Unit -1

Part 1: Overview of Computing Paradigm

What is computing?

- Computing is the utilization of computers to complete a task. It involves both hardware & software functions performing some sort of task with a computer.
- This activity includes both developing the software and hardware as well.
- Examples of computing being used in everyday life: sending an email, swiping credit/debit cards etc.
- The utilization of computer technology to complete the task is known as computing.

Recent trends in Computing

1. Grid Computing

- Grid computing consists of a large number of computers which are connected parallel and forms a computer cluster.
- "The Grid" links together computing resources like PCs, workstations, servers, storage elements and provides the mechanism needed to access them.
- This combination of connected computers uses to solve a complex problem.
- In grid computing, this service of the computer is connected and run independent tasks. Grid computing uses a wide range of applications, for instance, mathematical, scientific, and educational tasks through several computing resources.
- By implementing our proposed Intranet Grid, it is very easy to download multiple files very fast.
- No need to worry about the security as authenticating is done each and every step taking place in Grid.

Advantages of grid computing: -

- It can solve more complex problems in a very short span of time.
- It can easily combine with other organization.
- It can make better use of existing hardware.

Disadvantages of grid computing: -

- It starts **learning curve.** (The *learning curve* shows that if a person performs similar task again and again, then after a period of time there will be an improvement in his/her performance.)
- It is very non interactive.
- It evolves grid software and standards.

2. Cluster Computing

- Cluster computing or High-Performance computing frameworks is a form of computing in which bunch of computers (nodes) that are connected through a LAN so that, they behave like a single machine.
- A computer cluster help to solve complex operations more efficiently with much faster processing speed, better data integrity than a single computer and they only used for mission-critical applications.
- Some of the critical Applications of **Cluster Computers are Google Search Engine and Weather Forecasting.**
- Cluster can be classified into two categories **Open and Close Cluster**.
- Open Cluster: **All nodes in Open Cluster are needed IPs**, and that are accessible through internet/web that cause more security concern.
- Close Cluster: On the other hand, Close Cluster are **hide behind the gateway node** and provide better security.

Types of Cluster computing

1. **Load-balancing clusters:** As the name implies, this system is used to distribute workload across multiple computers. That system distributes the processing load as possible across a cluster of computers.
2. **High availability (HA) clusters:** A high availability clusters (HA cluster) are the bunch of computers that can reliably utilize for redundant operations in the event of nodes failure in Cluster computing.
3. **High performance (HP) clusters:** This computer networking methodology use supercomputers and Cluster computing to solve advanced computation problems.

Advantages of using Cluster computing

1. **Cost efficiency**: In a Cluster computing Cost efficiency is the ratio of cost to output, that is the connecting group of the computer as computer cluster much cheaper as compared to mainframe computers.
2. **Processing speed:** The Processing speed of computer cluster is the same as a mainframe computer.
3. **Expandability:** The best benefit of Cluster Computing is that it can be expanded easily by adding the additional desktop workstation to the system.

High availability of resources: If any node fails in a computer cluster, another node within the cluster continue to provide uninterrupted processing. When a mainframe system fails, the entire system fails.

3. Distributed Computing

- A Distributed computing is a model of computation that is tightly related to Distributed Systems, refers to as multiple computer systems located at different places linked together over a network and use to solve higher level computation without having to use an expensive supercomputer.

- All the computers are tied together in a network either a Local Area Network (LAN) or Wide Area Network (WAN), communicating with each other so that different portions of a Distributed applications run on different computers from any geographical location.
- Every node on the Distributed computing is **autonomous machines** (do not physically share memory or processors but thereby sharing resources such as printers and databases).
- Distributed Systems have broken down into two parts: **the front end and the back end**.
- Grid computing is a based on distributed architecture and is the form of "distributed computing" or "peer-to-peer computing "that involving large numbers of computers physically connected to solve a complex problem.
- Standalone applications are traditional applications (or 3-tier old systems) that run on a single system; distributed applications run on multiple systems simultaneously.
- Traditional applications need to be installed on every system and make it hard to maintain. However, In Distributed computing, applications run on both simultaneously.
- With distributed computing, if a workstation that goes down, another workstation can resume the jobs.
- The **advantages of distributed computing** increased the speed with "absolute performance" and lower cost with more reliability than a non-distributed system.
- It is currently quite popular, and many businesses are converting to it.
- Extremely well-known example of distributed systems and applications of distributed computing used in **Telephone networks and cellular networks, Computer networks such as the Internet, Wireless sensor networks, Routing algorithms.**

4. Utility Computing

- The term **Utility Computing** refers to utility computing technologies and business models, which provides a service provider to its customers IT services, and they charge you by consumption.
- Examples of such IT services are computing power, storage or applications.
- The term utility refers to utility services such as electricity, telephone, water and gas that are provided by a utility company.
- Similar to the electricity or telephone if the customer receives the utility computing, the computing power on a shared computer network, its consumption is measured and billed on that basis.
- Utility computing is very similar to virtualization so that the total amount of web storage space along with the computing power that is available to the users is much larger compared to that of the single time-sharing computer.
- Multiple backend web servers are often used to make this kind of web service possible.
- The dedicated web servers may be used in cluster forms which are specifically created and then leased to the end users.
- The method of using a single such 'calculation' on multiple web servers is called the distributed computing.

Advantages of Utility Computing

- Utility computing reduces the cost of IT, given that existing resources can be used more effectively.
- The costs are transparent and the various departments of a company can be directly assigned.
- The companies achieve greater flexibility, because their IT resources more quickly and easily adapt to changeable demand.
- Overall, it is easier to manage the entire IT structure, as there will no longer be made for each application, which is a benefit for specific IT infrastructure.

5. Cloud Computing

- Cloud computing is the delivery of different services through the Internet.
- These resources include tools and applications like data storage, servers, databases, networking, and software.
- Rather than keeping files on a proprietary hard drive or local storage device, cloud based makes it possible to save them to a remote database.
- As long as an electronic device has access to the web, it has access to the data and the software programs to run it.
- Cloud computing is a popular option for people and businesses for a number of reasons including cost savings, increased productivity, speed and efficiency, performance, and security.
- Cloud computing can be both public and private.
- Public cloud services provide their services over the Internet for a fee.
- Private cloud services, on the other hand, only provide services to a certain number of people. These services are a system of networks that supply hosted services.
- There is also a hybrid option, which combines elements of both the public and private services.
- Cloud computing is new service but is being used by a number of different organizations from **big corporations to small businesses**, **non-profits to government agencies**, and even **individual consumers**.

Types of Cloud Services

- Regardless of the kind of service, cloud computing services provide users with a series of functions including:

  - Email
  - Storage, backup, and data retrieval
  - Creating and testing apps
  - Analysing data
  - Audio and video streaming
  - Delivering software on demand

Evolution of cloud computing

- The trend toward cloud computing started **in the late 1980s** with the concept of grid computing when, for the first time, a large number of systems were applied to a single problem, usually scientific in nature and requiring exceptionally high levels of parallel computation.
- In Europe, long distance optical networks are used to tie multiple universities into a massive computing grid in order that resources could be shared and scaled for large scientific calculations.
- Grid computing provided a **virtual pool** of computation resources but it's different than cloud computing.
- Grid computing specifically used to take maximum advantages from connected computers in parallel to solve a particular, individual problem, or to run a specific application.
- Cloud computing, on the other hand, used to take maximum advantages from multiple resources, including computing resources, to deliver an integrated "service" to the end user.
- **In grid computing**, the focus is on moving a workload to the location of the needed computing resources, which are mostly remote and are readily available for use. Usually, a grid is a cluster of servers on which a large task could be divided into smaller tasks to run in parallel. From this point of view, a grid could actually be viewed as just one virtual server. Grids also require applications to conform to the grid software interfaces.
- **In a cloud environment**, computing and extended IT and business resources, such as servers, storage, network, applications and processes, can be dynamically shaped or carved out from the underlying hardware infrastructure and made available to a workload. In addition, while a cloud can provision and support a grid, a cloud can also support non-grid environments, such as a three-tier Web architecture running traditional or Web 2.0 applications
- **In the 1990s**, the concept of virtualization was expanded beyond virtual servers to higher levels of abstraction—first the virtual platform, including storage and network resources, and subsequently the virtual application, which has no specific underlying infrastructure. **Utility computing** offered clusters as virtual platforms for computing with a metered business model.
- More recently software as a service **(SaaS)** has raised the level of virtualization to the application, with a business model of charging not by the resources consumed but by the value of the application to subscribers. **The concept of cloud computing has evolved from the concepts of grid, utility and SaaS**. It is an emerging model through which users can gain access to their applications from anywhere, at any time, through their connected devices.
- Companies can choose to share resources using **public or private clouds**, depending on their specific needs. **Public clouds** expose services to customers, businesses and consumers on the Internet. **Private clouds** are generally restricted to use within a company behind a firewall and have fewer security exposures as a result.

- As more enterprises add cloud computing the level of applications is migrating toward more mission critical and SaaS will become a support of IT strategies.
- A number of companies, including **Google, Microsoft, Amazon, and IBM,** have built enormous datacentre-based computing capacity all over the world to support their Web service offerings search, instant messaging, web-based retail.

Business driver for adopting cloud computing

1. **Business growth**

   Business growth is one of the top benefits organizations realize as a result of cloud adoption, with 52% of enterprises reporting increased growth since going cloud (2015 Cloud Enterprise Report).

2. **Efficiency**

   Efficiency is an extremely common cloud driver, with 71% of organizations worldwide ranking it a top area they hope to approve through cloud technology (2015 Cloud Enterprise Report).

3. **Experience**

   Next among the business drivers is improving the quality of the customer experience, which 45% of enterprises worldwide rank as a top cloud driver (although that number jumps to 61% looking at only organizations in the UK and Australia).

4. **Assurance**

   Finally, there is assurance, which is the idea that data will be more secure in the cloud and the user will attain better uptime because its solutions are maintained by providers that have built their businesses around these competencies.

5. **Agility**

   Improving IT agility, or enabling IT to be more responsive to business needs and react faster to market changes, is a top technology driver for 66% of organizations worldwide (2015 Cloud Enterprise Report). This goal is very possible in the cloud environment, as SaaS technologies mean that IT no longer needs to be consumed with traditional application management tasks.

6. **Cost**

   The cost driver has two sides: Reducing IT expenses and restructuring these expenses to spread them out over time thanks to the licensing model of SaaS technologies. While 39% of organizations do consider reducing IT expenses a key cloud driver (2015 Cloud Enterprise Report).

Cluster computing v/s Grid Computing v/s Cloud computing

	Cluster Computing	**Grid Computing**	**Cloud Computing**
Basic Idea	Aggregation of resources.	Segregation of Resources.	Consolidation of Resources.

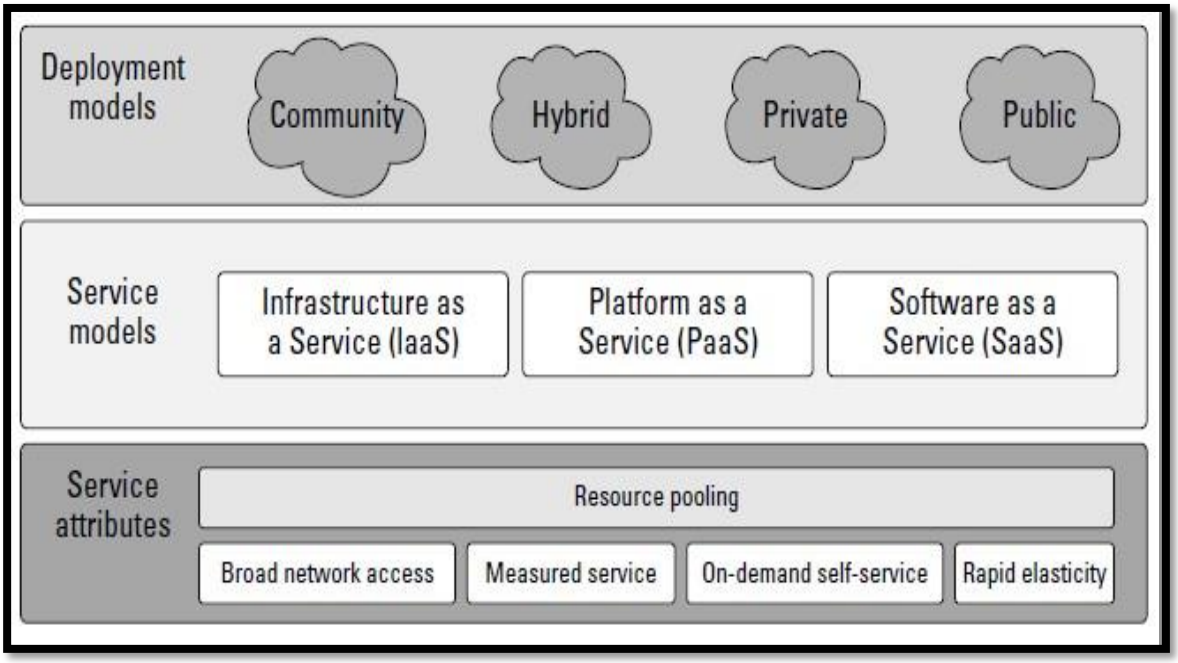
Running Processes	Same processes run on all computers over the cluster at the same time.	Job is divided into sub jobs each is assigned to an idle CPU so they all run concurrently.	Depends on service provisioning. Which computer offers a service and provisions it to the requesting clients.
Operating System	All nodes must run the same operating system.	No restriction is made on the operating system.	No restriction is made on the operating system.
Job Execution	Execution depends on job scheduling. So, jobs wait unit it's assigned a runtime.	Execution is scalable in a way that moves the execution of a job to an idle processor (node).	Self-Managed.
Suitable for Apps	Cascading tasks. If one tasks depends on another one.	Not suitable for cascading tasks.	On-demand service provisioning.
Location of nodes	Physically in the same location	Distributed geographically all over the globe.	Location doesn't matter
Homo/Heterogeneity	Homogenous	Heterogeneous	Heterogeneous
Virtualization	None	None	Virtualization is a key
Transparency	Yes	Yes	Yes
Security	High	High, but doesn't reach the level of cluster computing.	Lower than both types.
Interoperability	Yes	Yes	No
Application Domains	industrial sector, research centres, health care, and centres that offer services on the nation-wide level	industrial sector, research centres, health care, and centres that offer services on the nationwide level	Banking, Insurance, Weather Forecasting, Space Exploration, Business, IaaS, PaaS, SaaS
Implementation	Easy	Difficult	Difficult – need to be done by the host.
Management	Easy	Difficult	Difficult
Resource Management	Centralized (locally)	Distributed	Both centralized and distributed.

Internet	No internet access is required	Required	Required

Unit -1
Part 2: Introduction to Cloud Computing

Cloud Computing (NIST Model)

- Cloud computing is a model for enabling everywhere, 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.
- This cloud model is composed of five essential characteristics, three service models, and four deployment models



Service attributes:

- **On-demand self-service:** A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
- **Broad network access:** Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

- **Resource pooling:** The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. Examples of resources include storage, processing, memory, and network bandwidth.
- **Rapid elasticity:** Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
- **Measured service**: Cloud systems automatically control and optimize resource use by leveraging a metering capability[1] at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

Service Models:

- Cloud computing is based on service models. These are categorized into three basic service models which are –
- Infrastructure-as–a-Service (IaaS)
- Platform-as-a-Service (PaaS)
- Software-as-a-Service (SaaS)

Anything-as-a-Service (XaaS) is yet another service model, which includes Network-asa-Service, Business-as-a-Service, Identity-as-a-Service, Database-as-aService or Strategy-as-a-Service. The **infrastructure-as-a-Service (IaaS)** is the most basic level of service.

Infrastructure-as-a-Service (IaaS)

IaaS provides access to fundamental resources such as physical machines, virtual machines, virtual storage, etc.

Platform-as-a-Service (PaaS)

PaaS provides the runtime environment for applications, development and deployment tools, etc.

Software-as-a-Service (SaaS)

SaaS model allows to use software applications as a service to end-users.

Deployment Models:

Public Cloud

The **public cloud** allows systems and services to be easily accessible to the general public. Public cloud may be less secure because of its openness.

Private Cloud

The **private cloud** allows systems and services to be accessible within an organization. It is more secured because of its private nature.

Community Cloud

The **community cloud** allows systems and services to be accessible by a group of organizations.

Hybrid Cloud

The **hybrid cloud** is a mixture of public and private cloud, in which the critical activities are performed using private cloud while the non-critical activities are performed using public cloud.

History of cloud computing

- The concept of Cloud Computing came into existence in 1950 with implementation of mainframe computers, accessible via thin/static clients.
- Since then, cloud computing has been evolved from static clients to dynamic ones from software to services. The following diagram explains the evolution of cloud computing:

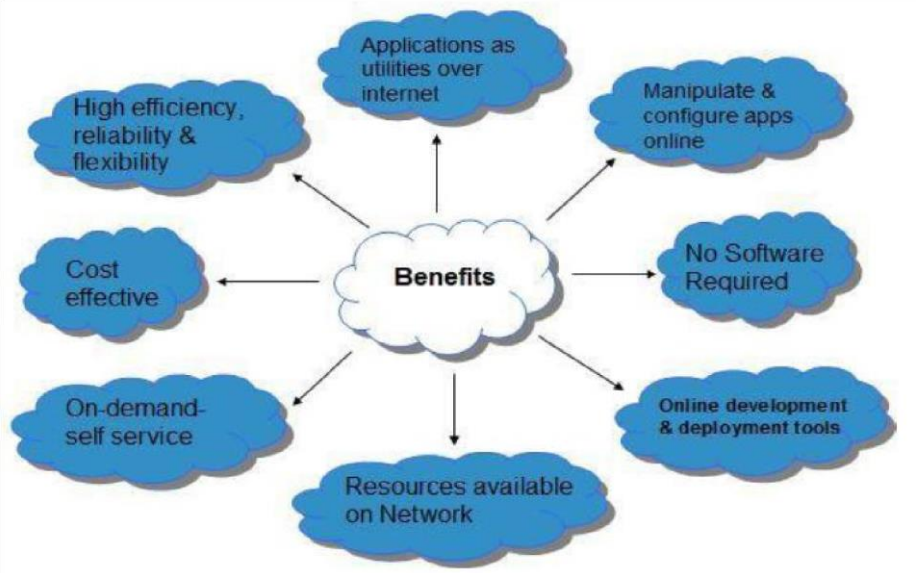
Date	Development
1950s	Large-scale servers at universities and companies were accessed by considerably weak terminals/clients.
1960s	John McCarthy foresaw that computing technology will be organized in the future like public electric and water utilities in 1960s.
1970s	Time sharing concept has arisen (Strachey, 1959).
1990s	In order to provide well-balanced band-width, telecommunication companies started to build virtual private networks (VPN) through point-to-point electric circuits.
2000s	2002: Amazon web service. 2006: Amazon s3. the first real cloud application. 2007-2008: Google and IBM created cloud service (Sevli, 2011). July 2010: Rackspace Hosting and NASA initiated an open-source cloud software entrepreneur which is known as Open Stack jointly. March 2011: IBM company introduced smart cloud framework. June 2012: Oracle company introduced Oracle Cloud.

Benefits of Cloud computing

Cloud Computing has numerous advantages. Some of them are listed below:

- One can access applications as utilities, over the Internet.
- Manipulate and configure the application online at any time.
- It does not require to install a specific piece of software to access or manipulate cloud application.
- Cloud Computing offers online development and deployment tools, programming runtime environment through Platform as a Service model.
- Cloud resources are available over the network in a manner that provides platform independent access to any type of clients.

- Cloud Computing offers on-demand self-service.
- The resources can be used without interaction with cloud service provider.
- Cloud Computing is highly cost effective because it operates at higher efficiencies with greater utilization. It just requires an Internet connection.
- Cloud Computing offers load balancing that makes it more reliable.



Cloud Service provider

- A cloud provider is a company that delivers cloud computing-based services and solutions to businesses and/or individuals.
- This service organization may provide rented and provider-managed virtual hardware, software, infrastructure and other related services.
- Cloud services are becoming increasingly desirable for companies because they offer advantages in terms of cost, scalability and accessibility.
- A cloud provider is also known as a utility computing provider.
- This role is typically related to that of a managed service provider (MSP), but usually, the latter provides other managed IT solutions.
- Following are few famous Cloud Service Provider

Amazon Web Services	Oracle Cloud
DigtialOcean	IBM Cloud
Rackspace	OpenNebula
LiquidWeb	Pivotal
Microsoft Azure	CloudSigma
Google Cloud Platform	Dell Cloud
VMware	LimeStone
Salesforce	Quadranet

Advantages of cloud computing

- **Lower costs:** Because cloud networks operate at higher efficiencies and with greater utilization, significant cost reductions are often encountered. **Ease of utilization:** Depending upon the type of service being offered, you may find that you do not require hardware or software licenses to implement your service.
- **Quality of Service:** The Quality of Service (QoS) is something that you can obtain under contract from your vendor.
- **Reliability:** The scale of cloud computing networks and their ability to provide load balancing and failover makes them highly reliable, often much more reliable than what you can achieve in a single organization.
- **Outsourced IT management:** A cloud computing deployment lets someone else manage your computing infrastructure while you manage your business. In most instances, you achieve considerable reductions in IT staffing costs.
- **Simplified maintenance and upgrade:** Because the system is centralized, you can easily apply patches and upgrades. This means your users always have access to the latest software versions.
- **Low Barrier to Entry:** In particular, upfront capital expenditures are dramatically reduced. In cloud computing, anyone can be a giant at any time.

