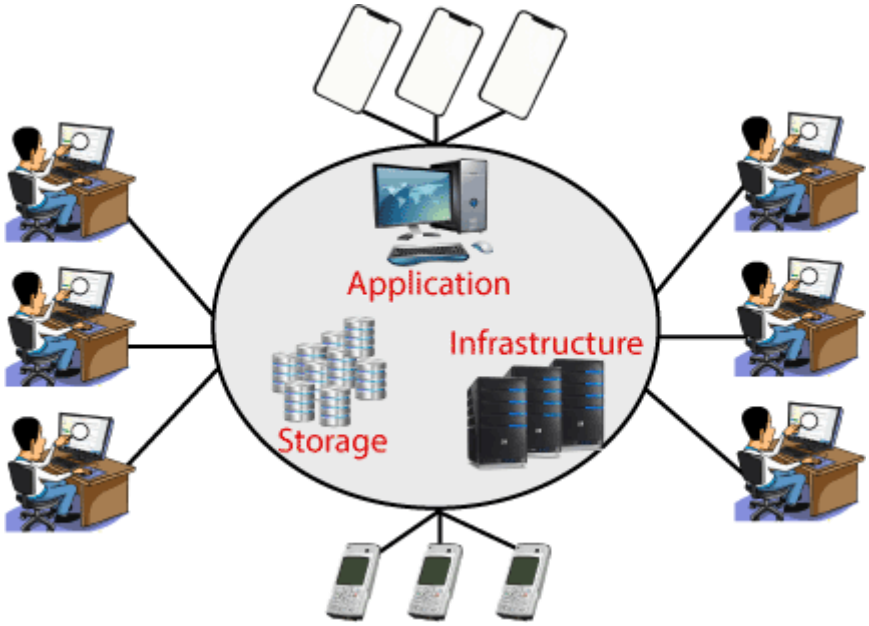
DEPARTMENT OF

COMPUTER SCIENCE AND ENGINEERING

LECTURE NOTES
ON
CLOUD COMPUTING

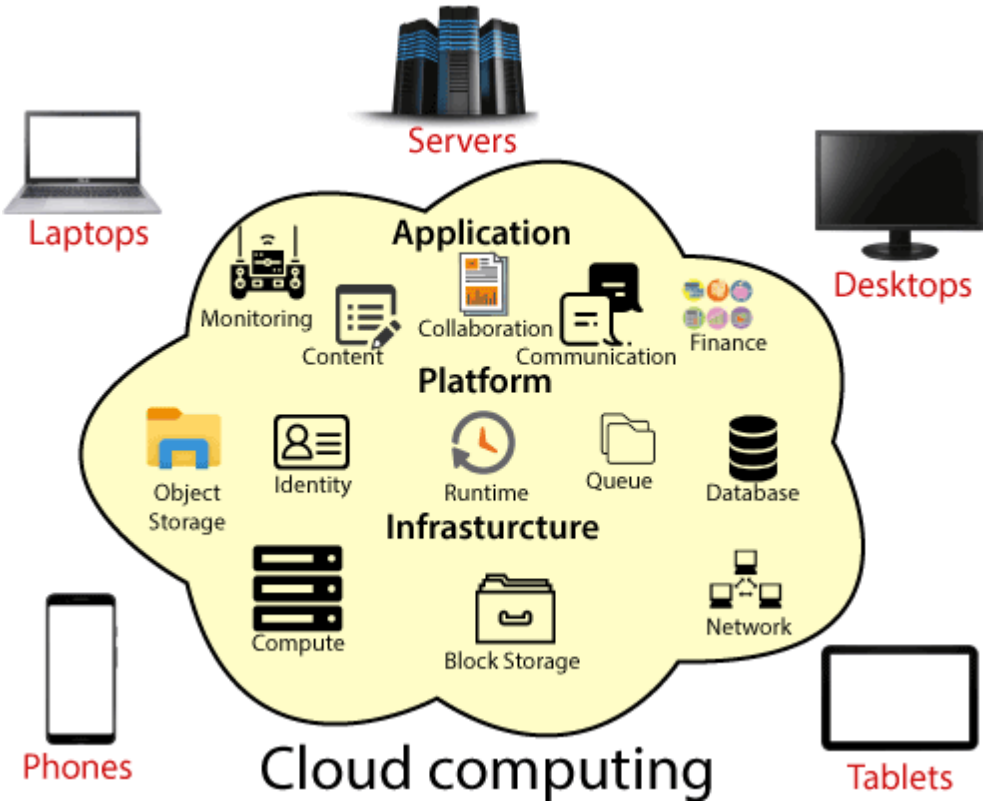
Introduction to Cloud Computing

Cloud Computing is the delivery of computing services such as servers, storage, databases, networking, software, analytics, intelligence, and more, over the Cloud (Internet).



Cloud Computing provides an alternative to the on-premises datacentre. With an on-premises datacentre, we have to manage everything, such as purchasing and installing hardware, virtualization, installing the operating system, and any other required applications, setting up the network, configuring the firewall, and setting up storage for data. After doing all the set-up, we become responsible for maintaining it through its entire lifecycle.

But if we choose Cloud Computing, a cloud vendor is responsible for the hardware purchase and maintenance. They also provide a wide variety of software and platform as a service. We can takeany required services on rent. The cloud computing services will be charged based on usage.



The cloud environment provides an easily accessible online portal that makes handy for the user to manage the compute, storage, network, and application resources. Some cloud service providers are in the following figure.

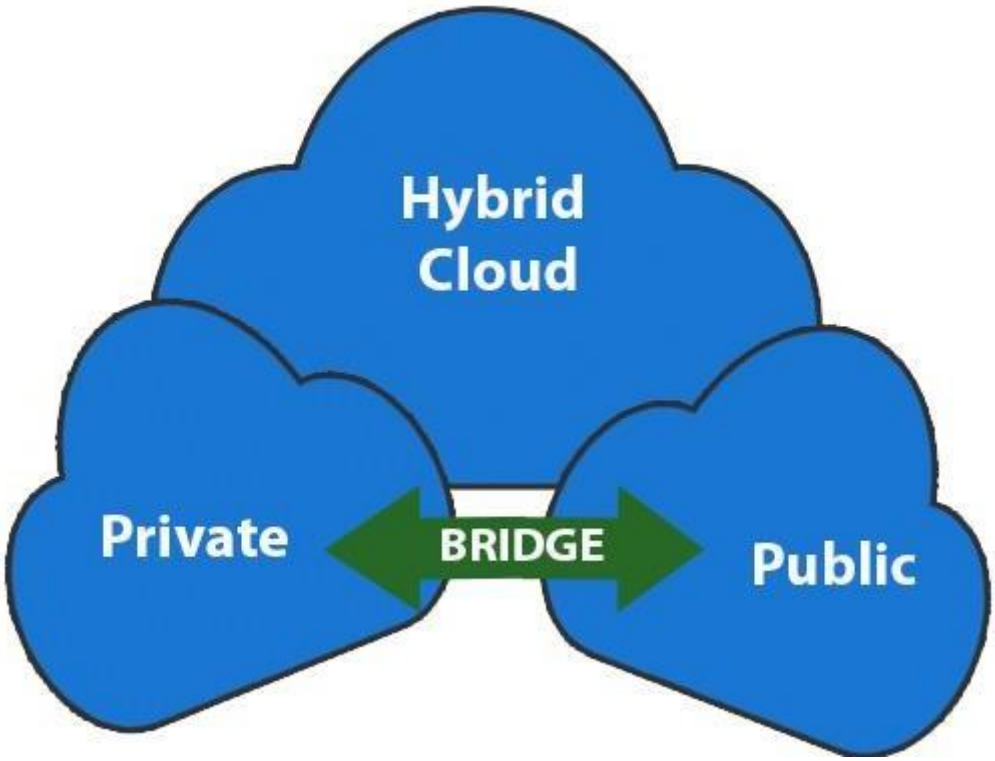
Advantages of cloud computing

- **Cost:** It reduces the huge capital costs of buying hardware and software.
- **Speed:** Resources can be accessed in minutes, typically within a few clicks.
- **Scalability:** We can increase or decrease the requirement of resources according to the business requirements.
- **Productivity:** While using cloud computing, we put less operational effort. We do not need to apply patching, as well as no need to maintain hardware and software. So, in this

way, the IT team can be more productive and focus on achieving business goals.

