using a thin client**.**

- Each mainframe system is designed to run at a high level of utilization without failure, and to support hardware up gradation.
- The mainframes can host multiple virtual instances of operating system and this is a crucial requirement for supporting scalability within cloud computing

❖ **UTILITY COMPUTING**

- Computing services that can be metered and billed to customers in the same way that electricity or telephony system operate, are known as utility computing services.
- The concept of utility computing is also associated with the commercialization of problem solving in supercomputing systems.

❖ **GRID AND SUPER COMPUTING**

- The use of specialist supercomputers, or large number of computers configured to run in parallel in a 'grid' to solve the complex problems such as predicting the weather or decrypting data encrypted with strong encrypting algorithms is known as Grid and Super Computing.

❖ **SCALABILITY AND ON DEMAND PROCESSING POWER**

- The use of a supercomputer or grid computing service provides a level of scalability to those needing resources that may be too cost prohibitive to purchase in house.
- The processing power within these systems can be shared and provided to multiple users concurrently to execute complex software programs.

❖ **WEB 2.0**

- The global presence of the internet and the introduction of wireless networking and mobile devices featuring always on internet connectivity has raised expectations of users and demand for services over the internet.
- Web 2.0 is the term given to describe a second generation of the World Wide Web that is focused on the ability for people to collaborate and share information online.
- Web 2.0 basically refers to the transition from static HTML Web pages to a more dynamic Web that is more organized and is based on serving Web applications to users.
- Other improved functionality of Web 2.0 includes open communication with an emphasis on Web-based communities of users, and more open sharing of information.
- Over time Web 2.0 has been used more as a marketing term than a computer-science-based term. wikis, and Web services are all seen as components of Web 2.0.

VISION OF CLOUD COMPUTING

- Cloud computing provides the facility to provision virtual hardware, runtime environment and services to a person having money.
- These all things can be used as long as they are needed by the user, there is no requirement for the upfront commitment.
- The whole collection of computing system is transformed into a collection of utilities, which can be provisioned and composed together to deploy systems in hours rather than days, with no maintenance costs.
- The long term vision of a cloud computing is that IT services are traded as utilities in an open market without technological and legal barriers.
- In the near future we can imagine that it will be possible to find the solution that matches with our requirements by simply entering our request in a global digital market that trades with cloud computing services.
- The existence of such market will enable the automation of the discovery process and its integration into its existing software systems.
- Due to the existence of a global platform for trading cloud services will also help service providers to potentially increase their revenue.
- A cloud provider can also become a consumer of a competitor service in order to fulfill its promises to customers.

CHARACTERISTICS OF CLOUD COMPUTING

NIST stands for National institute of standards and technology.

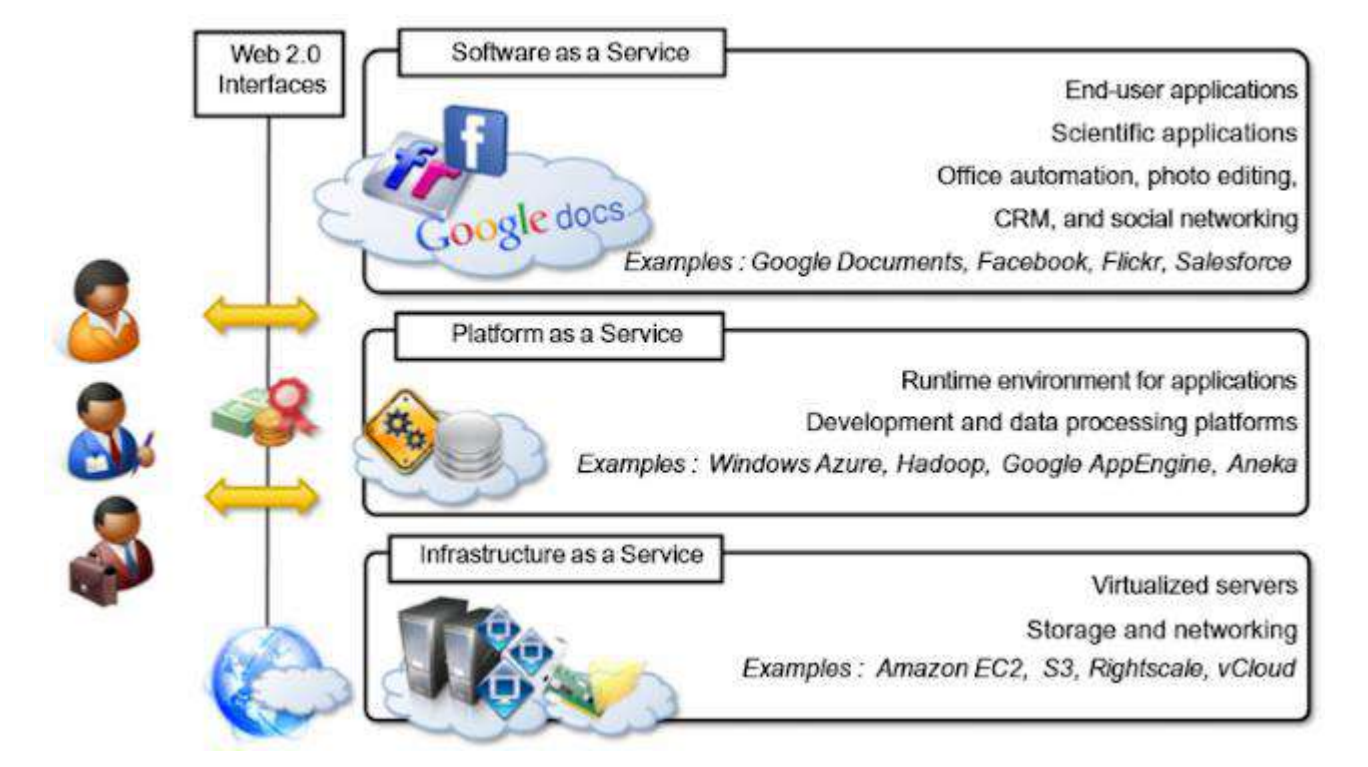
According to NIST there are five essential characteristics of cloud computing:

- On Demand Self Service
- Broad network access
- Resource pooling
- Rapid elasticity
- Measured service

1. **On Demand Self Service**
    - User gets on demand self-services. User can get computer services like email, applications etc. without interacting with each service provider.
    - Some of the cloud service providers are- Amazon Web Service, Microsoft, IBM, Salesforce.com.
2. **Broad network access**
    - Cloud services are available over the network and can be accessed through different clients such as mobile, laptops etc.
3. **Resource pooling**
    - Same resources can be used by more than one customer at a same time.
    - For example: storage, network bandwidth can be used by any number of customers and without knowing the exact location of that resource.
4. **Rapid elasticity**
    - On users demand cloud services can be available and released. Cloud service capabilities are unlimited and used in any quantity at any time.
5. **Measured service**
    - Resources used by the users can be monitored, controlled. This reports is available for both cloud providers and consumer.
    - On the basis of this measured reports cloud systems automatically controls and optimizes the resources based on the type of services. Services like- Storage, processing, bandwidth etc.

CLOUD COMPUTING REFERENCE MODEL:

The reference model for cloud computing is an abstract model that characterizes and standardizes a cloud computing environment by partitioning it into abstraction layers and cross-layer functions.



If we look in to the reference model as seen in above image we will find classification of Cloud Computing services:

1. Infrastructure-as-a-Service (IaaS),
2. Platform-as-a-Service (PaaS), and
3. Software-as-a-Service (SaaS).
4. Web 2.0

1. Infrastructure as a service (IaaS) is a cloud computing offering in which a vendor provides users access to computing resources such as servers, storage and networking.

2. Platform as a service (PaaS) is a cloud computing offering that provides users with a cloud environment in which they can develop, manage and deliver applications.

3. Software as a service (SaaS) is a cloud computing offering that provides users with access to a vendor's cloud-based software. Users do not install applications on their local devices. Instead, the applications reside on a remote cloud network accessed through the web or an API. Through the application, users can store and analyze data and collaborate on projects.

4. Web 2.0 is the term used to describe a variety of web sites and applications that allow anyone to create and share online information or material they have created. A key element of the technology is that it allows people to create, share, collaborate & communicate.

DEPLOYMENT OF CLOUD SERVICES

- **Public cloud**

  This type of cloud deployment model supports all users who want to make use of a computing resource, such as hardware (OS, CPU, memory, storage) or software (application server, database) on a subscription basis. Most common uses of public clouds are for application development and testing, non-mission-critical tasks such as file-sharing, and e-mail service.
- **Private cloud**

  A private cloud is typically infrastructure used by a single organization. Such infrastructure may be managed by the organization itself to support various user groups, or it could be managed by a service provider that takes care of it either on-site or off-site.

  Private clouds are more expensive than public clouds due to the capital expenditure involved in acquiring and maintaining them. However, private clouds are better able to address the security and privacy concerns of organizations today.

- **Hybrid cloud**

  In a hybrid cloud, an organization makes use of interconnected private and public cloud infrastructure. Many organizations make use of this model when they need to scale up their IT infrastructure rapidly, such as when leveraging public clouds to supplement the capacity available within a private cloud.

  For example, if an online retailer needs more computing resources to run its Web applications during the holiday season it may attain those resources via public clouds.
- **Community cloud**

  This deployment model supports multiple organizations sharing computing resources that are part of a community; examples include universities cooperating in certain areas of

research, or police departments within a county or state sharing computing resources. Access to a community cloud environment is typically restricted to the members of the community.

CLOUD COMPUTING ENVIRONMENT

- **Personal cloud computing environment**
  Single computer is used by single person. All the hardware devices are present at single location and packed as single unit.
- **Time sharing environment**
  Multiple computers are connected to a single large computers called server. Server share resources to all other system.
- **Client-server environment**
  The environment is similar to time sharing environment. Here server provides website.
- **Distributed computing environment**
  A single task is divided into parts and each part is executed by a different system. After execution the result is merged to get the final result

CLOUD SERVICE REQUIREMENTS

- **World class security**
  Provision world class security at every level.
- **Trust & transparency**
  Provide transparent, real-time, accurate service performance and availability information.
- **True multitenancy**
  Deliver maximum scalability and performance to customers with a true multitenant architecture.
- **Proven scale**
  Support millions of users with proven scalability.
- **High performance**
  Deliver consistent, high-speed performance globally.
- **Complete disaster recovery**
  Protect customer data by running the service on multiple, geographically dispersed data centers with extensive backup, data archive, and failover capabilities.
- **High availability**
  Equip world class facilities with proven high availability infrastructure and application software.

CLOUD AND DYNAMIC INFRASTRUCTURE

Cloud infrastructure

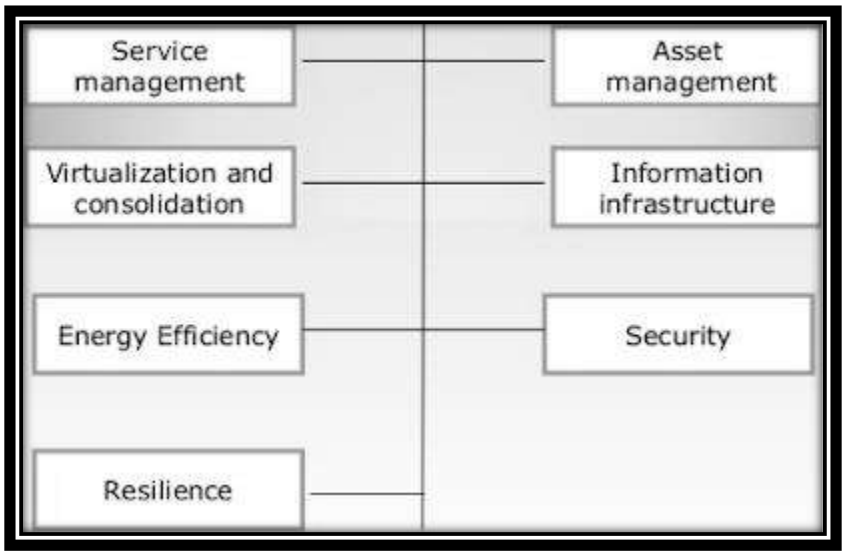
- Cloud infrastructure is a term used to describe the components needed for cloud computing, which includes hardware, abstracted resources, storage, and network resources.

Dynamic infrastructure

- Dynamic infrastructure refers to a collection of data center resources, such as compute, networking and storage that can automatically provision and adjust itself as workload demands change. IT administrators can also choose to manage these resources manually.

- Dynamic infrastructure relies primarily on software to identify, virtualize, classify and track data center resources. These resources are grouped into pools, regardless of their physical location within one or multiple data centers.

- By classifying data center resources, IT teams can establish and monitor multiple service tiers to ensure more demanding workloads receive more compute and storage resources.



Cloud and Dynamic infrastructure

1. Service management

This type of special facility or a functionality is provided to the cloud IT services by the cloud service providers. This facility includes visibility, automation and control to delivering the first class IT services.

2. Asset-Management

In this the assets or the property which is involved in providing the cloud services are getting managed.

3. Virtualization and consolidation

Consolidation is an effort to reduce the cost of a technology by improving its operating efficiency and effectiveness. It means migrating from large number of resources to fewer one, which is done by virtualization technology.

4. Information Infrastructure

It helps the business organizations to achieve the following: Information compliance, availability of resources retention and security objectives.

5. Energy-Efficiency

Here the IT infrastructure or organization sustainable. It means it is not likely to damage or effect any other thing.

6. Security

This cloud infrastructure is responsible for the risk management. Risk management Refers to the risks involved in the services which are being provided by the cloud-service providers.

7. Resilience

This infrastructure provides the feature of resilience means the services are resilient. It means the infrastructure is safe from all sides. The IT operations will not be easily get affected.

CLOUD ADOPTION

Cloud adoption means adopting a service or technology from another cloud service provide.

- Cloud means the environment of cloud where the cloud services are being operated.
- Adoption term states that accepting the services of new Technology.

- Adoption means following some kind of new trend or existing trend or a technology.
- This Cloud adoption is suitable for low priority business applications.
- It supports some interactive applications that combines two or more data sources.
- For example:-if a marketing company requires to grow his business in the whole country in a short span of time then it must need a quick promotion or short promotion across the country.
- Cloud Adoption is useful when the recovery management, backup recovery based implementations are required.
- By considering the above key points we conclude that it is only suitable for the applications that are modular and loosely coupled.
- It will work well with research and development projects.
- It means the testing of new services, design models and also the applications that can be get adjusted on small servers.
- Applications which requires different level of infrastructure throughout the day or throughout the month should be deployed through the cloud.
- The applications whose demand is unknown can also be deployed using clouds.

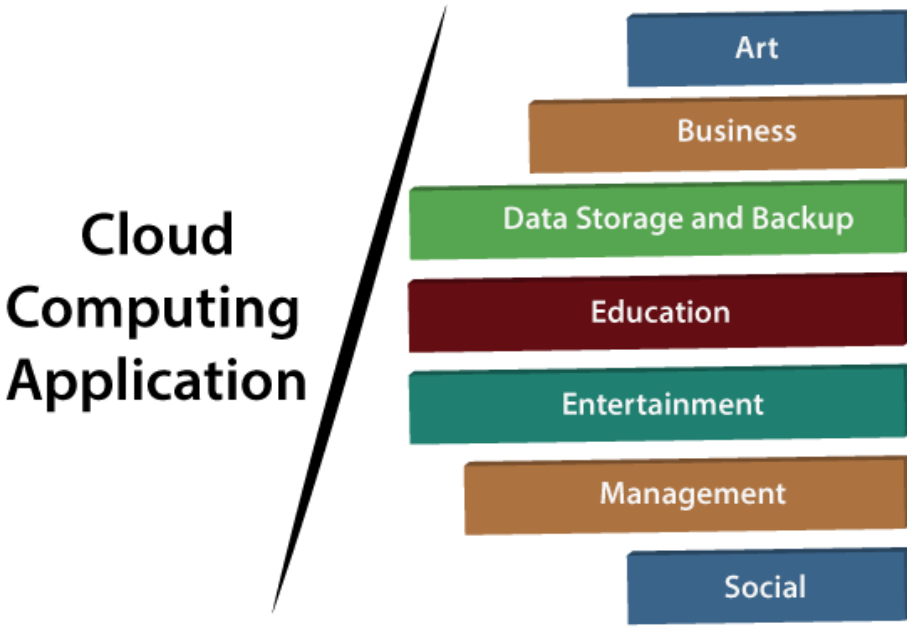
Benefits of cloud adoption:

- Data security
- Increased resource sharing
- Flexibility
- Business agility
- Facilitates innovation
- Great efficiency at lower price
- Better collaboration
- Better backup

CLOUD COMPUTING APPLICATIONS

Cloud service providers provide various applications in the field of art, business, data storage and backup services, education, entertainment, management, social networking, etc.

The most widely used cloud computing applications are given below -



1. Art Applications

Cloud computing offers various art applications for quickly and easily design **attractive cards, booklets,** and **images**. Some most commonly used cloud art applications are given below:

- **Moo**

  Moo is one of the best cloud art applications. It is used for designing and printing business cards, postcards, and mini cards.

- **Vistaprint**

  Vistaprint allows us to easily design various printed marketing products such as business cards, Postcards, Booklets, and wedding invitations cards.

- **Adobe Creative Cloud**

  Adobe creative cloud is made for designers, artists, filmmakers, and other creative professionals. It is a suite of apps which includes PhotoShop image editing programming, Illustrator, InDesign, TypeKit, Dreamweaver, XD, and Audition.

2. Business Applications

Business applications are based on cloud service providers. Today, every organization requires the cloud business application to grow their business. It also ensures that business applications are 24*7 available to users.

There are the following business applications of cloud computing -

- **MailChimp**

  MailChimp is an **email publishing platform** which provides various options to **design, send,** and **save** templates for emails.

- **Salesforce**

  Salesforce platform provides tools for sales, service, marketing, e-commerce, and more. It also provides a cloud development platform.

- **Chatter**

  Chatter helps us to **share important information** about the organization in real time.

- **Bitrix24**

  Bitrix24 is a **collaboration** platform which provides communication, management, and social collaboration tools.

- **Paypal**

  Paypal offers the simplest and easiest **online payment** mode using a secure internet account. Paypal accepts the payment through debit cards, credit cards, and also from Paypal account holders.

- **Slack**

  Slack stands for **Searchable Log of all Conversation and Knowledge**. It provides a **user-friendly** interface that helps us to create public and private channels for communication.

- **Quickbooks**

  Quickbooks works on the terminology "**Run Enterprise anytime, anywhere, on any device**." It provides online accounting solutions for the business. It allows more than 20 users to work simultaneously on the same system.

3. Data Storage and Backup Applications

Cloud computing allows us to store information (data, files, images, audios, and videos) on the cloud and access this information using an internet connection. As the cloud provider is responsible for providing security, so they offer various backup recovery application for retrieving the lost data.

A list of data storage and backup applications in the cloud are given below -

- **Box.com**

  Box provides an online environment for **secure content management, workflow,** and **collaboration**. It allows us to store different files such as Excel, Word, PDF, and images on the cloud. The main advantage of using box is that it provides drag & drop service for files and easily integrates with Office 365, G Suite, Salesforce, and more than 1400 tools.

- **Mozy**

  Mozy provides powerful **online backup solutions** for our personal and business data. It schedules automatically back up for each day at a specific time.

- **Joukuu**

  Joukuu provides the simplest way to **share** and **track cloud-based backup files**. Many users use joukuu to search files, folders, and collaborate on documents.

- **Google G Suite**

  Google G Suite is one of the best **cloud storage** and **backup** application. It includes Google Calendar, Docs, Forms, Google+, Hangouts, as well as cloud storage and tools

for managing cloud apps. The most popular app in the Google G Suite is Gmail. Gmail offers free email services to users.

4. Education Applications

Cloud computing in the education sector becomes very popular. It offers various **online distance learning platforms** and **student information portals** to the students. The advantage of using cloud in the field of education is that it offers strong virtual classroom environments, Ease of accessibility, secure data storage, scalability, greater reach for the students, and minimal hardware requirements for the applications.

There are the following education applications offered by the cloud -

- **Google Apps for Education**

  Google Apps for Education is the most widely used platform for free web-based email, calendar, documents, and collaborative study.

- **Chromebooks for Education**

  Chromebook for Education is one of the most important Google's projects. It is designed for the purpose that it enhances education innovation.

- **Tablets with Google Play for Education**

  It allows educators to quickly implement the latest technology solutions into the classroom and make it available to their students.

- **AWS in Education**

  AWS cloud provides an education-friendly environment to universities, community colleges, and schools.

5. Entertainment Applications

Entertainment industries use a **multi-cloud strategy** to interact with the target audience. Cloud computing offers various entertainment applications such as online games and video conferencing.

- **Online games**

  Today, cloud gaming becomes one of the most important entertainment media. It offers various online games that run remotely from the cloud. The best cloud gaming services are Shaow, GeForce Now, Vortex, Project xCloud, and PlayStation Now.

- **Video Conferencing Apps**

  Video conferencing apps provides a simple and instant connected experience. It allows us to communicate with our business partners, friends, and relatives using a cloud-based video conferencing. The benefits of using video conferencing are that it reduces cost, increases efficiency, and removes interoperability.

6. Management Applications

Cloud computing offers various cloud management tools which help admins to manage all types of cloud activities, such as resource deployment, data integration, and disaster recovery. These management tools also provide administrative control over the platforms, applications, and infrastructure.

Some important management applications are -

- **Toggl**

  Toggl helps users to track allocated time period for a particular project.

- **Evernote**

  Evernote allows you to sync and save your recorded notes, typed notes, and other notes in one convenient place. It is available for both free as well as a paid version. It uses platforms like Windows, macOS, Android, iOS, Browser, and Unix.

- **Outright**

  Outright is used by management users for the purpose of accounts. It helps to track income, expenses, profits, and losses in real-time environment.

- **GoToMeeting**

  GoToMeeting provides **Video Conferencing** and **online meeting apps**, which allows you to start a meeting with your business partners from anytime, anywhere using mobile phones or tablets. Using GoToMeeting app, you can perform the tasks related to the management such as join meetings in seconds, view presentations on the shared screen, get alerts for upcoming meetings, etc.

7. Social Applications

Social cloud applications allow a large number of users to connect with each other using social networking applications such as **Facebook, Twitter, LinkedIn,** etc.

There are the following cloud based social applications -

- **Facebook**

  Facebook is a **social networking website** which allows active users to share files, photos, videos, status, more to their friends, relatives, and business partners using the cloud storage system. On Facebook, we will always get notifications when our friends like and comment on the posts.

- **Twitter**

  Twitter is a **social networking** site. It is a **microblogging** system. It allows users to follow high profile celebrities, friends, relatives, and receive news. It sends and receives short posts called tweets.

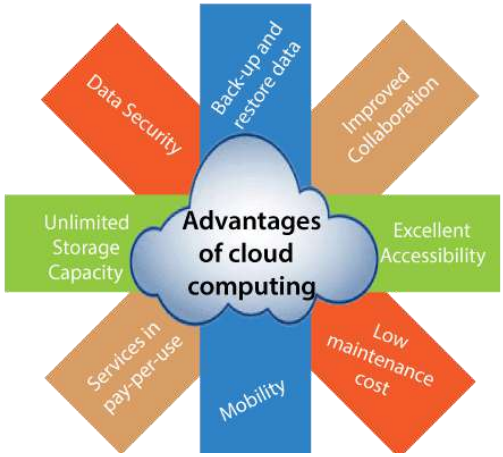
- **Yammer**

  Yammer is the **best team collaboration** tool that allows a team of employees to chat, share images, documents, and videos.

- **LinkedIn**

LinkedIn is a **social network** for students, fresher, and professionals.

ADVANTAGES OF CLOUD COMPUTING



1) Back-up and restore data

Once the data is stored in the cloud, it is easier to get back-up and restore that data using the cloud.

2) Improved collaboration

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

3) Excellent accessibility

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

4) Low maintenance cost

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

5) Mobility

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

6) Services in the pay-per-use model

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

7) Unlimited storage capacity

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

8) Data security

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

Disadvantages of Cloud Computing

1) Internet Connectivity

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

2) Vendor lock-in

Vendor lock-in is the biggest disadvantage of cloud computing. Organizations may face problems when transferring their services from one vendor to another. As different vendors provide different platforms, that can cause difficulty moving from one cloud to another.

3) Limited Control

Cloud infrastructure is completely owned, managed, and monitored by the service provider, so the cloud users have less control over the function and execution of services within a cloud infrastructure.

4) Security

Although cloud service providers implement the best security standards to store important information. But, before adopting cloud technology, you should be aware that you will be sending all your organization's sensitive information to a third party, i.e., a cloud computing

service provider. While sending the data on the cloud, there may be a chance that your organization's information is hacked by Hackers.

UNIT – 2
CLOUD COMPUTING ARCHITECTURE

CLOUD REFERENCE MODEL

- The cloud computing reference model is an abstract model that characterizes and standardizes the functions of a cloud computing environment by partitioning it into abstraction layers and cross-layer functions.
- This reference model groups the cloud computing functions and activities into five logical layers and three cross-layer functions.
- The five layers are physical layer, virtual layer, control layer, service orchestration layer, and service layer. Each of these layers specifies various types of entities that may exist in a cloud computing environment, such as compute systems, network devices, storage devices, virtualization software, security mechanisms, control software, orchestration software, management software, and so on. It also describes the relationships among these entities.
- The three cross-layer functions are business continuity, security, and service management.
- Business continuity and security functions specify various activities, tasks, and processes that are required to offer reliable and secure cloud services to the consumers.
- Service management function specifies various activities, tasks, and processes that enable the administrations of the cloud infrastructure and services to meet the provider's business requirements and consumer's expectations.

CLOUD COMPUTING LAYERS

Physical Layer

- Foundation layer of the cloud infrastructure.
- Specifies entities that operate at this layer: Compute systems, network devices and storage devices. Operating environment, protocol, tools and processes.
- Functions of physical layer: Executes requests generated by the virtualization and control layer.

Virtual Layer

- Deployed on the physical layer.
- Specifies entities that operate at this layer: Virtualization software, resource pools, virtual resources.
- Functions of virtual layer: Abstracts physical resources and makes them appear as virtual resources (enables multitenant environment). Executes the requests generated by control layer.

Control Layer

- Deployed either on virtual layer or on physical layer
- Specifies entities that operate at this layer : control software
- Functions of control layer: Enables resource configuration, resource pool configuration and resource provisioning. Executes requests generated by service layer. Exposes resources to and supports the service layer. Collaborates with the virtualization software and enables resource pooling and creating virtual resources, dynamic allocation and optimizing utilization of resources.

Service Orchestration Layer

- Specifies the entities that operate at this layer: Orchestration software.
- Functions of orchestration layer: Provides workflows for executing automated tasks. Interacts with various entities to invoke provisioning tasks.

Service Layer

- Consumers interact and consume cloud resources via those layer.
- Specifies the entities that operate at this layer: Service catalog and self-service portal.
- Functions of service layer: Store information about cloud services in service catalog and presents them to the consumers. Enables consumers to access and manage cloud services via a self-service portal.

CROSS-LAYER FUNCTION

Business continuity

- Specifies adoption of proactive and reactive measures to mitigate the impact of downtime.
- Enables ensuring the availability of services in line with SLA.
- Supports all the layers to provide uninterrupted services.

Security

- Specifies the adoption of: Administrative mechanisms (security and personnel policies, standard procedures to direct safe execution of operations) and technical mechanisms (firewall, intrusion detection and prevention systems, and antivirus).
- Deploys security mechanisms to meet GRC requirements.
- Supports all the layers to provide secure services.

Service Management

- Specifies adoption of activities related to service portfolio management and service operation management.

Service portfolio management:

- Define the service roadmap, service features, and service levels
- Assess and prioritize where investments across the service portfolio are most needed
- Establish budgeting and pricing
- Deal with consumers in supporting activities such as taking orders, processing bills, and collecting payments

Service operation management:

- Enables infrastructure configuration and resource provisioning
- Enable problem resolution
- Enables capacity and availability management
- Enables compliance conformance
- Enables monitoring cloud services and their constituent elements

CLOUD COMPUTING ARCHITECTURE

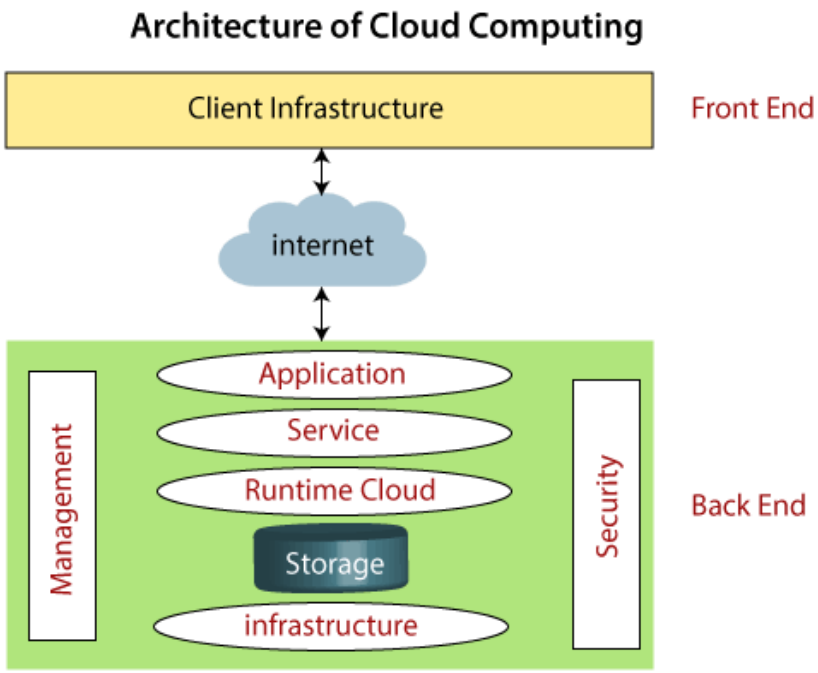
Cloud computing technology is used by both small and large organizations to **store the information** in cloud and **access** it from anywhere at any time using the internet connection.

Cloud computing architecture is a combination of **service-oriented architecture** and **event-driven architecture**.

Cloud computing architecture is divided into the following two parts -

- Front End
- Back End

The below diagram shows the architecture of cloud computing -



Front End

The front end is used by the client. It contains client-side interfaces and applications that are required to access the cloud computing platforms. The front end includes web servers (including Chrome, Firefox, internet explorer, etc.), thin & fat clients, tablets, and mobile devices.

Back End

The back end is used by the service provider. It manages all the resources that are required to provide cloud computing services. It includes a huge amount of data storage, security mechanism, virtual machines, deploying models, servers, traffic control mechanisms, etc.

Note: Both front end and back end are connected to others through a network, generally using the internet connection.

Components of Cloud Computing Architecture

There are the following components of cloud computing architecture -

1. **Client Infrastructure**

   Client Infrastructure is a Front end component. It provides GUI (Graphical User Interface) to interact with the cloud.

2. **Application**

   The application may be any software or platform that a client wants to access.

3. **Service**

   A Cloud Services manages that which type of service you access according to the client's requirement.

Cloud computing offers the following three type of services:

- **Software as a Service (SaaS) –**
  - It is also known as **cloud application services**. Mostly, SaaS applications run directly through the web browser means we do not require to download and install these applications.
  - SaaS is a service that delivers a software application—which the cloud service provider manages—to its users.
  - Typically, SaaS apps are web applications or mobile apps that users can access via a web browser. Software updates, bug fixes, and other general software

maintenance are taken care of for the user, and they connect to the cloud applications via a dashboard or API.

- SaaS also eliminates the need to have an app installed locally on each individual user's computer, allowing greater methods of group or team access to the software.
- **Example:** Google Apps, Salesforce Dropbox, Slack, Hubspot, Cisco WebEx.