Disadvantages of cloud computing

- **Requires good speed internet with good bandwidth:** To access your cloud services, you need to have a good internet connection always with good bandwidth to upload or download files to/from the cloud.
- **Downtime:** Since the cloud requires high internet speed and good bandwidth, there is always a possibility of service outage, which can result in business downtime.
- **Limited control of infrastructure:** Since you are not the owner of the infrastructure of the cloud, hence you don't have any control or have limited access to the cloud infra.
- **Restricted or limited flexibility:** The cloud provides a huge list of services, but consuming them comes with a lot of restrictions and limited flexibility for your applications or developments.
- **Ongoing costs:** Although you save your cost of spending on whole infrastructure and its management, on the cloud, you need to keep paying for services as long as you use them. But in traditional methods, you only need to invest once.
- **Security:** Security of data is a big concern for everyone. Since the public cloud utilizes the internet, your data may become vulnerable.
- **Vendor Lock-in:** Although the cloud service providers assure you that they will allow you to switch or migrate to any other service provider whenever you want, it is a very difficult process.
- **Technical issues:** Even if you are a tech whiz, the technical issues can occur, and everything can't be resolved in-house. To avoid interruptions, you will need to contact your service provider for support. However, not every vendor provides 24/7 support to their clients.

A list of advantages and disadvantages of cloud computing:

Advantages of Cloud	Disadvantages of Cloud
No cost of infrastructure	Good internet connection & bandwidth required
Minimum management and cost	Downtime
No administrative or management hassles	Limited control of infrastructure
Easy accessibility	Restricted or limited flexibility
Pay per use	Ongoing costs
Reliability	Security
Data control	Vendor lock-in
Data backup and recovery	Technical Issues
Huge cloud storage	NA

Assessing the Role of Open Standards

- When you consider the development of cloud computing to date, it is clear that the technology is the result of the convergence of many different standards.
- Cloud computing promise of scalability completely changes the manner in which services and applications are deployed.
- Without standards, the industry creates proprietary systems with vendor lock-in, sometimes referred to as “stovepipe” clouds. Because clients do not want to be locked into any single system, there is a strong industry push to create standards-based clouds.
- The cloud computing industry is working with these architectural standards:
  - Platform virtualization of resources
  - Service-oriented architecture
  - Web-application frameworks
  - Deployment of open-source software
  - Standardized Web services
  - Autonomic systems
  - Grid computing

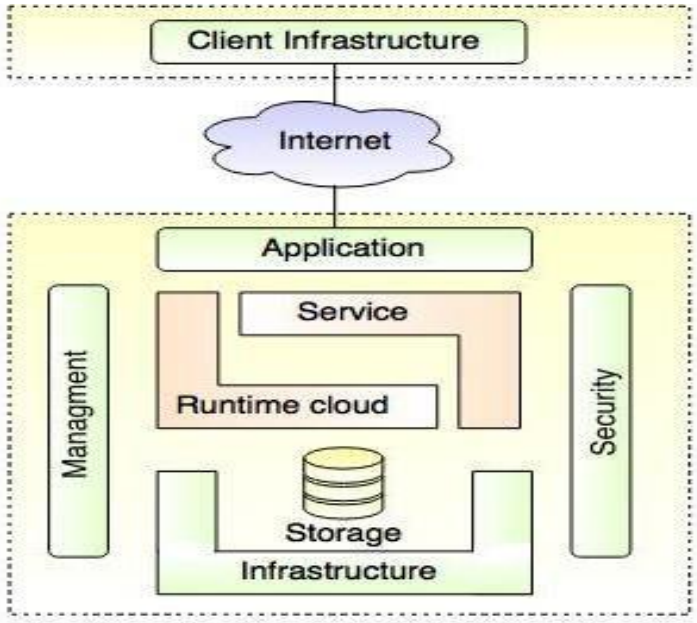
Unit -1
Part -3 Cloud Computing Architecture

Cloud Computing Architecture

- Cloud computing architecture consists of many loosely coupled cloud components.
- **The architecture is mainly dividing the cloud architecture into two parts:**
    1. Front End
    2. Back End

Each end is connected to others through a network, generally to the Internet.

View of cloud computing architecture



Front End

- The front end is the side of computer user or client.
- The cloud technology architecture also consists of **front-end** platforms called the cloud client which comprises **servers, thin & fat client, tablets & mobile devices**.
- It involves the interfaces and the applications that are necessary to access the Cloud Computing system.

Back End

- The back end is the cloud section of the system.
- It involves all the resources which are necessary to give Cloud computing services.
- It includes huge data storage, virtual machines, security mechanism, services, deployment models, servers etc.
- To give built-in security mechanism, traffic control and protocols is the responsibility of the back end.

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

Cloud computing v/s traditional computing architecture (client/server)

Meaning

- **Cloud** is everywhere and it manages the servers and network infrastructure management. The terms cloud-based refers to anything be it applications, resources or services that is made available to the users on demand through web-based tools via the Internet, as opposed to a direct connection to a server. It's called "cloud computing" because everything from applications to data centers to services is found in the cloud.
- **In Client-Server,** on the other hand, Server is a computer program that provides services to other computer programs and their users. Server based computing refers to the technology by which applications get implemented, controlled, and operated on the server rather than the client.

Technology

- **The term cloud** refers to a collection of dynamically configured shared resources based on network technology where each user has access to its own private resource called cloud that is offered by a third-party cloud service provider. These cloud service providers deliver their computing resources over the internet which can be further accessed through a web browser.
- **In Server based computing,** on the other hand, refers to the technology where a device or a program, otherwise known as a server, is designed to managing network resources. The servers accept and respond to requests made by another program, otherwise known as a client.

Application

- A **cloud-based** application is any software program or application that operates in the cloud space meaning it's a program running on a cloud infrastructure and can be accessed over the internet by various computing devices through a web browser or a program interface. The cloud applications can be installed on a private cloud.
- A **server-based application**, on the other hand, refers to a program or application stored on a remote server and accessed through a browser interface such as a web browser. Servers provide different services such as sharing resources or data among clients along with data access and persistence.

Architecture

- A **cloud computing** architecture is a conceptual model that encompasses all the components and subcomponents required for cloud computing in a cloud space. Cloud provides on-demand access to a networked collection of shared resources like servers, applications, storage, and networks, regardless of where the cloud is.
- **Server architecture**, on the other hand, is the basic foundation on which the server is created or deployed. It basically refers to a network in which clients request and receive service from

a centralized server and the server then responds to the requests. It defines how a server along with its components is designed, maintained and managed as a whole.

Cloud Computing	Client- Server computing
Cloud refers to a shared pool of computing resources that provides on-demand access to these resources via Internet.	Server refers to a dedicated computer which manages access to centralized resources in a network.
Cloud is based on Infrastructure-as-a-Service (IaaS) model that provides virtualized computing resources over the internet.	Server based computing refers to the technology where applications are implemented and controlled on the server.
A cloud based application is any software program or application that operates in the cloud space.	A server based application refers to a program or application stored on a remote server.
Cloud architecture is conceptual model that encompasses all the components and subcomponents required for cloud computing	Server architecture is the basic foundation on which the server is created or deployed.

How Cloud Computing Works?

- The cloud has to be divided into different layers.
- These layers are the **front-end** and **back-end** layers.
- Front-end layer is that part of the cloud which users can interact with.
- For example, when we log in to our Gmail account, we see the UI (user interface) where everything works on event-driven buttons and graphics.
- Similarly, a software also runs in the front end of the cloud.
- The back-end includes hardware as well as software that delivers the back-end data from the database to the front end.
- Cloud uses a network layer to connect different devices to provide access to resources that are residing in the centralized data center of the cloud.
- Cloud technology users can use the data center through the company's network or internet facilities.
- This technology provides various advantages: as users can access the cloud from **anywhere at any time**, but the network bandwidth should have to be more.
- This technology not only facilitates desktop and laptop users but the **mobile users** can also access their business systems based on their demand.
- As we already know that cloud computing is **fast and efficient**, applications running on the cloud take advantages of flexibility and computing power, i.e., the speed of processing a task.
- Many computers of a single organization work together along with their application on the cloud as if all the applications were running on a single machine. This flexibility of accessing the cloud resources allows users to use much or little of the resource based on the demand.
- In the Cloud computing system architecture, there is another mechanism of shifting the workload. Local machines don't have to perform massive lifting operations when it comes to

run applications. Cloud technology can handle those heavy loaded tasks automatically easily and efficiently. This brings down the hardware & software demands. The only thing that the users have to think is the cloud computing interface software of the system, which works merely as a web-browser in the front end of the user. The cloud's network takes care of the rest along with the back-end.

- The back-end is connected through a virtual network or internet. Other than that, there are few more components such as **Middleware, cloud resources**, etc. that includes the cloud computing architecture.
- The backend is used by service providers that include **various servers, computers, virtual machines & data storage facilities** that are combined to form the cloud technology. Its dedicated server handles each application in the system. The front end includes the cloud computing system or network that is used for accessing the cloud computing system. The cloud computing systems' interface varies from cloud to cloud.
- The back-end has two principal responsibilities:
    1. Provides traffic control mechanisms, security postures & governing the protocols
    2. To employ those internet protocols that are connected to the networked computer for communication
- One central server is used to manage the entire cloud system architecture. The server is only responsible for handling the smoothness of traffic without disruption.
- Middleware is a particular type of software that is used to perform processes & also connects networked computers. Depending on the demand of client/user, the storage is provided by the cloud technology's service provider.

Protocols used in Cloud computing

- Cloud computing protocols is a set of rules that allow 2 electronics item to connect and exchange information to one another. Used for storage, communication, for encryption, decryption, networking, security, user-login management etc.

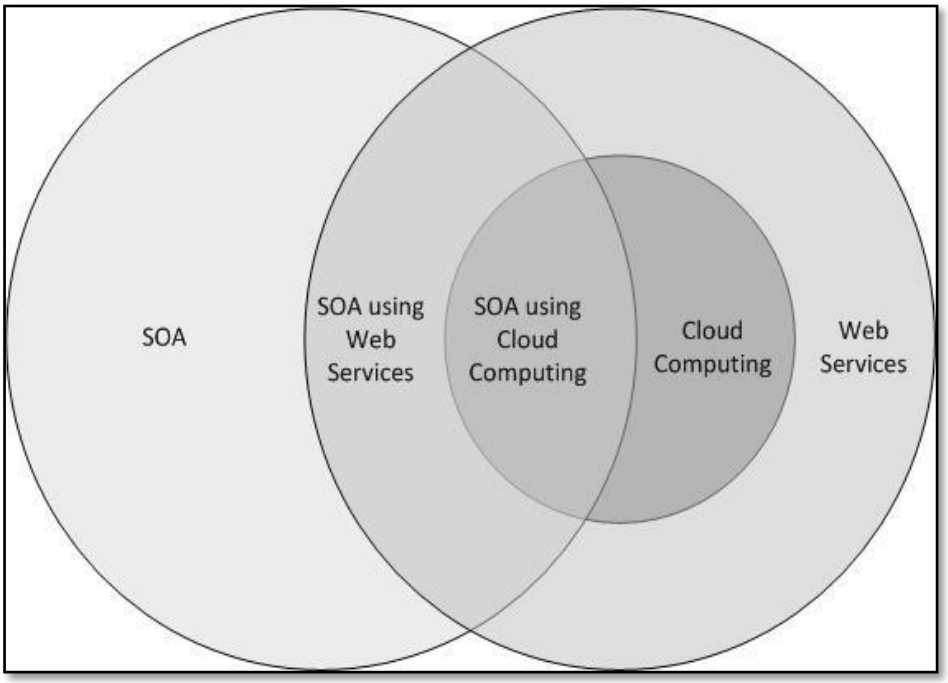
Examples of cloud computing protocols:

- ✓ Gossip Protocol
- ✓ Connection-less n/w protocol (CLNP)
- ✓ State Routing Protocol (SRP)
- ✓ Internet Group Management Protocol (IGMP)
- ✓ Secure Shell protocol (SSHP)
- ✓ Coverage Enhanced Ethernet Protocol (CEE)
- ✓ Media Transfer Protocol (MTP)

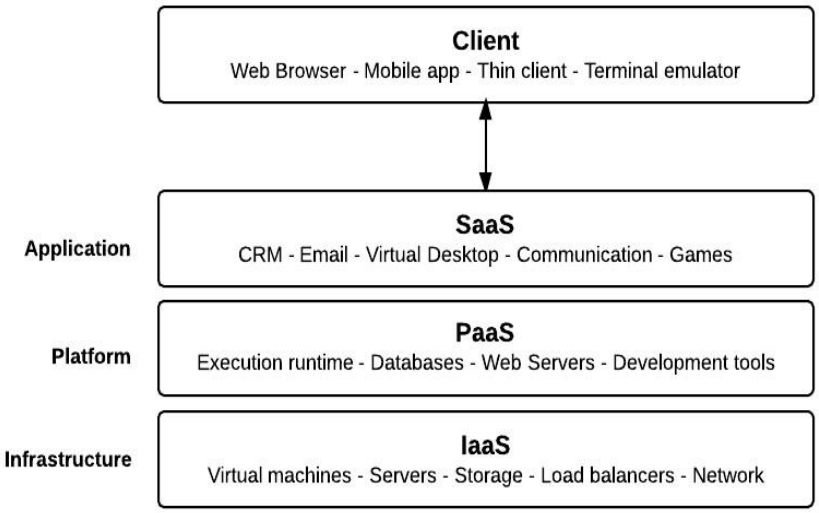
Role of Web Services in Cloud computing

- The following diagram illustrates the relationships among Web Services, service-oriented architecture (SOA), and Cloud Computing.
- Web Services encapsulates Cloud Computing in this diagram because Cloud Computing uses Web Services for connections.

- It is possible, however, to use Web Services in situations other than Cloud Computing.
- Web Services could be simply be a connection.
- It is possible to have a service-oriented architecture and not use Web Services for connections.
- The technology of Cloud computing entails the convergence of Grid and cluster computing, virtualization, Web services and Service Oriented Architecture (SOA) - it offers the potential to set IT free from the costs and complexity of its typical physical infrastructure, allowing concepts such as Utility Computing to become meaningful.
- Key players: IBM, HP, Google, Microsoft, Amazon Web Services, Salesforce.com, NetSuite, VMware.



Service Models of Cloud Computing



1. Software-as-a-Service (SaaS)

SaaS is known as 'On-Demand Software'.

- It is a software distribution model. In this model, the applications are hosted by a cloud service provider and publicized to the customers over internet.
- In SaaS, associated data and software are hosted centrally on the cloud server.
- User can access SaaS by using a thin client through a web browser.
- SAAS has become an increasingly widespread delivery model as underlying technologies that support Web services and service-oriented architecture (SOA) mature and new development approaches, such as Ajax, become popular.
- CRM, Office Suite, Email, games, etc. are the software applications which are provided as a service through Internet.
- The companies like Google, Microsoft provide their applications as a service to the end users.

Advantages of SaaS

- SaaS is **easy to buy** because the pricing of SaaS is based on monthly or annual fee and it allows the organizations to access business functionalities at a small cost, which is less than licensed applications.
- SaaS **needed less hardware**, because the software is hosted remotely, hence organizations do not need to invest in additional hardware.
- **Less maintenance cost** is required for SaaS and do not require special software or hardware versions.
- **Easier administration.**
- **Automatic updates and patch management.**
- **Compatibility:** all users will have the same version of software.
- **Global accessibility.**

Disadvantages of SaaS

- SaaS applications are totally dependent on Internet connection. They are not usable without Internet connection.
- It is difficult to switch amongst the SaaS vendors.

2. Platform-as-a-Service (PaaS)

- PaaS is a programming platform for developers. This platform is generated for the programmers to create, test, run and manage the applications.
- A developer can easily write the application and deploy it directly into PaaS layer.
- PaaS gives the runtime environment for application development and deployment tools.
- PAAS frees users from having to install in-house hardware and software to develop or run a new application.
- PAAS doesn’t replace a business’ entire infrastructure but instead, a business relies on PAAS providers for key services, such as Java development or application hosting.
- PAAS providers then charge for that access on a per-user basis or on a monthly basis.

- Users only need to log in and start using the platform-usually through a Web browser interface.
- **Google Apps Engine(GAE),** Windows Azure, SalesForce.com are the examples of PaaS.

Advantages of PaaS

- PaaS is easier to develop. Developer can concentrate on the development and innovation without worrying about the infrastructure.
- In PaaS, developer only requires a PC and an Internet connection to start building applications.
- Provides Security and redundancy.
- Build and deployment tools for rapid application management and deployment. Integration with other infrastructure components such as web services and databases Multi-tenancy, platform service that can be used by many concurrent users.
- Logging, reporting, and code instrumentation.

Disadvantages of PaaS

 One developer can write the applications as per the platform provided by PaaS vendor hence the moving the application to another PaaS vendor is a problem.

3. Infrastructure-as-a-Service (IaaS)

- IaaS is a way to deliver a cloud computing infrastructure like server, storage, network and operating system.
- The customers can access these resources over cloud computing platform i.e. Internet as an on-demand service.
- In IaaS, you buy complete resources rather than purchasing server, software, datacenter space or network equipment.
- IaaS was earlier called as Hardware as a Service(HaaS). It is a Cloud computing platform based model.
- HaaS differs from IaaS in the way that users have the bare hardware on which they can deploy their own infrastructure using most appropriate software.

Advantages of IaaS

- In IaaS, user can dynamically choose a CPU, memory storage configuration according to need.
- Users can easily access the vast computing power available on IaaS Cloud platform.

Disadvantages of IaaS

 IaaS cloud computing platform model is dependent on availability of Internet and virtualization services.

Deployment Models

There are four main cloud deployment models that differ significantly and for which most of the companies opt: a public, private, hybrid and a community one

1. **Private cloud:**

- The cloud infrastructure is provisioned for exclusive use by a **single organization** comprising multiple consumers.
- It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.
- The **advantages** of using a private cloud are:
  1. Individual development
  2. Storage and network components are customizable
  3. High control over the corporate information
  4. High security, privacy and reliability
- The Private cloud has the following **disadvantages**:
  1. **Poor scalability**: Private type of clouds is scaled within internal limited hosted resources.
  2. **Costly:** As it provides secured and more features, so it's more expensive than a public cloud.
  3. **Pricing:** is inflexible; i.e., purchasing new hardware for up-gradation is more costly.
  4. **Restriction:** It can be accessed locally within an organization and is difficult to expose globally.

2. Public Cloud

- Public cloud is a type of cloud hosting that allows the accessibility of systems & its services to its clients/users easily.

Some of the examples of those companies which provide public cloud facilities are IBM, Google, Amazon, Microsoft, etc.

