UNIT -1

Cloud Computing Fundamentals and Architecture-:

Cloud computing pertains to internet-based hosting and other services such as databases, applications, analytics, and other platforms. In other words, any service that can be given without being physically near the hardware qualifies. Netflix, for example, employs cloud computing to provide video streaming services

Cloud Computing Services Provider

Some of the popular cloud service providers are:

Amazon Web Services (AWS)
Microsoft Azure
Google Cloud
Oracle
IBM Cloud
Alibaba Cloud

Types of Cloud

Cloud architectures can be divided into three categories: public, private, hybrid and serverless. Let us understand in details the different types of cloud computing.

Public Clouds: Public clouds are hosted by an organization that provides resources, such as storage or processing power, to its customers on a pay-as-you-go basis. Customers can access the public cloud through a web browser or application programming interface (API). The most popular public clouds are Amazon Web Services (AWS), Google Cloud Platform (GCP), Microsoft Azure, and IBM SoftLayer.

Private Clouds: Private clouds are hosted by an organization that maintains control over the software, hardware, data centers, networking infrastructure, and security of the cloud. Private clouds are typically used by organizations that want to manage their own IT resources, such as applications and data. The most popular private clouds are Amazon Web Services (AWS), Google Cloud Platform (GCP), and Microsoft Azure. Amazon VPC, HPE, VMware, and IBM

Hybrid Clouds: Hybrid clouds are a combination of public and private clouds. A hybrid cloud enables you to use public or private clouds to deliver an application or service. For example, you can use AWS to host your web applications, and your on-premises infrastructure to host your storage. Typically, this will include VPN links to connect the clouds together and may include features such as the ability to “burst” workloads into the public cloud as necessary.

Multi-Cloud: Some organizations do not want to be locked into a contract till eternity with the cloud providers and prefer a multi-cloud approach. For example, if architected properly, the compute might be from Azure as the application is written in .NET, while the blob storage might be AWS Simple Storage Service, S3. This gives companies a greater flexibility and leverage to change cloud providers as and when needed. The most popular use case is combining the on-prem infrastructure with that of a cloud provider.

Cloud Computing Architecture

As with all the technology architectures, at basic level, you can divide it into two layers, front-end and back-end. These two layers are accompanied by things such as a networking, automation and security. More complex architectures are n-tiered with multiple layers in between the front end and the backend. Let us look at some of these components in a little more detail.

Front-end

Data storage, virtual machines, virtualization software, and other software and hardware components make up cloud infrastructure. Front-end systems (clients) access the cloud environment using the Internet or in some cases a virtual private network (VPN) link. This could be using a web browser, mobile app, or client-based software.

Backend

It's in charge of keeping track of all the programs that operate the applications on the front end. It has a significant number of servers and data storage systems. The backend may include the pooled cloud infrastructure resources, data, and applications. For high availability, these resources could be spread in more than one geographic location.

Application

This refers to either software or a platform. The application presents the output to an end-user (with resources) based on the client's requirements in the back end.

Storage

Storage could be a SQL based storage or a no-SQL storage to store and preserve data like files, movies, documents and relational data.

Service

In order for an application to connect to the storage, in most cases a service is used. Common example is WebServices or an API.

Management

Its job is to allocate specialized resources to specific tasks while also performing numerous cloud-related operations. It aids in administering applications, tasks, services, encryption, data storage, and cloud system resources. Management model is also dependent on if an organization choose IaaS, PaaS, SaaS or Serverless.