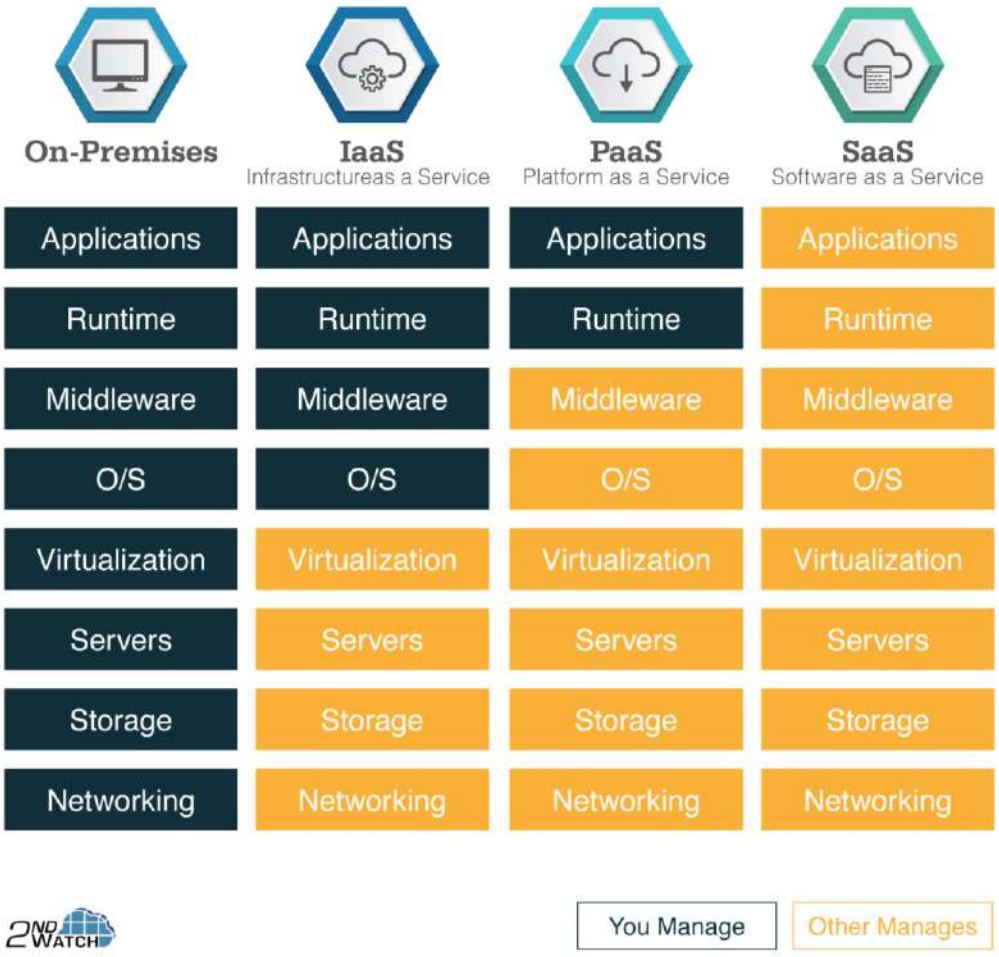
❖ **Platform as a Service (PaaS) –**

- It is also known as **cloud platform services**. It is quite similar to SaaS, but the difference is that PaaS provides a platform for software creation, but using SaaS, we can access software over the internet without the need of any platform.
- PaaS means the hardware and an application-software platform are provided and managed by an outside cloud service provider, but the user handles the apps running on top of the platform and the data the app relies on.
- Primarily for developers and programmers, PaaS gives users a shared cloud platform for application development and management (an important DevOps component) without having to build and maintain the infrastructure usually associated with the process.
- **Example:** Windows Azure, Force.com, Magento Commerce Cloud, OpenShift.

❖ **Infrastructure as a Service (IaaS) –**

- It is also known as **cloud infrastructure services**.
- It is responsible for managing applications data, middleware, and runtime environments.
- IaaS means a cloud service provider manages the infrastructure for you—the actual servers, network, virtualization, and data storage—through an internet connection.
- The user has access through an API or dashboard, and essentially rents the infrastructure.
- The user manages things like the operating system, apps, and middleware while the provider takes care of any hardware, networking, hard drives, data storage, and servers; and has the responsibility of taking care of outages, repairs, and hardware issues.
- This is the typical deployment model of cloud storage providers.

- **Example:** Amazon Web Services (AWS) EC2, Google Compute Engine (GCE), Cisco Metapod.



4. Runtime Cloud

Runtime Cloud provides the **execution and runtime environment** to the virtual machines.

5. Storage

Storage is one of the most important components of cloud computing. It provides a huge amount of storage capacity in the cloud to store and manage data.

6. Infrastructure

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

7. Management

Management is used to manage components such as application, service, runtime cloud, storage, infrastructure, and other security issues in the backend and establish coordination between them.

8. Security

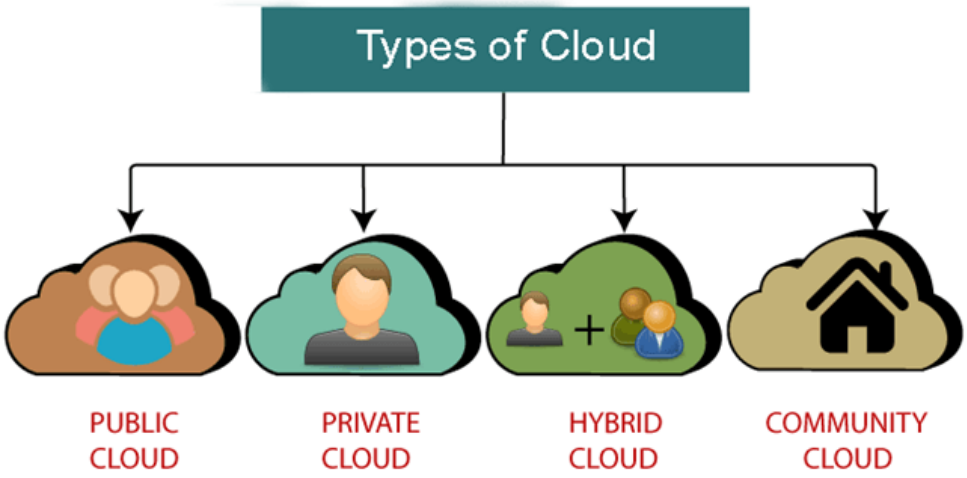
Security is an in-built back end component of cloud computing. It implements a security mechanism in the back end.

9. Internet

The Internet is medium through which front end and back end can interact and communicate with each other.

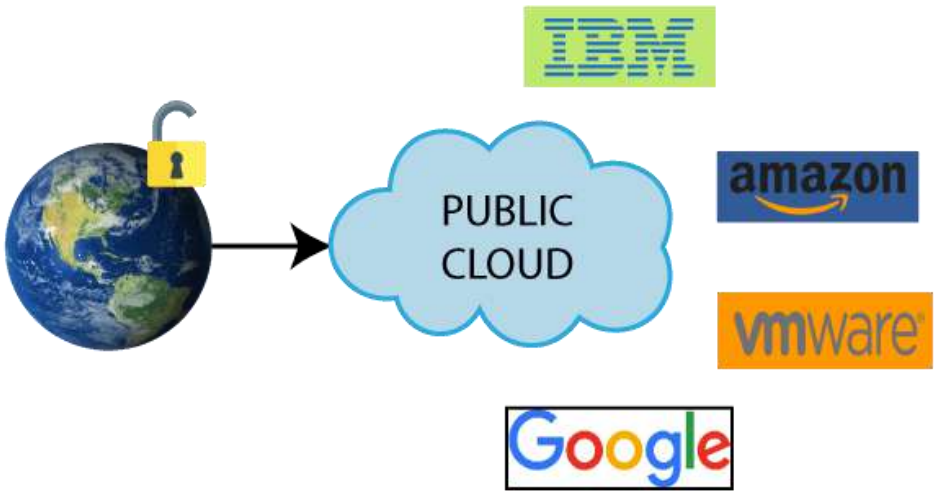
TYPES OF CLOUD

There are the following 4 types of cloud that you can deploy according to the organization's needs-



PUBLIC CLOUD

- Public Cloud provides a **shared platform** that is accessible to the **general public** through an Internet connection.
- Public cloud operated on the **pay-as-per-use model** and administrated by the **third party**, i.e., Cloud service provider.
- In the Public cloud, the same storage is being used by multiple users at the same time.
- Public cloud is **owned, managed,** and **operated** by businesses, universities, government organizations, or a combination of them.
- Amazon Elastic Compute Cloud (EC2), Microsoft Azure, IBM's Blue Cloud, Sun Cloud, and Google Cloud are examples of the public cloud.



ADVANTAGES OF PUBLIC CLOUD

1) Low Cost

Public cloud has a lower cost than private, or hybrid cloud, as it shares the same resources with a large number of consumers.

2) Location Independent

Public cloud is location independent because its services are offered through the internet.

3) Save Time

In Public cloud, the cloud service provider is responsible for the manage and maintain data centers in which data is stored, so the cloud user can save their time to establish connectivity, deploying new products, release product updates, configure, and assemble servers.

4) Quickly and easily set up

Organizations can easily buy public cloud on the internet and deployed and configured it remotely through the cloud service provider within a few hours.

5) Business Agility

Public cloud provides an ability to elastically re-size computer resources based on the organization's requirements.

6) Scalability and reliability

Public cloud offers scalable (easy to add and remove) and reliable (24*7 available) services to the users at an affordable cost.

DISADVANTAGES OF PUBLIC CLOUD

1) Low Security

Public Cloud is less secure because resources are shared publicly.

2) Performance

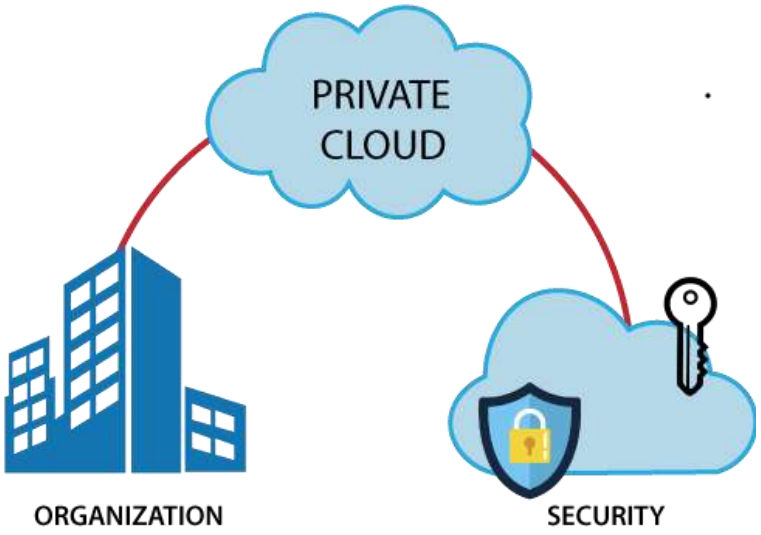
In the public cloud, performance depends upon the speed of internet connectivity.

3) Less customizable

Public cloud is less customizable than the private cloud

PRIVATE CLOUD

- Private cloud is also known as an **internal cloud** or **corporate cloud**.
- Private cloud provides computing services to a **private internal network (within the organization)** and **selected users** instead of the general public.
- Private cloud provides a **high level of security** and **privacy** to data through firewalls and internal hosting. It also ensures that operational and sensitive data are not accessible to third-party providers.
- HP Data Centers, Microsoft, Elastra-private cloud, and Ubuntu are the example of a private cloud.



ADVANTAGES OF PRIVATE CLOUD

1) More Control

Private clouds have more control over their resources and hardware than public clouds because it is only accessed by selected users.

2) Security & privacy

Security & privacy are one of the big advantages of cloud computing. Private cloud improved the security level as compared to the public cloud.

3) Improved performance

Private cloud offers better performance with improved speed and space capacity.

DISADVANTAGES OF PRIVATE CLOUD

1) High cost

The cost is higher than a public cloud because set up and maintain hardware resources are costly.

2) Restricted area of operations

Private cloud is accessible within the organization, so the area of operations is limited.

3) Limited scalability

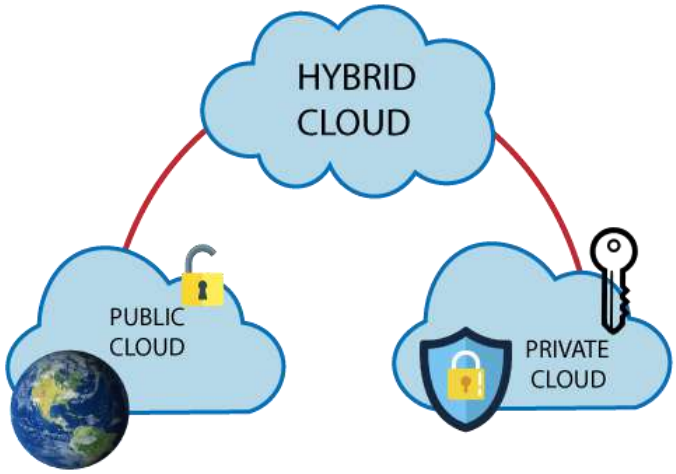
Private clouds are scaled only within the capacity of internal hosted resources.

4) Skilled people

Skilled people are required to manage and operate cloud services.

HYBRID CLOUD

- Hybrid cloud is a combination of **public and private** clouds. **Hybrid cloud = public cloud + private cloud**
- The main aim to combine these cloud (Public and Private) is to create a unified, automated, and well-managed computing environment.
- In the Hybrid cloud, **non-critical activities** are performed by the **public cloud** and **critical activities** are performed by the **private cloud**.
- Mainly, a hybrid cloud is used in finance, healthcare, and Universities.
- The best hybrid cloud provider companies are **Amazon, Microsoft, Google, Cisco,** and **NetApp**.



ADVANTAGES OF HYBRID CLOUD

1) Flexible and secure

It provides flexible resources because of the public cloud and secure resources because of the private cloud.

2) Cost effective

Hybrid cloud costs less than the private cloud. It helps organizations to save costs for both infrastructure and application support.

3) Cost effective

It offers the features of both the public as well as the private cloud. A hybrid cloud is capable of adapting to the demands that each company needs for space, memory, and system.

4) Security

Hybrid cloud is secure because critical activities are performed by the private cloud.

5) Risk Management

Hybrid cloud provides an excellent way for companies to manage the risk.

DISADVANTAGES OF HYBRID CLOUD

1) Networking issues

In the Hybrid Cloud, networking becomes complex because of the private and the public cloud.

2) Infrastructure Compatibility

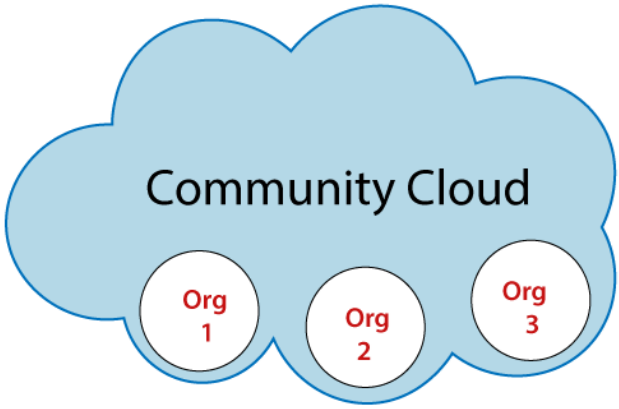
Infrastructure compatibility is the major issue in a hybrid cloud. With dual-levels of infrastructure, a private cloud controls the company, and a public cloud does not, so there is a possibility that they are running in separate stacks.

3) Reliability

The reliability of the services depends on cloud service providers.

COMMUNITY CLOUD

Community cloud is a cloud infrastructure that allows systems and services to be accessible by a group of several organizations to share the information. It is owned, managed, and operated by one or more organizations in the community, a third party, or a combination of them.



Example: Our government organization within India may share computing infrastructure in the cloud to manage data.

ADVANTAGES OF COMMUNITY CLOUD

Cost effective

Community cloud is cost effective because the whole cloud is shared between several organizations or a community.

Flexible and Scalable

The community cloud is flexible and scalable because it is compatible with every user. It allows the users to modify the documents as per their needs and requirement.

Security

Community cloud is more secure than the public cloud but less secure than the private cloud.

Sharing infrastructure

Community cloud allows us to share cloud resources, infrastructure, and other capabilities among various organizations.

DISADVANTAGES OF COMMUNITY CLOUD

- Community cloud is not a good choice for every organization.
- Slow adoption to data
- The fixed amount of data storage and bandwidth is shared among all community members.
- Community Cloud is costly than the public cloud.
- Sharing responsibilities among organizations is difficult.

COMAPARISON BETWEEN TYPES OF CLOUDS:

FEATURES / CLOUD	PUBLIC	PRIVATE	HYBRID	COMMUNITY
Host	Service provider	Enterprise	Enterprise	Community (Third party)
Suitable for	Large Enterprise	Large Enterprise	Small and mid-size	Financial, heath and legal companies
Access	Internet	Intranet, VPN	Intranet, VPN	Intranet, VPN
Security	Low	Most secured	Moderate	Secured
Cost	Cheapest	High Cost	Cost effective	Cost effective
Owner	Service provider	Enterprise	Enterprise	Community
Reliability	Moderate	Very High	Medium to High	Very High
Users	Organizations, public like individuals	Business organizations	Business organizations	Community members
Scalability	Very High	Limited	Very High	Limited

CLOUD INTEROPERABILITY AND STANDARDS

- ❖ Cloud interoperability refers to the ability of customers to use the same management tools, server images and other software with a variety of cloud computing providers and platforms.

- ❖ Standards are important in cloud computing for a variety of reasons. Standards for interoperability and data and application portability can ensure an open competitive market in cloud computing because customers are not locked-in to cloud providers and can easily transfer data or applications between cloud providers.

INTEROPERABILITY:

- It is defined as the capacity of at least two systems or applications to trade with data and utilize it. On the other hand, cloud interoperability is the capacity or extent at which one cloud service is connected with the other by trading data as per strategy to get results.
- The two crucial components in Cloud interoperability are usability and connectivity, which are further divided into multiple layers.
    1. Behavior
    2. Policy
    3. Semantic
    4. Syntactic
    5. Transport
    6. Portability
- It is the process of transferring the data or an application from one framework to others, making it stay executable or usable. Portability can be separated into two types: Cloud data portability and Cloud application portability.
    - **Cloud data portability –**
      It is the capability of moving information from one cloud service to another and so on without expecting to re-enter the data.
    - **Cloud application portability –**
      It is the capability of moving an application from one cloud service to another or between a client's environment and a cloud service.

Why cloud interoperability and standards?

- Vendor lock-in can prevent a customer from switching to another competitor's solution. If switching is possible, it happens at considerable conversion cost and requires significant amounts of time.
- Switching happen because may be customer wants to find a more suitable solution for customer needs. Or vendor may not be able to provide the service required.
- So, the presence of standards that are actually implemented and adopted in the cloud computing community gives power for interoperability and then lessen the risks resulting from vendor lock-in.

Categories of Cloud Computing Interoperability and portability:

The Cloud portability and interoperability can be divided into –

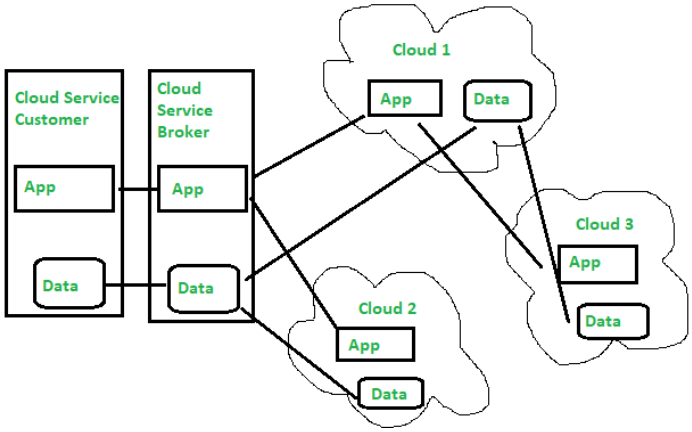
- Data Portability
- Platform Interoperability
- Application Portability
- Management Interoperability
- Platform Portability
- Application Interoperability
- Publication and Acquisition Interoperability

1. **Data Portability –**
   Data portability, which is also termed as cloud portability, refers to the transfer of data from one source to another source or from one service to another service, i.e. from one application to another application or it may be from one cloud service to another cloud service in the aim of providing a better service to the customer without affecting it's usability. Moreover, it makes the cloud migration process easier.
2. **Application Portability –**
   It enables re-use of various application components in different cloud PaaS services. If the components are independent in their cloud service provider, then application portability can be a difficult task for the enterprise. But if components are not platform specific, porting to another platform is easy and effortless.
3. **Platform Portability –**
   There are two types of platform portability- platform source portability and machine image portability. In the case of platform source portability, e.g. UNIX OS, which is mostly written in C language, can be implemented by re-compiling on various different hardware and re-

writing sections that are hardware-dependent which are not coded in C. Machine image portability binds application with platform by porting the resulting bundle which requires standard program representation.

4. **Application Interoperability –**
   It is the interoperability between deployed components of an application deployed in a system. Generally, applications that are built on the basis of design principles show better interoperability than those which are not.
5. **Platform Interoperability –**
   It is the interoperability between deployed components of platforms deployed in a system. It is an important aspect, as application interoperability can't be achieved without platform interoperability.
6. **Management Interoperability –**
   Here, the Cloud services like SaaS, PaaS or IaaS and applications related to self-service are assessed. It would be pre-dominant as Cloud services are allowing enterprises to work-in-house and eradicate dependency from third parties.
7. **Publication and Acquisition Interoperability –**
   Generally, it is the interoperability between various platforms like PaaS services and the online marketplace.

The below figure represents an overview of Cloud interoperability and portability:



CLOUD INTEROPERABILITY AND PORTABILITY

Major Scenarios where interoperability and portability is required:

Cloud Standards Custom Council (CSCC) has identified some of the basic scenarios where portability and interoperability is required.

- **Switching between cloud service providers –**

The customer wants to transfer data or applications from Cloud 1 to Cloud 2.

- **Using multiple cloud service providers-**
  The client may subscribe to the same or different services e.g. Cloud 1 and 2.
- **Directly linked cloud services-**
  The customer can use the service by linking to Cloud 1 and Cloud 3.
- **Hybrid Cloud configuration-**
  Here the customer connects with a legacy system not in a public, but, private cloud, i.e. Cloud 1, which is then connected to public cloud services i.e. Cloud 3.
- **Cloud Migration-**
  Clients migrate to one or more in-house applications to Cloud 1.

Challenges faced in Cloud Portability and Interoperability:

- If we move the application to another cloud, then, naturally, data is also moved. And for some businesses, data is very crucial. But unfortunately, most cloud service providers charge a small amount of money to get the data into the cloud.
- The degree of mobility of data can also act as an obstacle. Moving data from one cloud to another cloud, the capability of moving workload from one host to another should also be accessed.
- Interoperability should not be left out, otherwise data migration can be highly affected. So the functioning of all components and applications should be ensured.
- As data is highly important in business, the safety of customer's data should be ensured.

Cloud interoperability eradicates the complex parts by providing custom interfaces. Moving from one framework can be conceivable with a container service which improves scalability. Having a few hurdles, adaptability to change in service providers, better assistance in cloud clients will enhance the improvement of cloud interoperability.

CLOUD COMPUTING INTEROPERABILITY USE CASES

Cloud-computing interoperability use cases that are supported by standards:

1. **Workload migratio**n.

    - A workload that executes in one cloud provider can be uploaded to another cloud provider.

- Some standardization efforts that support this use case are Amazon Machine Image (AMI), Open Virtualization Framework (OVF), and Virtual Hard Disk (VHD).

2. **Data migration**.

    - Data that resides in one cloud provider can be moved to another cloud provider.
    - A standardization effort that supports this use case is Cloud Data Management Interface (CDMI).
    - In addition, even though SOAP (**Simple Object Access Protocol)** and REST (**Representational State Transfer)** are not data-specific standards, multiple cloud-storage providers support data- and storage-management interfaces that use SOAP and REST.

3. **User authentication**.

    - A user who has established an identity with a cloud provider can use the same identity with another cloud provider.
    - Standardization efforts that support this use case are Amazon Web Services Identity Access Management (AWS IAM), OAuth, Open ID, and WS-Security.

4. **Workload management**.

    - Custom tools developed for cloud workload management can be used to manage multiple cloud resources from different vendors.
    - Even though most environments provide a form of management console or command-line tools, they also provide APIs based on REST or SOAP.

ROLE OF STANDARDS IN CLOUD COMPUTING ENVIRONMENT

- As enterprises scale their usage, standards become a more prominent issue. They can reduce friction and risk for companies with large or complex operations. Similarly, if a company is using a cloud provider, it can ensure that its security capabilities are compatible to work together.
- Mature industries, where standards compliance may be a deciding factor, will be seeking familiar assurance, while organizations starting digitally led initiatives with a long-term horizon will find that standards adherence is an important factor in decision-making.

- Understanding the key issues behind cloud standards can provide assurance, helping professionals to evaluate options and plan with confidence.

UNIT – 3
SCALABILITY & FAULT TOLERANCE

CLOUD SCALABILITY

- Cloud Scalability is the ability to scale on-demand the facilities and services as and when they are required by the user.
- Cloud scalability in cloud computing refers to increasing or decreasing IT resources as needed to meet changing demand. Scalability is one of the hallmarks of the cloud and the primary driver of its explosive popularity with businesses.
- Data storage capacity, processing power, and networking can all be increased by using existing cloud computing infrastructure. Scaling can be done quickly and easily, usually without any disruption or downtime.
- Third-party cloud providers already have the entire infrastructure in place; in the past, when scaling up with on-premises physical infrastructure, the process could take weeks or months and require exorbitant expenses.
- This is one of the most popular and beneficial features of cloud computing, as businesses can grow up or down to meet the demands depending on the season, projects, development, etc.

Example:

Consider you are the owner of a company whose database size was small in earlier days but as time passed your business does grow and the size of your database also increases, so in this case you just need to request your cloud service vendor to scale up your database capacity to handle a heavy workload.

- Systems have four general areas that scalability can apply to:

    1. Disk I/O
    2. Memory
    3. Network I/O
    4. CPU

CLOUD ELASTICITY:

- The Elasticity refers to the ability of a cloud to automatically expand or compress the infrastructural resources on a sudden-up and down in the requirement so that the workload can be managed efficiently.
- This elasticity helps to minimize infrastructural cost. This is not applicable for all kind of environment, it is helpful to address only those scenarios where the resources requirements fluctuate up and down suddenly for a specific time interval. It is not quite practical to use where persistent resource infrastructure is required to handle the heavy workload.
- It is most commonly used in pay-per-use, public cloud services. Where IT managers are willing to pay only for the duration to which they consumed the resources.

Example:

Consider an online shopping site whose transaction workload increases during festive season like Christmas. So for this specific period of time, the resources need a spike up. In order to handle this kind of situation, we can go for Cloud-Elasticity service rather than Cloud Scalability. As soon as the season goes out, the deployed resources can then be requested for withdrawal.

Difference between Cloud Elasticity and Scalability:

	Cloud Elasticity	**Cloud Scalability**
1	Elasticity is used just to meet the sudden up and down in the workload for a small period of time.	Scalability is used to meet the static increase in the workload.
2	Elasticity is used to meet dynamic changes, where the resources need can increase or decrease.	Scalability is always used to address the increase in workload in an organization.
3	Elasticity is commonly used by small companies whose workload and demand increases only for a specific period of time.	Scalability is used by giant companies whose customer circle persistently grows in order to do the operations efficiently.
4	It is a short term planning and adopted just to deal with an unexpected increase in demand or seasonal demands.	Scalability is a long term planning and adopted just to deal with an expected increase in demand.

FEATURES OF CLOUD SCALABILITY

- **Sizeable difference.** Scaling involves a significant change. It doesn't mean a minor alteration.
- **Grow or shrink.** When a business scales, it changes in size. That can mean increasing or decreasing.
- **Speed.** Scaling via the cloud is quick. It's certainly faster than buying and setting up physical hardware yourself.
- **Ease.** It's relatively easy to scale using a cloud solution. Without virtualization, scaling would be expensive, via physical machines.
- **Not disruptive.** To scale doesn't mean to replace. You're adding or removing resources, meaning there should be minimal downtime.

  For example, let's say you own an online store, and the summer sales are coming. You can set up an auto-scale rule with Microsoft Azure to increase virtual machines when traffic hits a certain amount. That way, you can scale up to handle the additional load. By contrast, switching from Google Apps to Microsoft Office 365 is replacing, not scaling.

TYPES OF SCALING

- Vertical Scalability (Scaled-up)
- horizontal scalability
- diagonal scalability

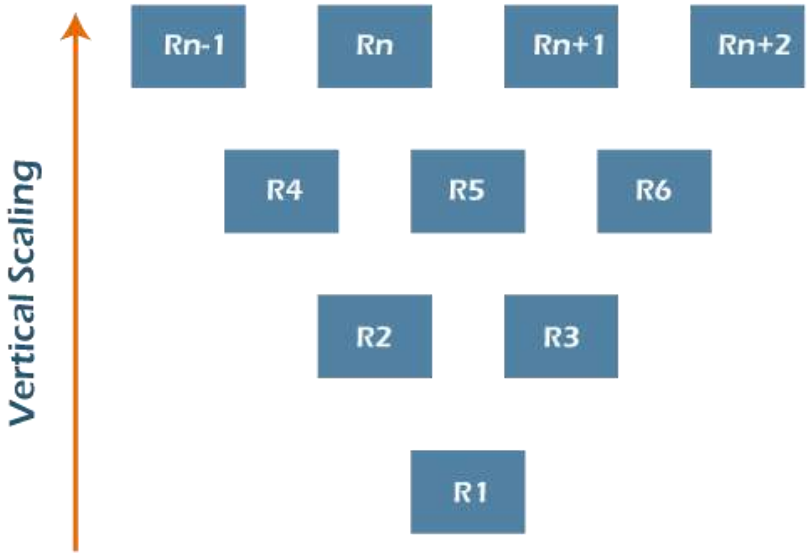
1. VERTICAL SCALING

- In this type of scalability, we increase the power of existing resources in the working environment in an upward direction.
- With computing, you can add or subtract resources, including memory or storage, within the server, as long as the resources do not exceed the capacity of the machine.
- Although it has its limitations, it is a way to improve your server and avoid latency and extra management. Like in the hotel example, resources can come and go easily and quickly, as long as there is room for them.

Example

- To understand vertical scaling, imagine a 20-story hotel. There are innumerable rooms inside this hotel from where the guests keep coming and going. Often there are spaces

available, as not all rooms are filled at once. People can move easily as there is space for them. As long as the capacity of this hotel is not exceeded, no problem. This is vertical scaling.



2. HORIZONTAL SCALING

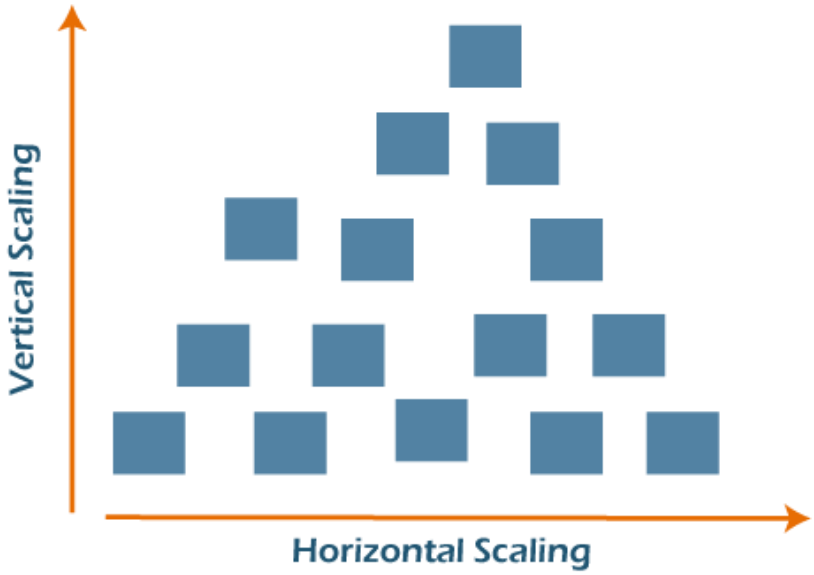
- In this kind of scaling, the resources are added in a horizontal row.
- Horizontal scaling refers to adding more servers to your network, rather than simply adding resources like with vertical scaling. This method tends to take more time and is more complex, but it allows you to connect servers together, handle traffic efficiently and execute concurrent workloads.

Example

- Horizontal scaling is a bit different. This time, imagine a two-lane highway. Cars travel smoothly in each direction without major traffic problems. But then the area around the highway develops - new buildings are built, and traffic increases. Very soon, this two-lane highway is filled with cars, and accidents become common. Two lanes are no longer enough. To avoid these issues, more lanes are added, and an overpass is constructed. Although it takes a long time, it solves the problem.

3. DIAGONAL SCALING

- It is a mixture of both Horizontal and Vertical scalability where the resources are added both vertically and horizontally. Well, you get diagonal scaling, which allows you to experience the most efficient infrastructure scaling.
- When you combine vertical and horizontal, you simply grow within your existing server until you hit the capacity. Then, you can clone that server as necessary and continue the process, allowing you to deal with a lot of requests and traffic concurrently.



WHY IS CLOUD SCALABLE?

- Scalable cloud architecture is made possible through virtualization. Unlike physical machines whose resources and performance are relatively set, virtual machines virtual machines (VMs) are highly flexible and can be easily scaled up or down. They can be

moved to a different server or hosted on multiple servers at once; workloads and applications can be shifted to larger VMs as needed.

- Third-party cloud providers also have all the vast hardware and software resources already in place to allow for rapid scaling that an individual business could not achieve cost-effectively on its own.

BENEFITS OF CLOUD SCALABILITY

Key cloud scalability benefits driving cloud adoption for businesses large and small:

- **Convenience**:

  Often, with just a few clicks, IT administrators can easily add more VMs that are available-and customized to an organization's exact needs-without delay. Teams can focus on other tasks instead of setting up physical hardware for hours and days. This saves the valuable time of the IT staff.

- **Flexibility and speed**:

  As business needs change and grow, including unexpected demand spikes, cloud scalability allows IT to respond quickly. Companies are no longer tied to obsolete equipment-they can update systems and easily increase power and storage. Today, even small businesses have access to high-powered resources that used to be cost-prohibitive.

- **Cost Savings**:

  Thanks to cloud scalability, businesses can avoid the upfront cost of purchasing expensive equipment that can become obsolete in a few years. Through cloud providers, they only pay for what they use and reduce waste.

- **Disaster recovery**:

  With scalable cloud computing, you can reduce disaster recovery costs by eliminating the need to build and maintain secondary data centers.