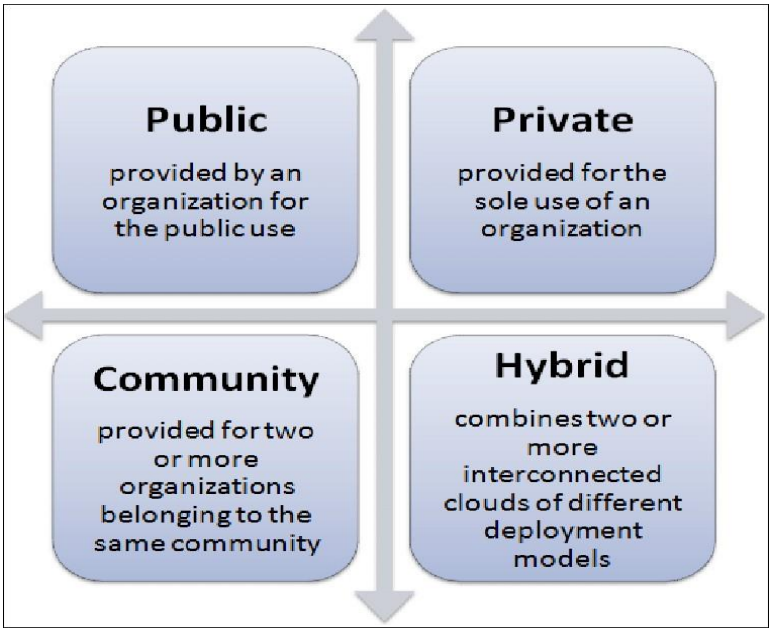
- This cloud service is open for use.
- Public clouds are available to the general public and data are created and stored on **third-party servers**.
- As server infrastructure belongs to service providers that manage them and administer pool resources, the need for user companies to buy and maintain their own hardware is eliminated.
- Provider companies offer resources as a service on a free of charge or pay-per-use basis via the Internet connection.
- At the same time, relying on a third party in running their infrastructure deprives users of knowing where their information is kept and who has access to it.
- The **advantages** of the Public cloud are:
  1. Flexible
  2. Reliable
  3. High Scalable
  4. Low cost
  5. Place independence
- This type also holds some **disadvantages** such as:
  1. Less Secured
  2. Poor Customizable

3. Community Cloud

- Community cloud is another type of cloud computing in which the setup of the cloud is shared manually among different organizations that belong to the same community or area.
- Example of such a community is where organizations/firms are there along with the financial institutions/banks.
- For joint business organizations, ventures, research organizations and tenders community cloud is the appropriate solution.
- The **advantages** of a community computing type include the following:
  1. Cost reduction
  2. Improved security, privacy and reliability
  3. Ease of data sharing and collaboration
- The disadvantages are:
  1. Higher cost than that of a public one
  2. Sharing of fixed storage and bandwidth capacity
  3. It is not widespread so far

4. **Hybrid cloud:**

- **Hybrid Cloud** is integrated, i.e., it can be a combination of two or more cloud servers, i.e., private, public or community combined as one architecture, but remain individual entities.
- Non-critical tasks such as development and test workloads can be done using public cloud whereas critical tasks that are sensitive such as organization data handling are done using a private cloud.
- In this Benefits of both public and private deployment models, as well as a community deployment model, are possible in a hybrid cloud hosting.
- It can cross isolation and overcome boundaries by the provider; hence, it cannot be simply categorized into any of the three deployments - public, private or community cloud.
- Advantages of Hybrid Cloud Computing are:
  1. Flexible
  2. Secure
  3. Cost Effective
  4. Rich Scalable
- Disadvantages of Hybrid Cloud are:
  1. Complex networking problem
  2. Organization's security Compliance


Public
provided by an organization for the public use
Private
provided for the sole use of an organization
Community
provided for two or more organizations belonging to the same community
Hybrid
combines two or more interconnected clouds of different deployment models

Unit – 2
Part -1 Infrastructure as a Service (IaaS)

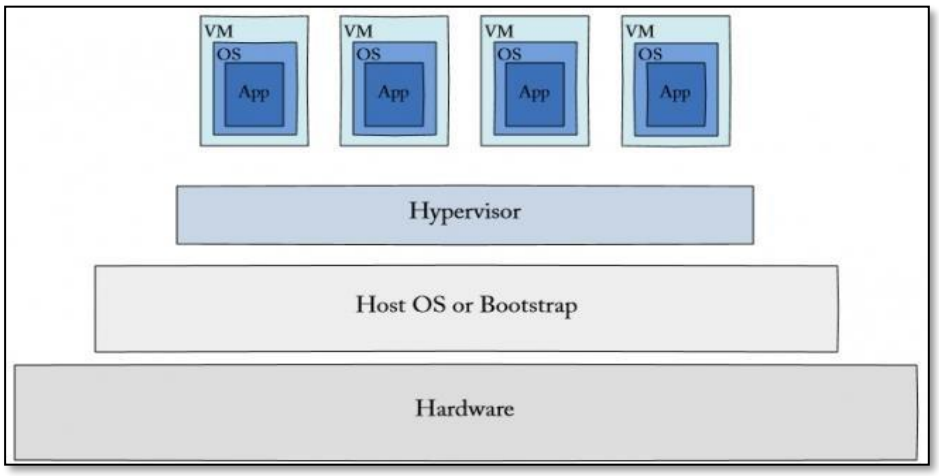
Introduction to IaaS

- Cloud infrastructure services, known as "Infrastructure as a Service" (IaaS), **deliver computer infrastructure, storage, and networking**.
- **IaaS**, as the name suggests, is a way of providing Cloud computing infrastructure such as virtual machines, storage drives, servers, operating systems & networks, which is also an on-demand service.
- Instead of purchasing servers or developing software, clients buy those resources as a fully outsourced service based on their requirement.
- "Public cloud" is considered as an infrastructure that consists of shared resources, based on a self-service over the Internet.
- In one word, it is the only layer of the cloud where the customer gets the platform for their organization to outsource IT infrastructure on a pay-per-use basis.
- IaaS provides users with:
  1. Load balancers
  2. Disk storage via virtual machines
  3. Software Packages
  4. IP address
  5. VLANs
- Advantages of IaaS are:
  1. **Dynamic:** Users can dynamically opt & configure devices such as CPU, storage drive, etc.
  2. **Easy Access:** Users can easily access the vast cloud computing power.
  3. **Renting:** Flexible and efficient while renting IT infrastructures.
  4. **Full control** of computer resources along with portability.
- Disadvantages of IaaS are as follows:
  1. Internet connection is a must.
  2. IaaS depends on virtualization services.
  3. This service restricts user-privacy & customization

Introduction to virtualization

- Virtualization is the ability which allows sharing the physical instance of a single application or resource among multiple organizations or users.
- This technique is done by assigning a name logically to all those physical resources & provides a pointer to those physical resources based on demand.

- Over an existing operating system & hardware, we generally create a virtual machine which and above it we run other operating systems or applications. This is called **Hardware Virtualization.**
- The virtual machine provides a separate environment that is logically distinct from its underlying hardware.
- Here, the system or the machine is the host & virtual machine is the guest machine. This virtual environment is managed by a firmware which is termed as a **hypervisor.**



- There are **several approaches** or ways to virtualizes cloud servers. These are:
- **Grid Approach**: where the processing workloads are distributed among different physical servers, and their results are then collected as one.
- **OS - Level Virtualization**: Here, multiple instances of an application can run in an isolated form on a single OS
- **Hypervisor-based Virtualization**: which is currently the most widely used technique
- With hypervisor's virtualization, there are various sub-approaches to fulfill the goal to run multiple applications & other loads on a single physical host.
- A technique is used to allow virtual machines to move from one host to another without any requirement of shutting down. This technique is termed as **"Live Migration"**.
- Another technique is used to actively load balance among multiple hosts to efficiently utilize those resources available in a virtual machine, and the concept is termed as **Distributed Resource Scheduling or Dynamic Resource Scheduling.**

Types of Virtualization

- The virtualization of cloud has been categorized into four different types based on their characteristics. These are:

1. Hardware Virtualization
2. Full Virtualization
3. Emulation Virtualization
4. Para-virtualization
5. Software Virtualization
6. OS Virtualization

7. Server Virtualization
8. Storage Virtualization

How Virtualization works in cloud?

- Virtualization plays a significant role in cloud technology and its working mechanism. Usually, what happens in the cloud - the users not only share the data that are located in the cloud like an application but also share their infrastructures with the help of virtualization.
- Virtualization is used mainly to provide applications with standard versions for the cloud customers & with the release of the latest version of an application the providers can efficiently provide that application to the cloud and its users and it is possible using virtualization only.
- By the use of this virtualization concept, all servers & software other cloud providers require those are maintained by a third-party, and the cloud provider pays them on a monthly or yearly basis.
- In reality, most of the today's hypervisor make use of a combination of different types of hardware virtualization. Mainly virtualization means running multiple systems on a single machine but sharing all resources (hardware) & it helps to share IT resources to get benefit in the business field.

Advantages of virtualization:

- The number of servers gets reduced by the use of virtualization concept
- Improve the ability of technology
- The business continuity also raised due to the use of virtualization
- It creates a mixed virtual environment
- Increase efficiency for development & test environment
- Lowers Total Cost of Ownership (TCO)

Features of virtualization:

1. Partitioning: Multiple virtual servers can run on a physical server at the same time
2. Encapsulation of data: All data on the virtual server including boot disks is encapsulated in a file format
3. Isolation: The Virtual server running on the physical server are safely separated & don't affect each other
4. Hardware Independence: When the virtual server runs, it can migrate to the different hardware platform

Different approaches to virtualization

- Server virtualization can be viewed as a part of overall virtualization trend in the IT companies that include network virtualization, storage virtualization & management of workload.
- This trend brings development in automatic computing.

For Server Virtualization, there are three popular approaches. These are:

1. Virtual Machine model
2. Para-virtual Machine model
3. Operating System (OS) layer Virtualization

1. **Virtual Machine model:**
   - It is based on host-guest paradigm, where each guest runs on a virtual replica of hardware layer.
   - This technique of virtualization provide guest OS to run without modification.
   - However it requires real computing resources from the host and for this a hypervisor or VM is required to coordinate instructions to CPU.
2. **Para-Virtual Machine model:**
   - It is also based on host-guest paradigm & uses virtual machine monitor too.
   - In this model the VMM modifies the guest operating system's code which is called 'porting'.
   - Like that of virtual machine, similarly the Para-virtual machine is also capable of executing multiple operating systems.
3. **Operating System Layer Virtualization**:
   - Virtualization at OS level functions in a different way and is not based on host-guest paradigm.
   - In this model the host runs a single operating system kernel as its main/core and transfers its functionality to each of the guests.
   - The guest must use the same operating system as the host.
   - This distributed nature of architecture eliminated system calls between layers and hence reduces overhead of CPU usage.
   - It is also a must that each partition remains strictly isolated from its neighbors because any failure or security breach of one partition won't be able to affect the other partitions.

Server Virtualization

- It is the division of physical server into several virtual servers and this division is mainly done to improvise the utility of server resource.
- In other word it is the masking of resources that are located in server which includes the number & identity of processors, physical servers & the operating system.
- This division of one physical server into multiple isolated virtual servers is done by server administrator using software.
- The virtual environment is sometimes called the **virtual private-servers**.
- In this process, the server resources are kept hidden from the user.
- This partitioning of physical server into several virtual environments; result in the dedication of one server to perform a single application or task.

Usage of Server Virtualization

- This technique is mainly used in web-servers which reduces the cost of web-hosting services.
- Instead of having separate system for each web-server, multiple virtual servers can run on the same system/computer.

The primary uses of server virtualization are:

- To centralize the server administration
- Improve the availability of server
- Helps in disaster recovery
- Ease in development & testing Make efficient use of server resources.

Advantages:

- **Cost Reduction:** Server virtualization reduces cost because less hardware is required.
- **Independent Restart:** Each server can be rebooted independently and that reboot won't affect the working of other virtual servers.

Types of Virtualization: Resource 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.

What does Virtual Provisioning mean?

- Virtual provisioning is a virtual storage network (VSAN)-based technology in which storage space is allocated on demand to devices.
- This process allows virtualized environments to control the allocation and management of physical disk storage connected with virtual machines (VM).
- Virtual provisioning is also known as **thin provisioning**. However, virtual provisioning is more relevant to a virtual environment, while thin provisioning is more relevant to physical computing implementations.

Hypervisor

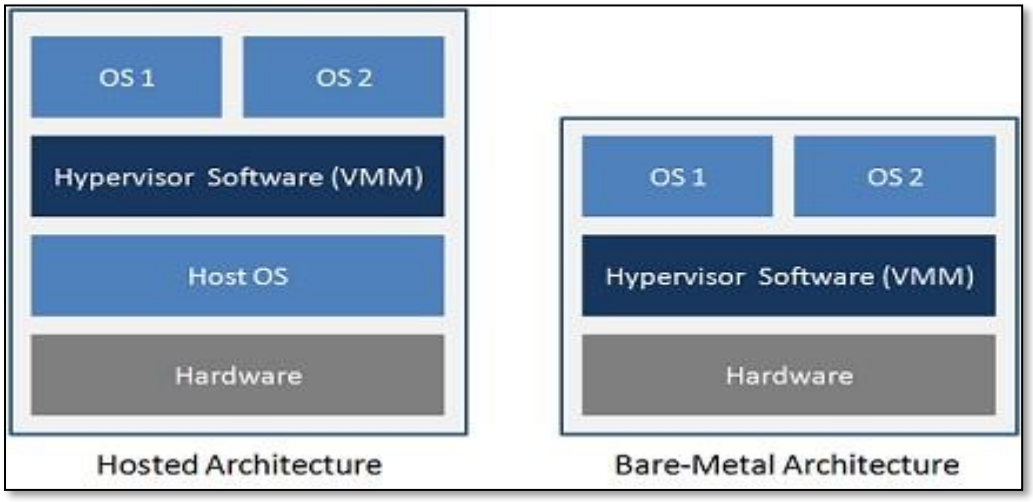
- A **hypervisor**, also known as a virtual machine monitor, is a process that creates and runs virtual machines (VMs).
- A hypervisor allows one host computer to support multiple guest VMs by virtually sharing its resources, like memory and processing. There are two types of hypervisors.
- Type 1 hypervisors, called **"bare metal,"** run directly on the host's hardware.
- Type 2 hypervisors, called **"hosted,"** run as a software layer on an operating system, like other computer programs.
- 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.

TYPE-1 Hypervisor:

- Hypervisor runs directly on 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.**

TYPE-2 Hypervisor:

- A Host operating system runs on underlying host system.
- It is also known as **'Hosted Hypervisor".**
- Basically a software installed on an operating system.
- Hypervisor asks operating system to make hardware calls.
- Example of Type 2 hypervisor include VMware Player or Parallels Desktop. Hosted hypervisors are often found on endpoints like PCs.



Machine Image

- Machine imaging is a process that is used to achieve the goal of system portability, provision, and deploy systems in the cloud through capturing the state of systems using a system image.
- A system image makes a copy or a clone of the entire computer system inside a single file.
- The image is made by using a program called system imaging program and can be used later to restore a system image.
- For example Amazon Machine Image (AMI) is a system image that is used in the cloud computing.
- The Amazon Web Services uses AMI to store copies of a virtual machine.
- An AMI is a file system image that contains an operating system, all device drivers, and any applications and state information that the working virtual machine would have.
- The AMI files are encrypted and compressed for security purpose and stored in Amazon S3 (Simple Storage System) buckets as a set of 10MB chunks.
- Machine imaging is mostly run on virtualization platform due to this it is also called as Virtual Appliances and running virtual machines are called instances.
- Because many users share clouds, the cloud helps you track information about images, such as ownership, history, and so on.
- The IBM Smart Cloud Enterprise knows what organization you belong to when you log in.
- You can choose whether to keep images private, exclusively for your own us e, or to share with other users in your organization.
- If you are an independent software vendor, you can also add your images to the public catalog.

Virtual Machine

- **A virtual machine**, known as a guest, is created within a computing environment, called a host.
- Multiple virtual machines can exist in one host at one time.

- Virtual machines are software computers that provide the same functionality as physical computers.
- Like physical computers, they run applications and an operating system.
- However, virtual machines are computer files that run on a physical computer and behave like a physical computer.
- In other words, virtual machines behave as separate computer systems.
- Virtual machines can also be used for other purposes such as server virtualization.
- Specialized software, called a hypervisor, emulates the PC client or server's CPU, memory, hard disk, network and other hardware resources completely, enabling virtual machines to share the resources.

Advantages of Virtual Machines:

- Provides disaster recovery and application provisioning options
- Virtual machines are simply managed, maintained, and are widely available Multiple operating system environments can be run on a single physical computer

Disadvantages of Virtual Machines:

- Running multiple virtual machines on one physical machine can cause unstable performance
- Virtual machines are less efficient and run slower than a physical computer.

Types of Virtual Machines:

1. **Process virtual machines**: Execute computer programs in a platform-independent environment. It masks the information of the underlying hardware or operating system. This allows the program to be executed in the same fashion on any platform.
2. **System virtual machines**: Support the sharing of a host computer's physical resources between multiple virtual machines.

Data storage in cloud computing(storage as a service)

Introduction

- Cloud storage is a service which enables saving the data on offside storage system.
- This data is managed by third-party.
- This data is accessible by a web services API.
- **Cloud Storage** is technology that allows you to save files in storage, and then access those files via the Cloud.
- Let's break down this definition. First, storage is the computer's ability to save files and other resources for later use.
- When you restart a computer, the files that are still available after the computer turns back on are saved and read from storage.
- Such storage commonly consists of a hard drive, a USB Flash drive, or another type of drive.
- Because local data drives can be damaged or stolen, an idea was developed to use data drives over a network as storage.
- This allows the drives to be secured in a data center and backed up automatically.

- Initially, network storage required fast local networks (LAN), but today we have a ubiquitous network called the Internet.
- The second part of Cloud Storage, the Cloud, represents the Internet. Any service, including storage, available over the Internet, is called Cloud service.
- For ex: GMAIL it is email in the Cloud and An Amazon MP3 player, that's music in the Cloud.

Storage Devices

Following are the categories of storage devices:

1) **Block Storage Devices –** This type of devices provide raw storage to the clients. This raw storage is separated for creating volumes. A volume is a recognizable unit of data storage.
2) **File Storage Devices –** The file storage devices are provided to the client in the form of files for maintaining its file system. Storage data is accessed using the Network File System(NFS).

Storage Classes of cloud

Following are the categories of storage classes:

1. Unmanaged Cloud Storage

- The storage is preconfigured for the customer, this is known as **unmanaged cloud storage.**
- The customer cannot format or install his own file system or change drive properties.

2. Managed Cloud Storage

- Managed cloud storage provides the online storage space on-demand.
- This system shows the user like raw disk that the user can partition and format.

Amazon Elastic Compute Cloud (Amazon EC2)

- **Amazon EC2 (Elastic Compute Cloud)** is a web service interface that provides resizable compute capacity in the AWS cloud.
- It is designed for developers to have complete control over web-scaling and computing resources.
- Using Amazon EC2 eliminates your need to invest in hardware up front, so you can develop and deploy applications faster.
- You can use Amazon EC2 to launch as many or as few virtual servers as you need, configure security and networking, and manage storage.
- Amazon EC2 enables you to scale up or down to handle changes in requirements or spikes in popularity, reducing your need to forecast traffic.

Features of Amazon EC2

Amazon EC2 provides the following features:

- Virtual computing environments, known as **instances**
- Preconfigured templates for your instances, known as Amazon Machine Images (AMIs), that package the bits you need for your server
- Various configurations of CPU, memory, storage, and networking capacity for your instances, known as **instance types**.

- Secure login information for your instances using key pairs.
- Storage volumes for temporary data that's deleted when you stop or terminate your instance, known as **instance store volumes**
- Persistent storage volumes for your data using Amazon Elastic Block Store, known as **Amazon EBS volumes**
- Multiple physical locations for your resources, such as instances and Amazon EBS volumes, known as **Regions and Availability Zones**
- A firewall that enables you to specify the protocols, ports, and source IP ranges that can reach your instances using security groups
- Static IPv4 addresses for dynamic cloud computing, known as Elastic IP addresses
- Metadata, known as tags, that you can create and assign to your Amazon EC2 resources
- Virtual networks you can create that are logically isolated from the rest of the AWS cloud, and that you can optionally connect to your own network, known as *virtual private clouds* (VPCs)

Pricing for Amazon EC2

- When you sign up for AWS, you can get started with Amazon EC2 for free using the AWS Free Tier
- Generally, Amazon EC2 priced on per instance / per hour basis.
- However, any instance can be rented on per month basis as well. In such case, Reserved and Spot Instances pricing can be applied resulting in significant discount. Instances are priced depending on their "size", namely how much CPU and RAM included.
- Amazon EC2 provides the following purchasing options for instances:

1. On-Demand Instances

Pay for the instances that you use by the second, with no long-term commitments or upfront payments.

2. Savings Plans

You can reduce your Amazon EC2 costs by making a commitment to a consistent amount of usage, in USD per hour, for a term of 1 or 3 years.

3. Reserved Instances

You can reduce your Amazon EC2 costs by making a commitment to a specific instance configuration, including instance type and Region, for a term of 1 or 3 years.

4. Spot Instances

Request unused EC2 instances, which can reduce your Amazon EC2 costs significantly.

Amazon EC2 Compute Unit

- Amazon's EC2 in addition to being one of the oldest and most mature cloud server platforms, also provides clearly defined CPU tiers across its 8 different instance sizes.
- These are defined in terms of ECUs (EC2 Compute Unit) where 1 ECU is the equivalent CPU capacity of a 1.0-1.2 GHz 2007 Opteron or 2007 Xeon processor.
- Their instance sizes includes the following:
  - ✓ Small/m1.small (32-bit) = 1 ECU
  - ✓ Large/m1.large = 4 ECUs
  - ✓ High-CPU Medium/c1.medium (32-bit) = 5 ECUs
  - ✓ High-Memory Extra Large/m2.xlarge = 6.5 ECUs

- ✓ Extra Large/m1.xlarge = 8 ECUs
- ✓ High-Memory Double Extra Large/m2.2xlarge = 13 ECUs
- ✓ High-CPU Extra Large/c1.xlarge = 20 ECUs
- ✓ High-Memory Quadruple Extra Large/m2.4xlarge = 26 ECUs

Storage of Amazon EC2

Economical, High-Scale Storage Choices

1. **Amazon Glacier-** It is an extremely low-cost storage service. It offers secure and fast storage for data archiving and backup.
2. **Amazon Elastic Block Store (EBS)-** It provides block-level storage to use with Amazon EC2 instances. Amazon Elastic Block Store volumes are network-attached and remain independent from the life of an instance.
3. **AWS Storage Gateway-** This AWS service is connecting on-premises software applications with cloud-based storage. It offers secure integration between the company's on-premises and AWS's storage infrastructure.

Companies using AWS

- Instagram
- Zoopla
- Pinterest
- Netflix
- Dropbox
- Etsy
- Talkbox
- Playfish
- Ftopia

Eucalyptus

- Eucalyptus is open source software for building AWS-compatible private and hybrid clouds.
- As an Infrastructure as a Service (IaaS) product, Eucalyptus allows your users to provision your compute and storage resources on-demand.
- Amazon has partnered with Eucalyptus to deliver an Infrastructure as a Service (IaaS) product.
- As part of the deal, Amazon Web Services (AWS) is letting the IaaS provider tap into its application programming interfaces (APIs).
- Eucalyptus says it is now “fully compatible with the Amazon Web Services API, which means you can use or reuse your existing AWS-compatible tools, images (AMIs), and scripts to manage your own hybrid and on premise clouds.”
- Eucalyptus’s IaaS service is now compatible with the following AWS services: EC2, EBS, AMI, S3, and IAM.