- **Reliability:** Backup and recovery of data are less expensive and very fast for business continuity.
- **Security:** Many cloud vendors offer a broad set of policies, technologies, and controls that strengthen our data security.

Types of Cloud Computing

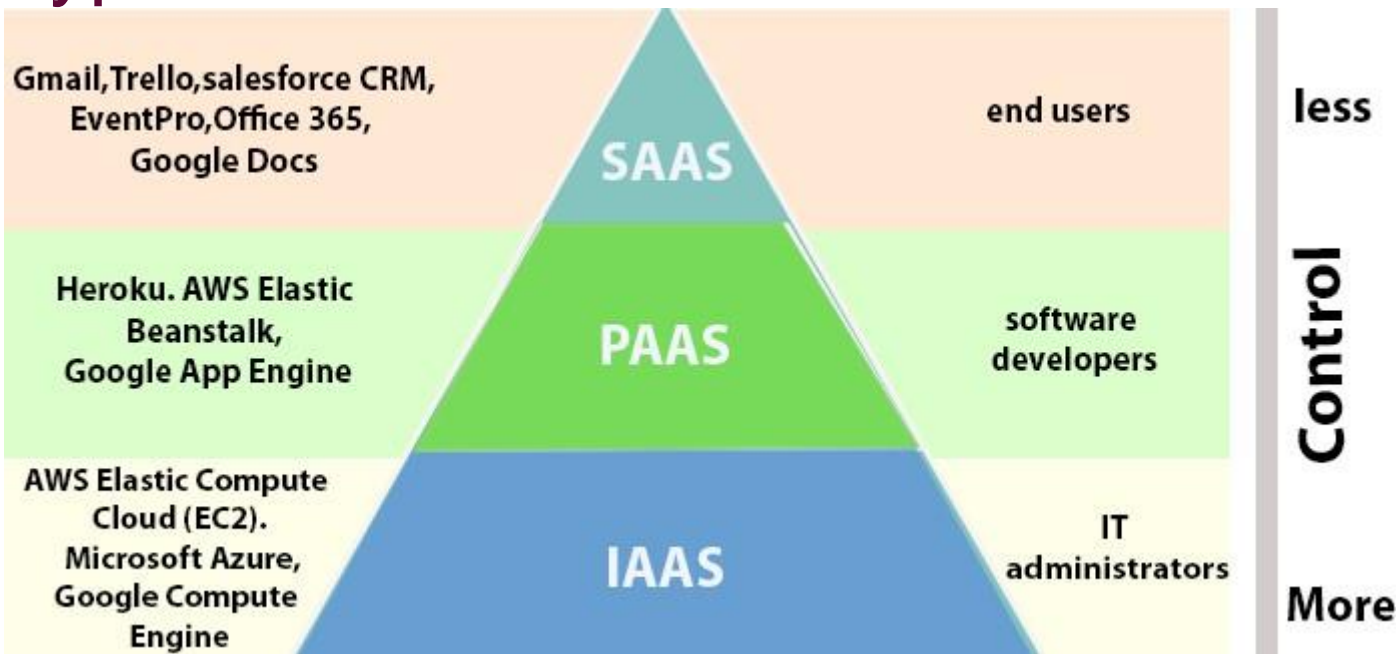


- **Public Cloud:** The cloud resources that are owned and operated by a third-party cloud service provider are termed

as public clouds. It delivers computing resources such as servers, software, and storage over the internet

- **Private Cloud:** The cloud computing resources that are exclusively used inside a single business or organization are termed as a private cloud. A private cloud may physically be located on the company's on-site datacentre or hosted by a third-party service provider.
- **Hybrid Cloud:** It is the combination of public and private clouds, which is bounded together by technology that allows data applications to be shared between them. Hybrid cloud provides flexibility and more deployment options to the business.