WHEN TO USE CLOUD SCALABILITY?

- Successful businesses use scalable business models to grow rapidly and meet changing demands. It's no different with their IT. Cloud scalability benefits help businesses stay agile and competitive.
- Scalability is one of the driving reasons for migrating to the cloud. Whether traffic or workload demands increase suddenly or increase gradually over time, a scalable cloud solution enables organizations to respond appropriately and cost-effectively to increased storage and performance.

FAULT TOLERANCE IN CLOUD COMPUTING

- Cloud Fault Tolerance is tolerating the faults by the cloud that are done by mistake by the user.
- Fault tolerance in cloud computing means creating a blueprint for ongoing work whenever some parts are down or unavailable. It helps enterprises evaluate their infrastructure needs and requirements and provides services in case the respective device becomes unavailable for some reason.
- It does not mean that the alternative system can provide 100% of the entire service. Still, the concept is to keep the system usable and, most importantly, at a reasonable level in operational mode. It is important if enterprises continue growing in a continuous mode and increase their productivity levels.

MAIN CONCEPTS BEHIND FAULT TOLERANCE IN CLOUD COMPUTING SYSTEM

- **Replication**: Fault-tolerant systems work on running multiple replicas for each service. Thus, if one part of the system goes wrong, other instances can be used to keep it running instead.

  For example, take a database cluster that has 3 servers with the same information on each. All the actions like data entry, update, and deletion are written on each. Redundant servers will remain idle until a fault tolerance system demands their availability.
- **Redundancy**: When a system part fails or goes downstate, it is important to have a backup type system. The server works with emergency databases that include many redundant services.

  For example, a website program with MS SQL as its database may fail midway due to some hardware fault. Then the redundancy concept has to take advantage of a new database when the original is in offline mode.

TECHNIQUES FOR FAULT TOLERANCE IN CLOUD COMPUTING

- Priority should be given to all services while designing a fault tolerance system. Special preference should be given to the database as it powers many other entities.
- After setting the priorities, the Enterprise has to work on mock tests. For example, Enterprise has a forums website that enables users to log in and post comments. When authentication services fail due to a problem, users will not be able to log in.
- Then, the forum becomes read-only and does not serve the purpose. But with fault-tolerant systems, healing will be ensured, and the user can search for information with minimal impact.

MAJOR ATTRIBUTES OF FAULT TOLERANCE IN CLOUD COMPUTING

- **None Point of Failure**: The concepts of redundancy and replication define that fault tolerance can occur but with some minor effects. If there is no single point of failure, then the system is not fault-tolerant.
- **Accept the fault isolation concept**: the fault occurrence is handled separately from other systems. It helps to isolate the Enterprise from an existing system failure.

EXISTENCE OF FAULT TOLERANCE IN CLOUD COMPUTING

- **System Failure**:

  This can either be a software or hardware issue. A software failure results in a system crash or hangs, which may be due to Stack Overflow or other reasons. Any improper maintenance of physical hardware machines will result in hardware system failure.

- **Incidents of Security Breach**:

  There are many reasons why fault tolerance may arise due to security failures. The hacking of the server hurts the server and results in a data breach. Other reasons for requiring fault tolerance in the **form of security breaches include ransomware, phishing, virus attacks, etc.**

CLOUD SOLUTIONS

- Cloud backup or cloud computer backup refers to backing up data to a remote, cloud based server.
- As a form of cloud storage, cloud backup data is stored in and accessible from multiple distributed & connected resources that comprise a cloud.
- Cloud backup solutions enable enterprises or individuals to store their data & computer files on the internet using a storage service provider, rather than storing the data locally on a physical disk, such as hard drive or tape backup.
- Backup providers enable customers to remotely access the service using a secure client log in application to backup files from the customer's computers or data center to the online storage server using an encrypted connection.

How to Restore a Cloud Backup:

- To update or restore a cloud backup, customers need to use the service provider's specific client application or a web browser interface.
- Files & data can be automatically saved to the cloud backup service on a regular, schedule basis, or the information can be automatically backed up anytime changes are made (also known as a "cloud sync").

CLOUD ECOSYSTEM

- Cloud ecosystem is a term used to describe the complex system of interdependent components that work together to enable cloud services.
- In nature, an ecosystem is composed of living and nonliving things that are connected and work together. In cloud computing, the ecosystem consists of hardware and software as well as cloud customers, cloud engineers, consultants, integrators and partners.

How a cloud ecosystem works

- The center of a cloud ecosystem is a public cloud provider. It might be an IaaS provider such as Amazon Web Services (AWS) or a SaaS vendor such as Salesforce.
- Radiating out from the center of the cloud are software companies that use the provider's anchor platform, as well as consultants and companies that have formed strategic alliances with the anchor provider. There is no vendor lock-in because these companies overlap, making the ecosystem more complex.

- For example, AWS is the center of its own ecosystem, but it's also a part of the Salesforce ecosystem. Salesforce runs a number of its services on AWS's infrastructure, and Salesforce customers can gain access, through devices called connectors, to pieces of AWS, such as its Simple Storage Service (S3).
- A robust ecosystem provides a cloud provider's customers with an easy way to find and purchase business applications and respond to changing business needs.
- When the apps are sold through a provider's app store such as AWS Marketplace, Microsoft Azure Marketplace (for cloud software) or Microsoft AppSource (for business applications), the customer essentially has access to a catalog of different vendors' software and services that have already been vetted and reviewed for security, risk and cost.

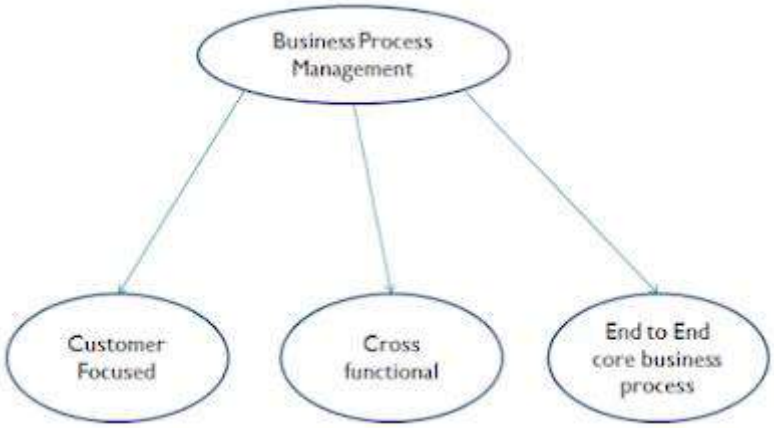
Benefits of a cloud ecosystem

- Companies can use a cloud ecosystem to build new business models. It becomes relatively easy for a medical device manufacturer, for example, to launch a heart-monitoring service on its cloud service provider's cloud infrastructure and then sell the service alongside its main business of manufacturing heart monitors for hospitals.
- In a cloud ecosystem, it is also easier to aggregate data and analyze how each part of the system affects the other parts. For example, if an ecosystem consists of patient records, smart device logs and healthcare provider records, it becomes possible to analyze patterns across an entire patient population.

CLOUD BUSINESS PROCESS MANAGEMENT

- Business process management (BPM) is a mature business discipline that has spawned a number of technologies to support it.
- Business process management (BPM) is how a company creates, edits, and analyzes the predictable processes that make up the core of its business.
- Today it is the agile who survive those organizations who are able to adapt to change, to innovate as well as continuously improve, and to continuously monitor and analyze the results of these adaptations.
- In the current web enabled business environment, processes in many cases depend on the discovery and recognition of components that exist as web services.

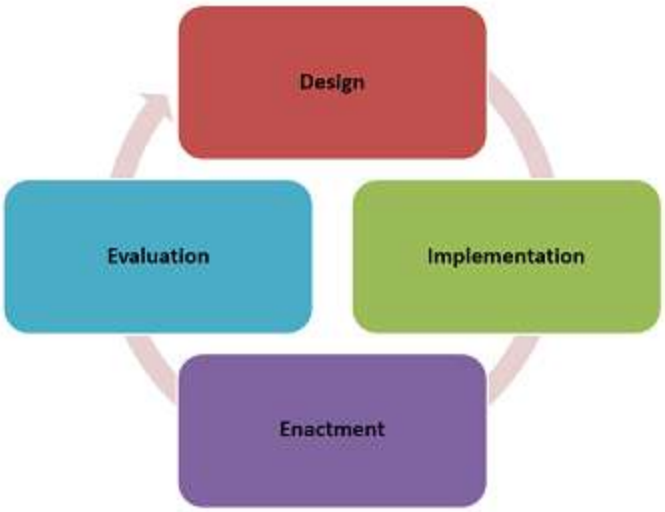
- The current trend is towards increased emphasis on mobility and collaboration as essential elements to support the agility and currency of business processes.
- This means that BPM vendors are increasingly seeking to augment their BPM packages by incorporating greater Web 2.0 type functionality.
- Cloud based BPM is one response to these new demands.
- BPM governs organizations cross functional, customer focused end to end core business process.



BPM Life Cycle

The **BPM life cycle** consists of four phases.

1. The **design** phase consists of identifying existing procedures and capturing these business processes into process models.
2. The **implementation** phase deploys the results of the design phase. A BPMS package can be used to house these processes.
3. The **enactment** phase is the runtime phase where the business processes are deployed into production and monitored by a BPMS.
4. The **evaluation** phase monitors the information gathered through the enactment phase and uses it to review the business process in action. Findings of the evaluation phase are input for the next iteration of the life cycle.



Components of BPM

- **Business Support**

  Business support entails the set of business-related services dealing with client & supporting processes.it includes the components used to run business operations that are client facing.

  - **Customer Management:** Manage customer accounts, open/close/terminate accounts, manage user profiles, manage customer relationships by providing points of contact &resolving customer issues & problems etc.
  - **Contract Management:** Manage service contracts, setup/negotiate/close/terminate contract etc.
  - **Inventory Management:** Set up & manage service catalogs etc.
  - **Accounting & Billing:** Manage customer billing information, send billing statements, process received payments, track invoices etc.
  - **Reporting & Auditing:** Monitor user operations, generate reports etc.
  - **Pricing & Rating:** Evaluate cloud services & determine prices, handle promotions & pricing rules based on a user's profile etc.

- **Provisioning & Configuration**

  - **Rapid provisioning:** Automatically deploying cloud systems based on the requested service/resources/capabilities.
  - **Resource changing:** Adjusting configuration/resource assignment for repairs, upgrades & joining new nodes into the cloud.

- **Monitoring & Reporting:** Discovering & monitoring virtual resources, monitoring cloud operations & events & generating performance reports.
- **Metering:** Providing a metering capability at some level of abstraction appropriate to the type of service (storage, processing, bandwidth & active user accounts).
- **SLA Management:** Encompassing the SLA contract definition (basic schema with the QoS parameters), SLA monitoring & SLA enforcement according to defined policies.

PORTABILITY & INTEROPERABILITY

Interoperability:

- Interoperability is the capacity of at least two applications or systems to trade data and to utilize the data that has been traded commonly. Cloud interoperability is the capacity of a client's framework to interface with a cloud service or the capacity for one cloud service to connect with other cloud benefits by trading data as per an endorsed strategy to get unsurprising outcomes.
- The two important elements of Cloud interoperability are usability and connectivity and have been separated into 5 layers:
    - ✓ Behaviour
    - ✓ Policy
    - ✓ Semantic
    - ✓ Syntactic
    - ✓ Transport

Portability:

- Portability, then again, is moving the applications or data starting with one framework then onto the next and having it stay executable or useable.
- Portability can be broken into two kinds: Cloud data portability and Cloud application portability.

  Cloud data portability:

  It is the capacity to effectively move information starting with one cloud service then onto the next without expecting to re-emerge the information.

  Cloud application portability:

  It is the capacity to move an application starting with one cloud service then onto the next or between a client's current circumstance and a cloud service.

CLOUD PORTABILITY AND INTEROPERABILITY CATEGORIES TO CONSIDER ARE:

- Publication and Acquisition Interoperability

- Management Interoperability
- Platform Interoperability
- Application Interoperability
- Platform Portability
- Application Portability
- Data Portability

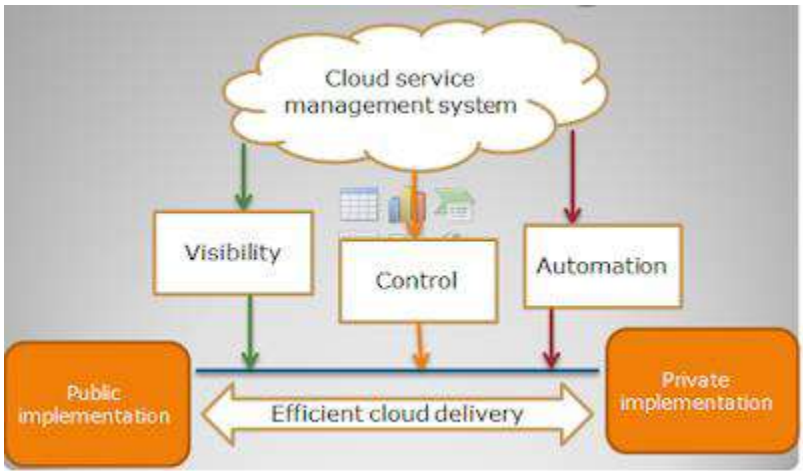
CLOUD SERVICE MANAGEMENT

Service management:

- A system integral of supply chain management that contents actual company sales and the customer.
- The goal of service management is to maximize service supply chains.
- The purpose of service management are to reduce high costs by integrating products and services and keep inventory levels smaller.

Cloud Service Management:

- Cloud monitoring and cloud service management tools allow cloud providers to ensure optimal performance, continuity and efficiency in virtualized, on-demand environments.
- The delivery of dynamic, cloud-based infrastructure, platform and application services doesn’t occur in a vacuum.
- In addition to best practices for effective administration of all the elements associated with cloud service delivery, cloud service management and cloud monitoring tools enable providers to keep up with the continually shifting capacity demands of a highly-elastic environment.
- The fig illustrates that service management provides the visibility, control and automation needed for efficient cloud delivery in both public and private implementations.



Simplify user interaction with it:

- The user friendly self-service accelerates time to value.
- Service catalogue enables standards which drives consistent service delivery.

Enable policies to lower cost with provisioning:

- Automatic allocating and de-allocating of resources will make delivery of services fast.
- Provisioning policies allow release and reuse of assets.

Increase system admin productivity:

- Providing the benefits to the broker will probably become a critical success factor in cloud computing.
- Due to the growth of service brokerage business will increase the ability of cloud consumers to use services in a trustworthy manner.
- These cloud mediators will help companies to choose the right platform, deploy the apps across multiple clouds.

Opportunities for cloud brokers:

- Cloud service intermediation: The broker must need to manage the additional securities or management capabilities over the cloud.
- Cloud aggregation: It includes the deployment of services over multiple cloud platforms.
- The ability to group an application across multiple clouds will become important i.e. if one service goes down the another can be started.

CLOUD OFFERINGS

- Patterns of this category cover different functionality found in clouds regarding the functionality they provide to customers and the behavior they display.

1. **Cloud Environments**

- Patterns of this category descibe the hosting environments of cloud in detail and refer to other offerings composed to form these environments.
  - ✓ Elastic Infrastructure
  - ✓ Elastic Platform
  - ✓ Node-based Availability
  - ✓ Environment-based Availability

2. **Processing Offerings**

- Patterns of this category describe how computation can be performed in the cloud.
  - ✓ Hypervisor
  - ✓ Execution Environment
  - ✓ Map Reduce

3. **Storage Offerings**

- Patterns of this category describe how data can be stored in the cloud.
  - ✓ Block Storage
  - ✓ Blob Storage
  - ✓ Relational Database
  - ✓ Key-Value Storage
  - ✓ Strict Consistency
  - ✓ Eventual Consistency

4. **Communication Offerings**

- Patterns of this category describe how data can be exchanged in the cloud.
  - ✓ Virtual Networking
  - ✓ Message-oriented Middleware
  - ✓ Exactly-once Delivery
  - ✓ At-least-once Delivery
  - ✓ Transaction-based Delivery

- ✓ Timeout-based Delivery

TESTING UNDER CONTROL

- Cloud testing typically involves monitoring and reporting on real-world user traffic conditions as well as load balance and stress testing for a range of simulated usage conditions.
- Load and performance testing conducted on the applications and services provided via cloud computing particularly the capability to access these services in order to ensure optimal performance and scalability under a wide variety of conditions.
- Consumers can access the IT resources in the test environment.
- Testing under the cloud gives very good sign by decreasing the manual intervention and reducing the processes in the typical testing environment.
- After enabling of resources as and when they are required, it reduces the investment on capital as well as enables the business to handle the ups and downs of the testing requirements.

Facts under cloud computing

- The fig clearly shows that on the basis of these six parameters a cloud testing process can be performed.

Advantages of Cloud Testing:

- Reduces capital investment and operational costs and not effect goal critical production application.
- Offers new and attractive services to the clients and present an opportunity to speed cycles of innovations and improve the solution quality

SECURITY ISSUES ASSOCIATED WITH THE CLOUD

There is no doubt that Cloud Computing provides various Advantages but there are also some security issues in cloud computing. Below are some following Security Issues in Cloud Computing as follows.

1. **Data Loss –**

   Data Loss is one of the issues faced in Cloud Computing. This is also known as Data Leakage. As we know that our sensitive data is in the hands of somebody else, and we don't have full control over our database. So if the security of cloud service is to break by hackers then it may be possible that hackers will get access to our sensitive data or personal files.

2. **Interference of Hackers and Insecure API's –**

   As we know if we are talking about the cloud and its services it means we are talking about the Internet. Also, we know that the easiest way to communicate with Cloud is using API. So it is important to protect the Interface's and API's which are used by an external user. But also in cloud computing, few services are available in the public domain. *An* is the vulnerable part of Cloud Computing because it may be possible that these services are accessed by some third parties. So it may be possible that with the help of these services hackers can easily hack or harm our data.

3. **User Account Hijacking –**

   Account Hijacking is the most serious security issue in Cloud Computing. If somehow the Account of User or an Organization is hijacked by Hacker. Then the hacker has full authority to perform Unauthorized Activities**.**

4. **Changing Service Provider –**

   Vendor lock In is also an important Security issue in Cloud Computing. Many organizations will face different problems while shifting from one vendor to another. For example, An Organization wants to shift from AWS Cloud to Google Cloud Services then they ace various problem's like shifting of all data, also both cloud services have different techniques and functions, so they also face problems regarding that. Also, it may be possible that the charges of AWS are different from Google Cloud, etc.

5. **Lack of Skill –**
   While working, shifting o another service provider, need an extra feature, how to use a feature, etc. are the main problems caused in IT Company who doesn't have skilled Employee. So it requires a skilled person to work with cloud Computing.
6. **Denial of Service (DoS) attack –**
   This type of attack occurs when the system receives too much traffic. Mostly DoS attacks occur in large organizations such as the banking sector, government sector, etc. When a DoS attack occurs data is lost. So in order to recover data, it requires a great amount of money as well as time to handle it.

CLOUD SECURITY CONTROLS

- Cloud computing security refers to the technical discipline and processes that IT organizations use to secure their cloud-based infrastructure.
- Through a cloud service provider, IT organizations can outsource management of every aspect of the technology stack, including networking, servers, storage, virtualization, operating systems, middleware, runtime, data and applications.
- Cloud computing security includes the measures that IT organizations take to secure all of these components against cyber-attacks, data theft and other threats.

Types of Cloud Computing Security Controls

- IT organizations and the cloud service providers they do business with share responsibility for implementing security controls to protect applications and data that are stored or deployed in the cloud.
- These controls include a variety of measures for reducing, mitigating or eliminating various types of risk: the creation of data recovery and business continuity plans, encrypting data, and controlling cloud access are all security controls.
- While many types of cloud computing security controls exist, they generally fall into one of four categories.

Deterrent Controls –

- Deterrent controls are designed to discourage nefarious actors from attacking a cloud system. These controls may act as a warning that an attack will be met with consequences. Insider attacks are a source of risk for cloud service providers, so an example of a deterrent control could be a cloud service provider conducting criminal background checks on employees.

Preventive Controls –

- Preventive controls make the cloud environment more resilient to attacks by eliminating vulnerabilities. A preventive control could be writing a piece of code that disables inactive ports to ensure that there are no available entry points for hackers. Maintaining a strong user authentication system is another way of reducing vulnerability to attack.

Detective Controls –

- The purpose of detective controls is to identify and react to security threats and events. Intrusion detection software and network security monitoring tools are examples of detective controls - their role is to monitor the network to determine when an attack could be happening.

Corrective Controls –

- Corrective controls are activated in the event of a security attack. Their role is to limit the damage caused by the incident. A developer might write a piece of code so that when a certain type of threat is detected, data servers are disconnected from the network to prevent data theft.

VIRTUAL DESKTOP INFRASTRUCTURE

❖ **Desktop virtualization**

- In cloud computing, the process of separating software (such as an operating system or an application) from the hardware that it runs on is called virtualization. This frees the software from needing to be run on a specific device—and allows it to be run on any device.
- So, virtualization is the process—and the "machines" created using this process are called virtual machines, or just VMs for short. While the hardware that makes up your

computer is physical and tangible, VMs are virtual computers that exist as code and whose "hardware" (CPU, hard drive, RAM, etc.) are defined using software.

- A VM is partitioned portions of a real physical server's resources so that multiple, independent VMs can share the same physical hardware. This process is also known as server virtualization and uses a nifty technology called a hypervisor, which is software that integrates the physical hardware and the VM's virtual "hardware". This allows IT pros to set up and manage VMs and allows VMs running different operating systems (such as Windows or Linux, to name a few) to run on the same hardware.

❖ **Remote Desktop Virtualization**

- Remote Desktop Virtualization Host (RD Virtualization Host) is a role service that supports Virtual Desktop Infrastructure (VDI) scenarios and lets multiple users run Windows-based applications in virtual machines hosted on a server running Windows Server and Hyper-V.

- Remote Desktop Virtualization is frequently used in the following scenarios:

  - ✓ In distributed environment with high availability requirements &where desk-side technical support is not readily available, such as branch office & retail environments

  - ✓ In environments where high network latency degrades the performance of conventional client/server applications.

  - ✓ In environments where remote access & data security requirements create conflicting requirements that can be addressed by retaining all (application) data within the data center with only display, keyboard & mouse information communicated with the remote client.

❖ **Virtual Desktop Infrastructure**

- VDI is a desktop virtualization technique where you leverage VMs to provision and manage applications and virtual desktops.

- VDI hosts the desktop environments—including the OSs, applications and desktops—on servers in a datacenter and deploys them to end-users on request.

- You can access VDI remotely from an endpoint and manage the OS, including the applications and files on it, as though they are running locally.

- VDI can allow users safe access to corporate files and applications from virtually any device—including thin clients and mobile devices—and platform.

- VDI leverages different components to present virtual desktops to users. Some of these **components** include the following:

    - ✓ **Hypervisor.** It segments physical servers into VMs, which in turn, host virtual desktops and applications.
    - ✓ **Connection broker.** It authenticates users to available virtual desktops. Connection brokers are useful when operating multiple hosts with different virtual desktop pools. They provide a way through which users can log in. Connection brokers redirect them to the appropriate desktop pool.
    - ✓ **Load balancer.** A load balancer distributes workloads evenly across multiple hosts. This ensures that no host gets overwhelmed while others are idle. In some instances, the connection broker can function as a load balancer.
    - ✓ **Client software.** Each endpoint connects to the VDI using a client application. The client software can leverage any of the remoting protocols such as PC over internet protocol (PCoIP), Remote Desktop Protocol (RDP) and Independent Computing Architecture (ICA) to connect to servers.

❖ **Remote Desktop Services (RDS)**

- Remote Desktop Services (RDS) is a platform offering from Microsoft that allows you to cost-effectively host Windows desktops and apps.
- RDS creates different server roles and each specific role enables multiple users to simultaneously login to a Windows Server. Once set up, you can connect to the published desktops and apps from various platforms and devices—using the Microsoft Remote Desktop application on Windows, Mac, iOS, and Android.

❖ **Application Virtualization**

- Traditionally running an application uses your existing operating system and its hardware resources. Essentially, you are running the application on top of your computer. Application virtualization encapsulates the application and separates it from

the underlying operating system. This gives you access to the application without installing it onto the native device.

- Application virtualization allows an administrator to install the application onto a server. Anyone with access to this server can then access the application and run it as if it were installed on their respective devices. This provides users with benefits such as portability, cross-platform operation, and the ability to run multiple instances of the application.

❖ **Layering**

- Desktop layering is a method of desktop virtualization that divides a disk image into logical parts to be managed individually.
- Layering can be applied to local physical disk images, client based virtual machines or host based desktops.
- Windows operating systems are not designed for layering, therefore each vendor must engineer their own proprietary solution.

❖ **Desktop-as-a-Service (DaaS)**

- Desktop-as-a-Service (DaaS) is a cloud-based desktop virtualization service hosted by a third-party enterprise.
- The third-party cloud provider manages all backend resources, such as desktop storage, compute and networking, including the virtual cloud machines that run the desktop operating systems.
- The desktop as a service provider streams the virtual desktops to end-user devices, allowing anytime, anywhere access to desktops and applications.
- Like most cloud services, DaaS is subscription-based in a multi-tenant environment. Organizations can also deploy a desktop infrastructure in a private cloud in a local datacenter.

UNIT – 4
CLOUD MANAGEMENT & VIRTUALIZATION

CREATE A VIRTUALIZED ARCHITECTURE

Create and deploy end-to-end virtualizations that help:

- Reduce cost
- Provision new application quickly
- Maintain a high level of application performance

Whether you want to start with server virtualizations, extent virtualization across the data centre or implement virtual desktop infrastructure, network solution and cisco provides a comprehensive architecture approach that helps reduce costs, protect application performance and secure the virtual infrastructure.

DATA CENTER

- A Datacenter can be described as a facility/space of networked computers and associated components (like telecommunications and storage) which helps business and organisations to function a large amount of data. These Data centers allow the data to organise, process, store and disseminate upon the application used by businesses.
- Data centers are composed of a number of technical elements. These can be broken down into three categories:

  - ✓ **Compute:** The memory and processing power to run the applications, generally provided by high-end servers
  - ✓ **Storage:** Important enterprise data is generally housed in a data center, on media ranging from tape to solid-state drives, with multiple backups
  - ✓ **Networking:** Interconnections between data center components and to the outside world, including routers, switches, application-delivery controllers, and more

Types of Data Center:

Businesses use different types of data centers which include:

- **Telecom Data Center:** It is a type of data center which are operated by telecommunications or service providers. It requires high-speed connectivity to function.
- **Enterprise Data Center:** It is a type of data center which is built and owned by a company that may or may not be onsite.
- **Colocation Data Center:** It is a type of data center that consists of one data center owner place which provides cooling to multiple enterprises and hyper-scale their customers.
- **Hyperscale Data Center:** It is a type of data center which are owned by and operated by the company itself.

Difference between Cloud and Data Center:

S.NO	CLOUD	DATA CENTER
1.	Cloud is a virtual resource that helps businesses to store, organize, and operate data efficiently.	Data Center is a physical resource that helps businesses to store, organize, and operate data efficiently.
2.	The scalability of the cloud required less amount of investment.	The scalability of Data Center is huge in investment as compared to the cloud.
3.	The maintenance cost is less than service providers maintain it.	The maintenance cost is high because developers of the organization do maintenance.
4.	Third-Party needs to be trusted for the organization's data to be stored.	The organization's developers are trusted for the data stored in data centers.
5.	Performance is huge as compared with investment.	Performance is less than compared to investment.
6.	It requires a plan to customize the cloud.	It is easily customizable without any hard plan.
7.	It requires a stable internet connection to provide the function.	It may and may not require an internet connection.
8.	Cloud is easy to operate and is considered a viable option.	Data Centers require experienced developers to operate and are considered not a viable option.

RESILIENCE

- Cloud Resiliency is the capacity to rapidly adapt and respond to risks, as well as opportunities. In simple words resiliency refers to improve our business for handle risks.
- This also maintains the continuous business operations that support growth.
- The assessment process examines business-driven, data-driven, and event-driven risks. The goal is to understand the risks to the company and the business process in one building.
- Risks in one geography are different from other locations. So we will be looking across different parts of the company, we have to find out common risks by focusing on one specific area first.
- By using resilience framework to look at different parts of the company, we are trying to understand whether we have a risk that we can accept or whether we have risk that we want to avoid.
- In other words either we may choose to do nothing about a risk, or we may improve our infrastructure handle the risks if they occur.
- The resiliency blueprint includes different layers- facilities, technology, applications and data, processes, organization, strategy and vision.
- The resiliency framework enables us to examine the business, understand what areas of vulnerability might come across business-driven, data-driven and event driven risks.

Resiliency capabilities:

The strategy combines multiple parts to mitigate risks (that means to reduce the effect of risks) and improve business resilience.

- From a facilities perspective, we may want to implement power protection.
- From a security perspective, to protect our data and applications we may want to implement remote backup, identity management, email filtering, or email archiving.
- From a process perspective, we may implement identification and documentation of most critical business processes.
- From a organizational perspective, we may want to implement a virtual workstation environment.

- From a strategy and vision perspective, we may want to look at the kind of crisis management process.

Resiliency tiers can be defined as a common set of infrastructure services that are delivered to meet or to provide a corresponding set of business availability expectations

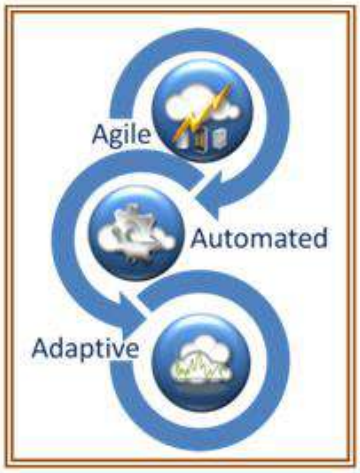
The three basic strategies that are used to improve a cloud system's resilience are:

- **Checking and monitoring**: An independent method continually ensures that the device meets the minimum behavioral requirements. This system is important for detecting failures and resource reconfiguration.
- **Checkpoint and restart**: Depending on such conditions, the state of the whole system is saved. System failures indicate a phase of restoration to the most recent correct checkpoint and recovery of the system.
- **Replication**: Using additional resources (hardware and software), the essential components of a device are replicated, ensuring that they are usable at any moment. With this strategy, the additional difficulty is the status synchronization task between the replicas and the main device.

AGILITY

- In a cloud computing context, agility often refers to the ability to rapidly develop, test and launch applications that drive business growth in a constantly changing IT environment.

- Cloud technology offers businesses a key means of promoting agility, and is a vital tool in the enterprise push toward better adaptability.
- Cloud Agility allows them to focus on other issues such as security, monitoring and analysis, instead of provisioning and maintaining the resources.



- In a business context, agility typically refers to the ability of an organization to rapidly adapt to market and environmental changes in productive and cost-effective ways.
- Strategic agility, or “business agility,” can be achieved by quickly adapting goods and services to meet customer demands.
- Agility is a concept that incorporates the ideas of flexibility, balance, adaptability, and coordination under one umbrella.
- It facilitates the adaptation of new IT strategies such as

    - ✓ Service oriented architecture (SOA)
    - ✓ Virtualization & on-demand computing allowing faster response to change

- Virtualized infrastructure with the ability to respond quickly to new application demands, service requirements, attacks or disruptions based on predefined policies.

You can achieve Agility in the cloud in a number of ways:

Quicker Time-to-market:

- Cloud computing allows companies to significantly decrease the time it takes to provision and de-provision IT infrastructure, speeding delivery of IT projects that are critical to revenue growth or cost reduction.
- While a physical server could take days or weeks to procure and provision, a cloud server takes minutes.
- Faster time to market means faster time to revenue.

Automated allocation of resources:

- Cloud computing simplifies provisioning, de-provisioning and re-deploying resources through automation and easy-to-use web consoles and APIs.
- The time for an IT systems administrator spent on managing and supporting cloud infrastructure is reduced greatly compared to that seen in a physical environment.

Flexibility and Scalability:

- Cloud computing allows the flexibility for businesses to scale up or down their resources to meet the on-demands or sudden burst in demand or website traffic to meet unpredictable application development or production needs.
- The pay-per-use flexibility of the cloud, allows end-users to scale fast or “fail fast” based on the demands of the business.
- Common workloads that require on-demand scalability: testing and development, load testing, seasonal spikes in traffic, a new application etc.

Adaptive Auto-Scaling:

- Cloud computing uses API’s, software etc. for accessibility of cloud platforms and services.
- It is easier to automate IT management and provisioning in a cloud environment. You can integrate business intelligence and analytics platforms, IT monitoring tools with the cloud, allowing the systems to be more adaptive.
- Ex. new servers can be automatically provisioned (or de-provisioned) when load balancing thresholds are met.

Faster Innovation:

- Cloud computing allows companies to support an increased pace of product development and marketing programs that better align IT infrastructure and management costs with the goals and objectives of the business.