Unit 2
Part -2 Cloud Security

Infrastructure Security

- Cloud computing utilizes three delivery models (SaaS, PaaS, and IaaS) to provide infrastructure resources, application platform and software as services to the consumer.
- These service models need different level of security in the cloud environment.
- Cloud service providers and customers are responsible for security and privacy in cloud computing environments but their level of responsibility will differ for different delivery models.
- Infrastructure as a Service (IaaS) serves as the foundation layer for the other delivery models, and a lack of security in this layer affects the other delivery models.
- In IaaS, although customers are responsible for protecting operating systems, applications, and content, the security of customer data is a significant responsibility for cloud providers.
- In Platform as a service (PaaS), users are responsible for protecting the applications that developers build and run on the platforms, while providers are responsible for taking care of the users' applications and workspaces from one another.
- In SaaS, cloud providers, particularly public cloud providers, have more responsibility than clients for enhancing the security of applications and achieving a successful data migration.
- In the SaaS model, data breaches, application vulnerabilities and availability are important issues that can lead to financial and legal liabilities.

INFRASTRUCTURE SECURITY: THE NETWORK LEVEL

- As network level of infrastructure security is concerned, it is important to distinguish between public clouds and private clouds.
- With private clouds, there are no new attacks, vulnerabilities, or changes in risk specific to this topology that information security personnel need to consider.
- If public cloud services, changing security requirements will require changes to the network topology and the manner in which the existing network topology interacts with the cloud provider's network topology should be taken into account.
- All data on the network need to be secured.
- Strong network traffic encryption techniques such as Secure Socket Layer (SSL) and the Transport Layer Security (TLS) can be used to prevent leakage of sensitive information.
- Several key security elements such as data security, data integrity, authentication and authorization, data confidentiality, web application security, virtualization vulnerability, availability, backup, and data breaches should be carefully considered to keep the cloud up and running continuously.

- There are four significant risk factors in this use case:
  1. Ensuring the confidentiality and integrity of organization's data-in-transit to and from a public cloud provider
  2. Ensuring proper access control
  3. Ensuring the availability of the Internet-facing resources
  4. Replacing the established model of network zones and tiers with domains.

INFRASTRUCTURE SECURITY - THE HOST LEVEL

- When reviewing host security and assessing risks, the context of cloud services delivery models (SaaS, PaaS, and IaaS) and deployment models public, private, and hybrid) should be considered.
- The host security responsibilities in SaaS and PaaS services are transferred to the provider of cloud services.
- IaaS customers are primarily responsible for securing the hosts provisioned in the cloud in terms virtualization software security, customer guest OS or virtual server security.

INFRASTRUCTURE SECURITY - THE APPLICATION LEVEL

- Software security or applications should be a crucial element of a security program.
- Most enterprises with information security programs have yet to introduce an application security program to address this domain.
- Most websites are secured at the network level while there may be security loopholes at the application level which may allow information access to unauthorized users.
- Software and hardware resources can be used to provide security to applications. In this way, attackers will not be able to get control over these applications and change them.
- XSS attacks, Cookie Poisoning, Hidden field manipulation, SQL injection attacks, and Google Hacking are some examples of threats to application level security which resulting from the unauthorized usage of the applications.
- Designing and implementing applications aims at deployment on a cloud platform will require existing application security programs to reexamine current practices and standards. The application security spectrum ranges from single-user applications to multiuser ecommerce applications used by many users.

The level is responsible for managing

- Application-level security threats;
- End user security;
- SaaS application security;
- PaaS application security;
- Customer-deployed application security
- IaaS application security
- Public cloud security limitations

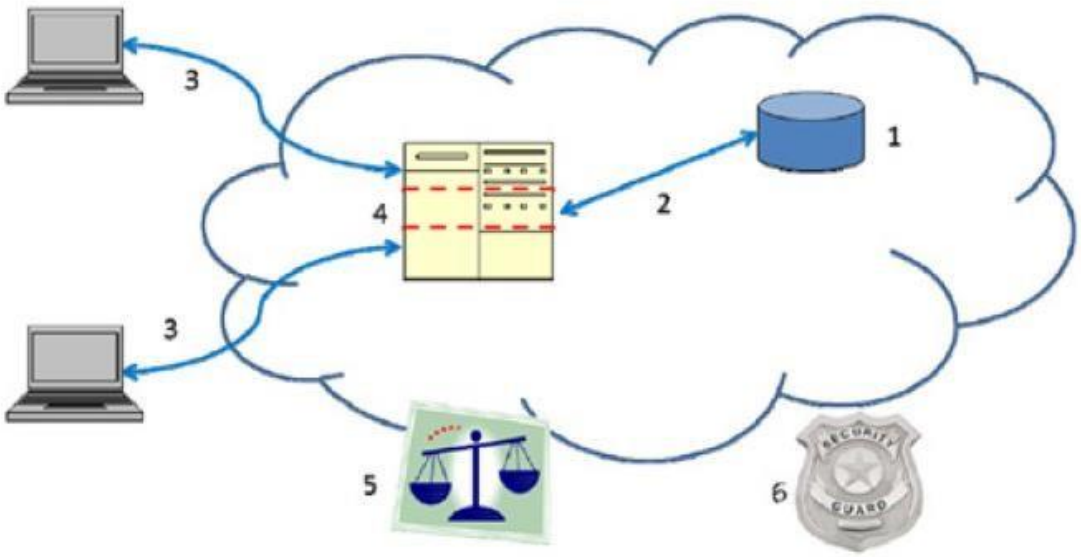
Data Security and Storage

- Majority of cloud service providers store customers' data on large data centers.

- Although cloud service providers say that data stored is secure and safe in the cloud, customers' data may be damaged during transition operations from or to the cloud storage provider.
- When multiple clients use cloud storage or when multiple devices are synchronized by one user, data corruption may happen.
- Different encryption techniques like public and private key encryption for data security can be used to control access to data.
- Backups or use of multiple providers can help companies to protect services from such failure and ensure data integrity in cloud storage.
- **Security** in cloud computing is a major concern. Data in cloud should be stored in encrypted form. To restrict client from accessing the shared data directly, proxy and brokerage services should be employed.

Data privacy and security Issues

- There are numerous security issues for cloud computing as it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management.
- Therefore, security issues for many of these systems and technologies are applicable to cloud computing. For example, the network that interconnects the systems in a cloud has to be secure.
- Virtualization paradigm in cloud computing leads to several security concerns. For example, mapping the virtual machines to the physical machines has to be carried out securely.
- Data security involves encrypting the data as well as ensuring that appropriate policies are enforced for data sharing.
- In addition, resource allocation and memory management algorithms have to be secure. These six areas of security are:
  (1) security of data at rest,
  (2) security of data in transit,
  (3) authentication of users/applications/ processes,
  (4) robust separation between data belonging to different customers, (5) cloud legal and regulatory issues, and (6) incident response.



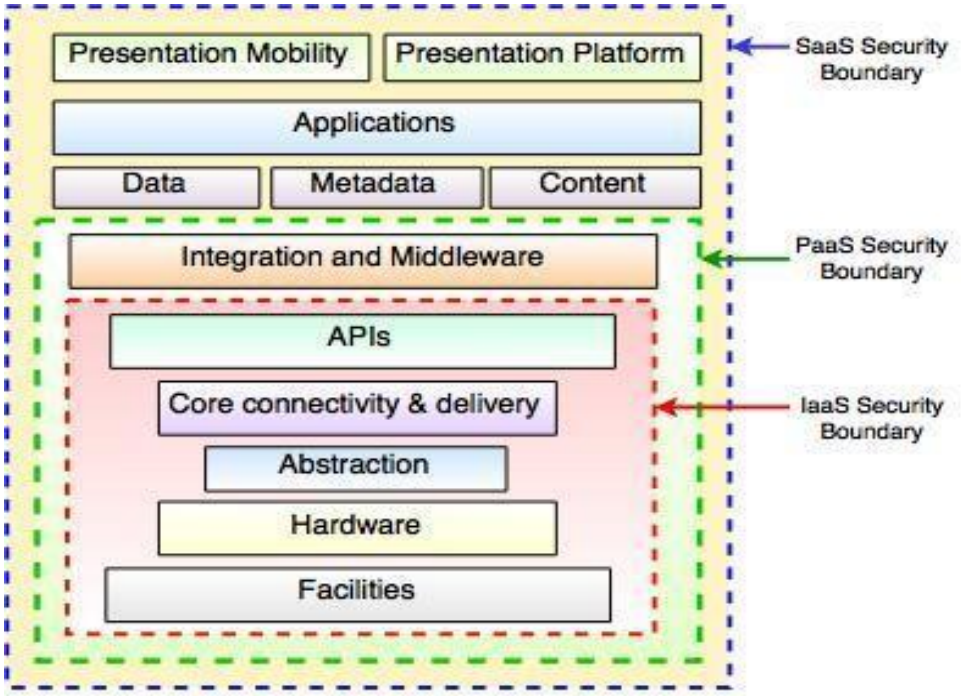
Security Planning

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

- Select resource that needs to move to the cloud and **analyze its sensitivity to risk**.
- Consider cloud service models such as IaaS, PaaS, and SaaS. These models require customer to be responsible for security at different levels of service.
- Consider the cloud type to be used such as public, private, community or hybrid.
- Understand the cloud service provider's system about 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

- A particular service model defines the boundary between the responsibilities of service provider and customer.
- **Cloud Security Alliance (CSA)** stack model defines the boundaries between each service model and shows how different functional units relate to each other.
- 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 of the service inherits capabilities and security concerns of the model below.
- IaaS provides the infrastructure, PaaS provides platform development environment, and SaaS provides operating environment.
- IaaS has the least level of integrated functionalities and integrated security while SaaS has the most.
- This model describes the security boundaries at which cloud service provider's responsibilities end and the customer's responsibilities begin.
- Any security mechanism below the security boundary must be built into the system and should be maintained by the customer.
- Although each service model has security mechanism, the security needs also depend upon where these services are located, in private, public, hybrid or community cloud.

Understanding Data Security

- Since all the data is transferred using Internet, data security is of major concern in the cloud. Here are key mechanisms for protecting data.
    - Access Control
    - Auditing
    - Authentication
    - Authorization

- All of the service models should incorporate security mechanism operating in all abovementioned areas.

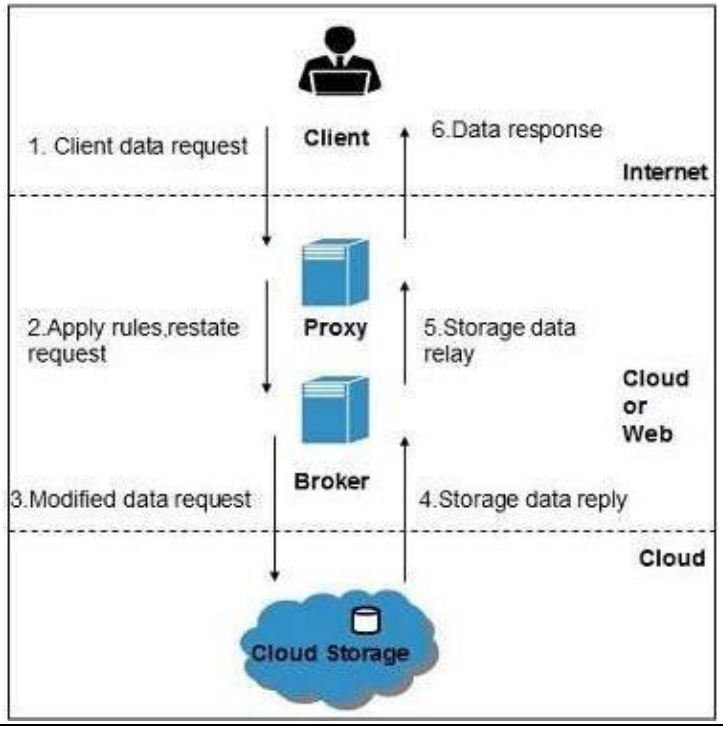
Isolated Access to Data

- Since data stored in cloud can be accessed from anywhere, we must have a mechanism to isolate data and protect it from client's direct access.
- Brokered Cloud Storage Access is an approach for isolating storage in the cloud. In this approach, two services are created:
    - A broker with full access to storage but no access to client.
    - A proxy with no access to storage but access to both client and broker.

Working Of Brokered Cloud Storage Access System

When the client issues request to access data:

- The client data request goes to the external service interface of proxy.
- The proxy forwards the request to the broker.
- The broker requests the data from cloud storage system.
- The cloud storage system returns the data to the broker.
- The broker returns the data to proxy.
- Finally the proxy sends the data to the client.
- All of the above steps are shown in the following diagram:



Authentication in cloud computing

- There are multiple methods to authenticate cloud users and many issues that come along with these methods.

- Cloud computing is helping businesses to store a large amount of data at relatively low costs but it is essential these service providers offer methods to ensure users are authenticated.
- There are multiple authentication techniques in cloud computing suited for different applications and use cases when it comes to the cloud.
- The best cloud authentication method depends on your preferences but each is a supported method.

Cloud Authentication Methods

1. **API Keys**
    - This method doesn't require client libraries and is transparent to the user.
    - This method identifies the project by creating a strong association between a key and a project.
    - API keys are less secure as they are vulnerable to man-in-the-middle attacks.
    - API keys can easily be added to any HTTP call as a query parameter in the header because they don't require a client library.
2. **Firebase Authentication**
    - This type of authentication provides backend services, app SDKs, and libraries to authenticate users to a mobile or web app.
    - This method authenticates users, using a variety of credentials like Google, Facebook, Twitter or GitHub.
    - The Firebase authentication method uses a client library to sign a JSON Web Token, JWT, with a private key after the user has successfully signed in.
    - This method then validates the JWT, through a proxy, was signed by Firebase and that the issuer matches the setting in API configuration.
3. **Auth0 Authentication**
    - This method not only authenticates and authorizes apps and APIs but it is also stack, device, and identity agnostic.
    - This method supports several providers and security assertion markup language specification.
    - Much like Firebase Authentication, this method also provides backend services, SDKs and user interface libraries for authenticating users in web and mobile apps.
    - Also, like Firebase Authentication, this method validates the JWT was signed and the issuer matches the API configuration.
4. **Google Authentication**
    - This authentication method allows users to authenticate by signing in with their Google account.
    - Once the user is authenticated, they have access to all Google services and a Google ID token can be used to make calls to Google APIs and Cloud Endpoints APIs.
    - This method also verifies that the JWT was signed by Google and the issuer is listed on the API configuration.

5. **Google Authorization and Service Accounts**
    - With this method, a JWT can be generated and signed using a service account and Google-provided client library for a Google Cloud Platform project.
    - This method uses the public key to validate a Google-signed JWT and to ensure that Google is listed as the issuer in the API configuration.
    - For this method, Google ID tokens are recommended for service accounts because the API producer only needs to white list Google as an issuer for all service accounts.

Cloud Computing Authentication Issues

1. Privacy Issues
2. Lack of Transparency
3. Security Issues
4. The Possibility of Exploitation of the Authentication Mechanism
5. Different Authentication Technologies Presents Challenges to Customers

- When it comes to cloud computing, service providers require customers to store their account information in the cloud, giving service providers access to this information.
- For many customers, this presents a privacy issue for them. The lack of transparency in the cloud makes it difficult for customers to ensure the proper rules are enforced.
- Customers using multiple cloud services have more copies of their information out there in the cloud. This causes security issues for customers and cloud service providers.
- Multiple copies of accounts lead to multiple authentication processes and provide the possibility to exploit the authentication mechanism.
- Cloud service providers use different authentication technologies for authenticating users and while this has less of an impact on SaaS than PaaS and IaaS, it presents challenges to customers.
- The major importance of authentication in cloud computing is for users to ensure their projects and information are safe and there when they need it.
- While there are still a few issues associated with cloud service providers being able to perform authentication methods without any challenges or security fears, it is important to remember just how new cloud computing is and the amount of room it has for progress.

Cloud contracting Model

1. **Selecting a cloud service:** Choosing the appropriate cloud service and deployment model is the critical first step in procuring cloud services.
2. **Cloud service provider and end-user agreements:** Terms of service and all CSP/customer-required agreements need to be integrated fully into cloud contracts.
3. **Service-level agreements:** SLAs need to define performance with clear terms and definitions, demonstrate how performance is being measured, and specify what enforcement mechanisms are in place to ensure that SLAs are met.
4. **CSP, agency, and integrator roles and responsibilities:** Careful delineation between the responsibilities and relationships among the federal agency, integrators and the CSP are needed in order to effectively manage cloud services.

5. **Standards:** The use of the National Institute of Standards and Technology's Cloud Computing Reference Architecture and agency involvement in standards are necessary for cloud procurements.
6. **Security:** Agencies must clearly detail the requirements for CSPs to maintain the security and integrity of data existing in a cloud environment.
7. **Privacy:** If cloud services host "privacy data," agencies must adequately identify potential privacy risks and responsibilities and address those needs in the contract.
8. **E-discovery:** Federal agencies must ensure that all data stored in a CSP environment is available for legal discovery by allowing all data to be located, preserved, collected, processed, reviewed and produced.
9. **Freedom of Information Act:** Federal agencies must ensure that all data stored in a CSP environment is available for appropriate handling under FOIA.
10. **E-records:** Agencies must ensure that CSPs understand and assist federal agencies in compliance with the Federal Records Act and obligations under that law.

COMMERCIAL AND BUSINESS CONSIDERATIONS

There are a number of contract types **Consumer to business:**

- Typically these contracts relate to free cloud services, such as Facebook, where the cloud provider makes its money through advertising and/or the secondary processing of customer data.
- This type of contract has no scope for negotiation, and consumers generally have few rights under the contract.

Business to business:

- These contracts generally relate to services which an enterprise is paying for.
- There is usually little scope for negotiation, but the contract will usually vest more rights to the consumer – although the cloud provider's liability for service performance (including data damage and loss) may in some cases be very limited.
- The contract may also permit the cloud provider to unilaterally modify both the service and the contract, and place technical and contractual constraints on switching from one provider to another.

Bespoke (personalized) contracts:

- Cloud providers rarely offer scope for negotiation of their contracts, it is not correct to say that there is never any negotiation.
- Cloud providers have been known to negotiate specific agreements with those consuming organizations viewed as particularly influential or large volume.
- Cloud contracts vary: some are balanced and fair to both parties, and others are unbalanced, favoring the cloud provider.

Explain data privacy and security issues.

CLOUD SECURITY ISSUES

- Security is a major issue in IT business environment.

- Since customers and users shifted from Grid computing to Cloud computing in their business, many security issues appeared, which is a major concern for the Cloud provider due to the risk of losing customers.
- The Cloud Computing is mainly built on virtualization environment, that increase more risk of securing the cloud.

Virtual Security issues:

- The virtual environment area of the cloud computing is the most sensitive and important part of the cloud.
- This is because all the devices in the cloud are connected virtually through virtual networks that are running and managing the IT infrastructures and virtual servers in the cloud.
- In virtualization technology, multiple Virtual Machines (VM's) can run on top of a single physical machine, and can run on any OS within each VM's to manage the infrastructure.

  One of the main **virtual security issues** in the cloud are attacks on the network between VM's, and the trust between different VM's .
- There are others problems, such as non-secure Apps and vulnerability in VM's, which allow any unauthorized access.

1) Network Attacks in Virtual cloud:

- Running many different virtualization products increases the attackers (especially the hackers) perimeter.
- Amazon's cloud computing service (EC2), could be used to hack into other systems by using EC2 cloud service to allow a brute force attack, that will fire 400,000 passwords per second at a secured wireless network.
- Within a period of twenty minutes the system would had been attacked.

The attackers hacked and shut down Sony's online customer networks in April 2011.

 Hackers used cloud based attacks to disrupt service to roughly 100 million users worldwide .

2) Distributed Denial of Service (DDOS) Attacks: This attack targets the networks and servers.

- It makes the network traffic and users being denied to access a certain Internet-based service in the cloud.
- In worst cases the attackers will use bonnets to perform DDOS. In order to stop hackers of attacking the network, face blackmail is provided.
- DDOS attacks should be considered as threats for cloud providers such AWS, Google Apps, and Microsoft Cloud.
- These scenarios show us that cloud computing network is still not secure, and this will drive us to non-secure applications.

3) Non-Secure Apps:

- Cloud applications security is a complicated issue for organizations and customers if they ignore securing their data before deploying it in the cloud.
- They need to consider the new threats and attacks spread
- Non-Secure applications opens the doors for further threats that could result in attacking the cloud through the network and Application Programming Interface (API).
- Man in The Middle attack is one of the problems for non-secure apps.
- This attack works as eavesdropping. Here, the attacker creates independent connections with the victims and transmits messages between them to make them believe that they are talking directly to each other over a private connection when in fact the entire conversation is run and controlled by the attacker.
- Facebook application is prone to Man- In -The -Middle attack (MITM) on users' data.

4) Domain Name Server (DNS) Attacks:

- It's easy for attackers to attack DNS in cloud computing when the users or customers try to call the server by name.
- Because, names are much easier to remember than Internet Protocol (IP) addresses, the attacker will create a temporary malicious cloud to fake the user or customers.

  Hence using IP address is not always feasible in DNS since customers will route malicious cloud.

- It may happen that even after all the DNS security procedures are implemented, security problems would exist based on the mode selected between the sender and the receiver.

Physical Security Issues

- Physical security issues are the other part of the cloud computing security.
- Although the data is stored in the virtual server in the cloud, it must also be stored in physical locations within physical hardware.
- Physical security in the cloud represents the physical machines and storage in the datacenter.
- Physical security issues shows as a loss of physical control, human attacks, power failure, access control, and third party trust.
- Those physical issues need to be protected also from any insider and outsider attackers.
- Usually the outside threats are easier to deal with than the inside threats because the outside attacks have been already prepared for through risk assessment plans.
- However, the internal physical security threats in cloud datacenter constitute the top risks in the cloud.