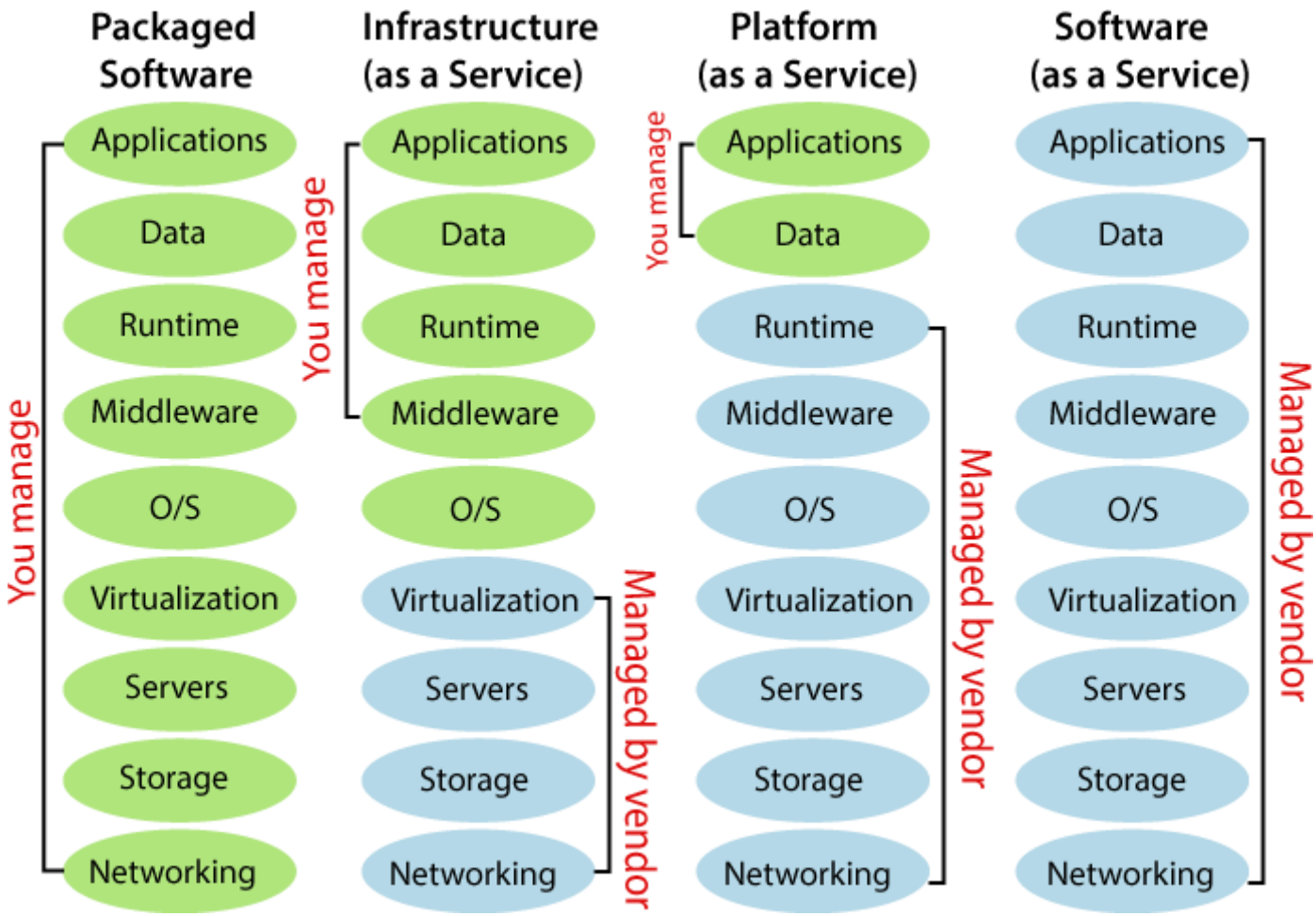
Types of Cloud Services



1. **Infrastructure as a Service (IaaS):** In IaaS, we can rent IT infrastructures like servers and virtual machines (VMs), storage, networks, operating systems from a cloud service vendor. We can create VM running Windows or Linux and install anything we want on it. Using IaaS, we don't need to care about the hardware or virtualization software, but other than that, we do have to manage everything else. Using IaaS, we get maximum flexibility, but still, we need to put more effort into maintenance.
2. **Platform as a Service (PaaS):** This service provides an on-demand environment for developing, testing, delivering, and managing software applications. The developer is

responsible for the application, and the PaaS vendorprovides the ability to deploy and run it. Using PaaS, the flexibility gets reduce, but the management of the environment is taken care of by the cloud vendors.

3. **Software as a Service (SaaS):** It provides a centrally hosted and managed software services to the end-users. It delivers software over the internet, on-demand, and typically on a subscription basis. E.g., Microsoft One Drive, Dropbox, WordPress, Office 365, and Amazon Kindle. SaaS is used to minimize the operational cost to the maximum extent.


Packaged Software
Infrastructure (as a Service)
Platform (as a Service)
Software (as a Service)
Applications
Data
Runtime
Middleware
O/S
Virtualization
Servers
Storage
Networking
You manage
Managed by vendor

Historical Development

In this, we will discuss the history of Cloud computing. And also cover the history of client server computing, distributed computing, and cloud computing.

- Before Computing was come into existence, client Server Architecture was used where all the data and control of client resides in Server side. If a single user want to access some data, firstly user need to connect to the server and after that user will get appropriate access. But it has many disadvantages. So, After Client Server computing,Distributed Computing was come into existence, in this typeof computing all computers are networked together with the help of this, user can share their resources when needed. It also has certain limitations. So in order to remove limitations faced in distributed system, cloud computing was emerged.
- During 1961, John MacCharty delivered his speech at MIT that "Computing Can be sold as a Utility, like Water and Electricity." According to John MacCharty it was a brilliant idea. But people at that time don't want to adopt this technology. They thought the technology they are using efficient enough for them. So, this concept of computing was not appreciated much so and very less will research on it. But as the time fleet the technology caught the idea after few years this idea is implemented. So, this is implemented bySalesforce.comin1999.

- This company started delivering an enterprise application over the internet and this way the boom of Cloud Computing wasstarted.

- In 2002, Amazon started Amazon Web Services (AWS), Amazon will provide storage, computation over the internet. In 2006 Amazon will launch Elastic Compute Cloud

Commercial Service which is open for everybody to use.

- After that in 2009, Google Play also started providing Cloud Computing Enterprise Application as other companies will see the emergence of cloud Computing they also started providing their cloud services. Thus, in 2009, Microsoft launch Microsoft Azure and after that other companies like Alibaba, IBM, Oracle, HP also introduces their Cloud Services. In today the Cloud Computing become verypopular and important skill.

Advantages :

- It is easier to get backup in cloud.
- It allows us easy and quick access stored information anywhere and anytime.
- It allows us to access data via mobile.
- It reduces both hardware ad Software cost, and it is easily maintainable.
- One of the biggest advantage of Cloud Computing is Database Security.

Disadvantages :

- It requires good internet connection.

User have limited control on the data

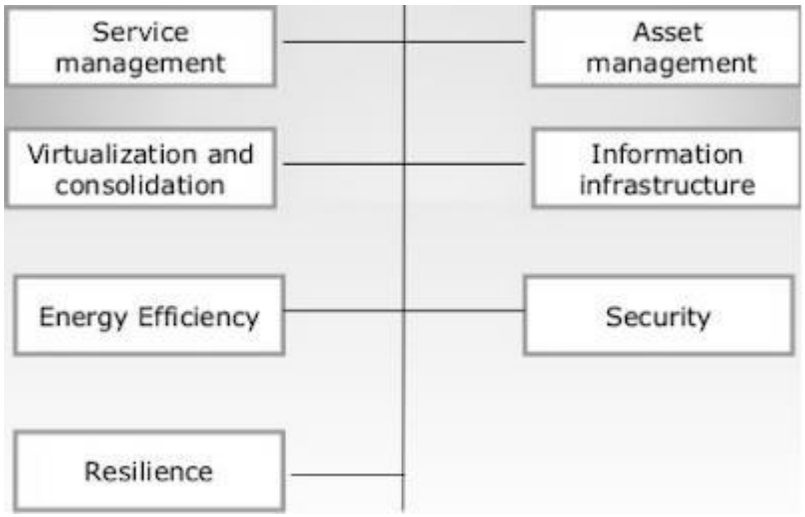
Vision of Cloud computing

In Simplest terms, cloud computing means storing and accessing the data and programs on remote servers that are hosted on internet instead of computer's hard drive or local server. Cloud computing is also referred as Internet based computing. These are following **Vision of Cloud Computing :**

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

10. The presence of this market will enable the acquisition process to automatically integrate with its integration into its existing software applications. The availability of a global cloud trading platform will also help service providers to increase their revenue.
11. A cloud provider can also be a buyer of a competitive service to fulfill its promises to customers.

cloud and dynamic infrastructure



1. Service management

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

2. Asset-Management

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

3. Virtualization and consolidation

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

4. Information Infrastructure

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

5. Energy-Efficiency

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

6. Security

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

7. Resilience

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

Cloud Adoption

What is cloud adoption?

Cloud Adoption is a strategic move by organisations of reducing cost, mitigating risk and achieving scalability of data base capabilities. Cloud adoption may be up to various degrees in an organisation, depending on the depth of adoption. In fact the depth of adoption yields insight into the maturity of best practices, enterprise-ready cloud services availability.

Organisations that go ahead with the strategic decision of adopting cloud based technologies have to identify potential security thefts and controls, required to keep the data and applications in the cloud secured. Hence there is a need for compliance assessment during cloud adoption. The following measures are taken for compliance assessment to ensure security and accountability of data and applications in the cloud services:

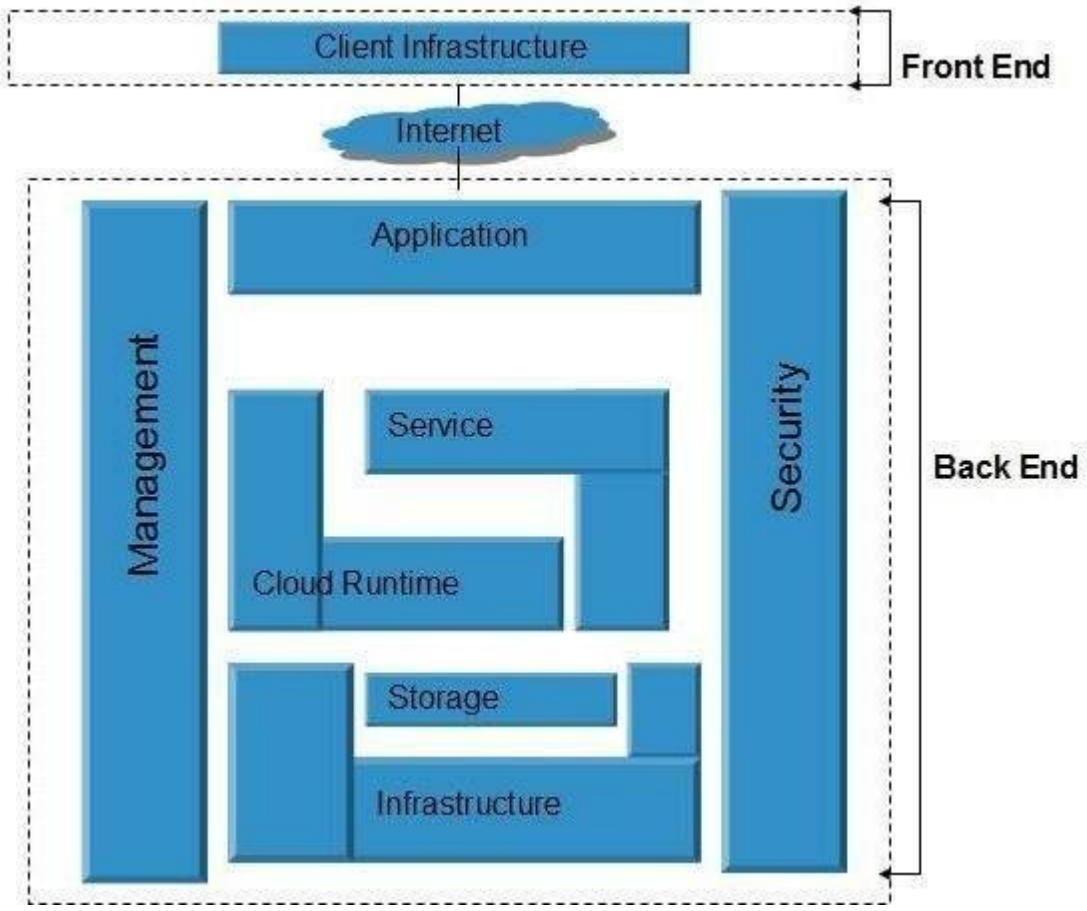
- Matching the security requirements of the organisation with the security capabilities of the cloud service provider
- Analysing the security policies of the cloud service provider along with history of transparency and security related practices
- Proper understanding of the technical aspects of data and traffic flow
- Proper understanding and documentation of the roles and responsibilities of the cloud service provider
- Understanding of the certifications and compliances that can be leveraged from the cloud service provider

Cloud Computing Architecture

Cloud Computing architecture comprises of many cloud components, which are loosely coupled. We can broadly divide the cloud architecture into two parts:

- Front End
- Back End

Each of the ends is connected through a network, usually Internet. The following diagram shows the graphical view of cloud computing architecture:



Front End

The **front end** refers to the client part of cloud computing system. It consists of interfaces and applications that are

required to access the cloud computing platforms, Example - Web Browser.

Back End

The **back End** refers to the cloud itself. It consists of all the resources required to provide cloud computing services. It comprises of huge data storage, virtual machines, security mechanism, services, deployment models, servers, etc.

Note

- It is the responsibility of the back end to provide built-in security mechanism, traffic control and protocols.
- The server employs certain protocols known as middleware, which help the connected devices to communicate with each other.

Cloud Interoperability Standards

Here, we are going to learn about the **Cloud Interoperability Standards**, **Types of Cloud CPortability and interoperability** are related to the ability to create systems that function together "out of the box" from interchangeable components.

The ability to share or exchange information between two or more systems or programs is called interoperability. Cloud interoperability is the ability in which a customer's system communicates with a cloud service or the ability of one cloud service to communicate with other cloud services by sharing information to achieve predictable results according to a specified process.

Cloud computing and interoperability demonstrate that public and private cloud providers recognize the APIs, their standard settings, data formats, authentication, and authorization. "Ideally, it is a standardized interface so that we can migrate from one cloud service to another as a customer with little effect as possible on our systems.

The types of cloud computing portability and interoperability are as follows -

1) Application Portability

Portability between development and operational environments is specific application portability that arises with cloud computing. From a financial perspective, Cloud PaaS is especially appealing for development environments because it eliminates the need for investment in costly infrastructure that would be unused until the development is complete. However, if a particular environment is to be used at runtime, either on in-house systems or on various cloud platforms, it is important that the applications between the two environments can be transferred. Cloud computing brings development and operations closer together and, indeed, contributes to the convergence of the two as develops gradually. This will only function if the same environment is used for development and operation, or if device portability exists between environments for development and operation.

2) Application Interoperability

Interoperability of the application manages application to application communications using external services (e.g., middleware services). Application interoperability translates the processing functions into new programs from existing systems.

3) Platform Portability

Platform portability is supported by the UNIX operating system. It is mostly written in the language of C programming, and by re-compiling and re-writing a few small hardware-dependent parts that are not coded in C, it can be implemented on different hardware. Similarly, many other operating systems may be ported. This is the conventional portability approach to platforms. It allows portability of applications because applications that use the standard interface of the operating system can similarly be re-compiled and run on devices with distinct hardware. It is demonstrated in the platform source portability.

4) Platform Interoperability

Interoperability of networks includes standard protocols for the discovery of resources and the exchange of knowledge. These implicitly enable the interoperability of the applications that use the platforms. Interoperability with software cannot be accomplished without interoperability with platforms.

Cloud computing interoperability use cases

Several cloud computing interoperability use cases have already been described in the current literature. The FP7 project Cloud4SOA (111) defines the following usage scenarios: deploying a service-based application on the Cloud4SOA platform, and migration to/deployment on a different platform as a service provider. In the other deliverable of the same project, four semantic interoperability use cases were defined (16):

• Deployment of an application on a PaaS offering

• Migration of an application deployed on one PaaS solution to a different PaaS offering • Hybrid clouds: PaaS systems/offering interoperation

• Integration between applications deployed on different PaaS offerings

Another FP7 project, Contrail (112), describes four use cases that represent a diverse set of requirements:

• Distributed provision of geo-referenced data which is an implementation of a 3D Virtual Tourist Guide (VTG service)

• Multimedia processing service marketplace that will exploit Contrail federated cloud to develop a marketplace offering multimedia services to end-users

SCALABILITY AND FAULT TOLERANCE

Cloud Scalability is the ability to scale on-demand the facilities and services as and when they are required by the user.

Cloud Fault Tolerance is tolerating the faults by the cloud that are done by mistake by the user.
Here the scaling is beyond the limits, it means we can't even imagine what will be the limit.
loud middleware is designed on the principle of scalability along different dimensions in mind e.g.:- performance, size and load.

The cloud middleware manages a huge number of resources and users which depends on the cloud to obtain that they can't obtain within the premises without affording the administrative and maintenance costs.

So in this overall scenario the ability to tolerate failure is normal but sometimes it becomes more important than providing an efficient & optimized system.

The overall conclusion says that “it is a challenging task for the cloud providers to develop such high scalable and fault tolerance systems who can get managed and at the same time they will provide a competitive performance.

What is a cloud ecosystem?

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

Werner Vogels, CTO at Amazon, first compared the cloud to an ecosystem in a keynote address at the Cloud Connect 2011 conference. At the time, enterprise cloud computing was usually thought of in terms of three broad service areas -- infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS) and software-as-a-service (SaaS). Vogels proposed that the cloud was really more complex and its description also needed to include the array of service providers that companies rely on to operate in the cloud.

How a cloud ecosystem works

The center of a cloud ecosystem is a public cloud provider. It might be an IaaS provider such as Amazon Web Services (AWS) or a SaaS vendor such as Salesforce. Radiating out from the center of the cloud are software companies that use the provider's anchor platform, as well as consultants and mpanies that have formed strategic alliances with the anchor provider.