CISCO DATA CENTER NETWORK ARCHITECTURE

A comprehensive architecture that enables IT executives to:

- Consolidate and virtualize computing, storage and network resources
- Deliver secure and optimized employee, partner and customer access to information and applications
- Protect and rapidly recover IT resources and applications

Cisco Data Center Network Architecture Built With:

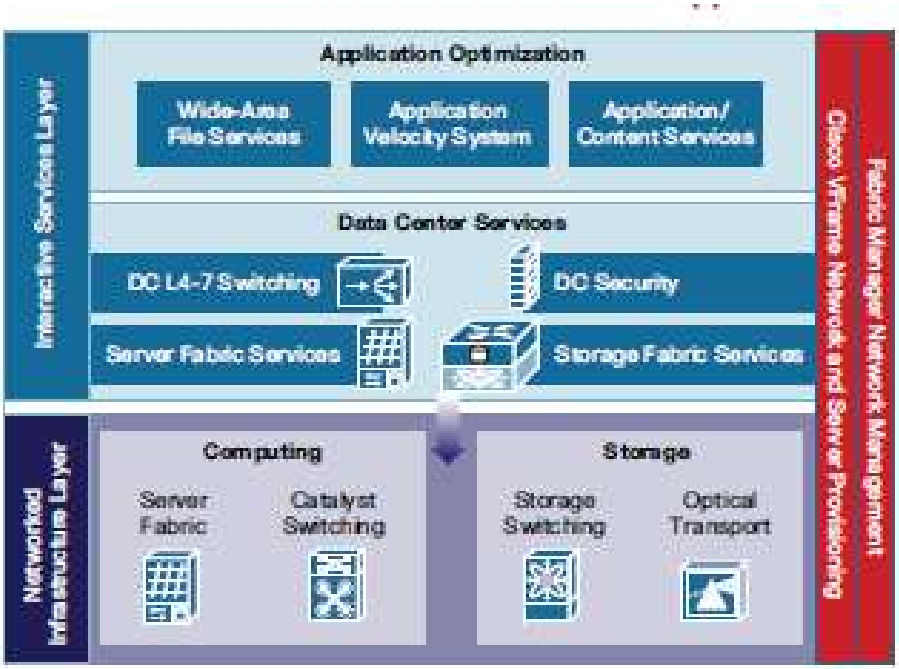
- **Networked Infrastructure:**
  - ✓ Gigabit/10Gigabit ethernet
  - ✓ Fibre channel switching on intelligent server farm
  - ✓ Server fabric
  - ✓ storage networking platform
  - ✓ DWDM, SONET & SDH optical transport platform
- **Interactive Services:**
  - ✓ Storage Fabric Services
  - ✓ computer services
  - ✓ security services
  - ✓ application optimization services
- **Management Framework:**
  - ✓ Fabric manager (element and network management) and
  - ✓ Cisco VFrame (server and service provisioning)
  - ✓ Configuration
  - ✓ Security
  - ✓ Change & fault management services

Cisco Data Center Network Architecture Based On:

- Cisco Service-Oriented Network Architecture (SONA),

- the enterprise implementation of the Intelligent Information Network (IIN) technology vision.
- Cisco SONA emphasizes the value of the interactive services provided in the networked infrastructure, such as application optimization, security, and server and storage fabric switching, to enhance business applications.

Cisco Data Center Network Architecture in Support of SONA



Benefits

- Lower-priced server and storage infrastructure
- Increased business agility and adaptability
- Ability to meet regulatory compliance standards with integrated network security and support for business continuance
- Tested and verified design and extensive service offerings for lower implementation costs and reduced risk
- Investment protection for core data center platforms offering multiyear deployment lifecycles
- Rapid application development and time to market of business-critical services

CLOUD STORAGE

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

How Does Cloud Storage Work?

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

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

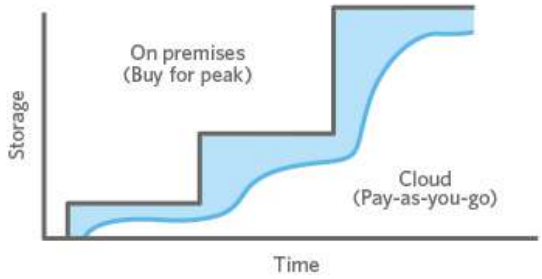
Benefits of Cloud Storage

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

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

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

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



Cloud Storage Requirements

Ensuring your company's critical data is safe, secure, and available when needed is essential. There are several fundamental requirements when considering storing data in the cloud.

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

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

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

Types of Cloud Storage

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

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

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

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

PROVISIONING

- Provisioning in layman's terms is to provide something. In technical terms, it is the set-up operation of IT infrastructure.
- Cloud Provisioning is the allocation of the cloud provider's resources to a client. It is exactly the process of amalgamation and execution of cloud computing resources within an IT organization.
- It is basically an important aspect of the cloud computing model, which tells how a client acquires cloud services and resources from a cloud supplier.
- The cloud services that customers can provision include:
    - ✓ Infrastructure as a service (IaaS)
    - ✓ Software as a service (SaaS)
    - ✓ Platform as a service (PaaS)

IaaS: Infrastructure as a service (IaaS) is one of the types of cloud computing service that provides essential compute, storage, and networking resources on demand.

SaaS: Software as a service (SaaS) is a distribution model of the software in which the applications are hosted by a cloud provider and are exposed to the end-users over the internet.

PaaS: Platform as a service is a cloud computing model where hardware and software tools are provided to users over the internet by a third-party provider.

Benefits of Cloud Provisioning

Cloud provisioning has numerous benefits for an organization that cannot be achieved by traditional provisioning approaches.

Scalability: A company makes a huge investment in its on-site infrastructure under the conventional IT provisioning model. This requires immense preparation and prophesying infrastructure needs. However, in the cloud provisioning model, cloud resources can scale up and scale down which is entirely dependant on the short-term consumption of usage. This way scalability can help the organizations.

Speed: Speed is another factor of the cloud's provisioning which can benefit the organizations. For this, the developers of the organization can schedule the jobs which in turn removes the need for an administrator who provisions and manages resources.

Cost Savings: It is another potential benefit of cloud provisioning. Traditional technology can incur a huge cost to the organizations while cloud providers allow customers to pay only for what they consume. This is another major reason why cloud provisioning is preferred.

Types of Cloud Provisioning

- **Network Provisioning:** Network Provisioning in the telecom industry is a means of referring to the provisions of telecommunications services to a client.
- **Server Provisioning:** Datacenter's physical infrastructure, installation, configuration of the software, and linking it to middleware, networks, and storage.
- **User Provisioning:** It is a method of identity management that helps us in keeping a check on the access and privileges of authorization. Provisioning is featured by the artifacts such as equipment, suppliers, etc.
- **Service Provisioning:** It requires setting up a service and handling its related data.

Tools and Softwares Used in Cloud Provisioning

Several enterprises can provide the services and resources manually as per their need, whereas public cloud providers offer tools to provide various resources and services such as:

- IBM Cloud Orchestrator
- Cloud Bolt
- Morpheus Data
- Flexera
- Cloud Sphere
- Scalr
- Google Cloud Deployment manager

Challenges Faced in Cloud Provisioning

- **Cost Monitoring:** Monitoring the consumption and pricing benchmarks is important. Putting control on the pricing and running the alerts about usage is also very crucial. But, this could be a real challenge in achieving the budget overrun.
- **Monitoring and Managing Complex Processes:** Optimized use of cloud services, companies can depend on multiple provisioning tools. When companies deploy workloads on more than one platform it makes it becomes challenging to provide a single console to display anything.
- **Resource and Service dependencies:** There are various workloads and applications in the cloud that often tap into the basic cloud infrastructure resources. Public cloud provider services carry dependencies that can lead to uncertainty and surprise costs.

CLOUD ASSET MANAGEMENT

Cloud Asset management is a dedicated application which is used to record and track an asset throughout its life cycle, from occupying to disposal. It provides an organization with information like where certain assets are located, who is using them, how they are being utilized and details about the asset.

CAM is primarily about managing the challenges of cloud applications, platforms and infrastructure (SaaS, PaaS and IaaS). For instance:

- Inability to track and manage the growing use of SaaS applications and providers
- Lack of a centralized view of Cloud resources and consumption

- Limited access to SaaS subscription data
- Limited access to actual SaaS, IaaS and PaaS usage data

Benefits of Cloud Asset Management (CAM):

- Accurate tracking of key applications delivered in the Cloud
- Overcome the limitations of Cloud portals, by providing access to a single centralized view
- Expanded access to data and improved analysis and reporting
- Granular insight into SaaS, IaaS and PaaS usage across your organization
- Combine Cloud and on-premise deployment data for a complete end-to-end view of your IT ecosystem
- Accurate, complete view of investments and their usage across the whole IT estate enables better cost control
- Access all the information needed to ensure a successful migration to the Cloud.

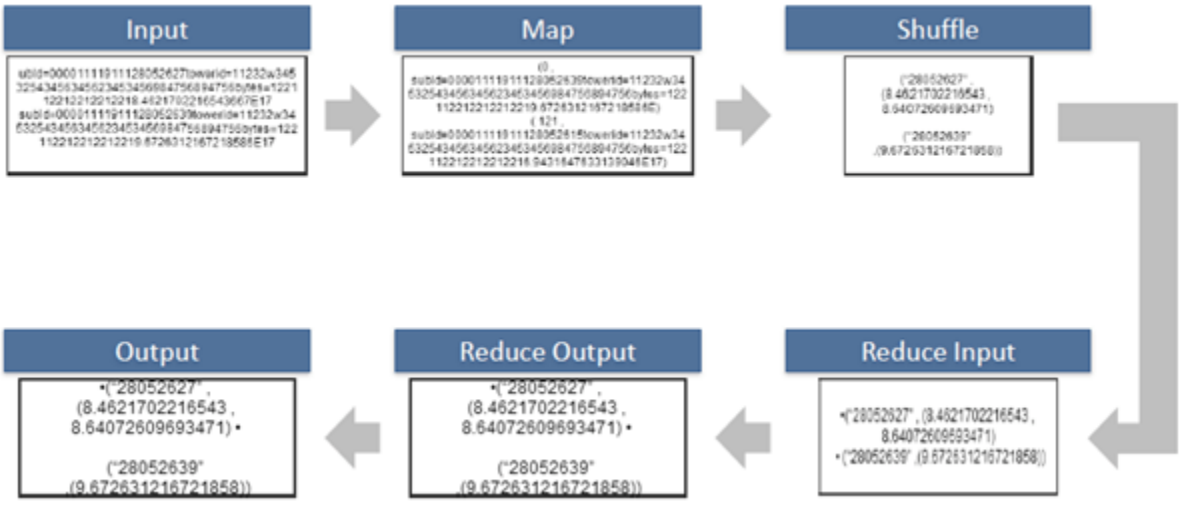
MAP REDUCE

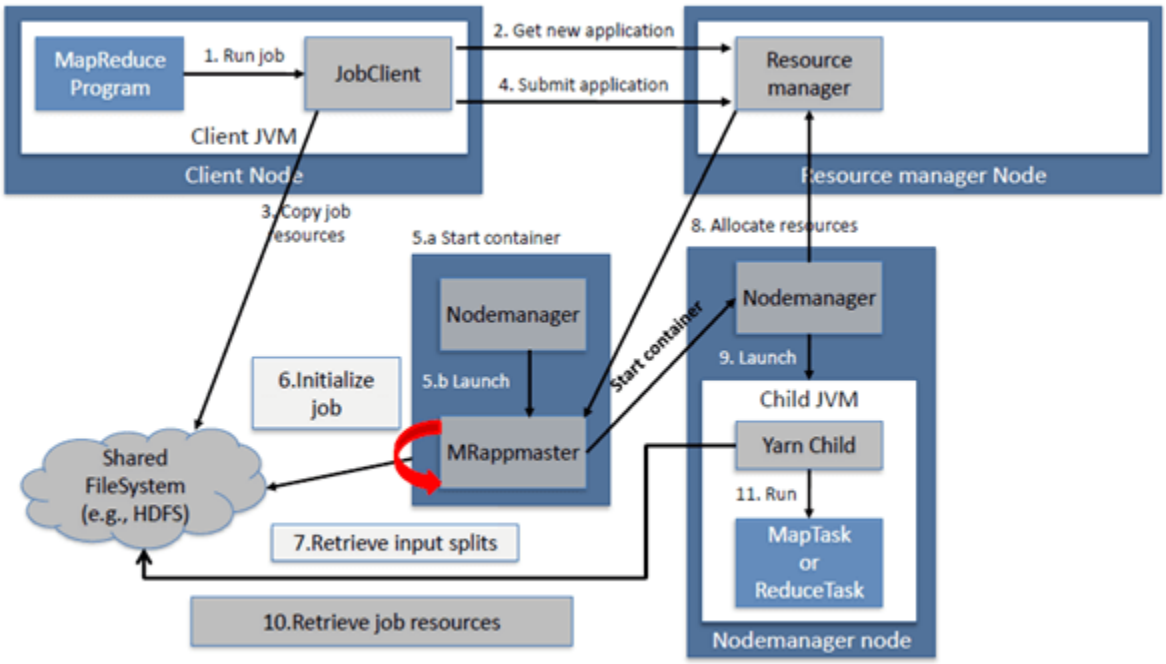
- A Map Reduce is a data processing tool which is used to process the data parallelly in a distributed form. It was developed in 2004, on the basis of paper titled as "Map Reduce: Simplified Data Processing on Large Clusters," published by Google.
- **Map Reduce** is a software framework and programming model used for processing huge amounts of data.
- The Map Reduce is a paradigm which has two phases, the mapper phase, and the reducer phase. In the Mapper, the input is given in the form of a key-value pair. The output of the Mapper is fed to the reducer as input. The reducer runs only after the Mapper is over. The reducer too takes input in key-value format, and the output of reducer is the final output.

Steps in Map Reduce

- The map takes data in the form of pairs and returns a list of <key, value> pairs. The keys will not be unique in this case.

- Using the output of Map, sort and shuffle are applied by the Hadoop architecture. This sort and shuffle acts on these list of <key, value> pairs and sends out unique keys and a list of values associated with this unique key <key, list(values)>.
- An output of sort and shuffle sent to the reducer phase. The reducer performs a defined function on a list of values for unique keys, and Final output <key, value> will be stored/displayed.





Sort and Shuffle

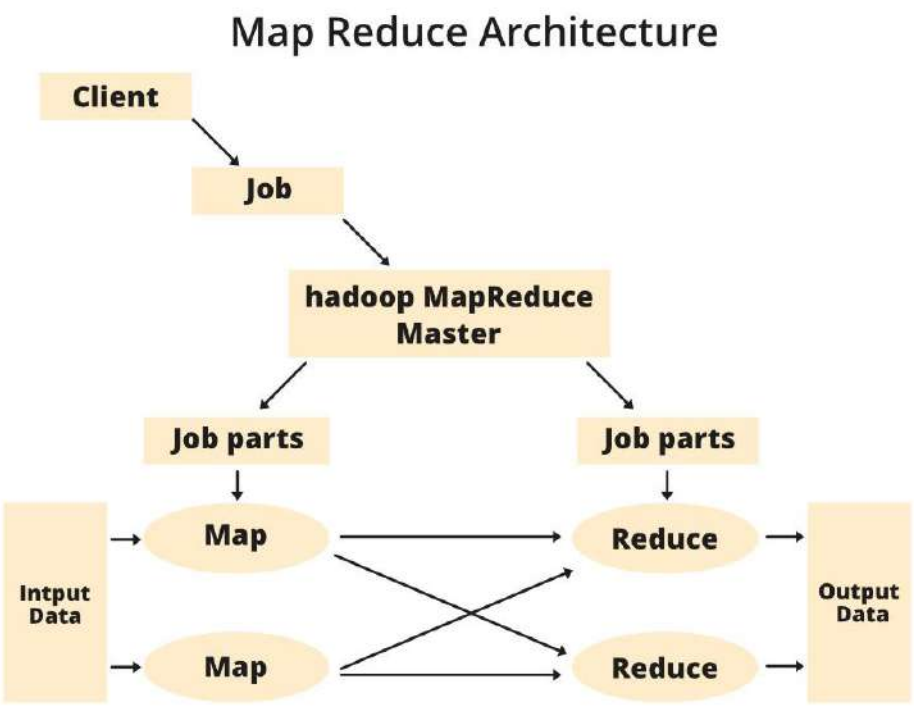
The sort and shuffle occur on the output of Mapper and before the reducer. When the Mapper task is complete, the results are sorted by key, partitioned if there are multiple reducers, and then written to disk. Using the input from each Mapper <k2,v2>, we collect all the values for each unique key k2. This output from the shuffle phase in the form of <k2, list(v2)> is sent as input to reducer phase.

Usage of Map Reduce

- It can be used in various application like document clustering, distributed sorting, and web link-graph reversal.
- It can be used for distributed pattern-based searching.
- We can also use MapReduce in machine learning.
- It was used by Google to regenerate Google's index of the World Wide Web.
- It can be used in multiple computing environments such as multi-cluster, multi-core, and mobile environment.

MapReduce Architecture

- Map Reduce and HDFS are the two major components of Hadoop which makes it so powerful and efficient to use.
- Map Reduce is a programming model used for efficient processing in parallel over large data-sets in a distributed manner. The data is first split and then combined to produce the final result.
- The libraries for Map Reduce is written in so many programming languages with various different-different optimizations.
- The purpose of Map Reduce in Hadoop is to Map each of the jobs and then it will reduce it to equivalent tasks for providing less overhead over the cluster network and to reduce the processing power.
- The Map Reduce task is mainly divided into two phases Map Phase and Reduce Phase.



Components of Map Reduce Architecture:

1. **Client:** The Map Reduce client is the one who brings the Job to the Map Reduce for processing. There can be multiple clients available that continuously send jobs for processing to the Hadoop Map Reduce Manager.
2. **Job:** The Map Reduce Job is the actual work that the client wanted to do which is comprised of so many smaller tasks that the client wants to process or execute.
3. **Hadoop Map Reduce Master:** It divides the particular job into subsequent job-parts.
4. **Job-Parts:** The task or sub-jobs that are obtained after dividing the main job. The result of all the job-parts combined to produce the final output.
5. **Input Data:** The data set that is fed to the Map Reduce for processing.
6. **Output Data:** The final result is obtained after the processing.

- In **Map Reduce**, we have a client. The client will submit the job of a particular size to the Hadoop Map Reduce Master.
- Now, the Map Reduce master will divide this job into further equivalent job-parts. These job-parts are then made available for the Map and Reduce Task. This Map and Reduce

task will contain the program as per the requirement of the use-case that the particular company is solving.

- The developer writes their logic to fulfill the requirement that the industry requires. The input data which we are using is then fed to the Map Task and the Map will generate intermediate key-value pair as its output.
- The output of Map i.e. these key-value pairs are then fed to the Reducer and the final output is stored on the HDFS.
- There can be n number of Map and Reduce tasks made available for processing the data as per the requirement.
- The algorithm for Map and Reduce is made with a much optimized way such that the time complexity or space complexity is minimum.

The Map Reduce task is mainly divided into **2 phases** i.e. Map phase and Reduce phase.

1. **Map:** As the name suggests its main use is to map the input data in key-value pairs. The input to the map may be a key-value pair where the key can be the id of some kind of address and value is the actual value that it keeps. The *Map()* function will be executed in its memory repository on each of these input key-value pairs and generates the intermediate key-value pair which works as input for the Reducer or *Reduce()* function.

2. **Reduce:** The intermediate key-value pairs that work as input for Reducer are shuffled and sort and send to the *Reduce()* function. Reducer aggregate or group the data based on its key-value pair as per the reducer algorithm written by the developer.

How Job tracker and the task tracker deal with Map Reduce:

1. **Job Tracker:** The work of Job tracker is to manage all the resources and all the jobs across the cluster and also to schedule each map on the Task Tracker running on the same data node since there can be hundreds of data nodes available in the cluster.

2. **Task Tracker:** The Task Tracker can be considered as the actual slaves that are working on the instruction given by the Job Tracker. This Task Tracker is deployed on each of the nodes available in the cluster that executes the Map and Reduce task as instructed by Job Tracker.

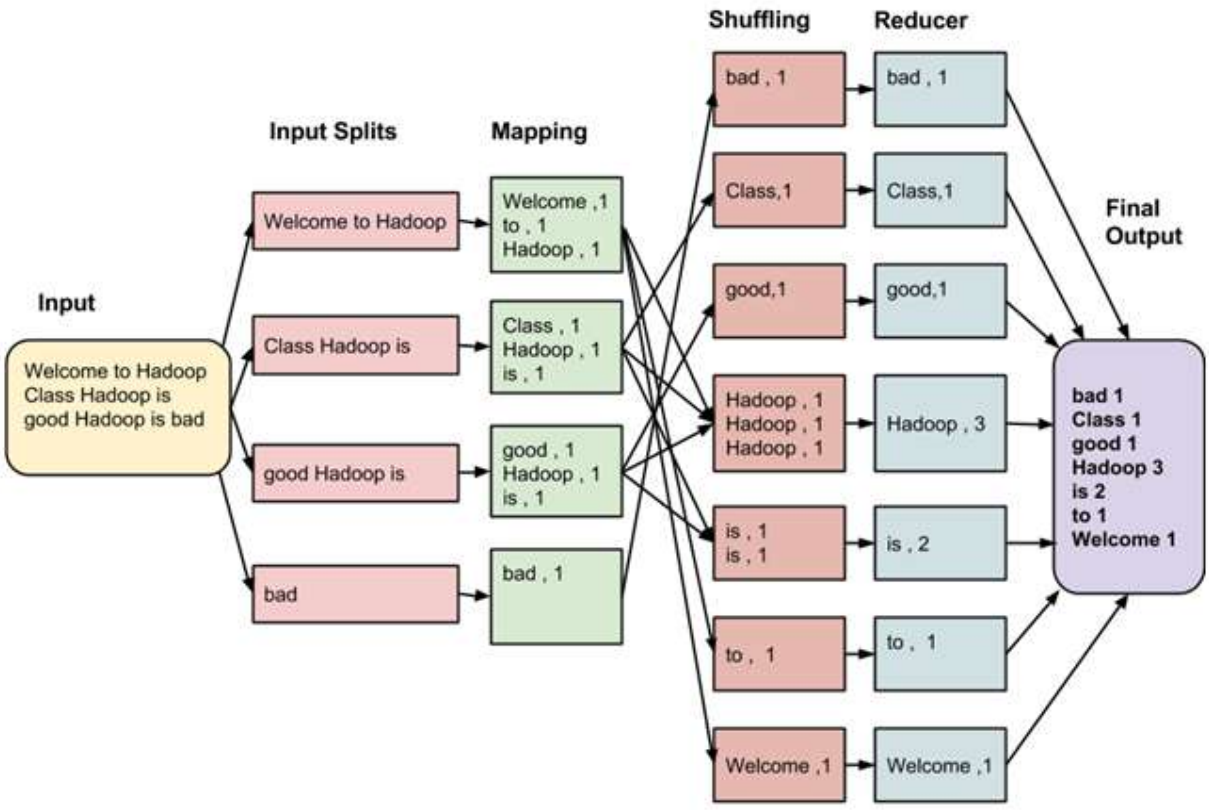
There is also one important component of Map Reduce Architecture known as **Job History Server**. The Job History Server is a daemon process that saves and stores historical information

about the task or application, like the logs which are generated during or after the job execution are stored on Job History Server.

EXAMPLE

Consider you have following input data for your MapReduce in Big data Program

Welcome to Hadoop Class
Hadoop is good
Hadoop is bad



MapReduce Architecture

The final output of the Map Reduce task is

bad	1
Class	1
good	1
Hadoop	3
is	2
to	1
Welcome	1

The data goes through the following phases of Map Reduce in Big Data

Input Splits:

An input to a Map Reduce in Big Data job is divided into fixed-size pieces called **input splits** Input split is a chunk of the input that is consumed by a single map

Mapping

This is the very first phase in the execution of map-reduce program. In this phase data in each split is passed to a mapping function to produce output values. In our example, a job of mapping phase is to count a number of occurrences of each word from input splits (more details about input-split is given below) and prepare a list in the form of <word, frequency>

Shuffling

This phase consumes the output of Mapping phase. Its task is to consolidate the relevant records from Mapping phase output. In our example, the same words are clubed together along with their respective frequency.

Reducing

In this phase, output values from the Shuffling phase are aggregated. This phase combines values from Shuffling phase and returns a single output value. In short, this phase summarizes the complete dataset.

In our example, this phase aggregates the values from Shuffling phase i.e., calculates total occurrences of each word.

Map Reduce Architecture explained in detail

- One map task is created for each split which then executes map function for each record in the split.
- It is always beneficial to have multiple splits because the time taken to process a split is small as compared to the time taken for processing of the whole input. When the splits are

smaller, the processing is better to load balanced since we are processing the splits in parallel.

- However, it is also not desirable to have splits too small in size. When splits are too small, the overload of managing the splits and map task creation begins to dominate the total job execution time.
- For most jobs, it is better to make a split size equal to the size of an HDFS block (which is 64 MB, by default).
- Execution of map tasks results into writing output to a local disk on the respective node and not to HDFS.
- Reason for choosing local disk over HDFS is, to avoid replication which takes place in case of HDFS store operation.
- Map output is intermediate output which is processed by reduce tasks to produce the final output.
- Once the job is complete, the map output can be thrown away. So, storing it in HDFS with replication becomes overkill.
- In the event of node failure, before the map output is consumed by the reduce task, Hadoop reruns the map task on another node and re-creates the map output.
- Reduce task doesn't work on the concept of data locality. An output of every map task is fed to the reduce task. Map output is transferred to the machine where reduce task is running.
- On this machine, the output is merged and then passed to the user-defined reduce function.
- Unlike the map output, reduce output is stored in HDFS (the first replica is stored on the local node and other replicas are stored on off-rack nodes). So, writing the reduce output

How Map Reduce Organizes Work?

Hadoop divides the job into tasks. There are two types of tasks:

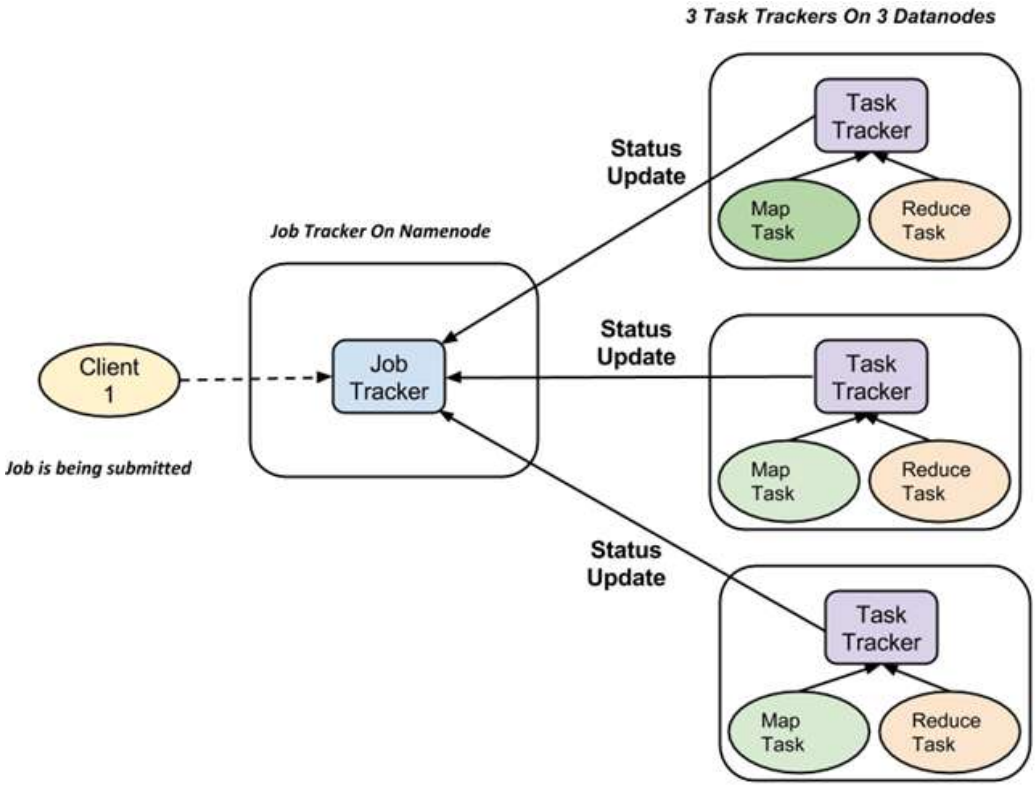
1. **Map tasks** (Splits & Mapping)
2. **Reduce tasks** (Shuffling, Reducing)

as mentioned above.

The complete execution process (execution of Map and Reduce tasks, both) is controlled by two types of entities called a

1. **Jobtracker**: Acts like a **master** (responsible for complete execution of submitted job)
2. **Multiple Task Trackers**: Acts like **slaves,** each of them performing the job

For every job submitted for execution in the system, there is one **Jobtracker** that resides on **Namenode** and there are **multiple tasktrackers** which reside on **Datanode**.



How Hadoop MapReduce Works

- A job is divided into multiple tasks which are then run onto multiple data nodes in a cluster.
- It is the responsibility of job tracker to coordinate the activity by scheduling tasks to run on different data nodes.
- Execution of individual task is then to look after by task tracker, which resides on every data node executing part of the job.
- Task tracker's responsibility is to send the progress report to the job tracker.
- In addition, task tracker periodically sends **'heartbeat'** signal to the Jobtracker so as to notify him of the current state of the system.
- Thus job tracker keeps track of the overall progress of each job. In the event of task failure, the job tracker can reschedule it on a different task tracker.

CLOUD GOVERNANCE

- It is the set of policies or principles that act as the guidance for the adoption use, and management of cloud technology services.
- It is an ongoing process that must sit on top of existing governance models.
- It is a set of rules you create to monitor and amend as necessary in order to control costs, improve efficiency, and eliminate security risks.

Need for Cloud Governance:

By implementing cloud governance, organizations can avoid the following issues as follows.

1. Security and privacy risks:

- This issue may arise due to unauthorized downloads/ installation of software, storage of illegal data, and access to restricted sites by users.
- Cloud Governance solutions cover multiple cloud security components. For example, Encryption, Security groups, Audit trails, Application access rules, Access controls.

2. Vendor lock-in:

- Many vendors opt for this, as this clause causes organizations to depend on the cloud service provider (or vendor) for products and services.
- This can be avoided by making changes to the SLA suitably and reduce dependencies on a single vendor, thus ensuring freedom to the organization.

3. Cloud Sprawl:

- This happens when employees of different departments use different programs and cloud infrastructure from third-party providers without involving the IT department and getting necessary approvals.
- If not detected and restricted, crowd sprawl may lead to fragmented, redundant, inefficient, and unmanaged cloud programs sitting on the enterprise cloud and unnecessarily creating trouble.

4. Shadow IT and unwarranted usage of cloud resources:

- This happens when employees in various departments do not follow the rules and regulations as imposed by the IT department on cloud usage resulting in security breaches and fragmented control throughout the organization.
- This leads to not getting sufficient results from the cloud in the long run.

5. Lack of data portability and interoperability:

- This happens when the cloud service provider or the inbuilt cloud infrastructure is incapable of connecting well with other software and products outside the organization.

- This may also lead to modules not compatible with each other and hence chaos in the cloud due to an inefficient system.

Cloud Governance Model Principles

The following five principles are a good starting point for building your cloud governance model:

1. **Compliance with policies and standards—**cloud usage standards must be consistent with regulations and compliance standards used by your organization and others in your industry.
2. **Alignment with business objectives**—cloud strategy should be an integral part of the overall business and IT strategy. All cloud systems and policies should demonstrably support business goals.
3. **Collaboration**—there should be clear agreements between owners and users of cloud infrastructure, and other stakeholders in the relevant organizational units, to ensure they make appropriate and mutually beneficial use of cloud resources.
4. **Change management**—all changes to a cloud environment must be implemented in a consistent and standardized manner, subject to the appropriate controls.
5. **Dynamic response**—cloud governance should rely on monitoring and cloud automation to dynamically respond to events in the cloud environment.

How to Design and Implement a Cloud Governance Framework

The following are the primary components of a cloud governance framework.

Components of a cloud governance framework

Cloud Financial Management

In many organizations, cloud costs quickly get out of hand. Cloud services often promise to reduce IT costs, but this only holds true if costs are duly managed. There are three elements of cloud financial management:

- **Financial policies** clarifying how the organization plans to use the cloud. For example, policies can define in which cases managed services should be used to reduce in-house operating costs, or specify a cost management checklist that must be followed before deploying new cloud services.
- **Budgets** define the specific allowance for different parts of the organization or different categories of cloud services.
- **Cost reporting** is difficult to achieve in a consistent way. Some cloud services have unpredictable charges that can appear in different places of the cloud infrastructure—for example, cloud snapshots used for backup can be stored across different regions and accounts. You can use cost reporting tools provided by the cloud vendor, or adopt third party tools that cover multiple clouds.

Cloud Operations Management

Operations management involves defining processes for deployment of services. These processes should include:

- A clear definition of resources allocated to the service over time
- Service-level agreements (SLAs) to define expected performance
- Ongoing monitoring to make sure SLAs are met
- Process and required checks before deploying code to production
- Access control requirements

Strong cloud operations management is an excellent way to prevent shadow IT. It can conserve costs by preventing unnecessary use of cloud resources, and can dramatically improve the return on investment of cloud expenditure in the long term.