Security

Security includes, policies, technologies, and controls that strengthen the security thereby helping protect the data, apps, and infrastructure from potential threats. It also integrates security management into the cloud server via virtual firewalls, limiting data loss

Roots of Cloud Computing

The roots of cloud computing are sub-divided into four types. They are,

- Internet Technologies
- Hardware
- System Management
- Distributed Computing

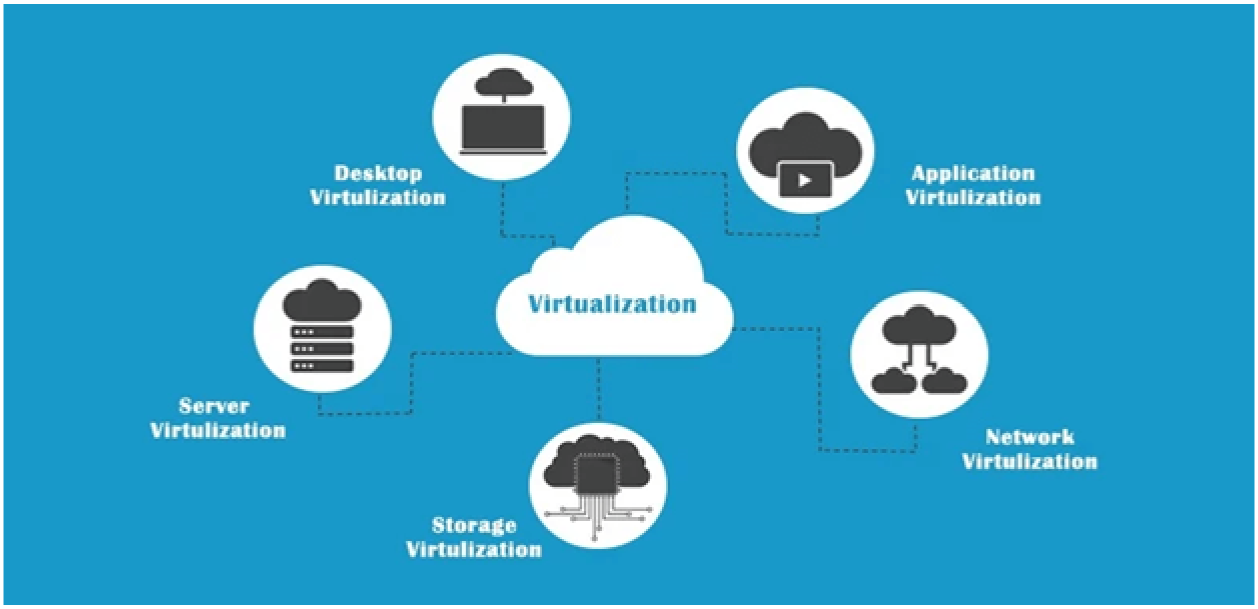
Internet Technologies in Cloud Computing

Virtualization and Service-Oriented Architecture

Virtualization is the process of deploying virtual resources in cloud infrastructures such as servers, storage management, and desktop. To reduce the cost and time effort of cloud providers this virtualization concept is introduced. Virtualization is subdivided into various types. The below-mentioned picture describes the various types of virtualization used in cloud computing

Desktop Virtualization

Desktop Virtualization is the concept of users accessing their desktops virtually from any location. For the end-user environment, this desktop virtualization is created. The types of desktop virtualization are as follows,



Virtual desktop Infrastructure-The actions are done in the central server which provides the virtual desktop service to the end-user.

Remote desktop Services-Users are allowed to work based on windows applications remotely

Desktop as a Service-In Desktop as a Service, a third party hosts the virtual application

Application Virtualization

In application virtualization, the users are all allowed to use the application in the system rather than one which is installed. The OS and system software are installed on many computers.

Network Virtualization

The combination of both hardware and software operations is called Network Virtualization. It establishes a connection between the application and the software system.

Storage Virtualization

The storage virtualization array consists of multiple arrays which are appeared to be single virtualization. It can be either called a disk array or a storage array.

Server Virtualization

Partitioning the single server into multiple servers which can run on their independent operating system.

Service-Oriented Architecture (SOA)

As the business grows, there is a large number of implementation of software and hardware requirements, which is difficult to manage. Hence SOA helps to maintain and implement the architecture.

Grid Computing

To manage and handle a large set of data, the networked computers are connected to perform the operations. The group of computers joins as a cluster to simplify the task.

Utility Computing

As the name itself denotes, the providers provide the computing service based on the user's demand. It is based on the process of pay peruse.