There is no vendor lock-in because these companies overlap, making the ecosystem more complex. For example, AWS is the center of its own ecosystem, but it's also a part of the Salesforce ecosystem. Salesforce runs a number of its services on AWS's infrastructure, and Salesforce customers can gain access, through devices called connectors, to pieces of AWS, such as its Simple Storage Service (S3).

A robust ecosystem provides a cloud provider's customers with an easy way to find and purchase business applications and respond to changing business needs. When the apps are sold through a provider’s app store such as AWS Marketplace, Microsoft Azure Marketplace (for cloud software) or Microsoft AppSource (for business applications), the customer essentially has access to a catalog of

different vendors' software and services that have already been vetted and reviewed for security, risk and cost.

The benefits of a cloud ecosystem

Companies can use a cloud ecosystem to build new business models. It becomes relatively easy for a medical device manufacturer, for example, to launch a heart-monitoring service on its cloud service provider's cloud infrastructure and then sell the service alongside its main business of manufacturing heart monitors for hospitals.

In a cloud ecosystem, it is also easier to aggregate data and analyze how each part of the system affects the other parts. For example, if an ecosystem consists of patient records, smart device logs and healthcare provider records, it becomes possible to analyze patterns across an entire patient population.

The term 'Virtualization' can be used in many respect for computers. It is the process of creating a virtual environment of something which may include hardware platforms, storage devices, OS, network resources, etc. The cloud's virtualization mainly deals with server virtualization and how it works, and why it is termed so?

CLOUD MANAGEMENT AND VIRTULATION TECHNOLOGY

Defining Virtualization

Virtualization is the ability that 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 that 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 & the virtual machine is the guest machine. This virtual environment is managed by firmware, which is termed as a hypervisor.

There are several approaches or ways to virtualizes cloud servers.

<u>These are:</u>

- **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 of running 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 shutting down. This technique is termed as "Live Migration". Another technique is used to actively load balance among multiple hosts to utilize those available resources in a virtual machine efficiently. The concept is termed as Distributed Resource Scheduling or Dynamic Resource Scheduling.

Types of Virtualization

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

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

5. 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 application but also share their infrastructures with the help of virtualization. Virtualization is used mainly to provide applications with standard versions for 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 using 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 today's hypervisors use 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 benefits in the business field.

Difference Between Virtualization and Cloud

1. Essentially there is a gap between these two terms, though cloud technology requires the concept of virtualization. Virtualization is a technology - it can also be treated as software that can manipulate hardware. At the same time, cloud computing is a service that is the result of manipulation.

2. Virtualization is the foundation element of cloud computing, whereas Cloud technology is the delivery of shared resources as a service-on-demand via the internet.
3. Cloud is essentially made-up of the concept of virtualization.

Advantages of Virtualization

- The number of servers gets reduced by the use of the virtualization concept.
- Improve the ability of technology.
- The business continuity was also raised due to the use of virtualization.
- It creates a mixed virtual environment.
- Increase efficiency for the development and 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 is safely separated and don't affect each other.
4. **Hardware Independence**: When the virtual server runs, it can migrate to a different hardware platform.

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

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

- Resources that can be moved to the cloud and test its sensitivity risk are picked.
- The type of cloud is to be considered.
- The risk in the deployment of the cloud depends on the types of cloud and service models.

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

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

Importance of cloud security :

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

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

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

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

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

- Control over cloud data
- Misconfiguration
- Ever changing workload
- Access Management
- Disaster recovery

What Is Cloud Security Architecture?

Cloud security architecture describes all the hardware and technologies designed to protect data, workloads, and systems within cloud platforms. Developing a strategy for cloud security architecture should begin during the blueprint and design process and should be integrated into cloud platforms from the ground up. Too often, cloud architects will focus entirely on performance first and then attempt to bolt security on after the fact.

Cloud Security Core Capabilities

Secure cloud computing architecture encompasses three core capabilities: confidentiality, integrity, and availability. Understanding each capability will help guide your efforts in planning a more secure cloud deployment.

- **Confidentiality** is the ability to keep information secret and unreadable to the people who shouldn't have access to that data, such as attackers or people inside an organization without the proper access level. Confidentiality also includes privacy and trust, or when a business pledges secrecy in handling their customers' data.
- **Integrity** is the idea that the systems and applications are exactly what you expect them to be, and function exactly as you expect them to function. If a system or application has been compromised to produce an

unknown, unexpected, or misleading output, this can lead to losses.

- **Availability** is the third capability and is generally the least considered by cloud architects. Availability speaks to denial-of-service (DoS) attacks. Perhaps an attacker can't see or change your data. But if an attacker can make systems unavailable to you or your customers, then you can't carry out tasks that are essential to maintain your business.

Secure Cloud Computing in Practice

There are numerous tools to address confidentiality, integrity, and availability in cloud platforms with the end goal of defining a trusted execution environment (TEE). These are just a few tools that cloud security architects and experts use to help safeguard systems and data, and they serve as a good starting point during your blueprint phase.

- Encryption protects text and data by translating it into ciphers that only authorized parties have the ability to decipher, access, and edit.
- Firmware resilience is about helping to prevent attacks to the firmware layer but also includes recovering from an attack and restoring the system back to a known good state.
- Establishing a root of trust includes boot integrity, which helps protect the system from malware injections during system startup.
- Stack validation seeks to establish that all components and software within a system stack have been validated

and are not compromised or changed, either before delivery, in transit to cloud architects, or during deployment.
- Secure systems are designed to isolate virtual machines (VMs), containers, data, and applications from each other as a key best practice.

Why Is Cloud Security Architecture Important?

The cloud, whether it's private cloud, public cloud, or hybrid cloud, holds the promise of agility, efficiency, and cost effectiveness. These are transformational qualities for any business, and they enable organizations to adapt to market changes with rapid services delivery and the ability to make data-informed decisions. However, businesses may be prevented from using cloud resources without exposing themselves and their data to risk. Cloud security architecture allows businesses to take advantage of all that the cloud offers—including software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS) offerings—while mitigating exposure and vulnerability. Without cloud security architecture, the risks associated with using the cloud could outweigh any potential benefit.

Cloud Security Architecture Threats

While planning your cloud deployment, you want to be prepared for common threats such as malware and privilege-based attacks. There are too many common threats to enumerate here, so instead this article will

provide a snapshot of high-profile threats that industry experts are thinking about right now.

- **Insider threats** include both workers within your own organization who have access to systems and data and also cloud service provider (CSP) administrators. When you subscribe to CSP services, you are essentially entrusting your data and workloads to the multitude of staff who are responsible for maintaining the CSP architecture. Another consideration is whether data is accessible to governmental entities. Security experts are paying more attention to the laws, regulations, and real-life practices that demonstrate whether a government can use court orders or other means to gain access to data in a private or public cloud.
- **DoS attacks** are a huge area of focus. Temporary direct denial-of-service (DDoS) attacks typically involve hammering a system with requests until it shuts down. Security perimeters can deflect these attacks using network compliance policies to filter out repeated requests. CSPs can also shift workloads and traffic to other resources while they work to restore the system. Permanent DoS attacks are more destructive and often inflict damage at the firmware level to render a server unbootable. In this case, a technician needs to physically reload the firmware and rebuild the system from scratch, which can result in servers being shut down for days or weeks.
- **The cloud edge** can refer to cloud-connected edge systems, but for a CSP it also refers to server

architecture that is not under the CSP's direct control. Global CSPs cannot build and run their own facilities in every corner of the planet, so they rely on partners to deliver services to smaller, geographically isolated, or rural regions. As a result, these CSPs don't have total control to monitor and ensure physical box integrity for the hardware or physical attack protections such as locking down access to USB ports.