Cloud Data Management

The cloud makes it easier to collect and analyze huge amounts of data, but this makes data management a much bigger challenge. Cloud governance should specify how to manage the entire data lifecycle in the cloud. This includes:

- Building a data classification scheme, and setting policies for data at different levels of sensitivity
- Ensuring all data is encrypted, at rest and in transit
- Putting in place appropriate access controls for each type of data
- Using data masking to reduce the risk of sensitive data when it is used for scenarios like development, testing, or training
- Developing a tiering strategy, moving data over time from high cost fast access systems to lower cost archival systems
- Ensuring that data lifecycle management is automated—this is critical to apply policies in large scale cloud deployments

Cloud Security and Compliance Management

Cloud governance takes responsibility for all the key topics of enterprise security. It determines what are the organization's security and compliance requirements, and ensuring they are enforced in the cloud environment:

- Risk assessment
- Identity and access management
- Data management and encryption
- Application security
- Disaster recovery

Cloud governance should strike a balance between business drivers and requirements, real security risks, and the requirements of compliance standards. It should use existing policies and security practices, extending them to the cloud and translating them to the cloud environment.

CLOUD LOAD BALANCING

- Cloud load balancing is the process of distributing workloads across computing resources in a cloud computing environment and carefully balancing the network traffic accessing those resources.
- Load balancing enables organizations to meet workload demands by routing incoming traffic to multiple servers, networks or other resources, while improving performance and protecting against disruptions in services.

- Load balancing also makes it possible to distribute workloads across two or more geographic regions.
- Cloud load balancing helps enterprises achieve high performance levels for potentially lower costs than traditional on-premises load balancing technology.
- Cloud load balancing takes advantage of the cloud's scalability and agility to meet the demands of distributed workloads with high numbers of client connections. It also improves overall availability, increases throughput and reduces latency.
- In addition to workload and traffic distribution, cloud load balancing services typically offer other features, such as application health checks, automatic scaling and failover and integrated certificate management.

Examples of cloud load balancing services

Many cloud providers offer load balancing services, including the three major platforms:

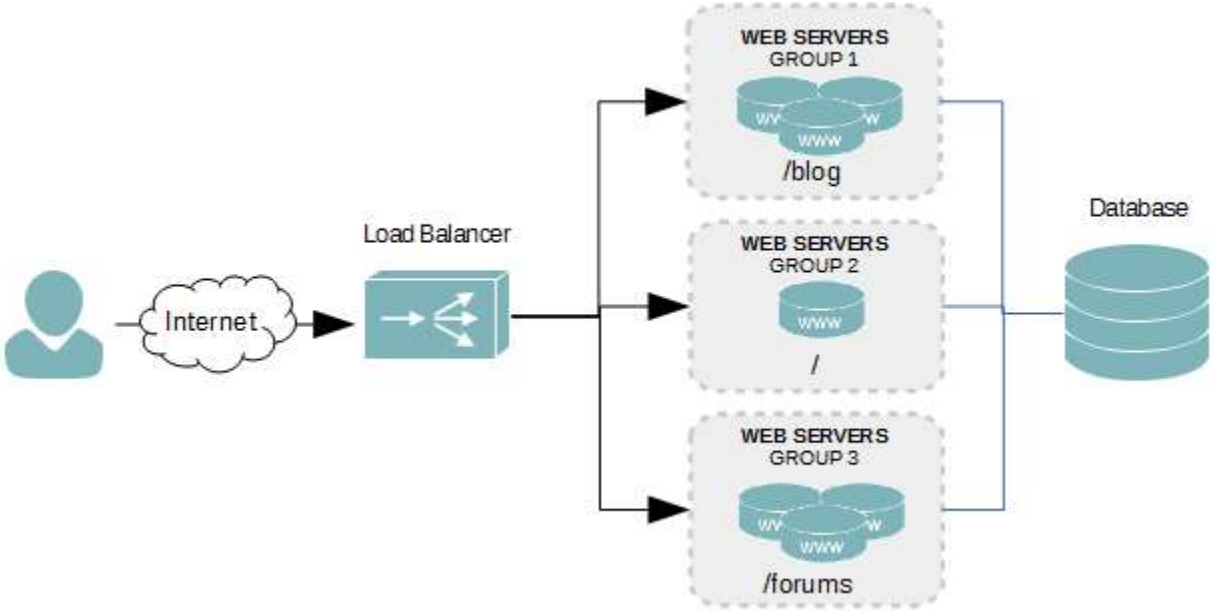
- Amazon Web Services (AWS) Elastic Load Balancing distributes incoming client traffic and routes it to registered targets such as EC2 instances. Elastic Load balancing supports four types of load balancers: Application, Network, Gateway and Classic. The load balancers differ in the features offered, the network layers at which they operate and supported communication protocols.
- The Cloud Load Balancing service available on Google Cloud Platform is built on the same front-end server infrastructure that powers Google. The service offers a range of load balancers that vary depending on whether the customer needs external or internal load balancing, global or regional load balancing, Premium or Standard network service tiers, proxy or pass-through services, among other factors.
- Microsoft Azure offers four load balancing services. Azure Traffic Manager is a (OSI model) layer 7 DNS-based traffic load balancer for delivering services across global Azure regions. Azure Load Balancer is a layer 4 network load balancer for routing traffic between VMs. Azure Application Gateway is a layer 7 delivery controller for regional applications. Azure Front Door is a highly secure, layer 7 global load balancer for microservice

Objectives of using load balancers are:

- To maintain system firmness.
- To improve system performance.
- To protect against system failures.

How does load balancing work?

- Here, load refers to not only the website traffic but also includes CPU load, network load and memory capacity of each server.
- A load balancing technique makes sure that each system in the network has same amount of work at any instant of time. This means neither any of them is excessively over-loaded, nor under-utilized.
- The load balancer distributes data depending upon how busy each server or node is. In the absence of a load balancer, the client must wait while his process gets processed, which might be too tiring and demotivating for him.
- Various information like jobs waiting in queue, CPU processing rate, job arrival rate etc. are exchanged between the processors during the load balancing process.
- Failure in the right application of load balancers can lead to serious consequences, data getting lost being one of them.



- Different companies may use different load balancers and multiple load balancing algorithms like static and dynamic load balancing. One of the most commonly used methods is **Round-robin load balancing.**
- It forwards client request to each connected server in turn. On reaching the end, the load balancer loops back and repeats the list again.
- The major benefit is its ease of implementation.
- The load balancers check the system heartbeats during set time intervals to verify whether each node is performing well or not.

Advantages of Cloud Load Balancing

a) High Performing applications

- Cloud load balancing techniques, unlike their traditional on-premise counterparts, are less expensive and simple to implement. Enterprises can make their client applications work faster and deliver better performances, that too at potentially lower costs.

b) Increased scalability

- Cloud balancing takes help of cloud's scalability and agility to maintain website traffic. By using efficient load balancers, you can easily match up the increased user traffic and distribute it among various servers or network devices.
- It is especially important for ecommerce websites, who deals with thousands of website visitors every second. During sale or other promotional offers they need such effective load balancers to distribute workloads.

c) Ability to handle sudden traffic spikes

- A normally running University site can completely go down during any result declaration. This is because too many requests can arrive at the same time. If they are using cloud load balancers, they do not need to worry about such traffic surges.
- No matter how large the request is, it can be wisely distributed among different servers for generating maximum results in less response time.

d) Business continuity with complete flexibility

- The basic objective of using a load balancer is to save or protect a website from sudden outages. When the workload is distributed among various servers or network units, even if one node fails the burden can be shifted to another active node.
- Thus, with increased redundancy, scalability and other features load balancing easily handles website or application traffic.

HIGH AVAILABILITY

- In simple words we can say that high availability refers to the availability of resources in a computer system.
- In terms of cloud computing it refers to the availability of cloud services.
- High availability is the heart of the cloud.
- It provides the idea of anywhere, anytime access to service of cloud environment.
- Availability is also related to reliability.
- Availability is a technology issue as well as business issue.

- High Availability can be simply defined by the simple equation:

$$HA = \frac{MTBF}{MTBF * MTTR}$$

Where, MTBF – mean time between failures, MTTR- means time to repair and HA- high availability.

- There is two way improve the availability:-
  - ✓ Increase MTBF to very large values.
  - ✓ Reduce MTTR to very low values.

DISASTER RECOVERY

- Disaster recovery (DR) is the process, policies and procedures that are related to preparing for recovery or continuation of technology infrastructure which are an organization after a natural or human-induced disaster.
- A disaster recovery is the process by which an organization can recover and access their software, data, and hardware.
- It is necessary for faster disasters recovery to have an infrastructure supporting high availability.
- The failure of disaster recovery plan mainly due to lack of high availability preparation, planning and maintenance to occurrence of the disaster.

Strategies of Disaster Recovery:

1. RTO (Recovery Time Objective):

- RTO is the period of time within which system, application, or functions must be discovered after an outage.
- RTOs are often used as the basis for the development of recovery strategies and as determinant as to whether or not to implement the recovery strategies during a disaster situation.

2. RPO (Recovery point objective):

- RPO is the point to time to which systems and data must be recovered after an outage.

- RPOs are often used as the basis for the development of backup strategies, and as a determinant of the amount of data that may need to be recreated after the systems or function have been recovered.

How is cloud disaster management working?

- Cloud disaster recovery is taking a much 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.

Selecting a Cloud disaster recovery provider

- When choosing a cloud disaster recovery provider, six factors must be considered:
    - ✓ Reliability
    - ✓ Location,
    - ✓ Security,
    - ✓ Compliance
    - ✓ Scalability.

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.

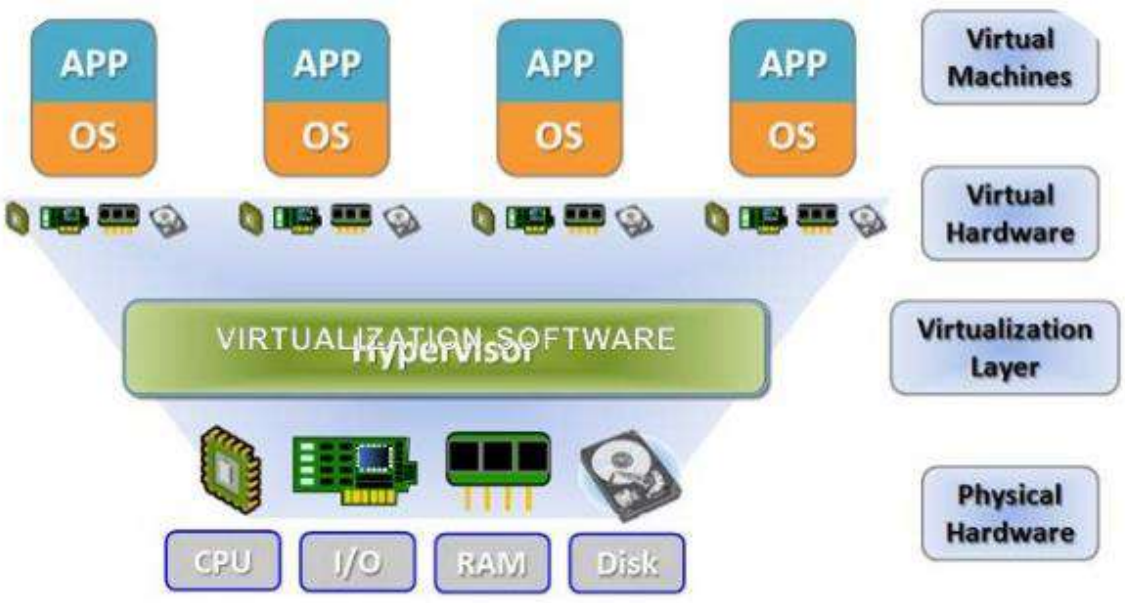
Testing is simple, and restoration is quick

- 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.

UNIT – 5 VIRTUALIZATION

VIRTUALIZATION

- **Virtualization** is a technique, which allows to share single physical instance of an application or resource among multiple organizations or tenants (customers). It does so by **assigning a logical name** to a physical resource and providing a **pointer to that physical resource** on demand.
- Creating a virtual machine over existing operating system and hardware is referred as Hardware Virtualization. Virtual Machines provide an environment that is logically separated from the underlying hardware.
- The machine on which the virtual machine is created is known as **host machine** and **virtual machine** is referred as a **guest machine.** This virtual machine is managed by a software or firmware, which is known as **hypervisor.**



Types of Virtualization:

1. Hardware Virtualization.
2. Operating system Virtualization.

3. Server Virtualization.
4. Storage Virtualization.

1) Hardware Virtualization:

- When the virtual machine software or virtual machine manager *(VMM) is directly installed on the hardware system* is known as hardware virtualization.
- The main job of hypervisor is to control and monitoring the processor, memory and other hardware resources.
- After virtualization of hardware system we can install different operating system on it and run different applications on those OS.

Usage:

- Hardware virtualization is mainly done for the server platforms, because controlling virtual machines is much easier than controlling a physical server.

2) Operating System Virtualization:

- When the virtual machine software or virtual machine manager *(VMM) is installed on the Host operating system* instead of directly on the hardware system is known as operating system virtualization.

Usage:

- Operating System Virtualization is mainly used for testing the applications on different platforms of OS.

3) Server Virtualization:

- When the virtual machine software or virtual machine manager *(VMM) is directly installed on the Server system* is known as server virtualization.

Usage:

- Server virtualization is done because a single physical server can be divided into multiple servers on the demand basis and for balancing the load.

4) Storage Virtualization:

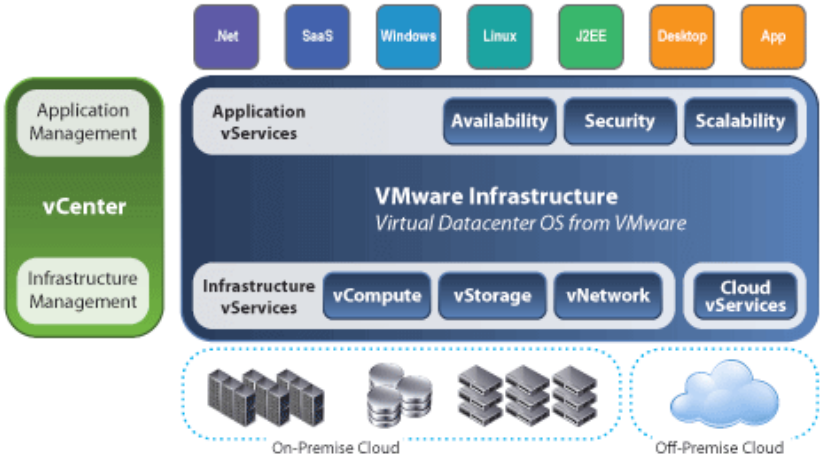
- Storage virtualization is the process of grouping the physical storage from multiple network storage devices so that it looks like a single storage device.
- Storage virtualization is also implemented by using software applications.

Usage:

- Storage virtualization is mainly done for back-up and recovery purposes.

How does virtualization work in cloud computing?

- **Virtualization** plays a very important role in the cloud computing technology, normally in the cloud computing, users share the data present in the clouds like application etc, but actually with the help of virtualization users shares the Infrastructure.
- The **main usage of Virtualization Technology** is to provide the applications with the standard versions to their cloud users, suppose if the next version of that application is released, then cloud provider has to provide the latest version to their cloud users and practically it is possible because it is more expensive.
- To overcome this problem we use basically virtualization technology, By using virtualization, all severs and the software application which are required by other cloud providers are maintained by the third party people, and the cloud providers has to pay the money on monthly or annual basis.



Characteristics of Virtualization

Resource Sharing.

- Virtualization enables users to create separate computing environments from one host machine–be it a single computer or a network of connected servers. This allows users to limit the number of active servers, reduce power consumption, and manage.

Isolation

- Virtualization software's self-contained VMs provide guest users (a designation that includes not only people but applications, OSs, and devices) with an isolated online environment. That separation protects sensitive information while also allowing guests to stay connected.

Availability

- Virtualization software offers several features you won't get with physical servers that help increase uptime, availability, fault tolerance, and more–helping users avoid downtime that undermines user productivity and introduces security threats and safety hazards.

Aggregation

- While virtualization allows multiple devices to share resources from a single machine, it can also be used to combine several devices into one powerful host.
- Aggregation requires cluster management software, which connects a homogeneous group of computers or servers together to create a unified resource center.

Reliability

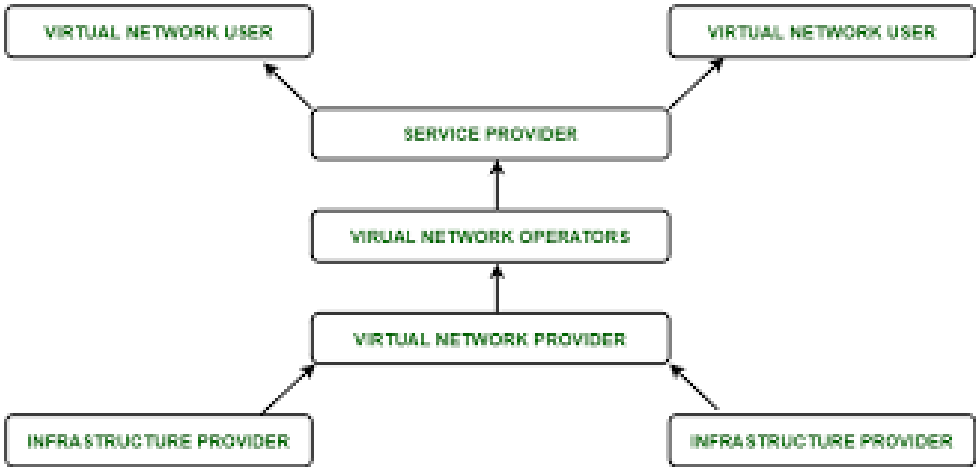
- These days, virtualization platforms ensure constant uptime via automated load balancing, which runs redundant servers on different host machines to prevent outages. That way, hardware failures are little more than a minor inconvenience. Do note that if downtime is a major concern, you might need to invest in some backup hardware to act as a fail-safe.

Benefits of virtualization

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

NETWORK VIRTUALIZATION

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



Functions of Network Virtualization:

- It enables the functional grouping of nodes in a virtual network.
- It enables the virtual network to share network resources.
- It allows communication between nodes in a virtual network without routing of frames.
- It restricts management traffic.
- It enforces routing for communication between virtual networks.

Network Virtualization in Virtual Data Center:

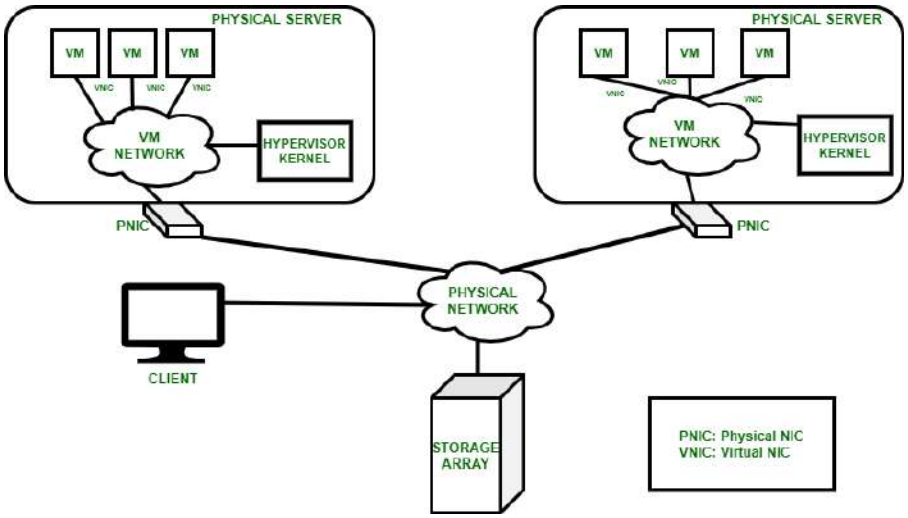
1. Physical Network

- Physical components: Network adapters, switches, bridges, repeaters, routers and hubs.
- Grants connectivity among physical servers running a hypervisor, between physical servers and storage systems and between physical servers and clients.

2. VM Network

- Consists of virtual switches.

- Provides connectivity to hypervisor kernel.
- Connects to the physical network.
- Resides inside the physical server.



Network Virtualization In VDC

Advantages of Network Virtualization:

Improves manageability

- Grouping and regrouping of nodes are eased.
- Configuration of VM is allowed from a centralized management workstation using management software.

Reduces CAPEX (Capital Expenditure)

- The requirement to set up separate physical networks for different node groups is reduced.

Improves utilization

- Multiple VMs are enabled to share the same physical network which enhances the utilization of network resource.

Enhances performance

- Network broadcast is restricted and VM performance is improved.

Enhances security

- Sensitive data is isolated from one VM to another VM.
- Access to nodes is restricted in a VM from another VM.

Disadvantages of Network Virtualization:

- It needs to manage IT in the abstract.
- It needs to coexist with physical devices in a cloud-integrated hybrid environment.
- Increased complexity.
- Upfront cost.
- Possible learning curve.

Examples of Network Virtualization:

Virtual LAN (VLAN)

- The performance and speed of busy networks can be improved by VLAN.
- VLAN can simplify additions or any changes to the network.

Network Overlays

- A framework is provided by an encapsulation protocol called VXLAN for overlaying virtualized layer 2 networks over layer 3 networks.
- The Generic Network Virtualization Encapsulation protocol (GENEVE) provides a new way to encapsulation designed to provide control-plane independence between the endpoints of the tunnel.

Network Virtualization Platform: VMware NSX (Network and Security Experts)

- VMware NSX Data Center transports the components of networking and security such as switching, firewalling and routing that are defined and consumed in software.
- It transports the operational model of a virtual machine (VM) for the network.

Applications of Network Virtualization:

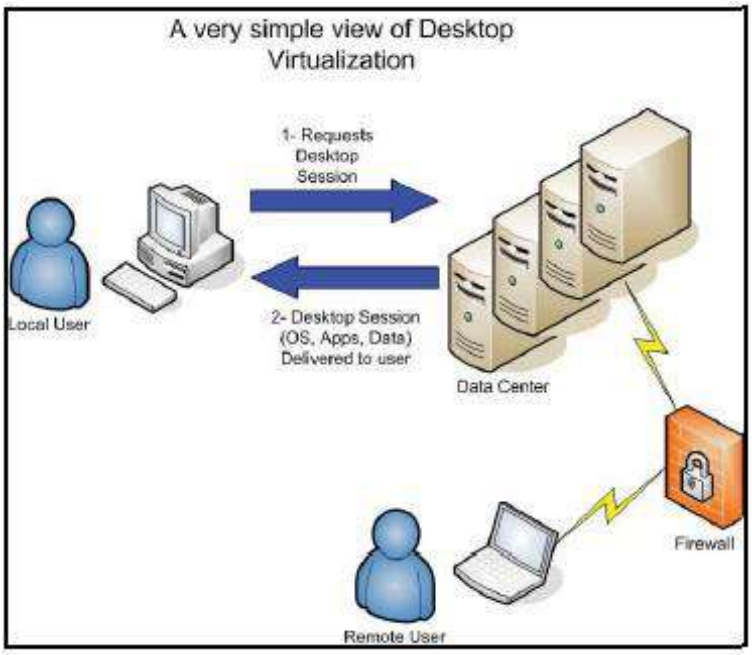
- Network virtualization may be used in the development of application testing to mimic real-world hardware and system software.
- It helps us to integrate several physical networks into a single network or separate single physical networks into multiple analytical networks.
- In the field of application performance engineering, network virtualization allows the simulation of connections between applications, services, dependencies, and end-users for software testing.
- It helps us to deploy applications in a quicker time frame, thereby supporting a faster go-to-market.
- Network virtualization helps the software testing teams to derive actual results with expected instances and congestion issues in a networked environment.

DESKTOP VIRTUALIZATION

- Desktop virtualization is technology that lets users simulate a workstation load to access a desktop from a connected device.
- It separates the desktop environment and its applications from the physical client device used to access it.
- Desktop virtualization is a key element of digital workspaces and depends on application virtualization.

How does desktop virtualization work?

- Desktop virtualization works by employing hardware virtualization technology. Virtual desktops exist as VMs, running on a virtualization host. These VMs share the host server's processing power, memory and other resources.
- Users typically run a remote desktop protocol (RDP) client to access the virtual desktop environment. This client attaches to a connection broker that links the user's session to a virtual desktop.
- Typically, virtual desktops are non-persistent, meaning the connection broker assigns the user a random virtual desktop from a virtual desktop pool. When the user logs out, this virtual desktop resets to a pristine, unchanged state and returns to the pool.
- However, some vendors offer an option to create persistent virtual desktops, in which users receive their own writable virtual desktop.



- Desktop virtualization can be achieved in a variety of ways, but the two most important types are based on whether the operating system instance is local or remote.

❖ **Local desktop virtualization**

- **Local desktop virtualization** means the operating system runs on a client device using hardware virtualization, and all processing and workloads occur on local hardware.
- This type of desktop virtualization works well when users do not need a continuous network connection and can meet application computing requirements with local system resources.
- However, because this requires processing to be done locally you cannot use local desktop virtualization to share VMs or resources across a network to thin clients or mobile devices.

❖ **Remote desktop virtualization**

- **Remote desktop virtualization** is a common use of virtualization that operates in a server computing environment.
- This allows users to run operating systems and applications from a server inside a datacenter while all user interactions take place on a client device such as a laptop, thin client, or smartphone.
- This type of virtualization gives IT more centralized control over applications and desktops, and can maximize an organization's investment in hardware through remote access to shared computing resources.

Benefits of Desktop Virtualization

1. **Flexibility**
    - Users can basically access their computer applications and data on any computing device, in any location worldwide, as long as they have internet access. As such, they do not need to be chained to their workplaces, or to rely on flash drives and email threads to transfer data from one place to another.
2. **Cost efficiency**
    - Desktop virtualization contributes major cost savings to businesses as it eliminates upfront capital expenses for equipment, extra personnel, hardware, storage, maintenance.
3. **Enhanced security**
    - Human error is the main reason that most security problems occur, not cloud infrastructures. Reliable desktop virtualization providers avail layers of cloud safeguards to protect one's data and eliminate threats, such as the highest quality encryptions, routers, switches, and continuous monitoring to ensure one's cloud remains safe.
4. **Environmentally Friendly**
    - Generally speaking, desktop virtualization augments an organization's ability to go green since it eliminates their need to purchase their own hardware. Thus, drastically reducing in-house energy usage and costs.
5. **Centralized management**
    - Desktop virtualization can benefit businesses by centralizing and simplifying computing resources management, including desktop control, data security, data control, backup, and disaster recovery.
6. **Disaster recovery**
    - With the full redundancy that desktop virtualization solutions provide, it's easier to recover data in case of a disaster. In practice, in case of system failure or catastrophic physical events, data centers can pick up from where you left off, and continue running as normal, thus minimal downtime.
7. **Increase Employee Productivity and Onboarding**
    - Releasing your employees from central workplaces doesn't mean compromising on important management functions like oversight and accountability. By using a DaaS,

controlling the access to data and applications no longer requires the scrutiny of hard networks and devices – it's possible to perform these tasks remotely

DESKTOP AS A SERVICE

- DaaS stands for Desktop as a Service.
- It is a cloud computing technology that lets users access the data and application through the internet from a centralized data server located remotely using a virtualized desktop.
- So, it is one type of desktop virtualization which is provided by third party hosts. DaaS is also known as a virtual desktop or hosted desktop service.

Example

- An organization lets its workforce work from home and soon it may be the future of IT work process. Now the organization is expected to support the workers to work on the projects by accessing the data in the organization from the devices the workforce are using, regardless of whether it's a laptop, tablet, or mobile phone.

- In this situation, the organization has to provide data in a centralized server so that all of the workers can access the data. This requirement can be satisfied by virtual desktop infrastructure(VDI).

- But setting up the virtual desktop infrastructure is too expensive and resource-consuming such as the need for servers, hardware, software, skilled staff to set up and maintain the VDI. This is when we need DaaS.
- DaaS helps people to access data and applications remotely with the help of the internet regardless of what devices they use to access. Desktop as a Service(DaaS) is cost-effective and ensures security and control.

Benefits of DaaS

- It is less expensive than setting up and maintaining the virtual desktop
- A new user can be added or an existing user can be removed rapidly, means it can be easily administered.
- It delivers high-performing workspaces to any user on any device from anywhere. These benefits become the reasons to choose DaaS over VDI.

Where can it be used ?

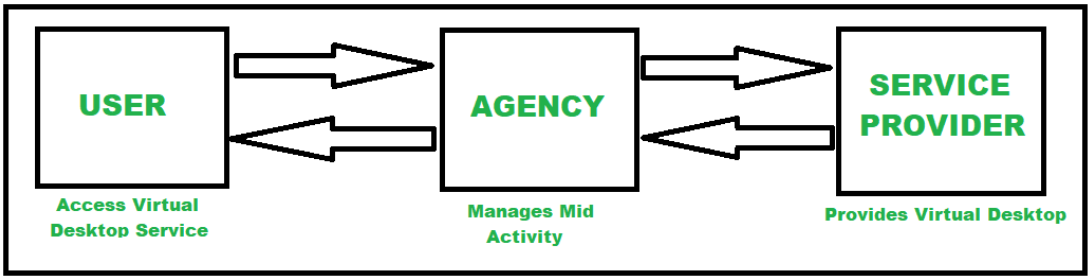
DaaS has a lot of use cases. It can be used by multiple platforms for multiple purposes.

1. Software developers
2. Call-center, part-time work
3. University lab
4. Remote and mobile workers
5. Shift and contract work

Work Process of DaaS :

- With DaaS, the service provider hosts infrastructure, network resources and storage in the cloud. Then the service provider streams the virtual desktop and the users can access the desktop data and applications through the internet.
- Because of this, users can access the graphics-intensive application seamlessly even though the users' devices usually can't run such a high-performance application without freezing and pixelating.
- The organization has total control and can add another user or revoke an existing user in a few taps.
- Security is high because the data is not stored on any local devices of users. All data is stored on a centralized data server. Even if a user's device falls into the wrong hands, access from the device to the data server can be denied instantly. Any security patches or updates can be done easily since they need to be done one time on the centralized server.
- Here, the service provider takes care of the backend management such as backup, updates and data storage. Users may only manage the security aspect of the services or the service provider will also handle it.

- The figure below represents the work process architecture.



The two types of desktops in DaaS are

1. Persistent desktop –

- In this type, the user can customize the looks of the virtual desktop and whenever the user logs back the details will remain the same.
- This needs more storage, so it's expensive.

2. Non-persistent desktop –

- The desktops are wiped off each time a user logs out and it just acts as a portal for shared cloud services.

Some DaaS Providers are:

There are multiple vendors in the market who provide virtual desktop services. Among them below are some demanding vendors –

1. Amazon Workspaces
2. Citrix Managed Desktops
3. Microsoft Windows Virtual Desktop
4. VMware Horizon Cloud
5. Evolve IP
6. Cloudalize Managed Desktops etc.

Advantages of DaaS :

- **Quick deployment and decommissioning of active end users –**
  DaaS can quickly give a service to the end user as well as it can revoke it faster also.
- **High cost savings –**
  It costs less to set up and maintain a virtual device infrastructure.
- **Easy user interface –**
  The interface is easy, a normal IT employee with usability skills can use it.

- **Increased device flexibility –**
  The number of users can be increased or decreased easily depending on the requirements.
- **Improved security –**
  It provides high security and reduces the fear of cyber-attacks and risks as it is a virtual service.

Disadvantages of DaaS :

- **Internet outage –**
  In case of an internet outage, employees may not be able to access their desktops as these desktops are hosted in the cloud and accessed over the internet.
- **Poor Virtual Performance –**
  Sometimes it may happen the end users will face poor virtual performance as it is accessed virtually, so any technical glitch cannot be avoided.

APPLICATION VIRTUALIZATION

- Application virtualization is technology that allows users to access and use an application from a separate computer than the one on which the application is installed. Using application virtualization software, IT admins can set up remote applications on a server and deliver the apps to an end user's computer. For the user, the experience of the virtualized app is the same as using the installed app on a physical machine.

How does application virtualization work?

- The most common way to virtualize applications is the server-based approach. This means an IT administrator implements remote applications on a server inside an organization's datacenter or via a hosting service.
- The IT admin then uses application virtualization software to deliver the applications to a user's desktop or other connected device.
- The user can then access and use the application as though it were locally installed on their machine, and the user's actions are conveyed back to the server to be executed.
- Application virtualization is an important part of digital workspaces and desktop virtualization.

Benefits of application virtualization

- **Simplified management:** Application virtualization makes it much easier for IT to manage and maintain applications across an organization. Rather than manually installing applications to every users' machine, app virtualization lets IT admins install an app once on a central server and then deploy the app as needed on user devices. In addition to saving installation time, this also makes it simpler to update or patch applications because IT only has to do so on a single server.
- **Scalability:** Application virtualization lets IT admins deploy virtual applications to all kinds of connected devices, regardless of those devices' operating systems or storage space. This allows thin client provisioning, where users access an application on a low-cost machine while centralized servers handle all the computing power necessary to run that application. As a result, the organization spends less on computing hardware because employees only require basic machines to access the apps they need for work. App virtualization also allows users to access applications that normally would not work on their machines' operating system, because the app is actually running on the centralized server. This is commonly used to virtually run a Windows application on a Linux operating system.
- **Security:** Application virtualization software gives IT admins central control over which users can access what applications. If a user's app permissions within an organization change, the IT admin can simply remove that user's access to an application. Without app virtualization, the IT admin would have to physically uninstall the app from the user's device. This central control over app access is especially important if a user's device is lost or stolen, because the IT admin can revoke remote access to sensitive data without having to track down the missing device.