1) Loss of Physical Control:

- The loss of physical access control occurs when the customers join the cloud either by keeping their applications in the cloud, or using cloud storage for saving their data.
- This loss of control results in issues and concerns for the customers, such as trust and privacy of their data in the cloud provider's datacenter, control over their data in the cloud, and legal restrictions by cloud provider

a) Privacy and Data

 With private, public and community clouds, customer's data may not remain in the same system. In other words, it will not be located in the customer premises any more.

b) Control over Data

Customers need to have a full control over their data, and not limited control and accountability within Public clouds such as (IAAS) implementation, and through (PAAS) operations.

 Customers need to have confidence that the provider will offer services with appropriate controls.

c) Legal and Regulatory Compliance

- It may be difficult or unrealistic for customers to utilize public clouds if their data need to be processed.
- This is a subject to legal restrictions or regulatory compliance.
- Customers should expect providers to build and certify their cloud to address the needs of regulated markets, and achieve certifications and trust confidentiality between customers and providers of the services.

2) Human Attacks:

- Human attacks happen when unauthorized personal tries to access the datacenter. This attack for datacenter could be man in the middle attack, or malicious insiders such as an employee of the datacenter.
- These kinds of attacks are examples of the cloud provider losing their significant control over securing datacenters and authorizing human attacker to enter their premises.

3) Power Failure:

- In the event that the datacenter of cloud providers is faced with any kind of problems which causes power failure, and the providers do not have any disaster recovery plan, then the data in the cloud is at risk if it is not saved by the customer and user during the downtime.
- This give rise to the possibility of attackers accessing the servers through the man in the middle attacks .
- Amazon’s cloud services infrastructure faced a power failure issue in their datacenter in August 2011 where many people who were using AWS were affected by such an outage because all the services were disconnect.

Unit - 3
Part 1- Platform as a Service (PaaS)

Introduction to PaaS: What is PaaS?

- PaaS cloud computing platform is a developer programming platform which is created for the programmer to develop, test, run and manage the applications.
- A developer is able to write the application as well as deploy it directly into this layer easily.
- PaaS extend and abstract the IaaS layer by removing the hassle of managing the individual virtual machine.
- In PaaS cloud computing platform, back end scalability is handled by the cloud service provider and the end user does not have to worry about to manage the infrastructure.
- All the infrastructure to run the applications will be over the internet.

Advantages of PaaS cloud computing layer

1. **Simplified Development**
   Developers can focus on development and innovation without worrying about the infrastructure.
2. **Lower risk**
   No requirements of up-front investment in hardware and software. Developers only need a PC and an internet connection to start building applications.
3. **Prebuilt business functionality**
   Some PaaS vendors also provide already defined business functionality so that users can avoid building everything from very scratch and hence can directly start the projects only.
4. **Instant community**
   PaaS vendors frequently provides online communities where developer can get the ideas, share experiences and seek advice from others.

5. **Scalability**
   Applications deployed can scale from one to thousands of users without any changes to the applications.

Disadvantages of PaaS cloud computing layer

1. **Vendor lock-in**
   One have to write the applications according to the platform provided by PaaS vendor so migration of an application to another PaaS vendor would be a problem.
2. **Data Privacy**
   Corporate data, whether it can be critical or not, will be private so if it is not located within the walls of the company there can be a risk in terms of privacy of data.
3. **Integration with the rest of the systems applications**
   It may happen that some applications are local and some are in cloud. So there will be chances of increased complexity when we want to use data which in the cloud with the local data.

Top vendors who are providing PaaS cloud computing platform

1. Google Apps Engine (GAE)
2. SalesFroce.com
3. Windows Azure
4. AppFog
5. Openshift
6. Cloud Foundary from VMware

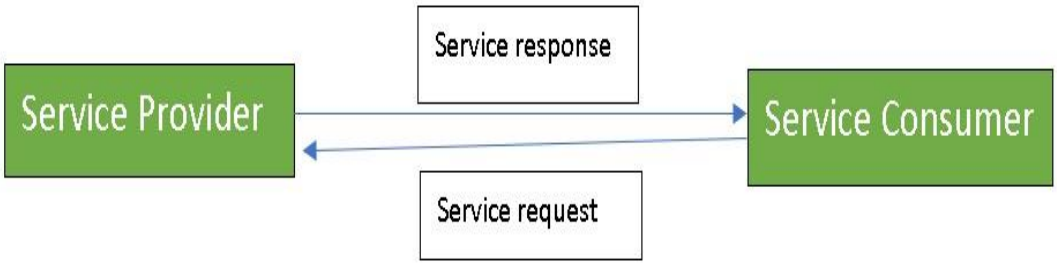
Service Oriented Architecture (SOA)

Service-Oriented Architecture (SOA) is an architectural approach in which applications make use of services available in the network. In this architecture, services are provided to form applications, through a communication call over the internet.

- SOA allows users to combine a large number of facilities from existing services to form applications.
- SOA includes a set of design principles that structure system development and provide means for integrating components into decentralized system.
- SOA based computing packages functionalities into a set of interoperable services, which can be integrated into different software systems belonging to separate business domains.
- SOA provides access to reusable Web services over a TCP/IP network, which makes this an important topic to cloud computing going forward.

There are two major roles within Service-oriented Architecture:

- **Service provider:** The service provider is the maintainer of the service and the organization that makes available one or more services for others to use.
- **Service consumer:** The service consumer can locate the service metadata in the registry and develop the required client components to bind and use the service.



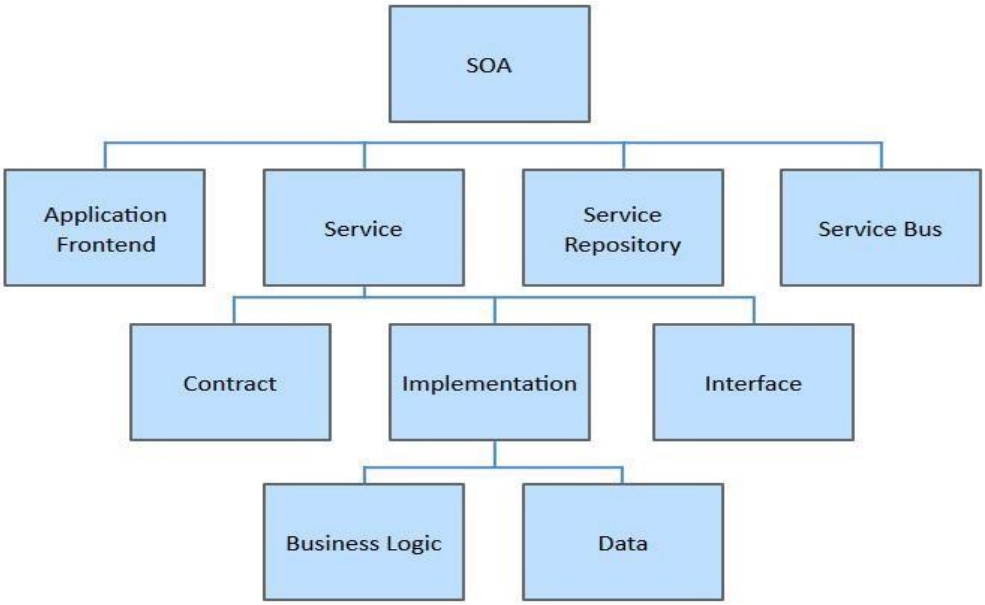
Advantages of SOA:

- **Service reusability:** In SOA, applications are made from existing services. Thus, services can be reused to make many applications.
- **Easy maintenance:** As services are independent of each other they can be updated and modified easily without affecting other services.
- **Platform independent:** SOA allows making a complex application by combining services picked from different sources, independent of the platform.
- **Availability:** SOA facilities are easily available to anyone on request.
- **Reliability:** SOA applications are more reliable because it is easy to debug small services rather than huge codes
- **Scalability:** Services can run on different servers within an environment, this increases scalability

Disadvantages of SOA:

- **High overhead:** A validation of input parameters of services is done whenever services interact this decreases performance as it increases load and response time.
- **High investment:** A huge initial investment is required for SOA.
- **Complex service management:** When services interact they exchange messages to tasks. the number of messages may go in millions. It becomes a unmanageable task to handle a large number of messages.

Elements/Components of SOA



Practical applications of SOA:

SOA is used in many ways around us whether it is mentioned or not.

1. SOA infrastructure is used by many armies and air force to deploy situational awareness systems.
2. SOA is used to improve the healthcare delivery.
3. Nowadays many apps are games and they use inbuilt functions to run. For example, an app might need GPS so it uses inbuilt GPS functions of the device. This is SOA in mobile solutions.
4. SOA helps maintain museums a virtualized storage pool for their information and content.

Unit - 3

Part 2- Software as a Service (SaaS)

Introduction to SaaS

- SaaS is a software distribution model in which applications are hosted by a cloud service provider and made available to customers over internet. SaaS is also known as "OnDemand Software".
- In SaaS, software and associated data are centrally hosted on the cloud server. SaaS is accessed by users using a thin client via a web browser.

Advantages of SaaS cloud computing layer

1. Easy to buy

SaaS pricing is based on a monthly fee or annual fee, SaaS allows organizations to access business functionality at a low cost which is less than licensed applications.

Unlike traditional software which is sold as a licensed based with an up-front cost (and often an optional ongoing support fee), SaaS providers generally pricing the applications using a subscription fee, most commonly a monthly or annually fee.

2. Less hardware required

The software is hosted remotely, so organizations don't need to invest in additional hardware.

3. Low Maintenance required

Software as a service removes the necessity of installation, set-up, and often daily unkeep and maintenance for organizations. Initial set-up cost for SaaS is typically less than the enterprise software. SaaS vendors actually pricing their applications based on some usage parameters, such as number of users using the application. So SaaS does easy to monitor and automatic updates.

4. No special software or hardware versions required

All users will have the same version of software and typically access it through the web browser. SaaS reduces IT support costs by outsourcing hardware and software maintenance and support to the IaaS provider.

Disadvantages of SaaS cloud computing layer

1. Security

Actually data is stored in cloud, so security may be an issue for some users. However, cloud computing is not more secure than in-house deployment. Learn more cloud security.

2. Latency issue

Because the data and application are stored in cloud at a variable distance from the end user, so there is a possibility that there may be more latency while interacting with the application than a local deployment. So, SaaS model is not suitable for applications whose demand response times are in milliseconds.

3. Total Dependency on Internet

Without internet connection, most SaaS applications are not usable.

4. Switching between SaaS vendors is difficult

Switching SaaS vendors involves the difficult and slow task of transferring the very large data files over the Internet and then converting and importing them into another SaaS also.

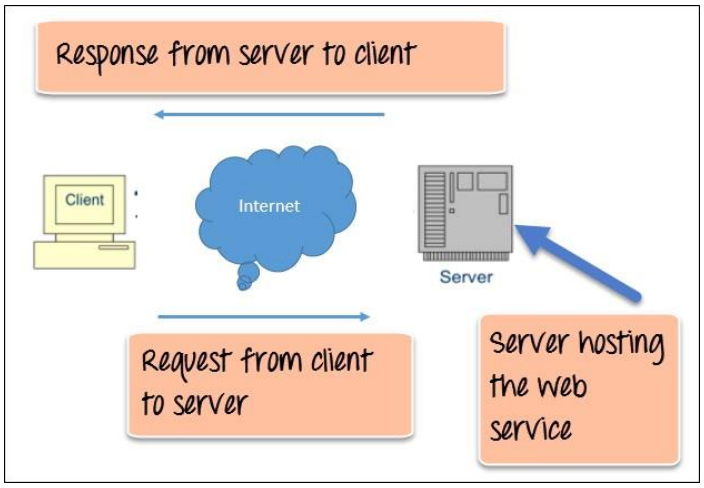
What is Web Service?

Web service is a standardized medium to propagate communication between the client and server applications on the World Wide Web.

A web service is a software module which is designed to perform a certain set of tasks.

- The web services can be searched for over the network and can also be invoked accordingly.

- When invoked the web service would be able to provide functionality to the client which invokes that web service.



- The client would invoke a series of web service calls via requests to a server which would host the actual web service.
- These requests are made through what is known as **remote procedure calls**. Remote Procedure Calls**(RPC)** are calls made to methods which are hosted by the relevant web service.
- As an example, **Amazon provides** a web service that provides prices for products sold online via amazon.com.
- The front end or presentation layer can be in **.Net or Java** but either programming language would have the ability to communicate with the web service.
- The main component of a web service is the data which is transferred between the client and the server, and that is XML.
- **XML (Extensible markup language)** is a counterpart to HTML and easy to understand the intermediate language that is understood by many programming languages.
- So when applications talk to each other, they actually talk in XML.
- This provides a common platform for application developed in various programming languages to talk to each other.
- Web services use something known as SOAP **(Simple Object Access Protocol)** for sending the XML data between applications.
- The data is sent over normal HTTP.
- The data which is sent from the web service to the application is called a SOAP message.
  - The SOAP message is nothing but an XML document.
- Since the document is written in XML, the client application calling the web service can be written in any programming language.

Type of Web Service

There are mainly two types of web services.

1. SOAP web services.
2. RESTful web services.

Advantages of web services

1. **Exposing Business Functionality on the network** - A web service is a unit of managed code that provides some sort of functionality to client applications or end users.
2. **Interoperability amongst applications** - Web services allow various applications to talk to each other and share data and services among themselves.
3. **A Standardized Protocol which everybody understands** - Web services use standardized industry protocol for the communication.
4. **Reduction in cost of communication** - Web services use SOAP over HTTP protocol, so you can use your existing low-cost internet for implementing web services.

Web 2.0

- Web 2.0 is the name used to the describe the second generation of the world wide web, where it moved static HTML pages to a more interactive and dynamic web experience.
- Web 2.0 is focused on the ability for people to collaborate and share information online via social media, blogging and Web-based communities.
- Web 2.0 are websites and applications that make use of user-generated content for endusers.
- Web 2.0 is characterized by greater user interactivity and collaboration, more persistent network connectivity and enhanced communication channels.
- One of the most significant differences between Web 2.0 and the traditional World Wide Web (WWW, retroactively referred to as Web 1.0) is greater collaboration among Internet users, content providers and enterprises.

Elements of Web 2.0

- **Wikis:** Websites that enable users to contribute, collaborate and edit site content. Wikipedia is one of the oldest and best-known wiki-based sites.
- The increasing prevalence of Software as a Service (SaaS), web apps and cloud computing rather than locally-installed programs and services.
- **Mobile computing**, also known as **nomadicity**, the trend toward users connecting from wherever they may be.
- **Mash-ups**: Web pages or applications that integrate complementary elements from two or more sources.
- **Social networking:** The practice of expanding the number of one's business and/or social contacts by making connections through individuals. Social networking sites **include Facebook, Twitter, LinkedIn and Google+**.
- **User-generated content (UGC):** Writing, images, audio and video content -- among other possibilities -- made freely available online by the individuals who create it.
- **Unified communications (UC):** The integration of multiple forms of call and multimedia/cross-media message-management functions controlled by an individual user for both business and social purposes.
- **Social curation**: The collaborative sharing of content organized around one or more particular themes or topics. Social content curation sites include Reddit, Digg, Pinterest and Instagram.

Web OS

- Web OS is designed as a distributed system.
- The Web OS framework enables a new paradigm for Internet services.
- Web OS goal is to provide a platform which allows the user to benefit from the computational potential offered by the Web.
- It's aimed is to make available to all sites of the network resources to execute computations for which local resources are missing.
- The kernel of a Web OS node is a system, a reactive system responding to requests from users or system.
- A Web OS-node integrates user, server, and applications.
- It is capable of providing a set of services, which can pass on to each other requests when appropriate.
- Each Web OS node is using its own warehouses to store and continuously update information about the node and available services and resources.
- It's basically a virtual desktop that gives user communication tools like email, productivity tools like word processing and ability to play games and any other application that user would find on a typical OS like Microsoft Windows.
- Web OS is network based service where a user can access his system through network. It is an introduction of one or more operating system in the category of Web operating systems.
- Web OS was introduced as a thought that one might be able to play with application, store data, for sharing on the web from anywhere.
- Today Web OS are capable of storing large amount of data as large as 30 GB. User can share applications.

Task of WebOS

- In these a company provides computer services to users through an Internet connection.
- The provider runs a system of computers that include application servers and databases.
- With some systems, people access the applications using Web browsers.
- With other systems, users must download a program that creates a system-specific client.
- A client is software that accesses information or services from other software.
- A Web OS might look like a traditional OS, but it doesn't manage user computer's hardware or software.
- A Web OS allows user to access applications stored not on user computer, but on the Web.
- The applications exist wholly or in part on Web servers within a particular provider network.
- When user saves information in an application, user might not store it on user computer. Instead, user saves the information to databases connected to the Internet.
- Some Web operating systems also give user the option to save information to user local hard disk drive.

CHARACTERISTICS OF WEB OPERATING SYSTEM:

- Free sign up for personal use Online application services.

- No maintain charge and security cost
- Access to any Website
- Work as a social networking
- While the operating system will work as well as the Website.

FEATURES AVAILABLE IN WEBOS

- **Open API:** the typology of Application Programming Interface that it uses
- **Open-source:** the possibility for users and developers to contribute to the enrichment of the Web OS by creating new applications and widgets
- **Integrated apps:** the applications that the Web OS features by default (text editor) **Audio-video Player:** the availability of a media player within the Web OS **Photo editing tool:** the availability of a tool that allows the user to edit images.
- **E-mail client:** the presence of an email client.
- **Instant Messaging:** the availability of an integrated instant messenger.
- **Calendar:** the existence of a calendar.
- **Collaboration** - Conferencing tools: the presence of online collaboration tools (such as VoIP)
- **Mini-Browser:** the integration of a Web browser
- **File storage:** the amount of space if available to store files online **File sharing support:** the support for file sharing with other users.
- **Desktop Search:** the presence of a desktop search engine within the Web OS

Case Study on SaaS

- **Organization: British Gas SaaS provider: Salesforce.com**
- **Application: CRM -** Customer relationship management *(*CRM) is a technology for managing all your company's relationships and interactions with customers and potential customers.
- **British Gas Services**, part of the Centrica group, is the leading domestic central heating and gas appliance installation company in the UK With **no centralized CRM system**, its Central Heating Installations (CHI) business wanted to overcome the inefficiencies. The business also wanted to improve on the manual, paper-based customer support processes that made tracking, accountability, and the ability to capture institutional knowledge difficult.
- BGS CHI implemented Salesforce.com and has seen considerable benefits. "Automated workflows route leads to appropriate individuals and provide preset responses to webcaptured leads," says Sexton.
- 'speed to market' is critical for us and therefore, as there is no infrastructure to "stand up", the solution can be ready to switch on in four months rather than six to 12 months for traditional solutions.
- Finally, cost profiling looks different as there is no large capital outlay as with a normal license purchase over time.
- However, where SaaS cost is consistent an on-premise solution will become cheaper.
- "We will now be able to systematically track sales leads and customer interaction, not possible with the former paper-based, disconnected support system.

- Sales and support benefit from new visibility into each other's respective activities with customers sharing one common view of customer issues allows for better customer service and more insight into up-sell and cross-sell opportunities."

Unit - 3
Part 3- Service Management in Cloud

Service Level Agreements (SLAs)

- A service-level agreement (SLA) is a contract between a service provider and its internal or external customers that documents what services the provider will provide and defines the service standards the provider is required to meet.
- Service providers need SLAs to help them manage customer expectations and define the situations under which they are not responsible for performance issues.
- Customers can also benefit from SLAs in that they describe the performance characteristics of the service, which can be compared with other vendors' SLAs.
- For a service provider, the SLA is typically one of two foundational agreements it has with customers.
- Many service providers establish a master services agreement to establish the general terms and conditions in which they will work with customers.
- Earlier, in cloud computing all Service Level Agreements were negotiated between a client and the service consumer.
- Nowadays, with the initiation of large utility-like cloud computing providers, most Service Level Agreements are standardized until a client becomes a large consumer of cloud services.
- Service level agreements are also defined at different levels which are mentioned below:

1. **Customer-based SLA**
   - A customer based SLA is an agreement with one customer, covering all the services used by this customer.
   - Let’s consider the relationship between you and your telecom operator.
   - You use the voice services, SMS services, data services, and several other services of the telecom operator.
   - For all these services, you have only one contract between you and the telecom operator.
   - Similarly, if the IT service provider provides several services for the business and the customers, and if all the service levels are documented in one service level agreement for the provided services, it will be a customer based SLA.
2. **Service-based SLA:**
   - A service based SLA covers one service for all customers.

- Let's consider that the IT service provider provides customer query service for many customers.
- In a service based service level agreement, the service level of the customer query service will be same for all customers that will be using this service.
- For instance, if the finance department and the human resources department are two customers which will be using this service, the same SLA will be valid between the IT service provider and these two departments since it is a service based SLA.