- **Customer control** influences how customers evaluate public cloud offerings. From the customer perspective, users are nervous about moving sensitive workloads to the public cloud. On the other hand, big cloud providers are typically much better equipped and have a much higher level of expertise in cloud security than the average enterprise running a private cloud. Generally, customers find it reassuring to be in total control of their most sensitive data, even if their security tools aren't as sophisticated.
- **Hardware limitations** mean that even with the most robust cloud security architecture in the world, a server can't help you create a better password. Passwords are one of the most common vectors of attack. Cloud security architects are focused on hardware, firmware, and software protections, but it will still fall on the shoulders of everyday users to follow best practices.

Cloud Security Architecture for SaaS, PaaS, and IaaS

From an IT perspective, there are big differences in security practices between cloud service models for SaaS,

PaaS, and IaaS. For cloud architects, the tools to help build confidentiality, integrity, and availability across SaaS, PaaS, and IaaS are essentially the same and include encryption, firmware resilience, stack validation, and establishing a root of trust.

PaaS providers must pay attention to multiparty usage and establish trust in moving data to and from the platform. IaaS providers must focus on runtime encryption and orchestration capabilities that empower customers to manage key encryption for any application they use in the cloud.

SaaS includes productivity software suites and is widely used by businesses and individuals alike. SaaS must be secured at the CSP level—by the CSP. Users and customers in these cases have little control over the SaaS offerings, but their contribution to security takes place through adherence to best practices. Using strong passwords and two-factor authentication, being careful with personally identifiable information on social media, and avoiding email phishing scams all factor in.

Intel Cloud Security Architecture Products and Solutions

It would be difficult to list every single technology that contributes to cloud security architecture. Intel has been building security features into processors and other technology offerings for decades, and its security technologies continue to evolve generation over generation. The goal of more recent advances and

offerings is to further the paradigm of confidential computing in the cloud.

Intel® Software Guard Extensions (Intel® SGX) helps create a trusted environment by integrating security capabilities for data while being processed in memory. Developers can use Intel® SGX to establish memory enclaves that provide extra layers of workload isolation. Cryptographic accelerators such as Intel® QuickAssist Technology (Intel® QAT) help deliver high performance even when heavy encryption and compression loads are needed.

The latest addition to the Intel® Xeon® Scalable platform also adds Intel® Total Memory Encryption (Intel® TME) and Intel® Platform Firmware Resilience (Intel® PFR). Intel® TME helps ensure that all memory accessed from the Intel® CPU is encrypted, including customer credentials, encryption keys, and other personally identifiable information. Intel® PFR equips cloud architects with the tools to increase protection against firmware interception, detect firmware corruption, and restore systems to a known good state.

Lastly, Intel collaborates with ecosystem partners to abstract and expand trusted execution capabilities and further the paradigm of confidential computing. This helps proliferate key technologies across a vast field of developers, system vendors, and system integrators. For example, Microsoft Azure uses Intel® SGX in building their cloud security architecture, and this benefits Microsoft Azure users even if they're not aware of it.

Security as Critical to Business Transformation

Confidential computing and platforms that deliver confidentiality, integrity, and availability are prerequisites to taking advantage of cloud resources. Businesses need their cloud infrastructure to be performant, but they also need it to be reliable and trustworthy. Effective cloud security architecture is reliant on cloud architects who understand that a trusted foundation has to be a top-of-mind consideration during the initial planning stages and not something to be tacked on after the fact. Security isn't a commodity; it is an essential ingredient.

Market Based Management of Clouds

As consumers rely on Cloud providers to supply all their computing needs, they will require specific QoS to be maintained by their providers in order to meet their objectives and sustain their operations. Cloud providers will need to consider and meet different QoS parameters of each individual consumer as negotiated in specific SLAs. To achieve this, Cloud providers can no longer continue to deploy traditional system-centric resource management architecture that do not provide incentives for them to share their resources and still regard all service requests to be of equal importance. Instead, market- oriented resource management is necessary to regulate the supply and demand of Cloud resources at market equilibrium, provide feedback in terms of economic incentives for both Cloud consumers and providers, and promote QoS-based resource allocation mechanisms that differentiate service requests based on their utility. Figure shows the high-level architecture for supporting market-oriented resource allocation in Data Centers and Clouds.

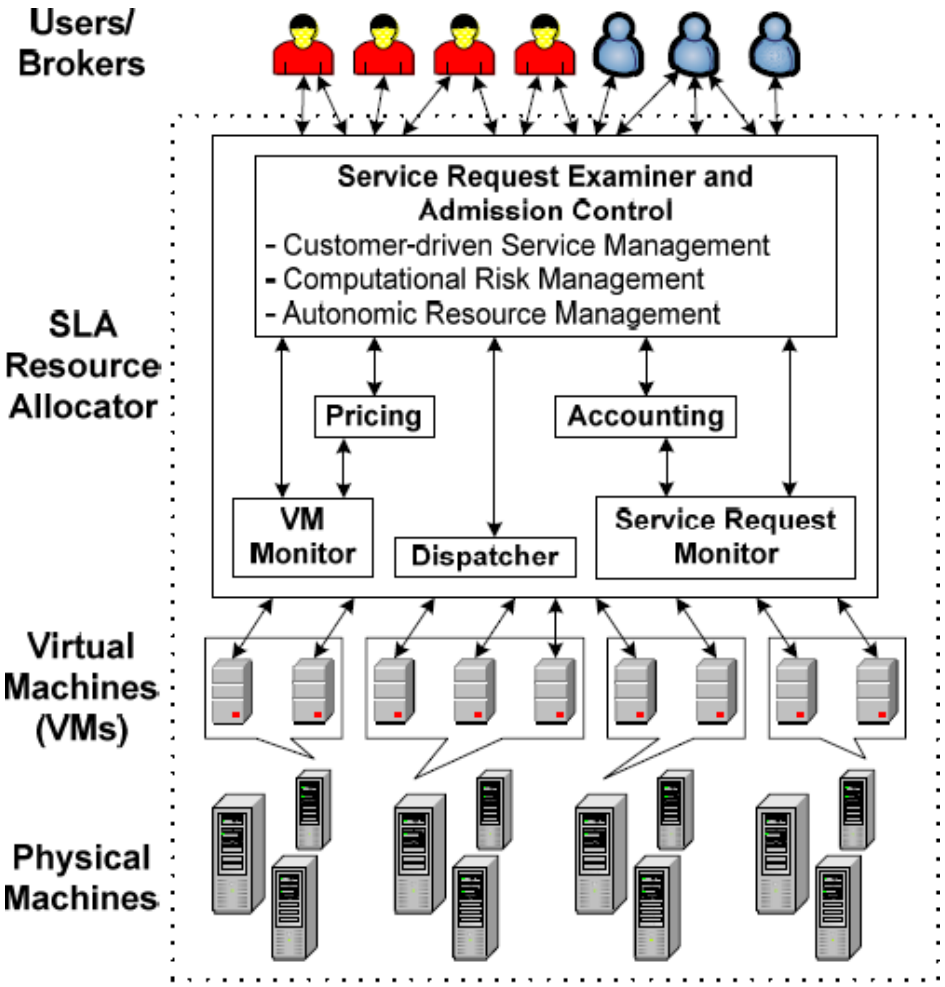


Figure 3: High-level market-oriented cloud architecture.

There are basically four main entities involved:

•Users/Brokers: Users or brokers acting on their behalf submit service requests from anywhere in the world to the Data Center and Cloud to be processed.