SERVER VIRTUALIZATION

- Server Virtualization is the process of dividing a physical server into several virtual servers, called **virtual private servers**. Each virtual private server can run independently.
- The concept of Server Virtualization widely used in the IT infrastructure to minimizes the costs by increasing the utilization of existing resources.

Types of Server Virtualization

1. Hypervisor

- In the Server Virtualization, Hypervisor plays an important role. It is a layer between the operating system (OS) and hardware.
- . There are two types of hypervisors.
    - Type 1 hypervisor (also known as bare metal or native hypervisors)
    - Type 2 hypervisor (also known as hosted or Embedded hypervisors)
- The hypervisor is mainly used to perform various tasks such as allocate physical hardware resources (CPU, RAM, etc.) to several smaller independent virtual machines, called "**guest**" on the host machine.

2. Full Virtualization

- Full Virtualization uses a **hypervisor** to directly communicate with the CPU and physical server. It provides the best isolation and security mechanism to the virtual machines.
- The biggest disadvantage of using hypervisor in full virtualization is that a hypervisor has its own processing needs, so it can slow down the application and server performance.
- **VMWare ESX server** is the best example of full virtualization.

3. Para Virtualization

- Para Virtualization is quite similar to the Full Virtualization. The advantage of using this virtualization is that it is **easier to use**, **Enhanced performance**, and **does not require emulation overhead**. Xen primarily and UML use the Para Virtualization.
- The difference between full and pare virtualization is that, in para virtualization hypervisor does not need too much processing power to manage the OS.

4. Operating System Virtualization

- Operating system virtualization is also called as system-lever virtualization. It is a **server virtualization technology** that divides one operating system into multiple isolated user-space called **virtual environments**. The biggest advantage of using server visualization is that it reduces the use of physical space, so it will save money.
- **Linux OS Virtualization** and **Windows OS Virtualization** are the types of Operating System virtualization.

- **FreeVPS**, **OpenVZ**, and **Linux Vserver** are some examples of System-Level Virtualization.
- **OS-Level Virtualization never uses a hypervisor.**

5. Hardware Assisted Virtualization

- Hardware Assisted Virtualization was presented by **AMD and Intel**. It is also known as **Hardware virtualization**, **AMD virtualization**, and **Intel virtualization**. It is designed to increase the performance of the processor.
- The advantage of using Hardware Assisted Virtualization is that it requires less hypervisor overhead.

6. Kernel-Level Virtualization

- Kernel-level virtualization is one of the most important types of server virtualization. It is an **open-source virtualization** which uses the Linux
- Kernel as a hypervisor. The advantage of using kernel virtualization is that it does not require any special administrative software and has very less overhead.
- **User Mode Linux** (UML) and **Kernel-based virtual machine** are some examples of kernel virtualization.

Advantages of Server Virtualization

1. Independent Restart

- In Server Virtualization, each server can be restart independently and does not affect the working of other virtual servers.

2. Low Cost

- Server Virtualization can divide a single server into multiple virtual private servers, so it reduces the cost of hardware components.

3. Disaster Recovery

- Disaster Recovery is one of the best advantages of Server Virtualization. In Server Virtualization, data can easily and quickly move from one server to another and these data can be stored and retrieved from anywhere.

4. Faster deployment of resources

- Server virtualization allows us to deploy our resources in a simpler and faster way.

5. Security

- It allows uses to store their sensitive data inside the data centers.

Disadvantages of Server Virtualization

1. The biggest disadvantage of server virtualization is that when the server goes offline, all the websites that are hosted by the server will also go down.
2. There is no way to measure the performance of virtualized environments.
3. It requires a huge amount of RAM consumption.
4. It is difficult to set up and maintain.
5. Some core applications and databases are not supported virtualization.
6. It requires extra hardware resources.

Uses of Server Virtualization

- Server Virtualization is used in the testing and development environment.
- It improves the availability of servers.
- It allows organizations to make efficient use of resources.
- It reduces redundancy without purchasing additional hardware components.

STORAGE VIRTUALIZATION

- Storage virtualization is a major component for storage servers, in the form of functional RAID (**Redundant Array of Independent Disks)** levels and controllers. Operating systems and applications with device can access the disks directly by themselves for writing. The controllers configure the local storage in RAID groups and present the storage to the operating system depending upon the configuration. However, the storage is abstracted and the controller is determining how to write the data or retrieve the requested data for the operating system.

Storage virtualization is becoming more and more important in various other forms:

File servers:

- The operating system writes the data to a remote location with no need to understand how to write to the physical media.

WAN Accelerators:

- Instead of sending multiple copies of the same data over the WAN environment, WAN accelerators will cache the data locally and present the re-requested blocks at LAN speed, while not impacting the WAN performance.

SAN and NAS:

- Storage is presented over the Ethernet network of the operating system. NAS(**Network-attached storage)** presents the storage as file operations (like NFS). SAN technologies present the storage as block level storage (like Fibre Channel). SAN technologies receive the operating instructions only when if the storage was a locally attached device.

Storage Tiering:

- Utilizing the storage pool concept as a stepping stone, storage tiering analyze the most commonly used data and places it on the highest performing storage pool. The lowest one used data is placed on the weakest performing storage pool.
- This operation is done automatically without any interruption of service to the data consumer.

Block and File level Storage Virtualization

Block-level Storage

- Block level storage or block storage is storage used for structured data and is commonly deployed in storage area network systems.
- In **block-level storage**, a storage device such as a hard disk drive (HDD) is identified as something called a storage *volume*. A storage volume can be treated as an individual drive, a “block”. This gives a server's operating system the ability to have access to the raw storage sections. The storage blocks can be modified by an administrator, adding more capacity when necessary, which makes block storage fast, flexible, and reliable.

  Note: Depending on the operating system used, storage volumes may be referred to with a different name. For example, Linux refers to storage volumes as *physical volumes*.
- It uses internet small computer systems interface (ISCSI) & fiber channel (FC) protocols.

Block-level Storage Architecture

- Block storage uses blocks, which are a set sequence of bytes to store structured workloads. Each block is assigned a unique hash value which functions as an address. In

block storage the data is stored without any metadata e.g. data format, type, ownership etc.

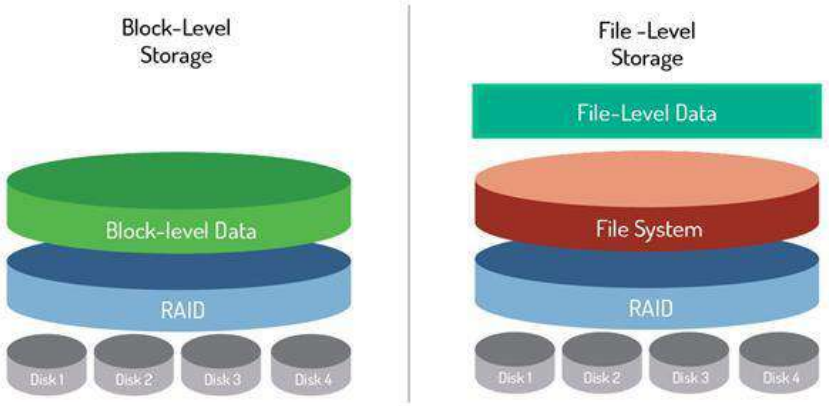
- The ability to store data in blocks deliver structured workloads such as databases, applications etc. the freedom to decide how blocks are accessed, combined or modified. Consequently this makes block storage faster than other storage.

File-level storage

- File level storage or file storage is storage used for unstructured data and is commonly deployed in network attached storage (NAS) systems.
- **File-level storage** is a type of storage that has a file system installed directly onto it where the storage volumes appear as a hierarchy of files to the server, rather than blocks.
- This is different from block type storage, which doesn't have a default file system and needs to have an administrator create one in order for non-administrator users to navigate and find data.
- It uses Network File System (NFS) for Linux and Common Internet File System (CIFS) or Server Message Block (SMB) protocols for windows.

File-level storage architecture

- File storage as opposed to block storage stores data in a hierarchical architecture as such that the data and its metadata are stored as is in the form of files & folders.
- Consequently the stored data appears in a similar fashion to both systems, the one writing it and the one reading it.



Advantages of Storage Virtualization

1. Data is stored in the more convenient locations away from the specific host. In the case of a host failure, the data is not compromised necessarily.
2. The storage devices can perform advanced functions like replication, reduplication, and disaster recovery functionality.
3. By doing abstraction of the storage level, IT operations become more flexible in how storage is provided, partitioned, and protected.

VIRTUAL MACHINE MONITOR

- A Virtual Machine Monitor (VMM) is a software program that enables the creation, management and governance of virtual machines (VM) and manages the operation of a virtualized environment on top of a physical host machine.
- VMM is also known as Virtual Machine Manager and Hypervisor.

Benefits of hypervisors

There are several benefits to using a hypervisor that hosts multiple virtual machines:

Speed:

- Hypervisors allow virtual machines to be created instantly, unlike bare-metal servers. This makes it easier to provision resources as needed for dynamic workloads.

Efficiency:

- Hypervisors that run several virtual machines on one physical machine's resources also allow for more efficient utilization of one physical server. It is more cost- and energy-efficient to run several virtual machines on one physical machine than to run multiple underutilized physical machines for the same task.

Flexibility:

- Bare-metal hypervisors allow operating systems and their associated applications to run on a variety of hardware types because the hypervisor separates the OS from the underlying hardware, so the software no longer relies on specific hardware devices or drivers.

Portability:

- Hypervisors allow multiple operating systems to reside on the same physical server (host machine). Because the virtual machines that the hypervisor runs are independent from the physical machine, they are portable. IT teams can shift workloads and allocate

networking, memory, storage and processing resources across multiple servers as needed, moving from machine to machine or platform to platform. When an application needs more processing power, the virtualization software allows it to seamlessly access additional machines.

Why use a hypervisor?

Hypervisors make it possible to use more of a system's available resources and provide greater IT mobility since the guest VMs are independent of the host hardware. This means they can be easily moved between different servers. Because multiple virtual machines can run off of one physical server with a hypervisor, a hypervisor reduces:

- Space
- Energy
- Maintenance requirements

Types of Hypervisor

TYPE-1 Hypervisor:

- The hypervisor runs directly on the underlying host system. It is also known as "Native Hypervisor" or "Bare metal hypervisor". It does not require any base server operating system. It has direct access to hardware resources.
- Examples of Type 1 hypervisors include VMware ESXi, Citrix XenServer and Microsoft Hyper-V hypervisor.

Pros & Cons of Type-1 Hypervisor:

Pros: Such kind of hypervisors are very efficient because they have direct access to the physical hardware resources(like Cpu, Memory, Network, Physical storage). This causes the empowerment the security because there is nothing any kind of the third party resource so that attacker couldn't compromise with anything.

Cons: One problem with Type-1 hypervisor is that they usually need a dedicated separate machine to perform its operation and to instruct different VMs and control the host hardware resources.

TYPE-2 Hypervisor:

- A Host operating system runs on the underlying host system. It is also known as 'Hosted Hypervisor". Such kind of hypervisors doesn't run directly over the underlying hardware rather they run as an application in a Host system(physical machine). Basically, software installed on an operating system. Hypervisor asks the operating system to make hardware calls.
- Example of Type 2 hypervisor includes VMware Player or Parallels Desktop. Hosted hypervisors are often found on endpoints like PCs.
- The type-2 hypervisor is are very useful for engineers, security analyst(for checking malware, or malicious source code and newly developed applications).

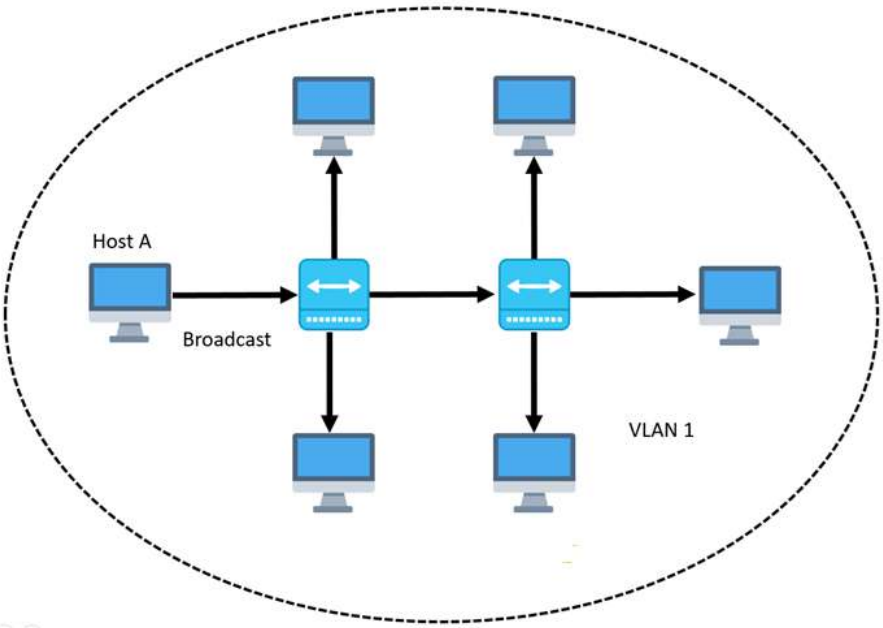
Pros & Cons of Type-2 Hypervisor:

Pros: Such kind of hypervisors allows quick and easy access to a guest Operating System alongside the host machine running. These hypervisors usually come with additional useful features for guest machine. Such tools enhance the coordination between the host machine and guest machine.

Cons: Here there is no direct access to the physical hardware resources so the efficiency of these hypervisors lags in performance as compared to the type-1 hypervisors, and potential security risks are also there an attacker can compromise the security weakness if there is access to the host operating system so he can also access the guest operating system.

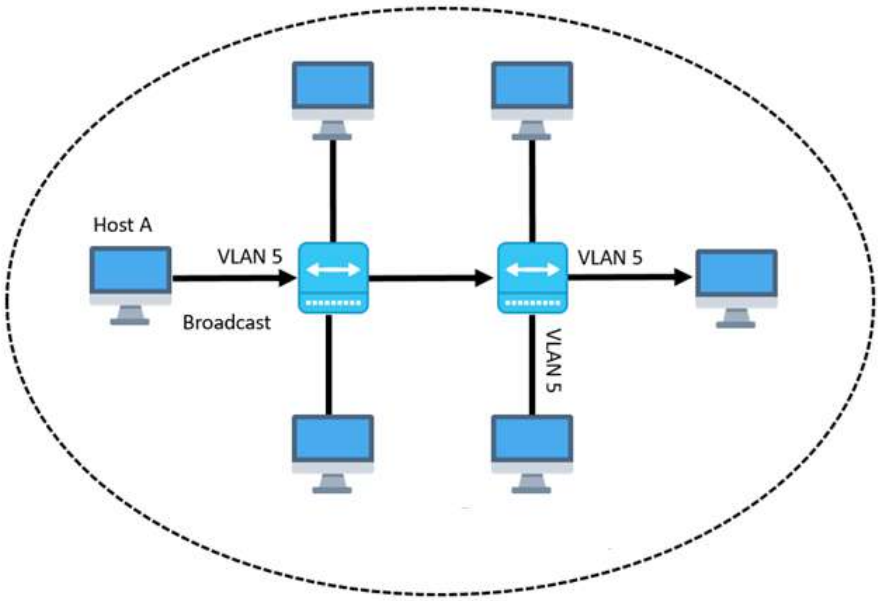
VLAN

- Virtual Local Area Network, commonly abbreviated as **VLAN**.
- **VLAN** is a custom network which is created from one or more local area networks. It enables a group of devices available in multiple networks to be combined into one logical network. The result becomes a virtual LAN that is administered like a physical LAN.
- The below topology depicts a network having all hosts inside the same virtual LAN:



Network having all hosts inside the same VLAN

- Without VLANs, a broadcast sent from a host can easily reach all network devices. Each and every device will process broadcast received frames. It can increase the CPU overhead on each device and reduce the overall network security.
- In case if you place interfaces on both switches into separate VLAN, a broadcast from host A can reach only devices available inside the same VLAN. Hosts of VLANs will not even be aware that the communication took place. This is shown in the below picture:



Host A can reach only devices available inside the same VLAN

- VLAN in networking is a virtual extension of LAN. A LAN is a group of computer and peripheral devices which are connected in a limited area such as school, laboratory, home, and office building. It is a widely useful network for sharing resources like files, printers, games, and other applications.

How VLAN works

- VLANs in networking are identified by a number.
- A Valid range is 1-4094. On a VLAN switch, you assign ports with the proper VLAN number.
- The switch then allows data which needs to be sent between various ports having the same VLAN.
- Since almost all networks are larger than a single switch, there should be a way to send traffic between two switches.
- One simple and easy way to do this is to assign a port on each network switch with a VLAN and run a cable between them.

VLAN Ranges

Range	Description
VLAN 0-4095	Reserved VLAN, which cannot be seen or used.
VLAN 1:	This is a default VLAN of switches. You cannot delete or edit this VLAN, but it can be used.
VLAN 2-1001:	It is a normal VLAN range. You can create, edit, and delete it.
VLAN 1002-1005:	These ranges are CISCO defaults for token rings and FDDI. You cannot delete this VLAN.
VLAN 1006-4094:	It is an extended range of VLANs.

Example of VLAN

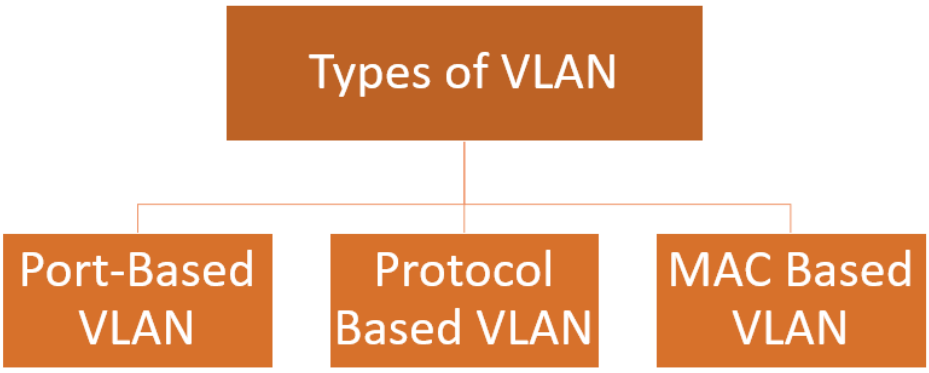
- In the below example, there are 6 hosts on 6 switches having different VLANs. You need 6 ports to connect switches together. It means, if you have 24 various VLANs, you will have only 24 hosts on 45 port switches.

Example of VLAN

Characteristics of VLAN

- Virtual LANs offer structure for making groups of devices, even if their networks are different.
- It increases the broadcast domains possible in a LAN.
- Implementing VLANs reduces the security risks as the number of hosts which are connected to the broadcast domain decreases.
- This is performed by configuring a separate virtual LAN for only the hosts having sensitive information.
- It has a flexible networking model that groups users depending on their departments instead of network location.
- Changing hosts/users on a VLAN is relatively easy. It just needs a new port-level configuration.
- It can reduce congestion by sharing traffic as individual VLAN works as a separate LAN.
- A workstation can be used with full bandwidth at each port.
- Terminal reallocations become easy.
- A VLAN can span multiple switches.
- The link of the trunk can carry traffic for multiple LANs.

Types of VLANs



Types of VLAN

Port-Based VLAN

- Port-based VLANs groups virtual local area network by port. In this type of virtual LAN, a switch port can be configured manually to a member of VLAN.
- Devices that are connected to this port will belong to the same broadcast domain that is because all other ports are configured with a similar VLAN number.
- The challenge of this type of network is to know which ports are appropriate to each VLAN. The VLAN membership can't be known just by looking at the physical port of a switch. You can determine it by checking the configuration information.

Protocol Based VLAN

- This type of VLAN processes traffic based on a protocol that can be used to define filtering criteria for tags, which are untagged packets.
- In this Virtual Local Area Network, the layer-3 protocol is carried by the frame to determine VLAN membership. It works in multi-protocol environments. This method is not practical in a predominately IP based network.

MAC Based VLAN

- MAC Based VLAN allows incoming untagged packets to be assigned virtual LAN and, thereby, classify traffic depending on the packet source address. You define a Mac address to VLAN mapping by configuring mapping the entry in MAC to the VLAN table.
- This entry is specified using source Mac address proper VLAN ID. The configurations of tables are shared among all device ports.

Advantages of VLAN

- It solves a broadcast problem.
- VLAN reduces the size of broadcast domains.
- VLAN allows you to add an additional layer of security.
- It can make device management simple and easier.
- You can make a logical grouping of devices by function rather than location.
- It allows you to create groups of logically connected devices that act like they are on their own network.
- You can logically segment networks based on departments, project teams, or functions.
- VLAN helps you to geographically structure your network to support the growing companies.
- Higher performance and reduced latency.
- VLANs provide increased performance.
- Users may work on sensitive information that must not be viewed by other users.
- VLAN removes the physical boundary.
- It lets you easily segment your network.
- It helps you to enhance network security.
- You can keep hosts separated by VLAN.
- You do not require additional hardware and cabling, which helps you to saves costs.
- It has operational advantages because of changing the IP subnet of the user is in software.
- It reduces the number of devices for particular network topology.
- VLAN makes managing physical devices less complex.

Disadvantages of VLAN

- A packet can leak from one VLAN to other.
- An injected packet may lead to a cyber-attack.
- Threat in a single system may spread a virus through a whole logical network.
- You require an additional router to control the workload in large networks.
- You can face problems in interoperability.
- A VLAN cannot forward network traffic to other VLANs.

Application/Purpose of VLAN

- VLAN is used when you have 200+ devices on your LAN.
- It is helpful when you have a lot of traffic on a LAN.
- VLAN is ideal when a group of users need more security or being slow down by many broadcasts.
- It is used when users are not on one broadcast domain.
- Make a single switch into multiple switches.

VSAN (Virtual Storage Area Network)

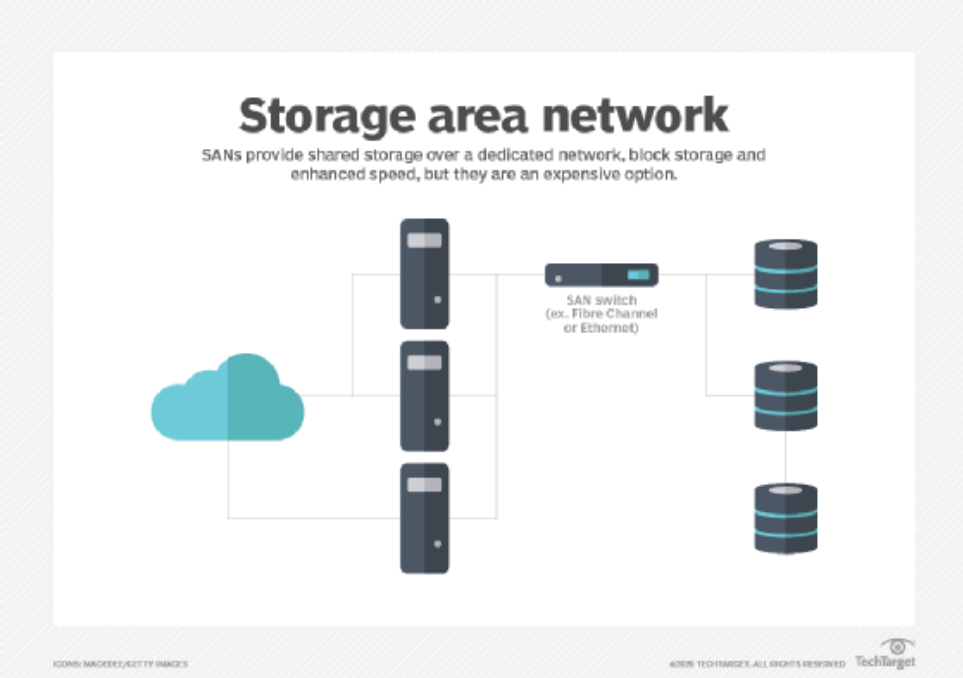
- A virtual storage area network (VSAN) is a logical partition in a physical storage area network (SAN). VSANs enable traffic to be isolated within specific portions of a storage area network, so if a problem occurs in one logical partition, it can be handled with a minimum of disruption to the rest of the network.
- The use of multiple, isolated VSANs can also make a storage system easier to configure and scale out. Subscribers can be added or relocated without needing to change the physical layout.

How VSAN works

- A virtual SAN appliance enables unused storage capacity on virtual servers to be pooled and accessed by virtual servers as needed.

- A virtual SAN appliance is most often downloaded as a software program that runs on a virtual machine, but some storage hardware vendors are beginning to incorporate virtual SAN appliances into their firmware.

- Depending on the vendor, a virtual SAN appliance might also be called a software-defined storage (SDS) appliance or, simply, a virtual storage appliance.



A physical storage area network consists of a fabric layer, host layer, SAN switches and a storage layer.

Benefits of Virtual Storage Area Networks

- **Non-disruptive data migration.** A VSAN enables adopters to migrate data between drives easily and without any downtime.
- **Better information lifecycle management.** Virtualization administrators can relocate frequently accessed data to high-performance storage, pushing rarely accessed data regions onto less expensive storage resources.
- **Improved manageability.** Although it's relatively easy to manage identical drives, the task can become much more difficult if storage resources involve several vendors or even several models from the same vendor. A VSAN isn't only easy to set up, but straightforward to manage and provision.
- **Overall simplicity.** Compared to the available alternatives, a VSAN is easy to provision and manage. This is because the VSAN is embedded directly within the hypervisor, enabling installation and configuration to be handled rapidly and
- **Reduced total cost of ownership.** A VSAN can be deployed on inexpensive x86 servers, eliminating the need for large upfront investments.

Difference between VLAN & VSAN

S.No.	VLAN(Virtual Local Area Network)	VSAN(Virtual Storage Area Network)
1	VLAN is a network technology used to logically separate large broadcast domains using layer 2 devices.	VSAN is a logical partition in a storage area network.
2	It divides the network into different virtual sub-networks reduces unnecessary traffic and improve performance.	VSANs allow traffic to be isolated within specific portions of a storage area network.
3	VLANs are implemented to achieve scalability, security and ease of network management.	The use of multiple VSAN's can make a system easier to configure and scale out.
4	VLAN's can quickly adapt to change in network requirements and relocation of workstations and server nodes.	In this subscribers can be added or relocated without the need for changing the physical layout.
5	The purpose of implementing a VLAN is to improve the performance of a network or apply appropriate security features.	The VSANs minimizes the total system's vulnerability, security is improved. VSANs also offer the possibility of data redundancy, minimizing the risk of catastrophic data loss.

UNIT – 6 CLOUD SECURITY

CLOUD SECURITY

Cloud security is the set of control-based security measures and technology protection, designed to protect online stored resources from **leakage, theft**, and **data loss**. Protection includes data from **cloud infrastructure, applications**, and **threats.** Security applications uses a software the same as **SaaS (Software as a Service)** model.

How to Manage Security in the Cloud?

Cloud service providers have many methods to protect the data.

- Firewall is the central part of cloud architecture. The firewall protects the network and the perimeter of end-users. It also protects traffic between various apps stored in the cloud.
- Access control protects data by allowing us to set access lists for various assets. For example, you can allow the application of **specific employees** while restricting others. It's a rule that employees can access the equipment that they required. We can keep essential documents which are stolen from **malicious insiders** or hackers to maintaining strict access control.
- Data protection methods include Virtual Private Networks (**VPN**), encryption, or masking. It allows remote employees to connect the network. VPNaccommodates the tablets and smartphone for remote access. Data masking maintains the data's integrity by keeping identifiable information private. A medical company share data with data masking without violating the **HIPAA** laws.
- For example, we are putting intelligence information at risk in order of the importance of security. It helps to protect mission-critical assets from threats. Disaster recovery is vital for security because it helps to recover lost or stolen data.

Benefits of Cloud Security System

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.

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.

Cloud Computing Attacks

- **Denial of service (DoS) attacks**
    - Some security professionals have argued that the cloud is more vulnerable to DoS attacks, because it is shared by many users, which makes DoS attacks much more damaging.
    - Twitter suffered a devastating DoS attack during 2009.
- **Side channel attacks**
    - An attacker could attempt to compromise the cloud by placing a malicious virtual machine in close proximity to a target cloud server & then launching a side channel attack.
- **Authentication attacks**

- Authentication is a weak point in hosted & virtual services & is frequently targeted. There are many different ways to authenticate users; for ex: based on what a person knows, has, or is.
- The mechanisms used to secure the authentication process & the methods used are a frequent target of attackers.

❖ **Man in the middle cryptographic attacks**

- This attack is carried out when an attacker places himself between two users.
- Anytime attackers can place themselves in the communication's path, there is the possibility that they can intercept and modify communications.

CLOUD SECURITY SERVICES

❖ **Authentication**

- Authentication is the testing or reconciliation of evidence of a user's identity. It establishes the user's identity & ensures that users are who they claim to be.
- For example, a user presents an identity to a computer login screen and then has to provide a password. The computer system authenticates the user by verifying that the password corresponds to the individual presenting the ID.

❖ **Authorization**

- Authorization refers to right & privileges granted to an individual or processes that enable access to computer resources & information assets.
- Once the user's identity & authentication are established, authorization levels determine the extent of system rights a user can hold.

❖ **Auditing**

- To maintain operational assurance , organizations use two basic methods:
  - ✓ **System audits:** A system audit is a one-time or periodic event to evaluate security.
  - ✓ **Monitoring:** Monitoring refers to an ongoing activity that examines either the system or the users, such as intrusion detection.
- These methods can be employed by the cloud customer, the cloud provider or both, depending on asset architecture & deployment.
- Information technology (IT) auditors are often divided into two types :
  - ✓ Internal: Internal auditors typically work for a given organization, whereas external auditors do not.

- ✓ External: External auditors are often certified public accountants (CPAs) or other audit professionals who are hired to perform an independent audit of an organization's financial statements.

- IT auditors typically audit the following functions:
  - ✓ System & transaction controls
  - ✓ Systems development standards
  - ✓ Backup controls
  - ✓ Data library procedures
  - ✓ Data center security
  - ✓ Contingency plans
- An audit trail or log is a set of records that collectively provide documentary evidence of processing, used to aid in tracing from original transactions forward to related records & reports and/or backward from records & reports to their component source transactions.
- Audit logs should record the following:
  - ✓ The transaction's date & time
  - ✓ Who processed the transaction
  - ✓ At which terminal the transaction was processed
  - ✓ Various security events relating to the transaction

❖ **Accountability**

- Accountability is the ability to determine the actions & behaviors of a single individual within a cloud system & to identify that particular individual.
- Audit trails & logs support accountability and can be used to conduct postmortem studies in order to analyze historical events and the individuals or processes associated with those events.
- Accountability is related to the concept of nonrepudiation, wherein an individual cannot successfully deny the performance of an action.

DESIGN PRINCIPLES

❖ **Implement a strong identity foundation**

- Implement the principle of least privilege and enforce separation of duties with the appropriate authorization for each interaction with your AWS resources.

- Centralize privilege management and reduce or even eliminate reliance on long-term credentials.

❖ **Enable traceability**

- Monitor, alert, and audit actions and changes to your environment in real-time. Integrate logs and metrics with systems to automatically respond and take action.

❖ **Apply security at all layers**

- Rather than just focusing on protecting a single outer layer, apply a defense-in-depth approach with other security controls.
- Apply to all layers, for example, edge network, virtual private cloud (VPC), subnet, load balancer, every instance, operating system, and application.

❖ **Automate security best practices**

- Automated software-based security mechanisms improve your ability to securely scale more rapidly and cost-effectively.
- Create secure architectures, including the implementation of controls that are defined and managed as code in version-controlled templates.

❖ **Protect data in transit and at rest**

- Classify your data into sensitivity levels and use mechanisms, such as encryption and tokenization where appropriate.
- Reduce or eliminate direct human access to data to reduce the risk of loss or modification.

❖ **Prepare for security events**

- Prepare for an incident by having an incident management process that aligns with your organizational requirements.
- Run incident response simulations and use tools with automation to increase your speed for detection, investigation, and recovery.

SECURE CLOUD SOFTWARE REQUIREMENTS

- The requirements for secure cloud software are concerned with nonfunctional issues such as minimizing or eliminating vulnerabilities & ensuring that the software will perform as required, even under attack.
- This goal is distinct from security functionality in software which address areas that derive from the information security policy, such as identification, authentication & authorization.

- Software requirements engineering is the process of determining customer software expectations & needs &it is conducted before the software design phase.
- The requirements have to be unambiguous, correct, quantifiable & detailed.
- United States Department Of Defense Data & Analysis Center For Software (DACS) states that all software share the following three security needs:
    - ✓ It must be dependable under anticipated operating conditions, & remain dependable under hostile operating conditions.
    - ✓ It must be trustworthy in its own behavior & in its inability to be compromised by an attacker through exploitation of vulnerabilities or insertion of malicious code.
    - ✓ It must be resilient enough to recover quickly to full operational capability with a minimum of damage to itself , the resources & data it handles , & the external components with which it interacts.

POLICY IMPLEMENTATION

- A policy is one of those terms that can mean several things. For ex, there are security policies on firewalls, which refer to the access control & routing list information.
- Standards, procedures & guidelines are also referred to as policies in the larger sense of a global information security policy.
- A policy can also provide protection from liability due to an employee's actions, or it can control access to trade secrets.