3. Multilevel SLA

- In multi-level SLA, aspects of SLA are defined according to the organization of the customer using some kind of inheritance with overall definitions with relevance for all subordinate levels.
- This SLA focuses on the organization of the customer. All services and their interrelationships with subordinate services are used when defining the multi-level service level agreement structure.
- Maintaining service level agreements are part of service level management. Every time a service change, or the service level target of a service change, the service level agreement needs to be reviewed and revised. The new service level agreement needs to reflect the changes made to the service or the service level targets.
- Few Service Level Agreements are enforceable as contracts, but mostly are agreements or contracts which are more along the lines of an Operating Level Agreement (OLA) and may not have the restriction of law.
- It is fine to have an brief review the documents before making a major agreement to the cloud service provider.
- Service Level Agreements usually specify **some parameters** which are mentioned below:

1. Availability of the Service (uptime)
2. Latency or the response time
3. Service components reliability
4. Each party accountability
5. Warranties

Billing & Accounting

- The billing management system mechanism is dedicated to the collection and processing of usage data as it pertains to cloud provider accounting and cloud consumer billing.
- Specifically, the billing management system relies on pay-per-use monitors to gather runtime usage data that is stored in a repository that the system components then draw from for billing reporting and invoicing purposes.
- The billing management system allows for the definition of different pricing policies as well as custom pricing models on a per-cloud consumer and/or per-IT resource basis.
- Pricing models can vary from the traditional pay-per-use models to flat-rate or pay-perallocation models, or combinations.

- Billing arrangements can be based on pre-usage and post-usage payments.
- The latter type can include pre-defined limits or can be set up to allow for unlimited usage.
- When limits are established, they are usually in the form of usage quotas.
- When quotas are exceeded, the billing management system can block further usage requests by cloud consumers.

Comparing Scaling Hardware: Traditional vs. Cloud

 Cloud computing is really popular nowadays. More and more companies prefer using cloud infrastructure rather than the traditional one.

The differences between cloud computing and traditional IT infrastructure

1. **Elasticity and flexibility**
   - Do not need to buy the hardware and maintain it with your own team.
   - The information in the cloud is stored on several servers at the same time.
   - It means that even if 1 or 2 servers are damaged, you will not lose your information.
   - It also helps to provide the high uptime, up to 99.9%.
   - When we talk about their traditional infrastructure, you will have to buy and maintain the hardware and equipment. If something happens, you can lose the data and spend a lot of time and money to fix the issues.
2. **Scalability and flexibility**
   - The cloud computing is the perfect Choice for those who do not require a high performance constantly but use it time by time.
   - You can get a subscription and use the resources you paid for.
   - Most providers even let pause the subscription if you do not need it.
   - At the same time, you're able to control everything and get instant help from the support team.
   - The traditional infrastructure is not so flexible. You have to buy an equipment and maintain it even if you do not use it. In many cases, it's even more expensive because you might need their own technical crew.
3. **Automation**
   - One of the biggest differences between cloud and traditional infrastructure is how they are maintained.
   - Cloud service is served by the provider's support team. They take care of all the necessary aspects including security, updates, hardware, etc.
   - The traditional infrastructure required the own team to maintain and monitor the system. It requires a lot of time and efforts.
4. **Cost**
   - With cloud computing, you do not need to pay for the services you don't use: the subscription model means you choose the amount of space, processing power, and other components that you really need.

- With traditional infrastructure, you are limited to the hardware you have. If your business is growing, you will regularly have to expand your infrastructure. At the same time, you will have to support and maintain it.

5. **Security**
   - Many people are not sure about the security of cloud services. Why can it be not so secure? As the company uses the third party solution to store data, it's reasonable to think that the provider can access the confidential data without permission. However, there are good solutions to avoid the leaks.
   - As for traditional infrastructure, you and only you are responsible for who will be able to access the stored data. For the companies who operate the confidential information, it's a better solution.

What kind of infrastructure is a good choice for your business? It depends on what your company does and what are your needs. Nevertheless, more and more organizations today prefer cloud infrastructure.

Economics of scaling: Benefitting enormously

- Cloud computing allows online access to a centralized data storage and other resources.
- This leads to economies of scale as multi-tenancy based solutions are deployed on one piece of hardware, with pooled resources that are shared among different users.
- Managing cloud resources using a browser and network devices such as a smart phone, tablet and computer make operations smooth and easy.
- An important part of cloud computing services is flexibility in resources which can be managed both up and down.
- Various companies around the world are benefiting from economies of scale that cloud computing & services practice brings about.
- It offers the following **advantages:**
- Fast implementation with loads of time savings
- Fast scaling to keep pace with sudden spikes in growth
- Reduction in cost of maintaining infrastructure
- Control over access and content as per the specified provisioning
- Increase in productivity of IT staff
- Reduced investment in infrastructure and maintaining facility.
- Look for a leading network infrastructure provider to make the most of your investment in such a high-end cloud based solution.
- You can use any popular web search engine to look for one.

- Make sure you choose one that is comfortable in running all types of applications in the cloud and has extensive experience in handling various cloud-based projects.

Managing Data: Looking at Data, Scalability & Cloud Services

What is Scalability in Cloud?

- Scalability is the capability of a process, network, software or appliance to grow and manage increased demands.
- This is one of the most valuable and prime feature of cloud computing.
- Through scalability you can scale up your data storage capacity or scale it down to meet the demands of your growing business.
- Scaling in the cloud provides you the best experience of flexibility of time and money for your business.
- When business demands are increasing, you can easily add nodes to increase your storage space, or you can increase the number of servers currently used.
- When the increased demand is reduced then you can move back to your original configuration.
- Scalability enables you to accommodate larger workloads without disruption or complete transformation of existing infrastructure.
- To effectively force scalability you need to understand the complexity and the types of scalability.
- Let's explore different types of scalability.

Three types of scalability – Vertical, Horizontal and Diagonal

1. Scale Vertically – Scale Up:

- Vertical Scaling or Scaling up is easy, it can be done by moving the application to bigger virtual machines deployed in the cloud or you can scale up by adding expansion units as well with your current infrastructure.
- This ability to add resources to accommodate increasing workload volumes is **vertical scaling**. It can resize your server with no change in your code.
- The downside to scaling up is that it increases storage capacity but the performance is reduced because the compute capacity remains the same.
- Workloads requiring higher throughput demand reduced latency and this can only by fulfilled by Horizontal Scaling / Scaling out.

2. Scale Horizontally – Scale out:

- Horizontal Scaling or Scaling out is the addition of nodes to the existing infrastructure to accommodate additional workload volumes.
- Contrary to Vertical Scaling, Horizontal Scaling also delivers performance along with storage capacity.
- The total workload volume is aggregated over the total number of nodes and latency is effectively reduced.

- This scaling is ideal for workloads that require reduced latency and optimized throughput.

3. Scale Diagonally:

- Diagonal scaling helps you combine the scaling up and scaling down.
- As the term suggests, scaling down is the removal of storage resources as requirements decrease.
- Diagonal scaling delivers flexibility for workload that require additional storage resources for specific instances of time.
- For ex, a website sets up diagonal scaling; as the traffic increases, the compute requirements are accommodated.
- As the traffic decreases, the computation capacity is restored to its original size.
- This type of scaling introduces enhanced budgeting and cost effectiveness for environments and businesses dealing with variable workload volumes.

Scalable Cloud Based Services:

- Infrastructure-as-a-Service (IaaS)
- Platform-as-a-Service (PaaS)
- Storage-as-a-Service (STaaS)
- Data-as-a-Service (DaaS)
- Database-as-a-Service (DBaaS)

Database & Data Stores in Cloud

- A cloud database is a collection of informational content, either **structured or unstructured,** that reside on a private, public or hybrid cloud computing infrastructure platform.
- From a structural and design perspective, a cloud database is no different than one that operates on a business's own on-premises servers.
- The critical difference lies in where the database resides.
- Where an on-premises database is connected to local users through a corporation's internal local area network (LAN), a cloud database resides on servers and storage furnished by a cloud or database as a service (DBaaS) provider and it is accessed only through the internet.
- To a software application, for example, a SQL database residing on-premises or in the cloud should appear identical.
- The behavior of the database should be the same whether accessed through direct queries, such as SQL statements, or through API calls.
- However, it may be possible to detect small differences in response time.
- An on-premises database, accessed with a LAN, is likely to provide a slightly faster response than a cloud-based database, which requires a round trip on the internet for each interaction with the database.

How Cloud Databases Work

- Cloud databases, like their traditional ancestors, can be divided into two broad categories: **relational and non-relational.**

- A relational database, typically written in **structured query language (SQL),** is composed of a set of interrelated tables that are organized into rows and columns.
- The relationship between tables and columns (fields) is specified in a **schema**.
- SQL databases, by design, rely on data that is highly consistent in its format , such as banking transactions or a telephone directory.
- Popular cloud platforms and cloud providers include **MySQL, Oracle, IBM DB2 and Microsoft SQL Server**.
- Some cloud platforms such as MySQL are open sourced.
- Non-relational databases, sometimes **called NoSQL,** do not employ a table model.
- Instead, they store content, regardless of its structure, as a single document.
- This technology is **well-suited for unstructured data**, such as social media content, photos and videos.

Types of Cloud Databases

- Two cloud database environment models exist: traditional and database as a service (DBaaS).
- In a traditional cloud model, a database runs on an IT department's infrastructure with a virtual machine. Tasks of database oversight and management fall upon IT staffers of the organization.
- The DBaaS model is a fee-based subscription service in which the database runs on the service provider's physical infrastructure. Different service levels are usually available. In a classic DBaaS arrangement, the provider maintains the physical infrastructure and database, leaving the customer to manage the database's contents and operation.
- Alternatively, a customer can set up a managed hosting arrangement, in which the provider handles database maintenance and management. This latter option may be especially attractive to small businesses that have database needs but lack adequate IT expertise.

Cloud database benefits

- Compared with operating a traditional database on an on-site physical server and storage architecture, a cloud database offers the following distinct advantages:
- **Elimination of physical infrastructure-** In a cloud database environment, the cloud computing provider of servers, storage and other infrastructure is responsible for maintenance and keeping high availability. The organization that owns and operates the database is only responsible for supporting and maintaining the database software and its contents. In a DBaaS environment, the service provider is responsible for managing and operating the database software, leaving the DBaaS users responsible only for their own data.
- **Cost savings**- Through the elimination of a physical infrastructure owned and operated by an IT department, significant savings can be achieved from reduced capital expenditures, less staff, decreased electrical and HVAC operating costs and a smaller amount of needed physical space.
- DBaaS benefits also include instantaneous scalability, performance guarantees, failover support, declining pricing and specialized expertise.

- Migrating legacy databases to the cloud
- An on-premises database can migrate to a cloud implementation. Numerous reasons exist for doing this, including the following:
- Allows IT to retire on-premises physical server and storage infrastructure.
- Fills the talent gap when IT lacks adequate in-house database expertise.
- Improves processing efficiency, especially when applications and analytics that access the data also reside in the cloud.
- Achieves cost savings through several means, including:
- Reduction of in-house IT staff.
- Continually declining cloud service pricing.
- Paying for only the resources consumed, known as pay-as-you-go pricing.

Relocating a database to the cloud can be an effective way to further enable business application performance as part of a wider software-as-a-service deployment. Doing so simplifies the processes required to make information available through internet-based connections. Storage consolidation can also be a benefit of moving a company's databases to the cloud. Databases in multiple departments of a large company, for example, can be combined in the cloud into a single hosted database management system.

Large Scale Data Analysis

- Large scale data analysis is a broad term that encompasses a series of different tools and systems to process big data.
- Typically, large scale data analysis is performed through two popular techniques: parallel database management systems (DBMS) or MapReduce powered systems.
- The parallel DBMS system requires that the data be in a DBMS supported schema, whereas the MapReduce option supports data in any form.
- Moreover, the data extracted or analyzed in large-scale data analysis can be displayed in various different forms, such as tables, graphs, figures and statistical analysis, depending on the analysis system.

Unit - 4

Virtualization

- Virtualization is the creation of virtual servers, infrastructures, devices and computing resources.
- A great example of how it works in your daily life is the separation of your hard drive into different parts.
- While you may have only one hard drive, your system sees it as two, three or more different and separate segments.
- Similarly, this technology has been used for a long time.
- It started as the ability to run multiple operating systems on one hardware set and now it a very important part of testing and cloud-based computing.

Virtualization objectives

- Virtualization is the backbone of Cloud Computing.
- Cloud Computing brings efficient benefits as well as makes it more convenient with the help of Virtualization, not only this, it also provides solutions for great challenges in the field of data security and privacy protection.
- Virtualization is the imitation of hardware within a software program.
- The role of multiple computers is allowed on a single computer.
- In a file or a web server, the usage of purchase, maintenance, depreciation, energy and floor space is double, but by creating virtual web or file server all of our objectives are fulfilled like the use of hardware resources to its maximum, flexibility, improvement in security, reduced cost.
- Efficient use of resources, increased security, portability, problem free testing, easier manageability, increased flexibility, fault isolation, rapid deployment are the benefits of virtualization.

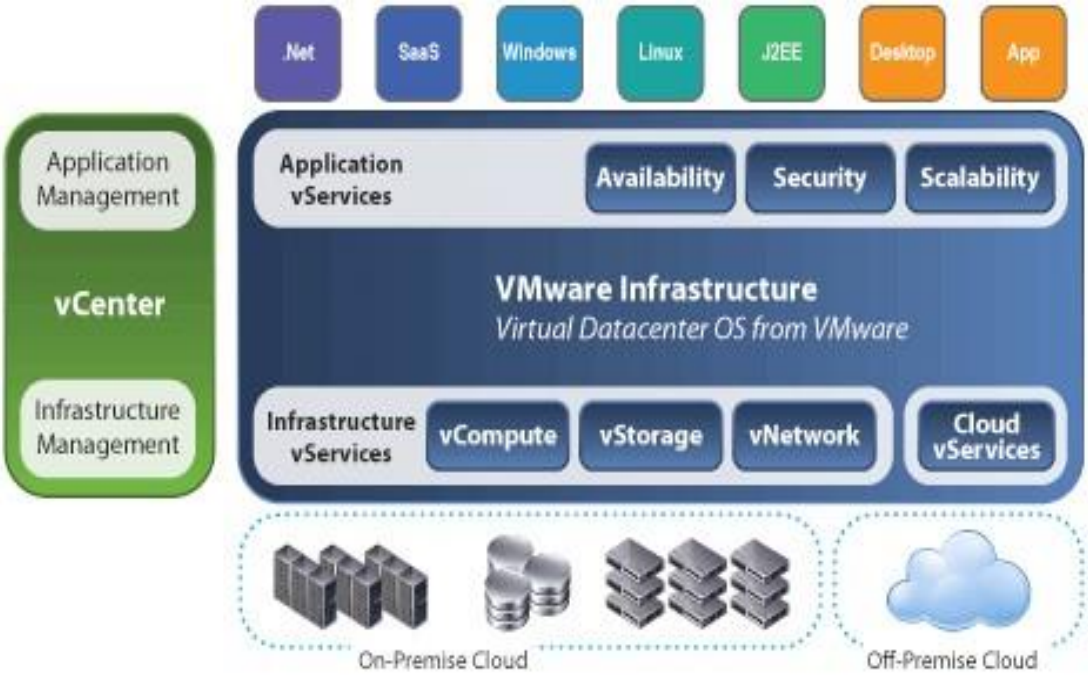
Virtualization in Cloud Computing:

- For combining local and network resources data storage virtualization.
- For grouping physical storage devices into the single unit
- For reaching the high level of availability or improving availability using virtualization
- Improving performance using virtualization
- Using virtualization using stripping and caching
- Capacity improvement
- A central computer hosting an application to multiple users, preventing the need for installing software repeatedly on every system **is virtualization in Cloud Computing**.
- The data from different hard drives, USB drives, and databases are merged into one location increasing its accessibility and security.
- The creation of virtual hardware, software, or an operating system or a storage or network device is virtualization in cloud computing.

- In IT virtual changes occur more rapidly than in a physical environment.

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.



Virtual servers introduction

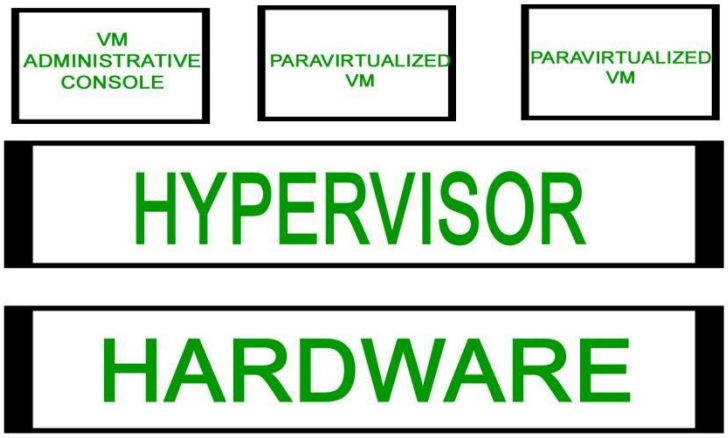
- Server Virtualization is the partitioning of a physical server into number of small virtual servers, each running its own operating system.
- These operating systems are known as **guest operating systems**. These are running on another operating system known as **host operating system**.
- Each guest running in this manner is unaware of any other guests running on the same host.
- Different virtualization techniques are employed to achieve this transparency.

Types of Server virtualization :

1. **Hypervisor –**
   - A Hypervisor or VMM(virtual machine monitor) is a layer that exits between the operating system and hardware.

- It provides the necessary services and features for the smooth running of multiple operating systems.
- It identifies traps, responds to privileged CPU instructions and handles queuing, dispatching and returning the hardware requests. A host operating system also runs on top of the hypervisor to administer and manage the virtaul machines.

2. **Para Virtualization –** □ It is based on Hypervisor.
   - Much of the emulation and trapping overhead in software implemented virtualisation is handled in this model.
   - The guest operating system is modified and recompiled before installation into the virtual machine.
   - Due to the modification in the Guest operating system, performance is enhanced as the modified guest operating system communicates directly with the hypervisor and emulation overhead is removed.
   - Example : Xen primarily uses Para virtualisation, where a customised Linux environment is used to supportb the administrative environment known as domain 0.

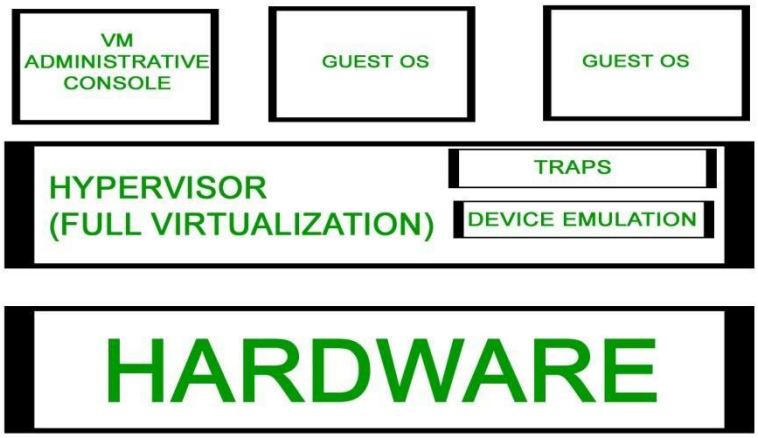


Advantages:
- Easier
- Enhanced Performance
- No emulation overhead **Limitations:**
- Requires modification to guest operating system

3. **Full Virtualization –**
   - It is very much similar to Para virtualisation.
   - It can emulate the underlying hardware when necessary.

The hypervisor traps the machine operations used by the operating system to perform I/O or modify the system status.

- After trapping, these operations are emulated in software and the status codes are returned very much consistent with what the real hardware would deliver.
- This is why unmodified operating system is able to run on top of the hypervisor.
- Example : VMWare ESX server uses this method. A customised Linux version known as Service Console is used as the administrative operating system. It is not as fast as Para virtualisation.



Advantages:

- No modification to Guest operating system required. **Limitations:**
- Complex
- Slower due to emulation
- Installation of new device driver difficult.

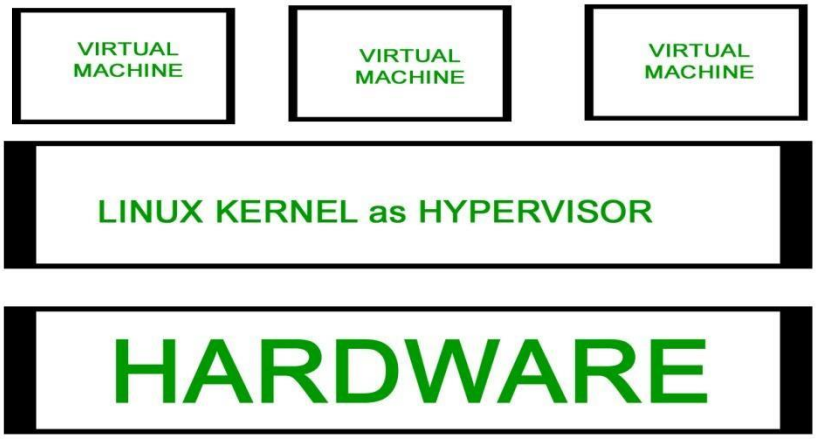
4. **Hardware Assisted Virtualization –**
   - It is similar to Full Virtualisation and Para virtualisation in terms of operation except that it requires hardware support.
   - Much of the hypervisor overhead due to trapping and emulating I/O operations and status instructions executed within a guest OS is dealt by relying on the hardware extensions of the x86 architecture.
   - Unmodified OS can be run as the hardware support for virtualisation would be used to handle hardware access requests, privileged and protected operations and to communicate with the virtual machine.
   - Examples : AMD – V Pacifica and Intel VT Vanderpool provides hardware support for virtualisation.