•SLA Res Data Center/Cloud service provider and external users/brokers. It requires the interaction of the following mechanisms to support SLA-oriented resource management:

- Service Request Examiner and Admission Control : When a service request is first submitted, the Service Request Examiner and Admission Control mechanism interprets the submitted request for QoS requirements before determining whether to

accept or reject the request. Thus, it ensures that there is no overloading of resources whereby many service requests cannot be fulfilled successfully due to limited resources available. It also needs the latest status information regarding resource availability (from VM Monitor mechanism) and workload processing (from Service RequestMonitor mechanism) in order to make resource allocation decisions effectively. Then, it assigns requests to VMs and determines resource entitlements for allocated VMs.

- Pricing: The Pricing mechanism decides how service requests are charged. For instance, requests can be charged based on submission time (peak/off-peak), pricing rates (fixed/changing) or availability of resources (supply/demand). Pricing serves as a basis for managing the supply and demand of computing resources within the Data Center and facilitates in prioritizing resource allocations effectively.
- Accounting: The Accounting mechanism maintains the actual usage of resources by requests so that the final cost can be computed and charged to the users. In addition, the maintained historical usage information can be utilized by the Service Request Examiner and Admission Control mechanism to improve resource allocation decisions.
- VM Monitor: The VM Monitor mechanism keeps track of the availability of VMs and their resource entitlements.
- Dispatcher: The Dispatcher mechanism starts the

execution of accepted service requests on allocated VMs.

- Service Request Monitor: The Service Request Monitor mechanism keeps track of the execution progress of service requests.

•VMs: Multiple VMs can be started and stopped dynamically on a single physical machine to meet accepted service requests, hence providing maximum flexibility to configure various partitions of resources on the same physical machine to different specific requirements of service requests. In addition, multiple VMs can concurrently run applications based on different operating system environments on a single physical machine since every VM is completely isolated from one another on the same physical machine.
•Physical Machines: The Data Center comprises multiple computing servers that provide resources to meet service demands.

Commercial offerings of market-oriented Clouds must be able to:

- support customer-driven service management based on customer profiles and requested service requirements,
- define computational risk management tactics to identify, assess, and manage risks involved in the execution of applications with regards to service requirements and customer needs,
- derive appropriate market-based resource

management strategies that encompass both

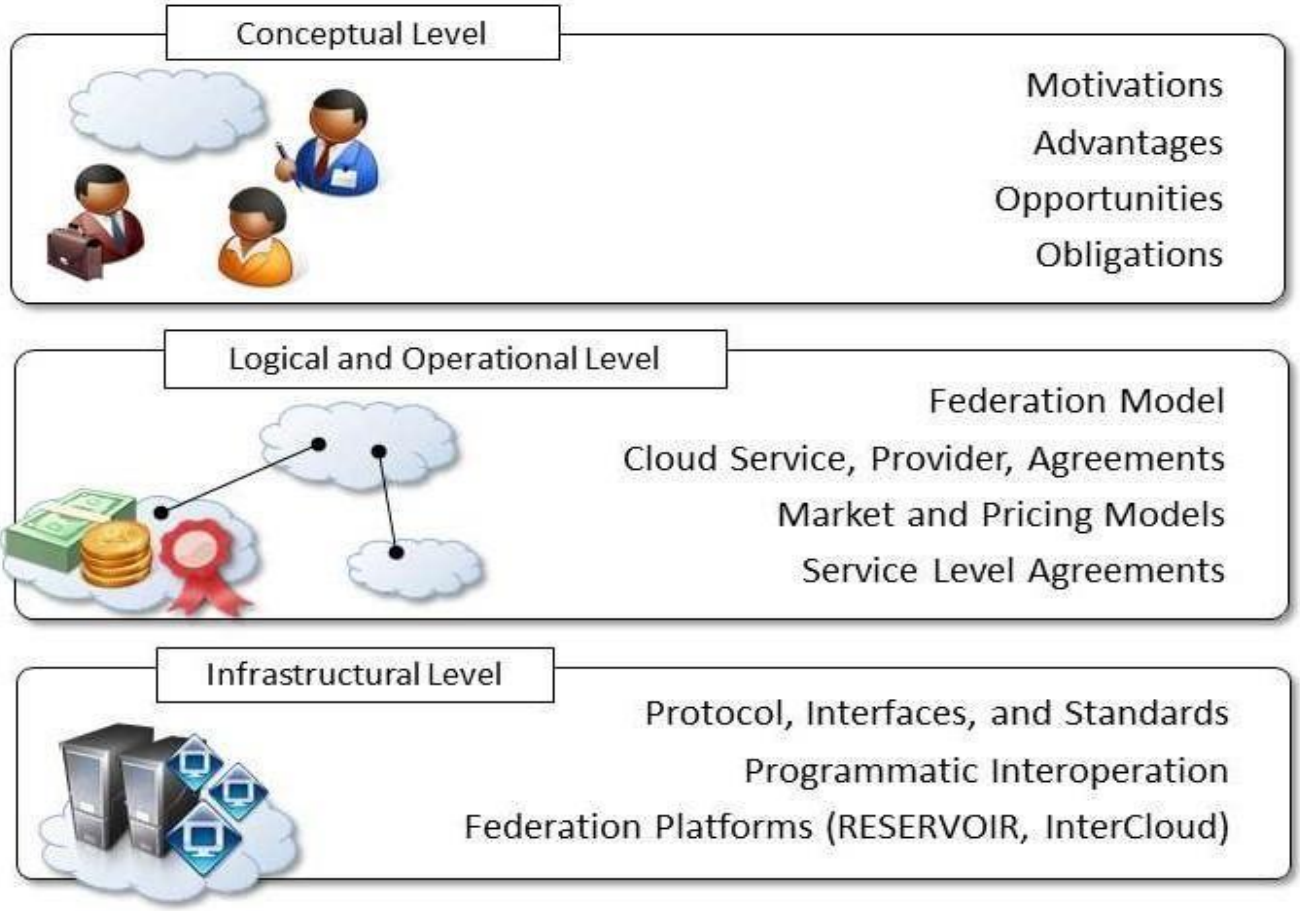
Federated Clouds/Inter Cloud

The terms cloud federation and InterCloud, often used interchangeably, convey the general meaning of an aggregation of cloud computing providers that have separate administrative domains. It is important to clarify what these two terms mean and how they apply to cloud computing.

The term federation implies the creation of an organization that supersedes the decisional and administrative power of the single entities and that acts as a whole. Within a cloud computing con-text, the word federation does not have such a strong connotation but implies that there are agree- ments between the various cloud providers, allowing them to leverage each other's services in a privileged manner. A definition of the term cloudfederation was given by Reuven Cohen,founder and CTO of EnomalyInc :
Cloud federation manages consistency and access controls when two or more independent geo-graphically distinct Clouds share either authentication, files, computing resources, command and control or access to storage resources.

InterCloud is a term that is often used interchangeably to express the concept of Cloudfederation. It was introduced by Cisco for expressing a composition of clouds that are interconnected by means of open

standards to provide a universal environment that leverages cloud computing services. By mimicking the Internet term, often referred as the “network of networks,” InterCloud represents a “Cloud of Clouds” and therefore expresses the same concept of federating together clouds that belong to different administrative organizations. The term InterCloud refers mostly to a global vision in which interoperability among different cloud providers is governed by standards, thus creating an open platform where applications can shift workloads and freely compose services from different sources. On the other hand, the concept of a cloud federation is more general and includes ad hoc aggregations between cloud providers on the basis of private agreements and proprietary interfaces


Conceptual Level
Motivations
Advantages
Opportunities
Obligations
Logical and Operational Level
Federation Model
Cloud Service, Provider, Agreements
Market and Pricing Models
Service Level Agreements
Infrastructural Level
Protocol, Interfaces, and Standards
Programmatic Interoperation
Federation Platforms (RESERVOIR, InterCloud)

Creating a cloud federation involves research and development at different levels: conceptual, logical and operational, and infrastructural. Figure 11.7 provides a comprehensive view of the challenges faced in designing and implementing an organizational structure that coordinates together cloud services that belong to different administrative domains and makes them operate within a context of a single unified service middleware. Each cloud federation level pres ents different challenges and operates at a different layer of the IT stack. It then requires the use of different approaches and technologies. Taken together, the solutions to the challenges faced at each of these levels constitute a reference model for a cloud federation.