Policy Types

- ❖ **Senior management statement of policy**
    - The first policy of any policy creation process is the senior management statement of policy.
    - This is a general, high level policy that acknowledges the importance of the computing resources to the business model; states support for information security throughout the enterprise; and commits to authorizing and managing the definition of the lower level standards, procedures & guidelines.
- ❖ **Regulatory policies**
    - Regulatory policies are security policies that an organization must implement due to compliance, regulation, or other legal requirements.
    - These companies might be financial institutions, public utilities, or some other type of organization that operates in the public interest.

- Such policies are usually very detailed and specific to the industry in which the organization operates.

❖ **Advisory policies**

- Advisory policies are security policies that are not mandated but strongly suggested, perhaps with serious consequences defined for failure to follow them.
- A company with such policies wants most employees to consider these policies mandatory. Most policies fall under this category.

❖ **Informative policies**

- Informative policies are policies that exist simply to inform the reader. There are not implied or specified requirements and the audience for this information could be certain internal or external parties.
- This does not mean that the policies are authorized for public consumption but that they are general enough to be distributed to external parties without a loss of confidentiality.

CLOUD COMPUTING SECURITY CHALLENGES

1. Data Security and Privacy

- Data security is a major concern when switching to cloud computing. User or organizational data stored in the cloud is critical and private. Even if the cloud service provider assures data integrity, it is your responsibility to carry out user authentication and authorization, identity management, data encryption, and access control.
- Security issues on the cloud include identity theft, data breaches, malware infections, and a lot more which eventually decrease the trust amongst the users of your applications. This can in turn lead to potential loss in revenue alongside reputation and stature. Also, dealing with cloud computing requires sending and receiving huge amounts of data at high speed, and therefore is susceptible to data leaks.

2. Cost Management

- Even as almost all cloud service providers have a “Pay As You Go” model, which reduces the overall cost of the resources being used, there are times when there are huge costs incurred to the enterprise using cloud computing.

- When there is under optimization of the resources, let's say that the servers are not being used to their full potential, add up to the hidden costs. If there is a degraded application performance or sudden spikes or overages in the usage, it adds up to the overall cost. Unused resources are one of the other main reasons why the costs go up.
- If you turn on the services or an instance of cloud and forget to turn it off during the weekend or when there is no current use of it, it will increase the cost without even using the resources.

3. Multi-Cloud Environments

- Due to an increase in the options available to the companies, enterprises not only use a single cloud but depend on multiple cloud service providers. Most of these companies use hybrid cloud tactics and close to 84% are dependent on multiple clouds. This often ends up being hindered and difficult to manage for the infrastructure team.
- The process most of the time ends up being highly complex for the IT team due to the differences between multiple cloud providers.

4. Performance Challenges

- Performance is an important factor while considering cloud-based solutions. If the performance of the cloud is not satisfactory, it can drive away users and decrease profits.
- Even a little latency while loading an app or a web page can result in a huge drop in the percentage of users. This latency can be a product of inefficient load balancing, which means that the server cannot efficiently split the incoming traffic so as to provide the best user experience.
- Challenges also arise in the case of fault tolerance, which means the operations continue as required even when one or more of the components fail.

5. Interoperability and Flexibility

- When an organization uses a specific cloud service provider and wants to switch to another cloud-based solution, it often turns up to be a tedious procedure since

applications written for one cloud with the application stack are required to be re-written for the other cloud.

- There is a lack of flexibility from switching from one cloud to another due to the complexities involved. Handling data movement, setting up the security from scratch and network also add up to the issues encountered when changing cloud solutions, thereby reducing flexibility.

6. High Dependence on Network

- Since cloud computing deals with provisioning resources in real-time, it deals with enormous amounts of data transfer to and from the servers.
- This is only made possible due to the availability of the high-speed network. Although these data and resources are exchanged over the network, this can prove to be highly vulnerable in case of limited bandwidth or cases when there is a sudden outage.
- Even when the enterprises can cut their hardware costs, they need to ensure that the internet bandwidth is high as well there are zero network outages, or else it can result in a potential business loss.
- It is therefore a major challenge for smaller enterprises that have to maintain network bandwidth that comes with a high cost.

7. Lack of Knowledge and Expertise

- Due to the complex nature and the high demand for research working with the cloud often ends up being a highly tedious task.
- It requires immense knowledge and wide expertise on the subject. Although there are a lot of professionals in the field they need to constantly update themselves.
- Cloud computing is a highly paid job due to the extensive gap between demand and supply. There are a lot of vacancies but very few talented cloud engineers, developers, and professionals.

- Therefore, there is a need for upskilling so these professionals can actively understand, manage and develop cloud-based applications with minimum issues and maximum reliability.

Security Issues in Cloud Computing:

There is no doubt that Cloud Computing provides various Advantages but there are also some security issues in cloud computing. Below are some following Security Issues in Cloud Computing as follows.

1. **Data Loss –**
    - Data Loss is one of the issues faced in Cloud Computing. This is also known as Data Leakage. As we know that our sensitive data is in the hands of somebody else, and we don't have full control over our database. So if the security of cloud service is to break by hackers then it may be possible that hackers will get access to our sensitive data or personal files.

2. **Interference of Hackers and Insecure API's –**
    - As we know if we are talking about the cloud and its services it means we are talking about the Internet. Also, we know that the easiest way to communicate with Cloud is using API. So it is important to protect the Interface's and API's which are used by an external user. But also in cloud computing, few services are available in the public domain. *An* is the vulnerable part of Cloud Computing because it may be possible that these services are accessed by some third parties. So it may be possible that with the help of these services hackers can easily hack or harm our data.

3. **User Account Hijacking –**
    - Account Hijacking is the most serious security issue in Cloud Computing. If somehow the Account of User or an Organization is hijacked by Hacker. Then the hacker has full authority to perform Unauthorized Activities**.**

4. **Changing Service Provider –**
    - Vendor lock In is also an important Security issue in Cloud Computing. Many organizations will face different problems while shifting from one vendor to another. For example, An Organization wants to shift from AWS Cloud to Google Cloud Services then they ace various problem's like shifting of all data, also both

cloud services have different techniques and functions, so they also face problems regarding that. Also, it may be possible that the charges of AWS are different from Google Cloud, etc.

5. **Lack of Skill –**
    - While working, shifting o another service provider, need an extra feature, how to use a feature, etc. are the main problems caused in IT Company who doesn't have skilled Employee. So it requires a skilled person to work with cloud Computing.

6. **Denial of Service (DoS) attack –**
    - This type of attack occurs when the system receives too much traffic. Mostly DoS attacks occur in large organizations such as the banking sector, government sector, etc. When a DoS attack occurs data is lost. So in order to recover data, it requires a great amount of money as well as time to handle it.

UNIT – 7
CLOUD COMPUTING SECURITY ARCHITECTURE

CLOUD COMPUTING SECURITY ARCHITECTURE

- A cloud security architecture (also sometimes called a “cloud computing security architecture”) is defined by the security layers, design, and structure of the platform, tools, software, infrastructure, and best practices that exist within a cloud security solution.
- A cloud security architecture provides the written and visual model to define how to configure and secure activities and operations within the cloud, including such things as identity and access management; methods and controls to protect applications and data; approaches to gain and maintain visibility into compliance, threat posture, and overall security; processes for instilling security principles into cloud services development and operations; policies and governance to meet compliance standards; and physical infrastructure security components.
- Cloud security, in general, refers to the protection of information, applications, data, platforms, and infrastructure that operate or exist within the cloud.
- Cloud security is applicable to all types of cloud computing infrastructures, including public clouds, private clouds, and hybrid clouds. Cloud security is a type of cybersecurity.

Security Planning

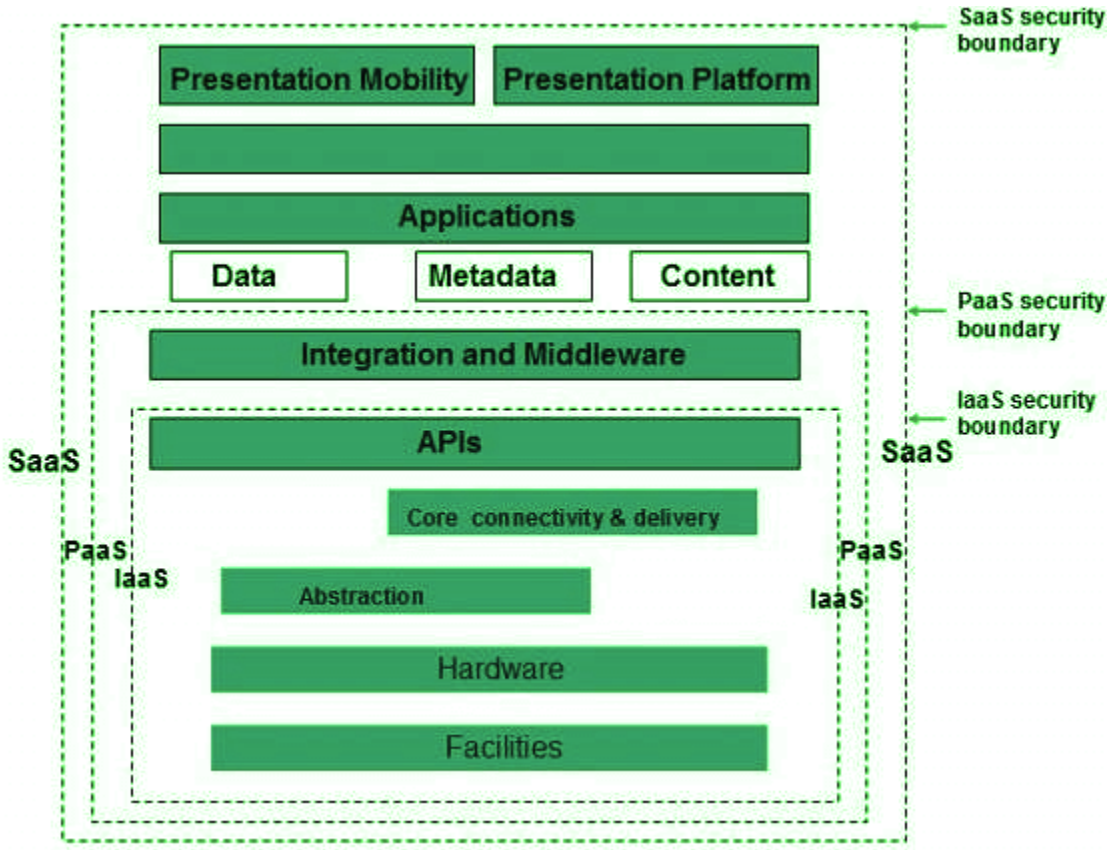
Before deploying a particular resource to the cloud, one should need to analyze several aspects of the resource, such as:

- A select resource needs to move to the cloud and analyze its sensitivity to risk.
- Consider cloud service models such as **IaaS, PaaS,**and These models require the customer to be responsible for Security at different service levels.
- Consider the cloud type, such as **public, private, community**, or
- Understand the cloud service provider's system regarding data storage and its transfer into and out of the cloud.
- The risk in cloud deployment mainly depends upon the service models and cloud types.

Understanding Security of Cloud

Security Boundaries

- The **Cloud Security Alliance (CSA)** stack model defines the boundaries between each service model and shows how different functional units relate. A particular service model defines the boundary between the service provider's responsibilities and the customer.
- The following diagram shows the **CSA stack model:**



Key Points to CSA Model

- IaaS is the most basic level of service, with PaaS and SaaS next two above levels of services.
- Moving upwards, each service inherits the capabilities and security concerns of the model beneath.
- IaaS provides the infrastructure, PaaS provides the platform development environment, and SaaS provides the operating environment.
- IaaS has the lowest integrated functionality and security level, while SaaS has the highest.

- This model describes the security boundaries at which cloud service providers' responsibilities end and customers' responsibilities begin.
- Any protection mechanism below the security limit must be built into the system and maintained by the customer.

Although each service model has a security mechanism, security requirements also depend on where these services are located, private, public, hybrid, or community cloud.

Understanding data security

Since all data is transferred using the Internet, data security in the cloud is a major concern. Here are the key mechanisms to protect the data.

- access control
- audit trail
- certification
- authority

The service model should include security mechanisms working in all of the above areas.

Separate access to data

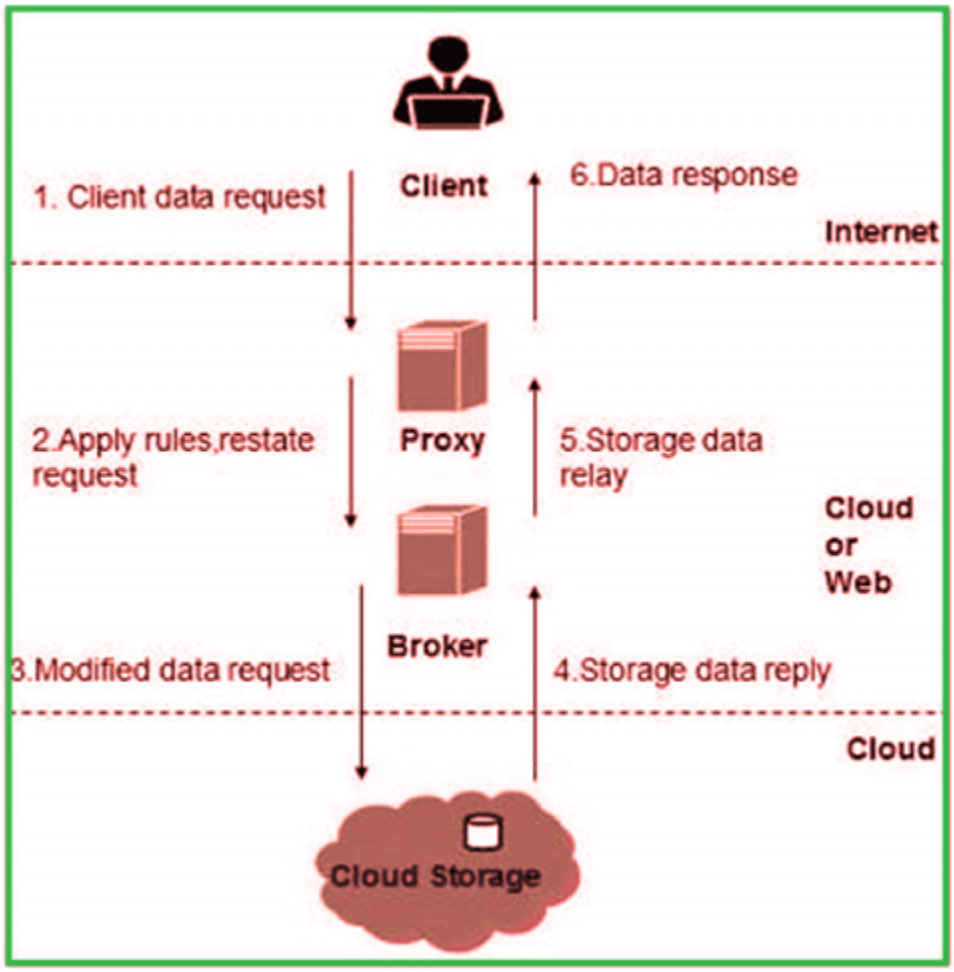
Since the data stored in the cloud can be accessed from anywhere, we need to have a mechanism to isolate the data and protect it from the client's direct access.

Broker cloud storage is a way of separating storage in the Access Cloud. In this approach, two services are created:

1. A broker has full access to the storage but does not have access to the client.
2. A proxy does not have access to storage but has access to both the client and the broker.
3. Working on a Brocade cloud storage access system
4. When the client issues a request to access data:
5. The client data request goes to the external service interface of the proxy.
6. The proxy forwards the request to the broker.
7. The broker requests the data from the cloud storage system.

8. The cloud storage system returns the data to the broker.
9. The broker returns the data to the proxy.
10. Finally, the proxy sends the data to the client.

All the above steps are shown in the following diagram:



Encoding

- Encryption helps to protect the data from being hacked. It protects the data being transferred and the data stored in the cloud. Although encryption helps protect data from unauthorized access, it does not prevent data loss.

Key Elements of a Cloud Security Architecture

When developing a cloud security architecture several critical elements should be included:

- Security at Each Layer
- Centralized Management of Components
- Redundant & Resilient Design
- Elasticity & Scalability
- Appropriate Storage for Deployments
- Alerts & Notifications
- Centralization, Standardization, & Automation

Shared Responsibility within Cloud Security Architectures

- The types of service models in use by a business define the types of cloud security architectures that are most applicable. The service models are: Infrastructure as a Service (IaaS), Software as a Service (SaaS), and Platform as a Service (PaaS).

Infrastructure as a Service (IaaS) Shared Responsibility

- With an IaaS, a business purchases the infrastructure from a cloud provider and the business typically installs their own operating systems, applications, and middleware.
- An example of an IaaS is Azure (Microsoft). In an IaaS, the customer is usually responsible for the security associated with anything they own or install on the infrastructure.

Software as a Service (SaaS) Shared Responsibility

- With a SaaS, an organization purchases the use of a cloud-based application from a provider.
- Examples of SaaS include Office 365 or Salesforce.
- In a SaaS, the customer is typically only responsible for the security components associated with accessing the software, such identity management, customer network security, etc. The software provider manages the security backend.

Platform as a Service (PaaS) Shared Responsibility

- With a PaaS, a business purchases a platform from a cloud provider to develop, run, and manage applications without developing or managing the underlying platform infrastructure required for the applications.
- An example of a PaaS would be Amazon Web Services (AWS).

- In a PaaS, the customer is responsible for the security associated with application implementation, configurations, and permissions.

Cloud Security Architectures by Service Model

IaaS Cloud Security Architecture Components

- Security architecture components in an IaaS cloud environment may include endpoint protection (EPP), a cloud access security broker (CASB), a vulnerability management solution, access management, and data and network encryption.

SaaS Cloud Security Architecture Components

- SaaS security architecture components should include application security, identity and access management as well as a cloud access security broker (CASB) to facilitate visibility, access controls and data protection using APIs, proxies, or gateways.

PaaS Cloud Security Architecture Components

- A PaaS security architecture may require both standard cloud security architecture solutions, as well as less common solutions, such as a Cloud Workload Protection Platform (CWPP).

Principles of Cloud Security Architecture

- **Identification**—Knowledge of the users, assets, business environment, policies, vulnerabilities and threats, and risk management strategies (business and supply chain) that exist within your cloud environment.
- **Security Controls**—Defines parameters and policies implemented across users, data, and infrastructure to help manage the overall security posture.
- **Security by Design**—Defines the control responsibilities, security configurations, and security baseline automations. Usually standardized and repeatable for deployment across common use cases, with security standards, and in audit requirements.
- **Compliance**—Integrates industry standards and regulatory components into the architecture and ensures standards and regulatory responsibilities are met.

- **Perimeter Security**—Protects and secures traffic in and out of organization's cloud-based resources, including connection points between corporate network and public internet.
- **Segmentation**—Partitions the architecture into isolated component sections to prevent lateral movement in the case of a breach. Often includes principles of 'least privilege'.
- **User Identity and Access Management**—Ensures understanding, visibility, and control into all users (people, devices, and systems) that access corporate assets. Enables enforcement of access, permissions, and protocols.
- **Data encryption**—Ensures data at rest and traveling between internal and external cloud connection points is encrypted to minimize breach impact.
- **Automation**—Facilitates rapid security and configuration provisioning and updates as well as quick threat detection.
- **Logging and Monitoring**—Captures activities and constant observation (often automated) of all activity on connected systems and cloud-based services to ensure compliance, visibility into operations, and awareness of threats.
- **Visibility**—Incorporates tools and processes to maintain visibility across an organization's multiple cloud deployments.
- **Flexible Design**—Ensuring architecture design is sufficiently agile to develop and incorporate new components and solutions without sacrificing inherent security.

Cloud Security Architecture Threats

- Cloud services are affected by the most common types of concerns and threats, including
  - ✓ data breaches,
  - ✓ malware injections,
  - ✓ regulatory non-compliance,
  - ✓ insider threats,
  - ✓ advanced persistent threats (APTs),
  - ✓ credential stuffing attacks,
  - ✓ insecure application programming interfaces (APIs),
  - ✓ zero-day attacks,
  - ✓ account hijacking through stolen or compromised credentials,
  - ✓ phishing, and service disruptions due to denial-of-service attacks or misconfigurations.
- If a breach occurs, liability for the breach is based on the shared responsibility model.

Some threats and issues may also be more specific to the type of cloud service:

- **IaaS Cloud Security Threats**
  - ✓ Availability disruption through denial-of-service attacks
  - ✓ Injection flaws
  - ✓ Broken authentication
  - ✓ Sensitive data exposure
  - ✓ XML external entities
  - ✓ Broken access control
  - ✓ Security misconfigurations
  - ✓ Cross-site scripting (XSS)
  - ✓ Insecure deserialization
  - ✓ Using components with known vulnerabilities
  - ✓ Insufficient logging and monitoring
  - ✓ Data leakage (through inadequate ACL)
  - ✓ Privilege escalation through misconfiguration
  - ✓ DoS attack via API
  - ✓ Weak privileged key protection
  - ✓ Virtual machine (VM) weaknesses
  - ✓ Insider data theft
- **PaaS Cloud Security Threats**
  - ✓ Privilege escalation via API
  - ✓ Authorization weaknesses in platform services
  - ✓ Run-time engine vulnerabilities
  - ✓ Availability disruption through denial-of-service attacks
  - ✓ Injection flaws
  - ✓ Broken authentication
  - ✓ Sensitive data exposure
  - ✓ XML external entities
  - ✓ Broken access control
  - ✓ Security misconfigurations
  - ✓ Cross-site scripting (XSS)
  - ✓ Insecure deserialization
  - ✓ Using components with known vulnerabilities

- ✓ Insufficient logging and monitoring
- ✓ Data leakage (through inadequate ACL)
- ✓ Privilege escalation through misconfiguration
- ✓ DoS attack via API
- ✓ Privilege escalation via API
- ✓ Weak privileged key protection
- ✓ Virtual machine (VM) weaknesses
- ✓ Insider data theft

- **SaaS Cloud Security Threats**
  - ✓ Weak or immature identity and access management
  - ✓ Weak cloud security standards
  - ✓ Zero-day vulnerabilities
  - ✓ Shadow IT/unsanctioned cloud applications/software
  - ✓ Service disruption through denial-of-service attacks
  - ✓ Phishing
  - ✓ Credential stuffing attacks
  - ✓ Weak compliance and auditing oversight
  - ✓ Stolen or compromised credentials
  - ✓ Weak vulnerability monitoring

INFORMATION CLASSIFICATION

1. **Information Classification Objectives**
   - There are several good reason to classify information. Not all data has the same value to an organization.
   - For ex: some data is more valuable to upper management, because it aids them in making strategic long range or short range business direction decision.
   - Some data such as trade secrets, formulas & new product information, is so valuable that its loss could create a significant problem for the enterprise in the market place, either by creating public embarrassment or by causing a lack of credibility.
   - Information classification has the longest history in the government sector. its value has long been established and it is a required component when securing trusted systems.

- In this sector information classification is used primarily to prevent the unauthorized disclosure of information and the resultant failure of confidentiality.

2. **Information Classification Benefits**
   - It demonstrate an organization's commitment to security protections.
   - It helps identify which information is the most sensitive or vital to an organization.
   - It supports the tenets of confidentiality, integrity, & availability as it pertains to data.
   - It helps identify which protections apply to which information.
   - It might be required for regulatory, compliance or legal reasons.
3. **Information Classification Concepts**
   - The information that an organization processes must be classified according to the organizations sensitivity to its loss or disclosure.
   - The information system owner is responsible for defining the sensitivity level of the data.
   - Classification according to a defined classification scheme enables security controls to be properly implemented.

Public data

- Information that is similar to unclassified information, all of a company's information that does not fit into any of the next categories can be considered public.
- While its unauthorized disclosure may be against policy, it is not expected to impact seriously or adversely the organization, its employees and /or its customers.

Sensitive data

- Information that requires a higher level of classification than normal data.
- This information is protected from a loss of confidentiality as well as from a loss of integrity due to an unauthorized alteration.
- This classification applies to information that requires special precautions to ensure its integrity by protecting it from unauthorized modification or deletion.
- It is information that requires a higher than normal assurance of accuracy and completeness.

Private data

- This classification applies to personal information that is intended for use within the organization.
- Its unauthorized disclosure could seriously and adversely impact the organization and/or its employees.
- For example: salary levels and medical information are considered private.

Confidential data

- This classification applies to the most sensitive business information that is intended strictly for use within the organization.
- Its unauthorized disclosure could seriously and adversely impact the organization, its stockholders, its business partners, and/or its customers.
- This information is exempt from disclosure under the provisions of the freedom of information act or other applicable federal laws or regulations.
- For ex: information about new product development, trade secret, and merger negotiations is considered confidential.

4. **Classification Criteria**

Several criteria may be used to determine the classification of an information object:

Value:

- Value is the number one commonly used criteria for classifying data in the private sector.
- If the information is valuable to an organization or its competitors, then it needs to be classified.

Age:

- The classification of information might be lowered if the information's value decreases over time.
- In the U.S. Department of Defense, some classified documents are automatically declassified after a predetermined time period has passed.

Useful life:

- If the information has been made obsolete due to new information, substantial changes in the company, or other reasons, the information can often be declassified.

Personal association:

- If information is personally associated with specific individuals or is addressed by a privacy law, it might need to be classified.
- For ex: investigative information that reveals informant names might need to remain classified.

5. **Information Classification Procedures**
   - Identify the appropriate administrator and data custodian. The data custodian is responsible for protecting the information, running backups, & performing data restoration.
   - Specify the criteria for classifying and labeling the information.
   - Classify the data by its owner, who is subject to review by a supervisor.
   - Specify & document any expectations to the classification policy.
   - Specify the controls that will be applied to each classification level.
   - Specify the termination procedures for declassifying the information or for transferring custody of the information to another entity.
   - Create an enterprise awareness program about the classification controls.
6. **Distribution of classified Information**

   External distribution of sensitive or classified information stored on a cloud is often necessary, and the inherent security vulnerabilities need to be addressed. Some of the instances when this distribution is required are as follows:

   Court order:
   - Classified or sensitive information might need to be disclosed to comply with a court order.

   Government contracts:
   - Government contractors might need to disclose classified or sensitive information in accordance with the procurement agreements related to a government project.

   Senior level approval
   - A senior level executives might authorize the release of classified or sensitive information to external entities or organizations.
   - This release might require the signing of a confidentiality agreement by the external party.

7. Employee Termination

- It is important to understand the impact of employee terminations on the integrity of information stored in a cloud environment. This issue applies to employees of cloud client as well as the cloud provider.
- Typically, there are two types of terminations, friendly and unfriendly, and both require specific actions.
- Friendly terminations should be accomplished by implementing a standard set of procedures for outgoing and transferring employees. This activity normally includes the following:
    - ✓ The removal of access privileges, computer accounts, authentication tokens.
    - ✓ The briefing on the continuing responsibilities of the terminated employee for confidentiality and privacy.
    - ✓ The return of company computing property, such as laptops.
    - ✓ Continued availability of data. In both the manual and electronic worlds, this may involve documenting procedures or filing schemes, such as how documents are stored on the hard disk and how they are backed up. Employees should be instructed whether or not to" clean up" their PC before leaving.
    - ✓ If cryptography is used to protect data, the availability of cryptographic keys to management personnel must be ensured.
- Given the potential for adverse consequences during an unfriendly termination, organizations should do the following:
    - ✓ System access should be terminated as quickly as possible when an employee is leaving a position under less than friendly terms. If employees are to be fired, system access should be removed at the same time (or just before) the employees are notified of their dismissal.
    - ✓ When an employee resigns and it can reasonably assumed that it is on unfriendly terms, system access should be immediately terminated, or as soon as feasible.
    - ✓ During the notice of termination period, it may be necessary to restrict the individual to a given area and function. This may be particularly true for employees capable of changing programs or modifying the system or applications.
    - ✓ In some cases, physical removal from the offices may be necessary.

8. **Security Awareness, Training & Education**
    - Security awareness is often overlooked as an element affecting cloud security architecture because most of a security practitioner's time is spent on controls, intrusion detection, risk assessment & proactively or reactively administering security.
    - Employees of both the cloud client & the cloud provider must be aware of the need to secure information & protect the information assets of an enterprise.
    - The purpose of computer security awareness , training & education is to enhance security by doing the following:
        - ✓ Improving awareness of the need to protect system resources.
        - ✓ Developing skills & knowledge so computer users can perform their jobs more securely.
        - ✓ Building in-depth knowledge, as needed to design, implement, or operate security programs for organizations and systems.
    - An effective computer security awareness & training program requires proper planning, implementation, maintenance, & periodic evaluation.
    - In general , a computer security awareness & training program should encompass the following seven steps:
        - ✓ Identify program scope, goals & objectives
        - ✓ Identify training staff
        - ✓ Identify target audiences
        - ✓ Motivate management & employees
        - ✓ Administer the program
        - ✓ Maintain the program
        - ✓ Evaluate the program

Benefits of security awareness

- They can reduce the unauthorized actions attempted by personnel.
- They can significantly increase the effectiveness of the protection controls.
- They help to prevent the fraud, waste & abuse of computing resources.

The following activities can be used to improve security within an organization without incurring large costs or draining resources:

- **Live/Interactive presentations:** Lectures, videos, and computer based training (CBT).

- **Publishing/Distribution:** Posters, company newsletters, bulletins, and the intranet.
- **Incentives:** Awards and recognition for security related achievements.
- **Reminders:** Log-in banner messages and marketing paraphernalia such as mugs, pens, sticky notes, and mouse pads.

Training and Education: Training is different from awareness in that it provides security information in a more formalized manner, such as classes, workshops, or individualized instruction. The following types of training are related to cloud security:

- Security – related job training for operators and specific users.
- Awareness training for specific departments or personnel groups with security – sensitive positions.
- Technical security training for senior managers, functional managers, and business unit managers.

SECURE EXECUTION ENVIRONMENT & COMMUNICATIONS

Secure Execution Environment:

- Configuring computing platforms for secure execution is a complex task; and in many instances it is not performed properly because of the large number of parameters that are involved.
- This provides opportunities for malware to exploit vulnerabilities, such as downloading code embedded in data and having the code executed at a high privilege level.
- In cloud computing, the major burden for establishing a secure execution environment is transferred from the client to the cloud provider.
- However, protected data transfers must be established through strong authentication mechanisms, and the client must have practices in place to address the privacy and confidentiality of information that is exchanged with the cloud.
- In fact, the client's port to the cloud might provide an attack path if not properly provisioned with security measures.
- Therefore, the client needs assurance that computations and data exchanges are conducted in a secure environment. This assurance is affected by trust enabled by cryptographic methods.

Secure Communications:

- Secure cloud communications involves the structure, transmission methods, transport formats, and security measures that provide confidentiality, integrity, availability, and authentications for transmissions over private public communications networks.
- Secure cloud computing communications should ensure the following:

Confidentiality:

- Ensures that only those who are supposed to access data can retrieve it. Loss of confidentiality can occur through intentional release of private company information or through a misapplication of network rights.
- Some of the elements of telecommunications used to ensure confidentiality are as follows:
    - ✓ Network security protocols
    - ✓ Network authentication services
    - ✓ Intrusion detection services

Integrity:

- Ensures that data has not been changed due to an accident or malice.
- Integrity is the guarantee that the message sent is the message received and that the message is not intentionally or unintentionally altered. Integrity also contains the concept of nonrepudiation of a message source.
- Some of the constituents of integrity are as follows:
    - ✓ Firewall services
    - ✓ Communications security management
    - ✓ Intrusion detection services

Availability:

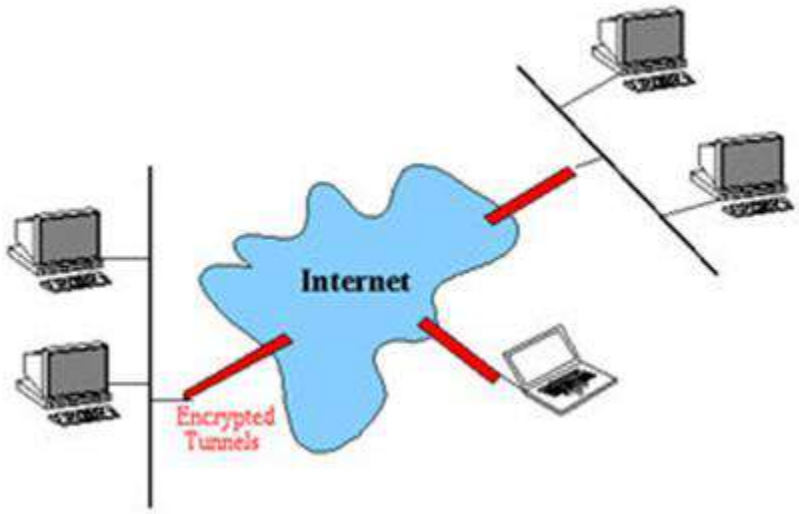
- Ensures that data is accessible when and where it is needed, and that connectivity is accessible when needed, allowing authorized users to access the network or systems. Also included In that assurance is the guarantee that security services for the security practitioner are usable when they are needed.
- Some of the elements that are used to ensure availability are as follows:
    - ✓ Fault tolerance for data availability, such as backups and redundant disk systems.
    - ✓ Acceptable logins and operating process performances.
    - ✓ Reliable and interoperable security processes and network security mechanisms.