   Advantages:

   - No modification to guest operating system required.
   - Very less hypervisor overhead **Limitations:**

   Hardware support Required
5. **Kernel level Virtualization –**

- Instead of using a hypervisor, it runs a separate version of the Linux kernel and sees the associated virtual machine as a user – space process on the physical host.
- This makes it easy to run multiple virtual machines on a single host.
- A device driver is used for communication between the main Linux kernel and the virtual machine.
- Processor support is required for virtualisation(Intel VT or AMD – v).
- A slightly modified QEMU process is used as the display and execution containers for the virtual machines.
- In many ways, kernel level virtualization is a specialised form of server virtualization.
- Examples: User – Mode Linux(UML) and Kernel Virtual Machine(KVM)

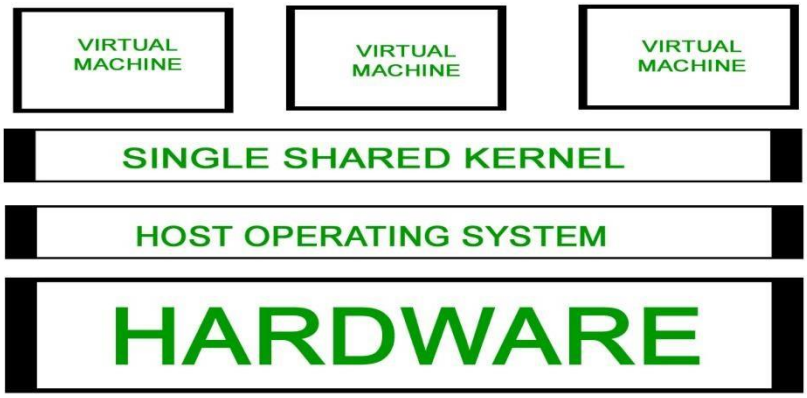


Advantages:

- No special administrative software required.
- Very less overhead **Limitations:**
- Hardware Support Required

6. **System Level or OS Virtualization –**
   - Runs multiple but logically distinct environments on a single instance of operating system kernel.
   - Also called shared kernel approach as all virtual machines share a common kernel of host operating system.
   - Based on change root concept “chroot”.chroot starts during boot up.
   - The kernel uses root filesystems to load drivers and perform other early stage system initialisation tasks.
   - It then switches to another root filesystem using chroot command to mount an on -disk file system as its final root filesystem, and continue system initialization and configuration within that file system.
   - The chroot mechanism of system level virtualisation is an extension of this concept. It enables the system to start virtual servers with their own set of processes which execute relative to their own filesystem root directories.

- The main difference between system level and server virtualisation is wether different operating systems can be run on different virtual systems.
- If all virtual servers must share the same copy of operating system it is system level virtualisation and if different servers can have different operating systems it is server virtualisation.
- Examples: FreeVPS, Linux Vserver and OpenVZ are some examples.



Advantages:

- Significantly light weight than complete machines(including a kernel)
- Can host many more virtual servers
- Enhanced Security and isolation **Limitations:**
- Kernel or driver problem can take down all virtual servers.

Virtual Servers

Hyper V

- Hyper-V is Microsoft's hardware virtualization product.
- It lets you create and run a software version of a computer, called a *virtual machine*.
- Each virtual machine acts like a complete computer, running an operating system and programs.
- When you need computing resources, virtual machines give you more flexibility, help save time and money, and are a more efficient way to use hardware than just running one operating system on physical hardware.
- Hyper-V runs each virtual machine in its own isolated space, which means you can run more than one virtual machine on the same hardware at the same time.

Hyper-V can help you:

- Establish or expand a private cloud environment.
- Use your hardware more effectively.
- Improve business continuity.
- Establish or expand a virtual desktop infrastructure (VDI).

- Make development and test more efficient.

VMware

- VMware offers its VMware Server, a free entry-level hosted virtualization product for Linux and Windows servers.
- The product is available for download at www.vmware.com/products/server/.
- "Virtualization and VMware have become mainstream in the past year, and many customers have deployed thousands of VMware server environments across their enterprises.
- With VMware Server, we are ensuring that every company interested in, considering or evaluating server virtualization for the first time has access to the industryleading
- virtualization technology," said Diane Greene, VMware president.
- "VMware Server makes it easy and compelling for companies new to virtualization to take the first steptoward enterprise-wide virtual infrastructure."

Features

VMware Server, the successor to VMware GSX Server, enables users to quickly provision new server capacity by partitioning a physical server into multiple virtual machines, bringing the powerful benefits of virtualization to every server.

VMware Server is feature-packed with the following market-leading capabilities:

- Support for any standard x86 hardware
- Support for a wide variety of Linux and Windows host operating systems, including 64-bit operating systems
- Support for a wide variety of Linux, NetWare, Solaris x86, and Windows guest operating systems, including 64-bit operating systems
- Support for Virtual SMP, enabling a single virtual machine to span multiple physical processors
- Quick and easy, wizard-driven installation similar to any desktop software
- Quick and easy virtual machine creation with a virtual machine wizard
- Virtual machine monitoring and management with an intuitive, user-friendly remote console

Unit - 5

Case Study on Open Source & Commercial Clouds

Eucalyptus

- Eucalyptus is a paid and open-source computer software for building Amazon Web Services (AWS)-compatible private and hybrid cloud computing environments, originally developed by the company Eucalyptus Systems.
- Eucalyptus is an acronym for **Elastic Utility Computing Architecture for Linking Your Programs to Useful Systems**.
- Eucalyptus enables pooling compute, storage, and network resources that can be dynamically scaled up or down as application workloads change.
- Mårten Mickos was the CEO of Eucalyptus.
- In September 2014, Eucalyptus was acquired by **Hewlett-Packard** and then maintained by DXC Technology.
- After DXC stopped developing the product in late 2017, AppScale Systems forked the code and started supporting Eucalyptus customers.
- Eucalyptus commands can manage either Amazon or Eucalyptus instances. Users can also move instances between a Eucalyptus private cloud and the Amazon Elastic Compute Cloud to create a hybrid cloud. Hardware virtualization isolates applications from computer hardware details.

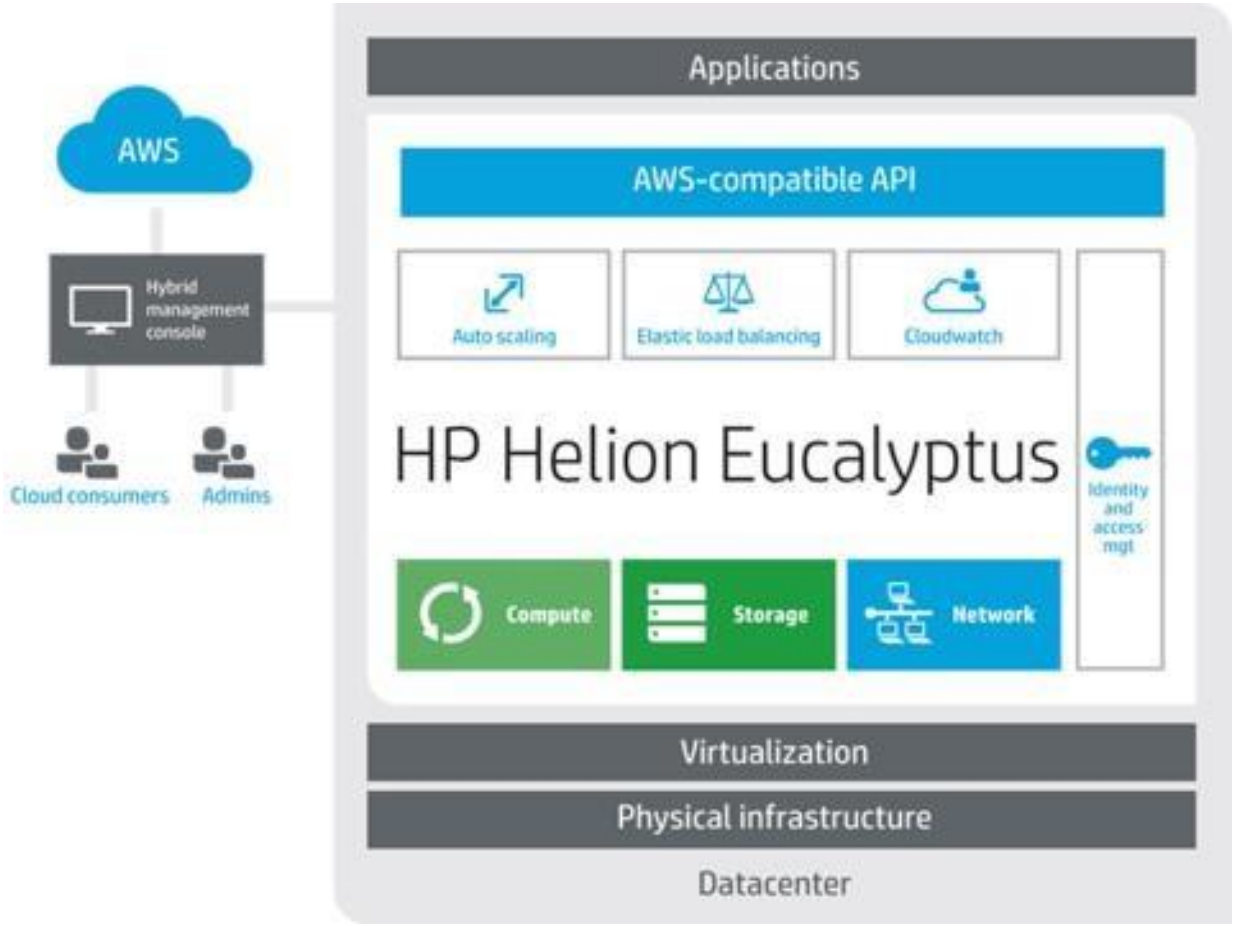
Eucalyptus uses the terminology:

- **Images** – An image is a fixed collection of software modules, system software, application software, and configuration information that is started from a known baseline (immutable/fixed). When bundled and uploaded to the Eucalyptus cloud, this becomes a Eucalyptus machine image (EMI).
- **Instances** – When an image is put to use, it is called an instance. The configuration is executed at runtime, and the Cloud Controller decides where the image will run, and storage and networking is attached to meet resource needs.
- **IP addressing** – Eucalyptus instances can have public and private IP addresses. An IP address is assigned to an instance when the instance is created from an image. For instances that require a persistent IP address, such as a web-server, Eucalyptus supplies elastic IP addresses. These are pre-allocated by the Eucalyptus cloud and can be reassigned to a running instance.
- **Security** – TCP/IP security groups share a common set of firewall rules. This is a mechanism to firewall off an instance using IP address and port block/allow functionality. Instances are isolated at TCP/IP layer 2. If this were not present, a user could manipulate

  the networking of instances and gain access to neighboring instances violating the basic cloud tenet of instance isolation and separation.
- **Networking** – There are three networking modes. In Managed Mode, Eucalyptus manages a local network of instances, including security groups and IP addresses. In System Mode, Eucalyptus assigns a MAC address and attaches the instance's network interface to the physical network through the Node Controller's bridge. System Mode does not offer elastic IP addresses, security groups, or

VM isolation. In Static Mode, Eucalyptus assigns IP addresses to instances. Static Mode does not offer elastic IPs, security groups, or VM isolation.

- **Access Control** – A user of Eucalyptus is assigned an identity, and identities can be grouped together for access control.



Microsoft Azure

What is Azure?

- Azure is Microsoft's cloud platform, just like Google has it's Google Cloud and Amazon has it's Amazon Web Service or AWS.000.
- Generally, it is a platform through which we can use Microsoft's resource.
- For example, to set up a huge server, we will require huge investment, effort, physical space and so on.
- In such situations, Microsoft Azure comes to our rescue. It will provide us with virtual machines, fast processing of data, analytical and monitoring tools and so on to make our work simpler.
- The pricing of Azure is also simpler and cost-effective.
- Popularly termed as "Pay As You Go", which means how much you use, pay only for that. Microsoft unveiled Windows Azure in early October 2008 but it went to live after February 2010.
- Later in 2014, Microsoft changed its name from **Windows Azure to Microsoft Azure**.
- Azure provided a service platform for .NET services, SQL Services, and many Live Services.
- Many people were still very skeptical about "the cloud".
- Microsoft Azure is getting bigger and better in coming days.
- More tools and more functionalities are getting added. It has two releases as of now.
- It's famous version **Microsoft Azure v1** and later **Microsoft Azure v2**.

- Microsoft Azure v1 was more like JSON script driven then the new version v2, which has interactive UI for simplification and easy learning. Microsoft Azure v2 is still in the preview version.

Amazon EC2

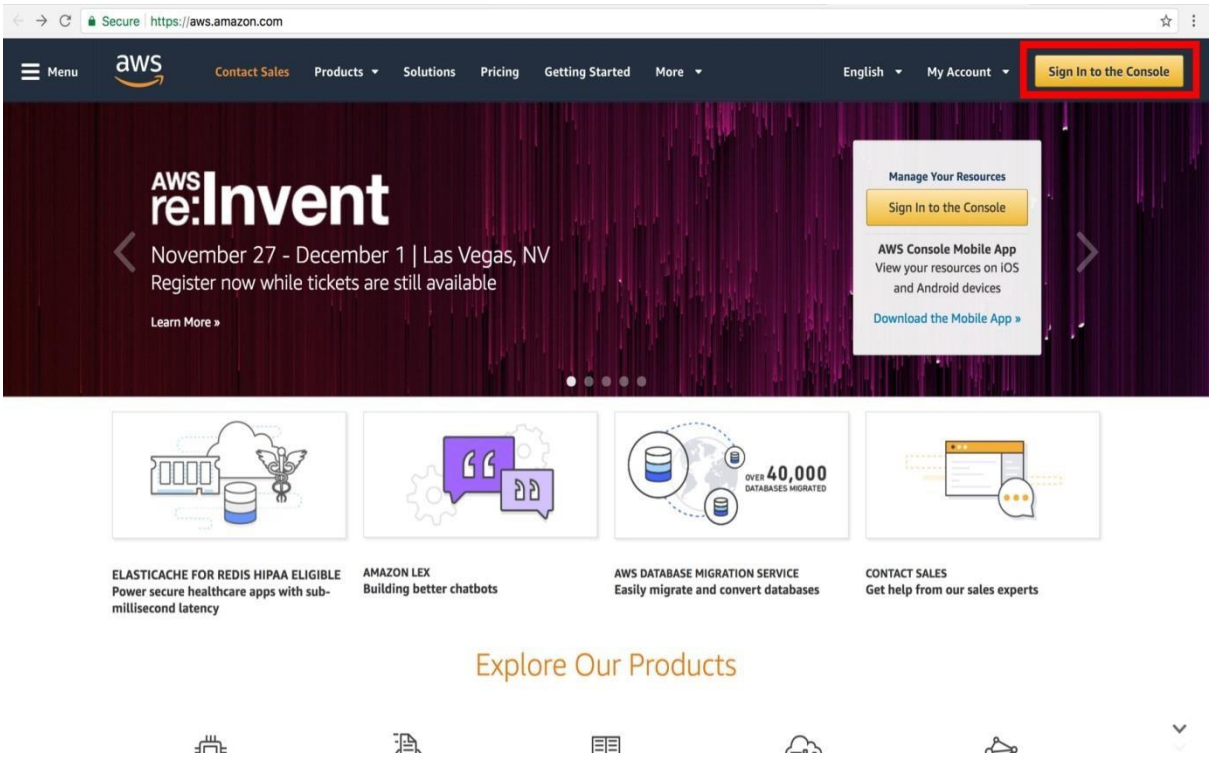
- There are times when one is limited by the capabilities of a desktop or laptop.
- Suppose a data scientist has a large dataset that they would like to do some analysis on.
- The scientist proceeds to try and load the entire dataset into memory and an error like the one below occurs.

```
> data <- read.csv(file = 'massiveFile.csv')
Error: cannot allocate vector of size 500.0 Mb
```

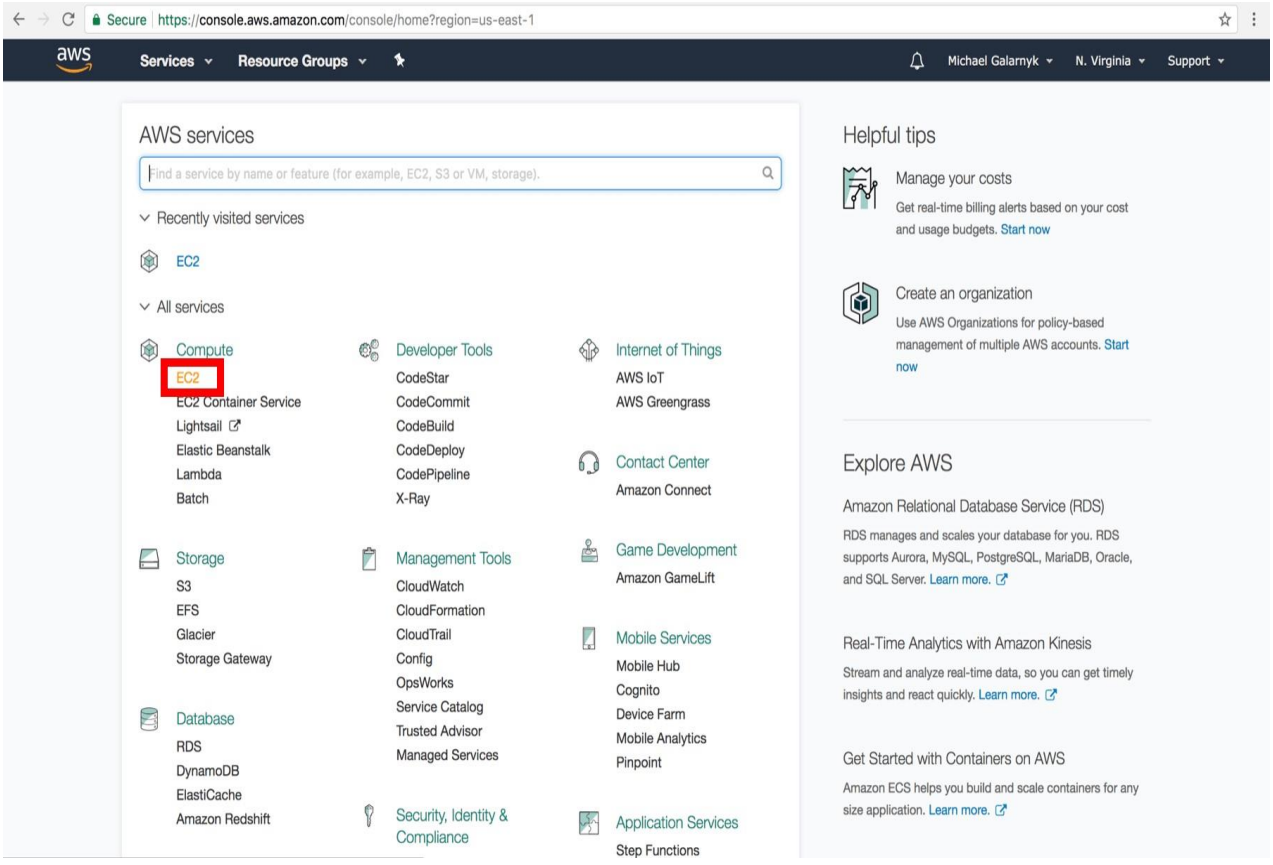
- The error resulted because the available RAM was exhausted.
- The operating system couldn't allocate another 500Mb of RAM.
- While there are many different solutions to this type of problem, one possible solution could be to upgrade the RAM of the computer.
- Besides having to make an investment in more RAM, there are limits to how far some computers can be upgraded. The potential solution explored in this tutorial is to use a virtual machine in the cloud (AWS) with more RAM and CPU.
- Virtual machines on AWS EC2, also called instances, have many advantages.
- A few of the advantages include being highly scalable, they are easy to start and stop and they allow for the selection of different platforms (operating systems).
- An important point thing to emphasize is that although this tutorial covers how to launch a Windows based virtual machine, there are many different types of virtual machines for many different purposes.
- With that, let's get started.

Create an AWS Account and Sign into AWS.

1. On the Amazon Web Services site click on "Sign In to the Console".
2. Sign in if you have account. If you don't, you will need to make one.