The conceptual level addresses the challenges in presenting a cloud federation as a favorable solution with respect to the use of services leased by single cloud providers. In this level it is important to clearly identify the advantages for either service providers or service consumers in joining a federation and to

delineate the new opportunities that a federated environment creates with respect to the single-provider solution. The conceptual level addresses the challenges in presenting a cloud federation as a favorable soluion with respect to the use of services leased by

single cloud providers. In this level it is important to clearly identify the advantages for either service providers or service consumers in joining a federation and to delineate the new opportunities that a federated environment creates with respect to thesingle-provider solution. Elements of concern at this level are:

- Motivations for cloud
providers to join a federation
Motivations for service
consumers to leverage a
federation
- Advantages for providers in leasing their services to other providers

- Obligations of providers once they have joined the federation
- Trust agreements between providers • Transparency versus consumers

The logical and operational level of a federated cloud identifies and addresses the challenges in devising a framework that enables the aggregation of providers that belong to different administrative domains within a context of a single overlay infrastructure, which is the cloud federation. At this level, policies and rules for interoperation are defined. Moreover, this is the layer at which decisions are made as to how and when to lease a service to—or to leverage a service from—another provider. The logical component defines a context in which agreements among providers are settled and services are negotiated, whereas the operational component characterizes and shapes the dynamic behavior of the federation as a result of the single providers' choices. This is the level where MOCC is implemented and realized.

The infrastructural level addresses the technical challenges involved in enabling heterogeneous cloud

computing systems to interoperate seamlessly. It deals with the technology barriers that keep separate cloud computing systems belonging to different administrative domains. By having standardized protocols and interfaces, these barriers can be overcome. In other words, this level for the federation is what the TCP/IP stack is for the Internet: a model and a reference implementation of the technologies enabling the interoperation of systems. The infrastructural level lays its foundations in the IaaS and PaaS layers of the Cloud Computing Reference Model. Services for interoperation and interface may also find implementation at the Saa S level, especially for the realization of negotiations and of federated clouds.

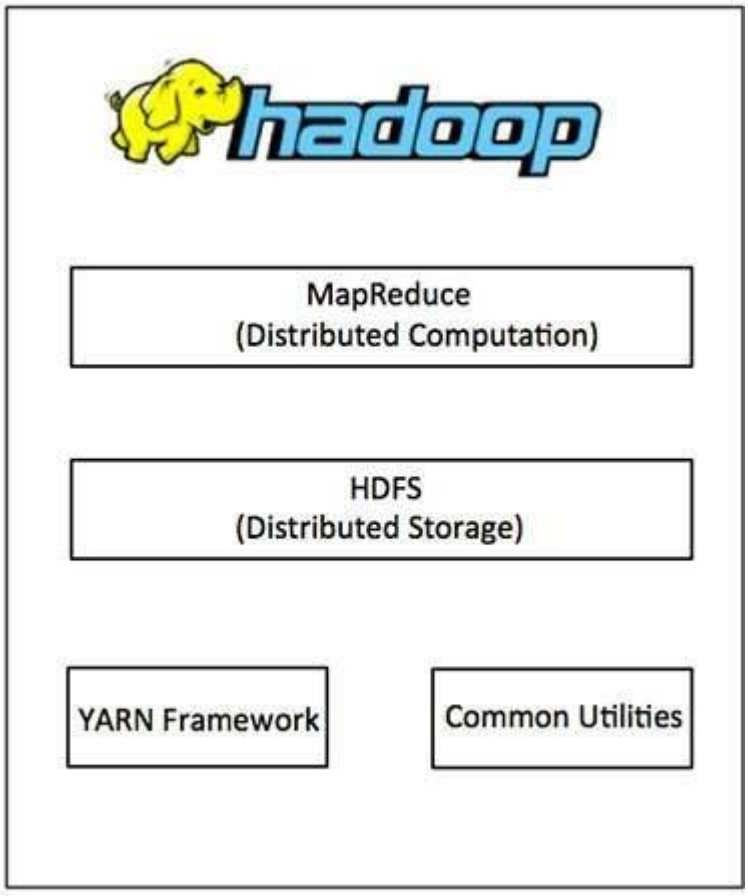
Hadoop

Hadoop is an Apache open source framework written in java that allows distributed processing of large datasets across clusters of computers using simple programming models. The Hadoop framework application works in an environment that provides distributed *storage* and *computation* across clusters of computers. Hadoop is designed to scale up from single server to thousands of machines, each offering local computation and storage.

Hadoop Architecture

At its core, Hadoop has two major layers namely −

- Processing/Computation layer (MapReduce), and
- Storage layer (Hadoop Distributed File System).



MapReduce

MapReduce is a parallel programming model for writing distributed applications devised at Google for efficient processing of large amounts of data (multi-terabyte data-sets), on large clusters (thousands of nodes) of commodity hardware in a reliable, fault-tolerant manner.

The MapReduce program runs on Hadoop which is an Apache open-source framework.

Hadoop Distributed File System

The Hadoop Distributed File System (HDFS) is based on the Google File System (GFS) and provides a distributed file system that is designed to run on commodityhardware. It has many similarities with existing distributed file systems. However, the differences from other distributed file systems are significant. It is highly fault- tolerant and is designed to be deployed on low-cost hardware. It provides high throughput access to application data and is suitable for applications havinglarge datasets.

Apart from the above-mentioned two core components, Hadoop framework also includes the following two modules −

- **Hadoop Common** − These are Java libraries and utilities required by other Hadoop modules.
- **Hadoop YARN** − This is a framework for job scheduling and cluster resource management.

How Does Hadoop Work?

It is quite expensive to build bigger servers with heavy configurations that handle large scale processing, but as an alternative, you can tie together many commodity computers with single-CPU, as a single functional distributed system and practically, the clustered machines can read the dataset in parallel and provide a much higher throughput. Moreover, it is cheaper than one high-

end server. So this is the first motivational factor behind using Hadoop that it runs across clustered and low-cost machines.

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

- Data is initially divided into directories and files. Files are divided into uniform sized blocks of 128M and 64M (preferably 128M).
- These files are then distributed across various cluster nodes for further processing.
- HDFS, being on top of the local file system, supervises the processing.
- Blocks are replicated for handling hardware failure.
- Checking that the code was executed successfully.
- Performing the sort that takes place between the map and reduce stages.
- Sending the sorted data to a certain computer.
- Writing the debugging logs for each job.

Advantages of Hadoop

- Hadoop framework allows the user to quickly writeand test distributed systems. It is efficient, and it automatic distributes the data and work across the machines and in turn, utilizes the underlying parallelism of the CPU cores.

- Hadoop does not rely on hardware to provide fault-tolerance and high availability (FTHA), rather Hadoop library itself has been designed to detect and handle failures at the application layer.
- Servers can be added or removed from the cluster dynamically and Hadoop continues to operate without interruption.
- Another big advantage of Hadoop is that apart from being open source, it is compatible on all the platforms since it is Java based.