APIs:

- Common vulnerabilities such as weak antivirus software, unattended computing platforms, poor passwords, weak authentication mechanisms, inadequate intrusion detection that can impact communications must be more stringently analyzed, and proper APIs must be used.

VPN: VIRTUAL PRIVATE NETWORK

- VPN stands for Virtual Private Network. It refers to a safe and encrypted network that allows you to use network resources in a remote manner.
- Using VPN, you can create a safe connection over a less secure network, e.g. internet. It is a secure network as it is completely isolated from rest of the internet.
- The government, businesses, military can use this network to use network resources securely.



- VPN is free to use and it uses site-to-site and remote access methods to work. It uses an arrangement of encryption services to establish a secure connection. It is an ideal tool for encryption; it provides you strong AES256 encryption with an 8192bit key.

How VPN Works?

- VPN works by creating a secure tunnel using powerful VPN protocols. It hides your IP address behind its own IP address that encrypts all your communication. Thus, your

communication passes through a secure tunnel that allows you use network resources freely and secretly.

Types of VPN

- **Remote Access VPN**
  - A Remote Access VPN allows people to connect to a private network and remotely access all of its resources and services. The person's connection to the private network is made over the Internet, and the connectivity is safe and confidential.
  - Remote Access VPN is beneficial to both residential and business users.
  - While away from the office, a corporate employee utilizes a VPN to connect to his or her employer's private network and remotely access files and resources on the private network.
  - Private VPN users or home VPN users typically utilize VPN services to circumvent regional Internet censorship and access restricted websites.
- **Site-to-Site VPN**
  - A Site-to-Site VPN, also known as a Router-to-Router VPN, is widely employed in big corporations.
  - Site-to-site VPN is used by businesses and organizations with branches offices in different places to link the network of one office location to the network of another office location.
    - ✓ **Intranet-based VPN** − This form of VPN is used when many offices of the same organization are linked using Site-to-Site VPN technology.
    - ✓ **Extranet-based VPN** − Extranet-based VPN is used when a firm uses a Site-to-site VPN type to connect to the office of another organization.
  - Site-to-site VPN, in essence, creates an artificial link between networks at geographically separated workplaces and connects them over the Web to maintain a safe and private connection between the networks. Because Site-to-Site VPN relies on Router-to-Router communication, one router serves as a VPN Client and another as a VPN Server.

- Communication can commence only when the two routers' authenticity has been validated. Only once the authentication between the two routers is verified then communication begins.

VPN Tunneling

- Tunneling is a protocol that allows for the secure movement of data from one network to another.
- Tunneling involves allowing private network communications to be sent across a public network, such as the Internet, through a process called encapsulation.
- The encapsulation process allows for data packets to appear as though they are of a public nature to a public network when they are actually private data packets, allowing them to pass through unnoticed.
- Tunneling is also known as port forwarding.
- In tunneling, the data are broken into smaller pieces called packets as they move along the tunnel for transport.
- As the packets move through the tunnel, they are encrypted and another process called encapsulation occurs.
- The private network data and the protocol information that goes with it are encapsulated in public network transmission units for sending.
- The units look like public data, allowing them to be transmitted across the Internet.
- Encapsulation allows the packets to arrive at their proper destination. At the final destination, de-capsulation and decryption occur.

There are various protocols that allow tunneling to occur, including:

- **Point-to-Point Tunneling Protocol (PPTP):** PPTP keeps proprietary data secure even when it is being communicated over public networks. Authorized users can access a private network called a virtual private network, which is provided by an Internet service provider. This is a private network in the “virtual” sense because it is actually being created in a tunneled environment.
- **Layer Two Tunneling Protocol (L2TP):** This type of tunneling protocol involves a combination of using PPTP and Layer 2 Forwarding.

Tunneling is a way for communication to be conducted over a private network but tunneled through a public network. This is particularly useful in a corporate setting and also offers security features such as encryption options.

PUBLIC KEY INFRASTRUCTURE & ENCRYPTION KEY MANAGEMENT

- To secure communications, data that is being exchanged with a cloud should be encrypted, calls to remote servers should examined for embedded malware & digital certificates should be employed & managed.
- PKI (or Public Key Infrastructure) is the framework of encryption and cybersecurity that protects communications between the server (your website) and the client (the users).
- PKI is essential in building a trusted and secure business environment by being able to verify and exchange data between various servers and users.
- Through encryption and decryption, PKI is based on digital certificates that verify the identity of the machines and/or users that ultimately proves the integrity of the transaction.
- As the number of machines is increasing dramatically in today's digital age, it's important that our information is trusted and protected against attacks.
- These services provide integrity, access control, confidentiality, authentication, & nonrepudiation for electronic transactions.
- The PKI includes the following elements:
    - ✓ Digital certificates
    - ✓ Certificate authority
    - ✓ Registration authorities
    - ✓ Policies & procedures
    - ✓ Certificate revocation
    - ✓ Nonrepudiation support
    - ✓ Time stamping
    - ✓ Lightweight directories access protocol
    - ✓ Security enabled applications

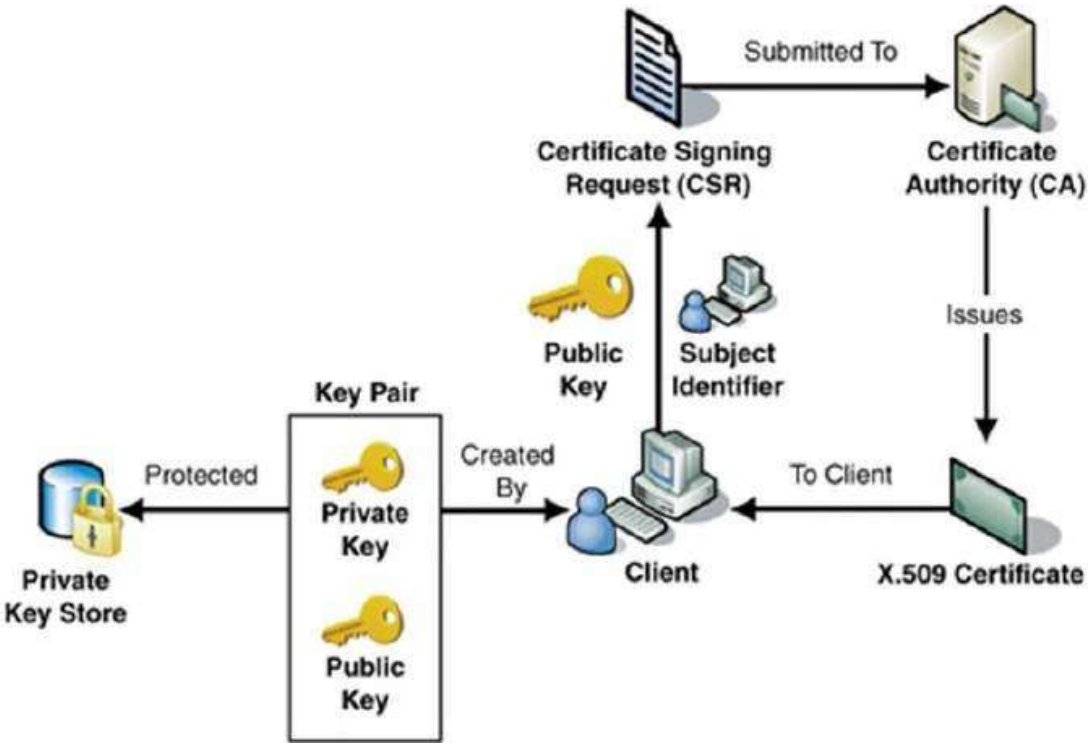
DIGITAL CERTIFICATE

- Digital certificate is issued by a trusted third party which proves sender's identity to the receiver and receiver's identity to the sender.
- A digital certificate is a certificate issued by a Certificate Authority (CA) to verify the identity of the certificate holder.
- The CA issues an encrypted digital certificate containing the applicant's public key and a variety of other identification information. Digital certificate is used to attach public key with a particular individual or an entity.

Digital certificate contains:-

1. Name of certificate holder.
2. Serial number which is used to uniquely identify a certificate, the individual or the entity identified by the certificate
3. Expiration dates.
4. Copy of certificate holder's public key.(used for decrypting messages and digital signatures)
5. Digital Signature of the certificate issuing authority.

- Digital certificate is also sent with the digital signature and the message.
- Digital Certificates are not only issued to people but they can be issued to computers, software packages or anything else that need to prove the identity in the electronic world.
    - ✓ Digital certificates are based on the ITU standard X.509 which defines a standard certificate format for public key certificates and certification validation. Hence digital certificates are sometimes also referred to as X.509 certificates.
    - ✓ Public key pertaining to the user client is stored in digital certificates by The Certification Authority (CA) along with other relevant information such as client information, expiration date, usage, issuer etc.
    - ✓ CA digitally signs this entire information and includes digital signature in the certificate.
    - ✓ Anyone who needs the assurance about the public key and associated information of client, he carries out the signature validation process using CA's public key. Successful validation assures that the public key given in the certificate belongs to the person whose details are given in the certificate.
- The process of obtaining Digital Certificate by a person/entity is depicted in the following illustration.



- As shown in the illustration, the CA accepts the application from a client to certify his public key. The CA, after duly verifying identity of client, issues a digital certificate to that client.

Some of the different types of certificates that are issued include the following:

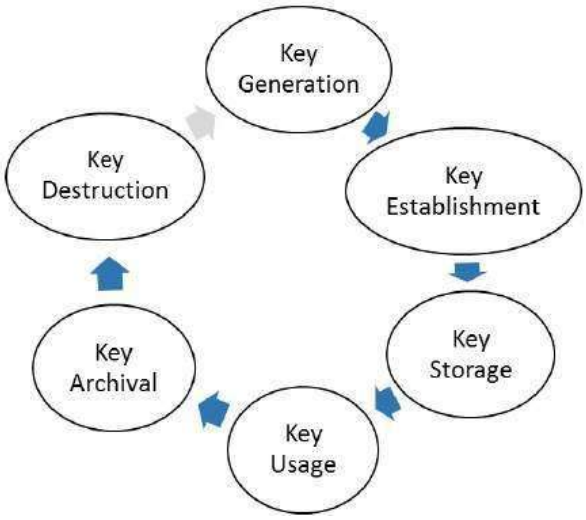
- **CA Certificates**: Issued to CAs, these certificates contains the public keys used to verify digital signatures on CRLs and certificates.
- **End Entity Certificates**: Issued to entities that are not CAs, these certificates contain the public keys that are needed by the certificate's user in order to perform key management or verify a digital signature.
- **Self-Issued Certificate**: These certificates are issued by an entity to itself to establish points of trust and to distribute a new signing public key.
- **Rollover Certificates**: These certificates are issued by a CA to transition from an old public key to a new one.

KEY MANAGEMENT

- Key management forms the basis of all data security. Data is encrypted and decrypted via the use of encryption keys, which means the loss or compromise of any encryption key would invalidate the data security measures put into place.
- Keys also ensure the safe transmission of data across an Internet connection. With authentication methods, like **code signing,** attackers could pretend to be a trusted service like Microsoft, while giving victim's computers malware, if they steal a poorly protected key.
- Keys provide compliance with certain standards and regulations to ensure companies are using best practices when protecting cryptographic keys. Well protected keys are only accessible by users who need them.
- It goes without saying that the security of any cryptosystem depends upon how securely its keys are managed. Without secure procedures for the handling of cryptographic keys, the benefits of the use of strong cryptographic schemes are potentially lost.
- It is observed that cryptographic schemes are rarely compromised through weaknesses in their design. However, they are often compromised through poor key management.

There are some important aspects of key management which are as follows −

- Cryptographic keys are nothing but special pieces of data. Key management refers to the secure administration of cryptographic keys.
- Key management deals with entire key lifecycle as depicted in the following illustration −



- There are two specific requirements of key management for public key cryptography.
    - ✓ **Secrecy of private keys.** Throughout the key lifecycle, secret keys must remain secret from all parties except those who are owner and are authorized to use them.
    - ✓ **Assurance of public keys.** In public key cryptography, the public keys are in open domain and seen as public pieces of data. By default there are no assurances of whether a public key is correct, with whom it can be associated, or what it can be used for. Thus key management of public keys needs to focus much more explicitly on assurance of purpose of public keys.
- The most crucial requirement of 'assurance of public key' can be achieved through the public-key infrastructure (PKI), a key management systems for supporting public-key cryptography.

MEMORY CARDS

Memory cards provide nonvolatile storage of information, but they do not have any processing capability. A memory card stores encrypted passwords and other related identifying information. A telephone calling card and an ATM card are examples of memory cards.

Smart cards

- Smart cards provide even more capability than memory cards by incorporating additional processing power on the cards. These credit-card-size devices comprise microprocessor and memory and are used to store digital signatures, private keys, passwords, and other personal information.

Biometrics

- An alternatives to using passwords for authentication in logical or technical access control is biometrics. Biometrics is based on the type 3 authentication mechanism – something you are.
- Biometrics is defined as an automated means of identifying or authenticating the identity of a living person based on physiological or behavioral characterstics.
- In biometrics, identification is a one-to-many search of an individual's characteristics from a database of stored images.
- Authentication is a one-to-one search to verify a claim to an identity made by a person. Biometrics is used for identification in physical controls and for authentication in logical controls.

- There are three main performance measures in biometrics:
  - ✓ **False Rejection Rate (FRR) Or Type I Error:** The percentage of valid subjects that are falsely rejected.
  - ✓ **False Acceptance Rate (FAR) Or Type II Error:** The percentage of invalid subjects that are falsely accepted.
  - ✓ **Crossover Error Rate (CER):** The percentage at which the FRR equals the FAR. The smaller the CER, the better the device is performing.
- The following are typical biometric characteristics that are used to uniquely authenticate an individuals identity:
  - ✓ **Fingerprints:** fingerprint characteristics are captured and stored. Typical CERs are 4-5%.
  - ✓ **Retina Scans:** the eye is placed approximately two inches from a camera and an invisible light source scans the retina for blood vessel patterns. CERs are approximately 1.4%.
  - ✓ **Iris Scans:** A video camera remotely captures iris patterns and characteristics. CER values are around 0.5%.
  - ✓ **Hand Geometry:** cameras capture three-dimensional hand characteristics. CERs are approximately 2%.
  - ✓ **Voice:** Sensors capture voice characteristics, including throat vibrations and air pressure, when the subject speaks a phrase. CERs are in the range of 10%.
  - ✓ **Handwritten Signature Dynamics:** The signing characteristics of an individual making a signature are captured and recorded. Typical characteristics including writing pressure and pen direction. CERs are not published at this time.

IMPLEMENTING IDENTITY MANAGEMENT

- Effective identity management requires a high-level corporate commitment and dedication of sufficient resources to accomplish the task. Typical undertakings in putting identity management in place include the following:
  - ✓ Establishing a database of identities and credentials.
  - ✓ Managing user's access rights.
  - ✓ Enforcing security policy.
  - ✓ Developing the capability to create and modify accounts.
  - ✓ Setting up monitoring of resource accesses.
  - ✓ Installing a procedure for removing access rights.

- ✓ Providing training in proper procedures.

- The open group and the World Wide Web consortium (W3C) are working toward a standard for a global identity management system that would be interoperable, provide for privacy, implement accountability, and be portable.
- Identity management is also addressed by the XML-based eXtensible Name Service (XNS) open protocol for universal addressing. XNS provides the following capabilities:
  - ✓ A permanent identification address for a container of an individual's personal data and contact information.
  - ✓ Means to verify whether an individual's contact information is valid.
  - ✓ A platform for negotiating the exchange of information among different entities.

Access Control

- Access control is intrinsically tied to identity management and is necessary to preserve the confidentiality, integrity and availability of cloud data.
- Three things that must be considered for the planning and implementation of access control mechanisms are threat to the system, the system's vulnerability to these threats and the risk that the threats might materialize.
  - ✓ **Threat:** An event or activity that has the potential to cause harm to the information systems or networks.
  - ✓ **Vulnerability:** A weakness or lack of a safeguard that can be exploited by a threat, causing harm to the information systems or networks.
  - ✓ **Risk:** The potential for harm or loss to an information system or network, the probability that a threat will materialize.

CONTROLS

- Controls are implemented to mitigate risk & reduce the potential for loss. Two important control concepts are separation of duties and the principle of least privilege.
  1. Separation of duties requires an activity or process to be performed by two or more entities for successful completion.
  2. Least privileges means that the entity that has a task to perform should be provided with the minimum resources and privileges required to complete the task for the minimum necessary period of time.
- Control measures can be administrative, logical (also called technical), and physical in their implementation.

1. Administrative controls include policies and procedures, security awareness training, background checks, work habit checks, a review of vacation history, and increased supervision.
2. Logical or technical controls involve the restriction of access to systems and the protection of information. Examples of these types of controls are encryption, smart cards, access control lists and transmission protocols.
3. Physical controls incorporate guards and building security in general, such as the locking of doors , the securing of server rooms or laptops , the protection of cables , the separation of duties, and the backing up of files.

Models for Controlling Access:

- Controlling access by a subject (an active entity such as an individual or process) to an object (a passive entity such as a file) involves setting up access rules. These rules can be classified into three categories or models.
  - ✓ **Mandatory Access Control:**
    The authorization of a subject's access to an object depends upon labels, which indicate the subject's clearance, and the classification or sensitivity of the objects.
  - ✓ **Discretionary Access Control:**
    With discretionary access control, the subject has authority, within certain limitations, to specify what objects are accessible.
  - ✓ **Non-Discretionary Access Control:**
    A central authority determines which subjects can have access to certain objects based on the organizational security policy. The access controls might be based on the individual's role in the organization (role-based) or the subject's responsibilities and duties (task based).
- Access control can also be characterized as context-dependent or content-dependent.
  - ✓ Context-dependent access control is a function of factors such as location, time of day, and previous access history. It is concerned with the environment or context of the data.
  - ✓ In content dependent access control, access is determined by the information contained in the item being accessed.

Single Sign-On (SSO)

- Single sign-on (SSO) addresses the cumbersome situation of logging on multiple times to access different resources.
- When users must remember numerous passwords and IDs, they might take shortcuts in creating them that could leave them open to exploitation.
- In SSO a user provides one ID and password per work session and is automatically logged on to all the required applications. For SSO security, the passwords should not be stored or transmitted in the clear.
- SSO applications can run either on a user's workstation or on authentication servers.
- The advantages of SSO include having the ability to use stronger passwords, easier administration of changing or deleting the passwords, and less time to access resources.
- The disadvantages of many SSO implementation is that once users obtain access to the system through the initial logon, they can freely roam the network resources without any restrictions.

AUTONOMIC SYSTEMS

- Automatic systems are based on the human autonomic nervous system, which is self-managing, monitors changes that affect the body, and maintain the internal balances.
- Therefore, an autonomic computing system that has the goal of performing self-management to maintain correct operations despite perturbations to the system. Such a system requires sensory inputs, decision-making capability, and the ability to implement remedial activities to maintain an equilibrium state of normal operation.
- Examples of events that would have to be handled autonomously include the following:
    - ✓ Malicious attacks
    - ✓ Hardware or software faults
    - ✓ Excessive CPU utilization
    - ✓ Power failures
    - ✓ Organizational policies
    - ✓ Inadvertent operator errors
    - ✓ Interaction with other systems
    - ✓ Software updates

IBM introduced the concept of autonomic computing and its eight defining characteristics as follows:

- **Self-Awareness:** An autonomic application/system “knows itself” and is aware of its state and its behaviors.
- **Self-Configuring:** An autonomic application/system should be able to configure and reconfigure itself under varying and unpredictable conditions.
- **Self-Optimizing:** An autonomic application/system should be able to detect sub-optimal behaviors and optimize itself to improve its execution.
- **Self-Healing:** An autonomic application/system should be able to detect and recover from potential problems and continue to function smoothly.
- **Self-Protecting:** An autonomic application/system should be capable of detecting and protecting its resources from both internal and external attack and maintaining overall system security and integrity.
- **Context-Aware:** An autonomic application/system should be aware of its execution environment and be able to react to changes in the environment.
- **Open:** An autonomic application/system must function in a heterogeneous world and should be portable across multiple hardware and software architectures. Consequently, it must be built on standard and open protocols and interfaces.
- **Anticipatory:** An autonomic application/system should be able to anticipate, to the extent possible, its needs and behaviors and those of its context, and be able to manage itself proactively.

Autonomic Protection:

- Autonomic self-protection involves detecting a harmful situation and taking actions that will mitigate the situation. These systems will also be designed to predict problems from analysis of sensory inputs and initiate corrective measures.
- An autonomous system security response is based on network knowledge, capabilities of connected resources, information aggregation, the complexity of the situation, and the impact on affected applications.
- Autonomous protection systems should, therefore, adhere to the following guidelines:
    - ✓ Minimize overhead requirements.
    - ✓ Be consistent with security policies.
    - ✓ Optimize security related parameters.
    - ✓ Minimize impact on performance.
    - ✓ Minimize potential for introducing new vulnerabilities.

- ✓ Conduct regression analysis & return to previous software versions if problems are introduced by changes.
- ✓ Ensure that reconfiguration processes are secure.

Autonomic Self-Healing

- Autonomic self-healing systems can provide the capability to detect & repair software problems & identify hardware faults without manual intervention.
- The objective of the autonomous self-healing process is to keep the elements operating according to their design specifications.

UNIT-9 HADOOP

Hadoop

Hadoop is an open source framework from Apache and is used to store process and analyze data which are very huge in volume. Hadoop is written in Java and is not OLAP (online analytical processing). It is used for batch/offline processing.It is being used by Facebook, Yahoo, Google, Twitter, LinkedIn and many more. Moreover it can be scaled up just by adding nodes in the cluster.

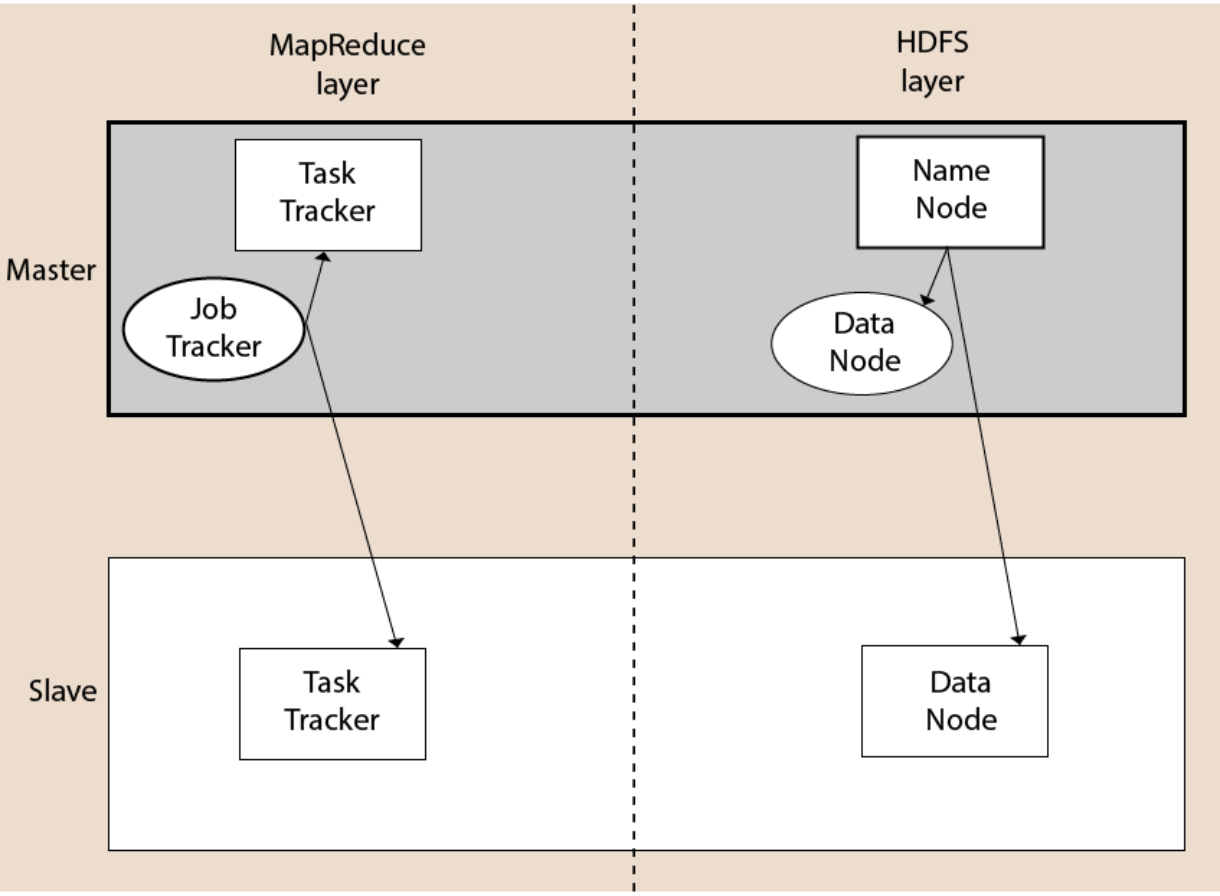
Modules of Hadoop

1. **HDFS:** Hadoop Distributed File System. Google published its paper GFS and on the basis of that HDFS was developed. It states that the files will be broken into blocks and stored in nodes over the distributed architecture.
2. **Yarn:** Yet another Resource Negotiator is used for job scheduling and manage the cluster.
3. **Map Reduce:** This is a framework which helps Java programs to do the parallel computation on data using key value pair. The Map task takes input data and converts it into a data set which can be computed in Key value pair. The output of Map task is consumed by reduce task and then the out of reducer gives the desired result.
4. **Hadoop Common:** These Java libraries are used to start Hadoop and are used by other Hadoop modules.

Hadoop Architecture

The Hadoop architecture is a package of the file system, MapReduce engine and the HDFS (Hadoop Distributed File System). The MapReduce engine can be MapReduce/MR1 or YARN/MR2.

A Hadoop cluster consists of a single master and multiple slave nodes. The master node includes Job Tracker, Task Tracker, NameNode, and DataNode whereas the slave node includes DataNode and TaskTracker.



Hadoop Distributed File System

The Hadoop Distributed File System (HDFS) is a distributed file system for Hadoop. It contains a master/slave architecture. This architecture consist of a single NameNode performs the role of master, and multiple DataNodes performs the role of a slave.

Both NameNode and DataNode are capable enough to run on commodity machines. The Java language is used to develop HDFS. So any machine that supports Java language can easily run the NameNode and DataNode software.

NameNode

- It is a single master server exist in the HDFS cluster.
- As it is a single node, it may become the reason of single point failure.
- It manages the file system namespace by executing an operation like the opening, renaming and closing the files.
- It simplifies the architecture of the system.

DataNode

- The HDFS cluster contains multiple DataNodes.
- Each DataNode contains multiple data blocks.
- These data blocks are used to store data.
- It is the responsibility of DataNode to read and write requests from the file system's clients.
- It performs block creation, deletion, and replication upon instruction from the NameNode.

Job Tracker

- The role of Job Tracker is to accept the MapReduce jobs from client and process the data by using NameNode.
- In response, NameNode provides metadata to Job Tracker.

Task Tracker

- It works as a slave node for Job Tracker.
- It receives task and code from Job Tracker and applies that code on the file. This process can also be called as a Mapper.

MapReduce Layer

The MapReduce comes into existence when the client application submits the MapReduce job to Job Tracker. In response, the Job Tracker sends the request to the appropriate Task Trackers. Sometimes, the TaskTracker fails or time out. In such a case, that part of the job is rescheduled.

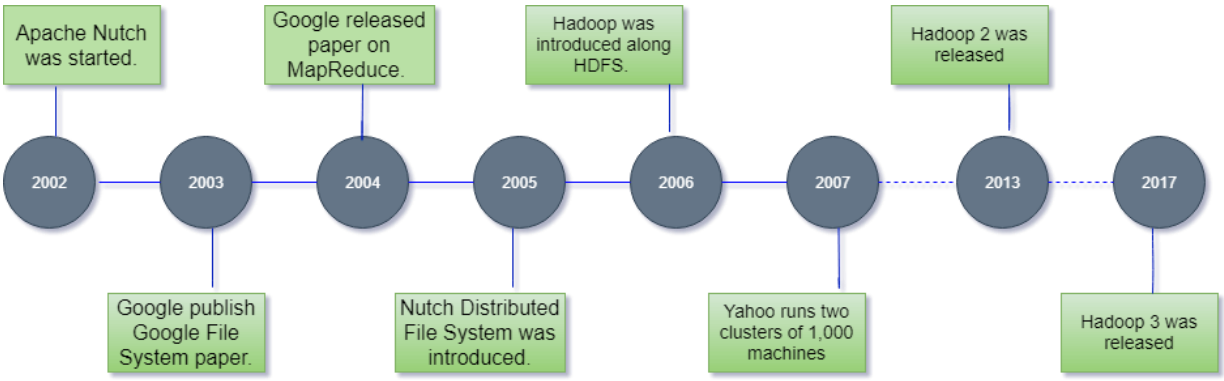
Advantages of Hadoop

- **Fast:** In HDFS the data distributed over the cluster and are mapped which helps in faster retrieval. Even the tools to process the data are often on the same servers, thus reducing the processing time. It is able to process terabytes of data in minutes and Peta bytes in hours.
- **Scalable:** Hadoop cluster can be extended by just adding nodes in the cluster.

- **Cost Effective:** Hadoop is open source and uses commodity hardware to store data so it really cost effective as compared to traditional relational database management system.
- **Resilient to failure:** HDFS has the property with which it can replicate data over the network, so if one node is down or some other network failure happens, then Hadoop takes the other copy of data and use it. Normally, data are replicated thrice but the replication factor is configurable.

History of Hadoop

The Hadoop was started by Doug Cutting and Mike Cafarella in 2002. Its origin was the Google File System paper, published by Google.



Let's focus on the history of Hadoop in the following steps: -

- In 2002, Doug Cutting and Mike Cafarella started to work on a project, **Apache Nutch.** It is an open source web crawler software project.
- While working on Apache Nutch, they were dealing with big data. To store that data they have to spend a lot of costs which becomes the consequence of that project. This problem becomes one of the important reason for the emergence of Hadoop.
- In 2003, Google introduced a file system known as GFS (Google file system). It is a proprietary distributed file system developed to provide efficient access to data.
- In 2004, Google released a white paper on Map Reduce. This technique simplifies the data processing on large clusters.

- In 2005, Doug Cutting and Mike Cafarella introduced a new file system known as NDFS (Nutch Distributed File System). This file system also includes Map reduce.
- In 2006, Doug Cutting quit Google and joined Yahoo. On the basis of the Nutch project, Dough Cutting introduces a new project Hadoop with a file system known as HDFS (Hadoop Distributed File System). Hadoop first version 0.1.0 released in this year.
- Doug Cutting gave named his project Hadoop after his son's toy elephant.
- In 2007, Yahoo runs two clusters of 1000 machines.
- In 2008, Hadoop became the fastest system to sort 1 terabyte of data on a 900 node cluster within 209 seconds.
- In 2013, Hadoop 2.2 was released.
- In 2017, Hadoop 3.0 was released.

Year	Event
2003	Google released the paper, Google File System (GFS).
2004	Google released a white paper on Map Reduce.
2006	- Hadoop introduced. - Hadoop 0.1.0 released. - Yahoo deploys 300 machines and within this year reaches 600 machines.
2007	- Yahoo runs 2 clusters of 1000 machines. - Hadoop includes HBase.
2008	- YARN JIRA opened - Hadoop becomes the fastest system to sort 1 terabyte of data on a 900 node cluster within 209 seconds. - Yahoo clusters loaded with 10 terabytes per day. - Cloudera was founded as a Hadoop distributor.

2009	- Yahoo runs 17 clusters of 24,000 machines. - Hadoop becomes capable enough to sort a petabyte. - MapReduce and HDFS become separate subproject.
2010	- Hadoop added the support for Kerberos. - Hadoop operates 4,000 nodes with 40 petabytes. - Apache Hive and Pig released.
2011	- Apache Zookeeper released. - Yahoo has 42,000 Hadoop nodes and hundreds of petabytes of storage.
2012	Apache Hadoop 1.0 version released.
2013	Apache Hadoop 2.2 version released.
2014	Apache Hadoop 2.6 version released.
2015	Apache Hadoop 2.7 version released.
2017	Apache Hadoop 3.0 version released.
2018	Apache Hadoop 3.1 version released.

How Does Hadoop Work?

It is quite expensive to build bigger servers with heavy configurations that handle large scale processing, but as an alternative, you can tie together many commodity computers with single-CPU, as a single functional distributed system and practically, the clustered machines can read the dataset in parallel and provide a much higher throughput. Moreover, it is cheaper than one high-end server. So this is the first motivational factor behind using Hadoop that it runs across clustered and low-cost machines.

Hadoop runs code across a cluster of computers. This process includes the following core tasks that Hadoop performs −

- Data is initially divided into directories and files. Files are divided into uniform sized blocks of 128M and 64M (preferably 128M).

- These files are then distributed across various cluster nodes for further processing.
- HDFS, being on top of the local file system, supervises the processing.
- Blocks are replicated for handling hardware failure.
- Checking that the code was executed successfully.
- Performing the sort that takes place between the map and reduce stages.
- Sending the sorted data to a certain computer.
- Writing the debugging logs for each job.