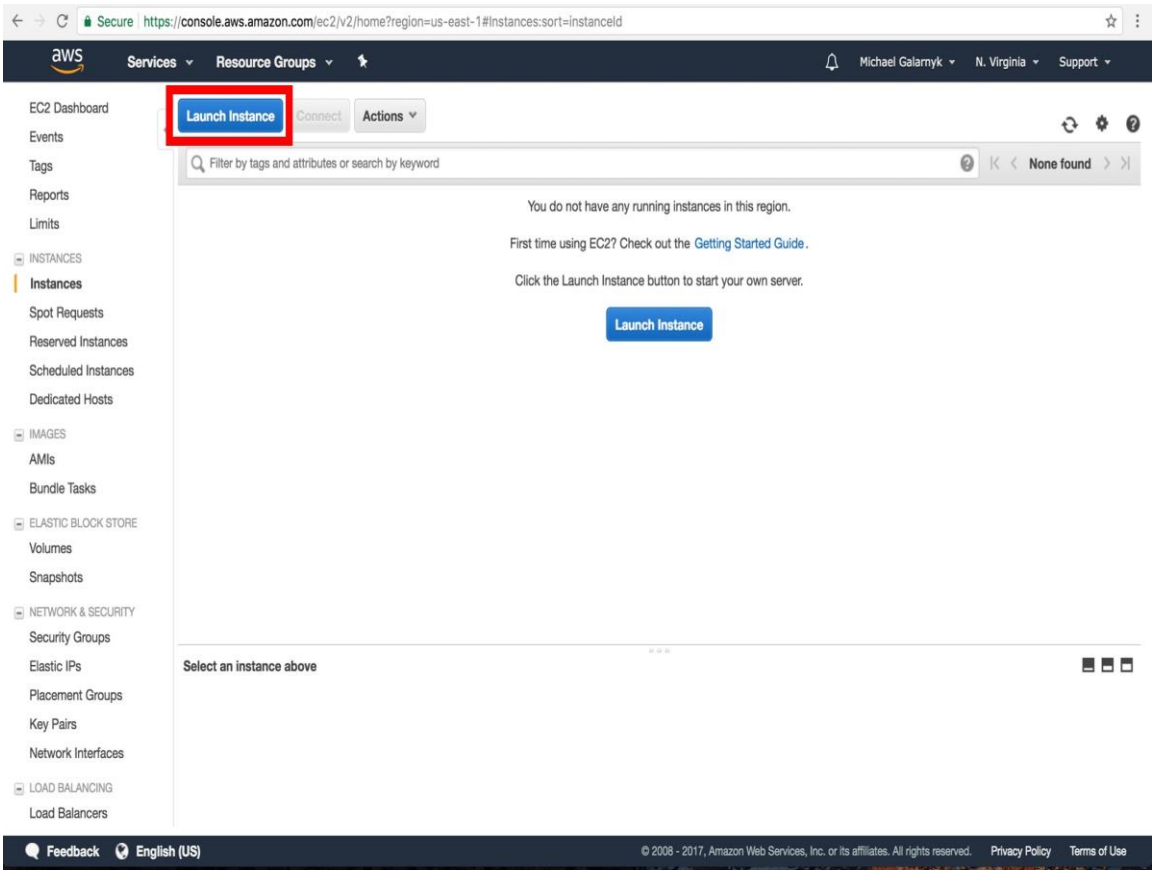


3. On the EC2 Dashboard, click on EC2.

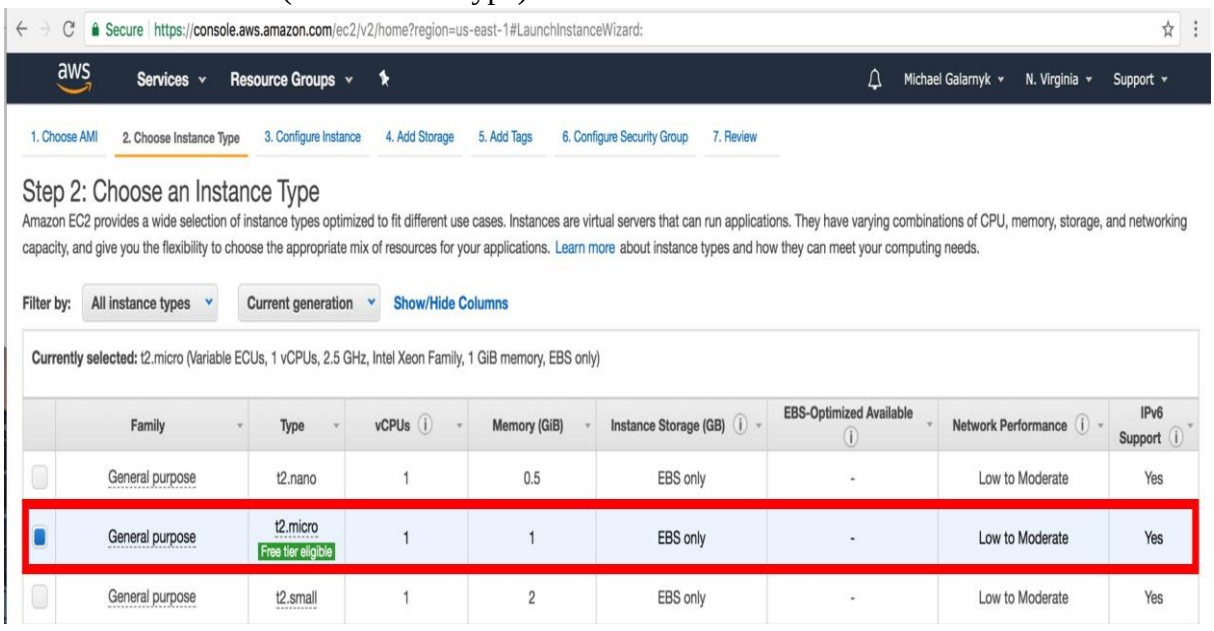


Create an Instance

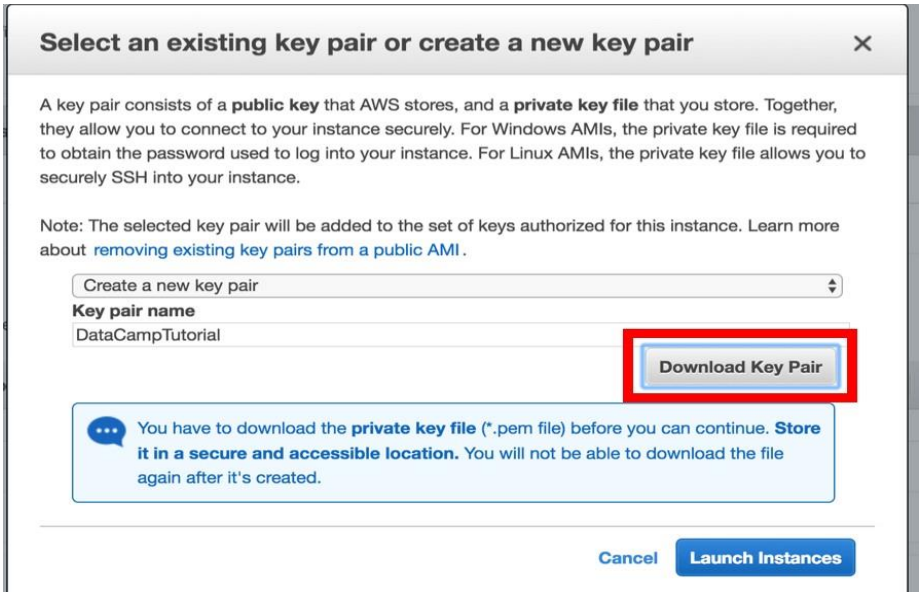
4. On the Amazon EC2 console, click on Launch Instance.



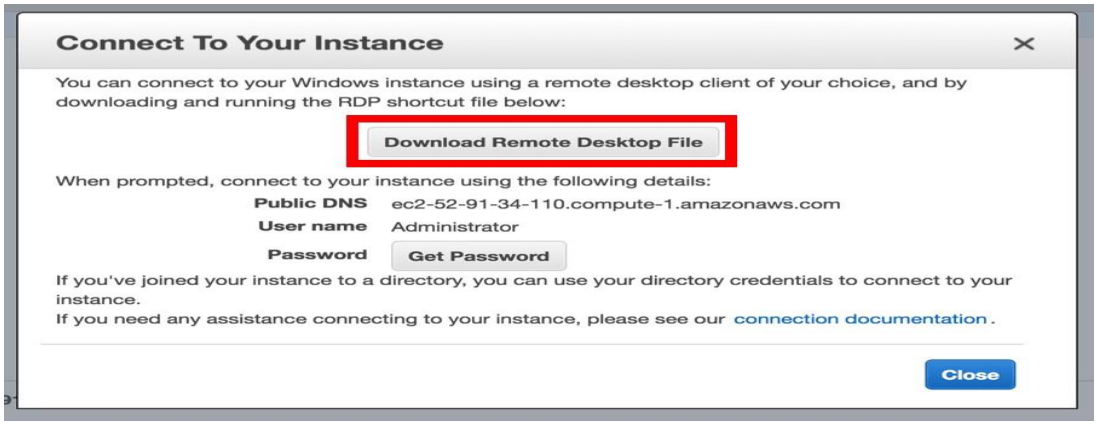
5. Click on the "Select" button in the row with Microsoft Windows Server 2016 Base. Please note that this will create a Windows based instance instead of a typical Linux based instance. This effects how you will connect to the instance.
6. Make sure t2 micro (free instance type) is selected. and click on "Review and Launch"



7. Click on Launch.
8. Select "Create a new key pair". In the box below ("Key pair name"), fill in a key pair name. I named my key DataCampTutorial, but you can name it whatever you like. Click on "Download Key Pair". This will download the key. Keep it somewhere safe. 9. Next, click on "Launch Instances"



10. The instance is now launched. Go back to the Amazon EC2 console. I would recommend that you click on what is enclosed in the red rectangle as it will bring you back to the console.
11. Wait till you see that "Instance State" is running before you proceed to the next step. This can take a few minutes.
12. Click on connect.
13. Click on "Download Remote Desktop File". Save the remote desktop file (rdp) file somewhere safe.



14. Click on "Get Password". Keep in mind that you have to wait at least 4 minutes after you launch an instance before trying to retrieve your password.
15. Choose the pem file you downloaded from step 7 and then click "Decrypt Password"
16. After you decrypt your password, save it somewhere safe. You will need it to log into your instance.
17. Open your rdp file. Click on continue. If your local computer is a Mac, you will need to download "Microsoft Remote Desktop" from the App Store to be able to open your rdp file. 18. Enter your password you got from step 15


Other user
Administrator
Password

Difference between AWS (Amazon Web Services), Google Cloud and Azure

	AWS	Google Cloud	Azure
Technology	EC2 (Elastic Compute Cloud)	Google Compute Engine (GCE)	VHD (Virtual Hard Disk)
Databases Supported	AWS fully supports relational and NoSQL databases and Big Data.	Technologies pioneered by Google, like Big Query, Big Table, and Hadoop, are naturally fully supported.	Azure supports both relational and NoSQL databases, and Big Data, through Windows Azure Table and HDInsight.
Pricing	Per hour – rounded up	Per minute – rounded up (minimum 10 minutes)	Per minute – rounded up commitments (pre-paid or monthly)
Models	On demand, reserved, spot	On demand – sustained use	On demand – short term commitments (pre-paid or monthly)
Difficulties	Many enterprises find it difficult to understand the company's cost structure	Fewer features and services.	Less "enterprise-ready"
Storage Services	• Simple Storage Service (S3) • Elastic Block Storage (EBS) • Elastic Block Storage (EBS)	• Blob Storage • Queue Storage • File Storage • Disk Storage • Data Lake Store	• Cloud Storage • Persistent Disk • Transfer Appliance
Machine Learning	• Sage Maker • Lex • Polly • And many more	• Machine Learning • Azure Bot Service • Cognitive Service	• Cloud Speech API • Cloud Video Intelligence • Cloud Machine Learning Engine • And many more.

Case study on Eucalyptus

- **Rafter is an educational software company** that operates BookRenter.com, which was the first online textbook rental service.

- The company's Rails-based platform requires considerable cloud resources for application development and testing. , it needed a way to lower its own spending on public cloud infrastructure and meet developer requirements for additional testing and development.
- By building a Eucalyptus cloud, Rafter realized immediate advantages over its previously Amazon Web Services (AWS)-only infrastructure.
- This provided better automation and image management than virtualization tools such as VMware or hosted services such as Rackspace and much more economically feasible than Amazon Reserved Instances.
- Overall, Eucalyptus gave them variable AWS costs and benefit from a more predictable and affordable configuration.
- Organizations can use or reuse AWS-compatible scripts to manage their own onpremise IaaS environments.
- The AWS API is implemented on top of Eucalyptus, so tools in the cloud ecosystem that can communicate with AWS can use the same API with Eucalyptus.
- If your company started with an entirely AWS environment, then you can go on using the same tools, scripts and images with Eucalyptus. Or, if Eucalyptus is the first part of your cloud journey, then our deep AWS API compatibility sets you up to efficiently scale and automate hybrid cloud infrastructure as operations grow." □ Eucalyptus is compatible with the following AWS features:
    - ○ Amazon Elastic Compute Cloud (EC2) ○ Amazon Elastic Block Storage (EBS) ○ Amazon Machine Image (AMI) ○ Amazon Simple Storage Service (S3) ○ Amazon Identity and Access Management (IAM) ○ Auto Scaling ○ Elastic Load Balancing ○ Amazon CloudWatch
- Datacenter IT and DevOps teams are responsible for managing the company's Eucalyptus implementation.
- Eucalyptus featured the AWS compatibility, flexibility and advanced features necessary to improve Rafter's development and test environment.
- Eucalyptus works with popular AWS tools for making it easy to migrate applications from the public cloud without rewriting or duplicating code.

Benefits of Eucalyptus

- Empowered software engineers to easily provision their own instances, reducing the IT department’s burden
- Easily integrated with existing EC2-based code and dev/test infrastructure, due to Eucalyptus’ AWS API compatibility
- Allowed for easy capacity expansion as the private cloud demand continues to grow
- Multiplied engineering productivity by using the latest hardware available, at a fraction of the cost to similar public cloud options
- Greatly reduced costs, while still making it easy to leverage hybrid capabilities and scale to the public cloud when needed
- The private and hybrid solution lowered costs .
- Allowed Rafter to use much more powerful hardware by using private cloud rather than public.
- Rafter could retain AWS's considerable capacity and elasticity for specific workloads.

- Eucalyptus doubled Rafter's cloud capacity, increased engineering productivity and generated substantial cost savings.
- It has twice as many instances on Eucalyptus as it did under the original AWS setup, with minimal monthly operating expenses. At the same time, Rafter's integration of Eucalyptus increased its flexibility with cloud vendors, preventing it from being too dependent on any single service.
- On the cost side, Rafter has been able to better control the expenses of Amazon Reserved Instances, on-demand instances and EBS storage/snapshots.
- Eucalyptus has replaced the high variable costs of AWS with much lower fixed costs.

Case study on Microsoft Azure

- Globally recognized for its ground-breaking approach towards delivering business value, increasing speed digital innovation and enabling business platforms to be futureready enterprises, Wipro Ltd. is one of the most successful IT companies in India and around the world.
- It is a trusted IT partner of choice for global businesses looking to 'differentiate at the front' and 'standardize at the core' through technology interventions.

Wipro Before Cloud

- Wipro began the transformation of its internal application background a couple of years back and has been progressing forcefully to provide a great digital experience to its employees, simplified workflows and systems, enhanced automation and innovation.
- Its focus has been to develop applications and services, which would give employees a great user experience, open up new revenue generation streams, enhance productivity and make IT more responsive and cost effective.
- To build a strong digital core, it was important that the organization transformed its legacy enterprise applications into fully renovated, mobile enabled and analytics driven ones.
- In order to do so and cope up with the expectation of rapid app development and deployment, it was very important that the organization upgraded its infrastructure and moved from on premises to cloud.
- Apart from elasticity in infrastructure, cloud adoption would also mean increased efficiencies related to data center footprint, network planning and utilization, hardware refreshes, standardized business processes, which would bring significant cost benefits on a large scale.
- Additionally, since Wipro has been a pioneer in cloud adoption, it would also help in opening new streams of revenue for the organization.
- **Wipro was therefore looking out for a cost-effective, elastic and enterprise friendly IT infrastructure solution.**

Introduction of Microsoft Azure

- Post detailed evaluation of different vendors, Wipro chose Microsoft Azure as it Cloud partner because of agility, stability, cost effectiveness and the deep integration it offered with Office Suite of apps.

- To start off with it was important for the company to have a higher availability with infrastructure, scale up and down as per demand and this aspect was fundamental for the Wipro.
- Real value of cloud comes with the ease of management, insights and the micro services
- We are happy we chose the Azure platform from Microsoft. They have worked with us in shaping up our platform roadmap," says Senior Vice President of Wipro Limited.

How Microsoft Azure Benefited Wipro

- Migrating to Microsoft Azure has given Wipro elasticity on its infrastructure, as well as increased efficiencies related to data center.
- To reduce cost of infrastructure and take advantage of the platform, the application was developed and deployed in MS Azure PaaS.
- All the modules in the system were written in a new architecture, Web and API layers.
- The front end was developed using modern JQuery libraries to make the application fast.
- Entire application was developed and deployed in just 6 weeks. It was estimated that the overall cost of this application was reduced by more than 60%

Other benefits are:

Scalability:

- Many enterprise applications at Wipro have a cyclical usage period, requiring scalability, concurrency and high performance for short period of time.
- High availability is a must during that period and demands high scalability of resources.
- Wipro can now easily scale up and down based on demand and pay for what is being consumed.

Cost-effectiveness:

- With Azure, The infrastructure costs on the cloud platform were calculated based on usage, it gave the organization the ability to pay for what's being used and not be bound to pay for unused services and resources.

Time-to-market of new applications:

- Earlier, due to the unavailability of the latest hardware or very time-intensive cycles, the time-to-market of the applications was much high.
- With Microsoft Azure, all these issues were solved. Microsoft acted as an end-to-end 'cloud partner' capable of providing an entire scope of services on the cloud.

Conclusion

 The Azure platform has helped us build modern applications, which offer simplicity and great user experience with extensive leverage of open source technology. And thanks to the great set of micro services, which could be consumed with ease, the apps could be developed at a very short time span. --- **General Manager and Head of Applications, Information Systems**

Introduction to AWS

Amazon Web Services (AWS) is a collection of remote computing services, also called web services, that make up a cloud computing platform by Amazon.com. The most central and well-known of these services are Amazon EC2 and Amazon S3. The service is advertised as providing a large computing capacity (potentially many servers) much faster and cheaper than building a physical server farm. **Benefits:-**

1. **Easy to use:-** AWS is designed to allow application providers, ISVs, and vendors to quickly and securely host your applications – whether an existing application or a new SaaS-based application. You can use the AWS Management Console or well-documented web services APIs to access AWS's application hosting platform.
2. **Flexible:-** AWS enables you to select the operating system, programming language, web application platform, database, and other services you need. With AWS, you receive a virtual environment that lets you load the software and services your application requires. This eases the migration process for existing applications while preserving options for building new solutions.
3. **Cost effective:-** You pay only for the compute power, storage, and other resources you use, with no long-term contracts or up-front commitments. For more information on comparing the costs of other hosting alternatives with AWS, see the AWS Economics Center.
4. **Reliable:-** With AWS, you take advantage of a scalable, reliable, and secure global computing infrastructure, the virtual backbone of Amazon.com's multibillion dollar online business that has been honed for over a decade.
5. **Scalable and High Performance:-** Using AWS tools, Auto Scaling, and Elastic Load Balancing, your application can scale up or down based on demand. Backed by Amazon's massive infrastructure, you have access to compute and storage resources when you need them.
6. **Secure:-** AWS utilizes an end-to-end approach to secure and harden our infrastructure, including physical, operational, and software measures. For more information, see the AWS Security Center.

Application Solutions:- AWS offers a reliable and flexible cloud infrastructure platform that enables customers to run any type of business application, from small departmental solutions to mission-critical applications in a secure and robust environment.

AMAZON EC2 CASE STUDY

- Amazon Elastic Compute Cloud (EC2) is a central part of Amazon.com's cloud computing platform, Amazon Web Services (AWS).
- EC2 allows users to rent virtual computers on which to run their own computer applications.
- EC2 allows scalable deployment of applications by providing a Web service through which a user can boot an Amazon Machine Image to create a virtual machine, which Amazon calls an "instance", containing any software desired.
- A user can create, launch, and terminate server instances as needed, paying by the hour for active servers, hence the term "elastic".
- EC2 provides users with control over the geographical location of instances that allows for latency optimization and high levels of redundancy.

Case study

- HDM:- The company first launched in 1999 as "Hungama.com", a promotional marketing portal.
- In 2000 the company acquired Indiafm and in the following years began to work marketing campaigns for companies such as Coca-Cola and Nike.
- In 2007 Hungama launched their gaming portal and in 2009, the company re-launched their website and company name, changing it to Hungama Digital Media Entertainment.
- In 2012 Hungama Digital Media Entertainment launched Artist aloud!, a digital platform for artists and music fans.

Challenges:-

- Before migrating to AWS, the company ran its servers in local data centers. This solution soon became expensive, time-consuming, and inefficient.
- Hungama wanted to turn projects around quickly but old equipment caused delays in implementation and service launches.
- In 2008, Hungama migrated to AWS to take advantage of the cost effectiveness, flexibility, and fast time-to-market offered by the cloud.
- “Our migration to AWS in 2008 reduced IT costs considerably,” Hungama.
- The cost savings allowed Hungama to focus its engineering resources on getting products and services to market more quickly.
- The company began to grow rapidly, but as more internal teams started using AWS, its monthly costs also grew.
- Hungama’s infrastructure team engaged AWS Support to help them find ways to optimize costs.

Solution by AWS:-

- As a content provider and aggregator, Hungama requires enormous amounts of storage. The company uses Amazon Simple Storage Service (Amazon S3) to host more than 60 TB of content.
- For server and storage management, Hungama uses Amazon Elastic Compute Cloud (Amazon EC2) and Amazon Relational Database Service (Amazon RDS) with Amazon S3. The flexibility of the AWS solution enables the Bollywood moviemaker to develop applications on multiple platforms and programming models including Java, PHP, .NET, Oracle, MySQL, and SQL technologies.
- As an AWS Support, Enterprise-level tier customer, Hungama has access to AWS Trusted Advisor, which customers can use to audit their AWS usage against known best practices.
- AWS Trusted Advisor identifies opportunities to save money, improve system performance, and security.
- Hungama used AWS Trusted Advisor to run Cost Optimizing checks, which audited Amazon EC2 instances and Amazon Elastic Block Store (Amazon EBS) volumes in Hungama’s environment.