Platform As A Service (PAAS)

As the name itself indicates "platform" means it gives a complete technical platform to the customer such as hardware, software, and infrastructure for developing and deploying the application. The advantage of PAAS is, that it supplies networking, storage, server, operating system (OS), etc.., a complete cloud platform to the user for developing and running their application without worrying about building and maintaining the cloud infrastructure required to develop and launch the app.

Infrastructure as a service (IAAS)

It is purely an infrastructure-based cloud computing service that provides complete infrastructure like supporting web applications, and services based on user facility. As it is based o storage and infrastructure the customer has to use this on by pay-as-you-go basis based on their demand. It reduces the cost of buying and managing physical servers and data infrastructures.

increases the scale and performance of IT workloads and reduces the expenditure on buying external hardware tools. Examples of IAAS are Amazon Web Services, Google compute engine (GCE), Green Cloud Technologies, and Microsoft Azure.

Software as a Service (SAAS)

SAAS enables the end-user to use cloud-based applications utilizing the web. It is defined as “On-Demand Software “hosted by the cloud service provider. The users are allowed to subscribe to those cloud-based applications than purchasing. The users were given login credentials to use those applications which are running on cloud servers. One of the simple and easiest examples is Gmail.

Hardware

The hardware components of cloud computing include,

- Storage array
    - Switches
    - Router
    - Firewall
    - Backup devices
    - Servers
    - Load balancers

System Management

Cloud management consists of public, private, and hybrid clouds. Cloud computing performs the overall control and work of the system.

Public cloud: The public cloud is common to everyone and is easily accessible by anyone. It is provided over the internet to general people or major industry groups. Simple examples are Gmail and Google drive.

Private cloud: The difference between public and private is, that the latter ensures the privacy and security of the data through firewalls and internet hosting. If large IT organizations and business groups are looking for secure cloud options, the best option is the Private cloud. Examples of private clouds are Amazon Web Services, IBM, VMware, and Microsoft azure.

Multi-cloud: The name itself indicates partial meaning that the organization uses one or more cloud services such as public and private cloud or both public and private cloud. Examples of multi-cloud are Amazon Web Services (AWS), Google Cloud Platform (GCP), and IBM.

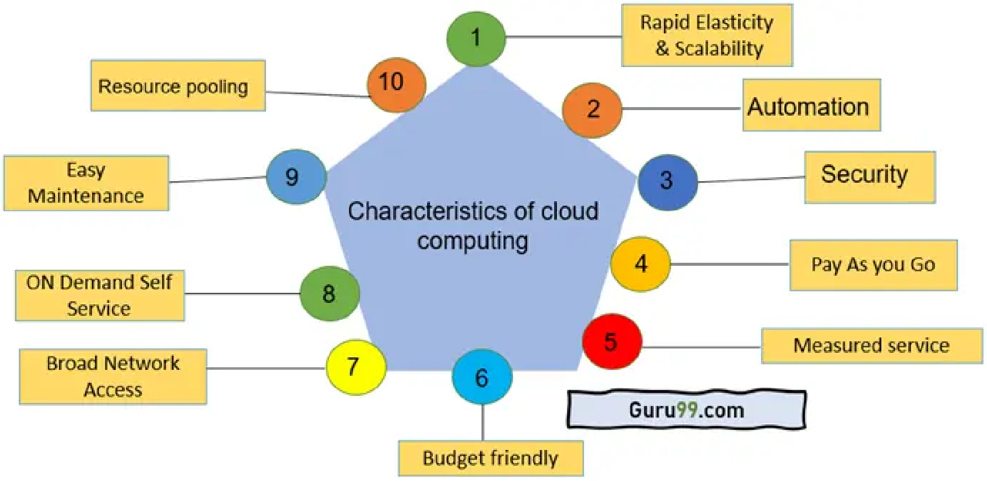
Hybrid cloud: The difference between multi and hybrid cloud is that the latter combines two or more different types of the cloud while multi-clouds combines different clouds of the same type. Examples include Azure Stack, Azure arc, and Google antos.

Distributed Computing

Distributed Computing is the connection of one or more several computers which are connected to form a network to share information. A wide number of computers are connected to a single network. Examples include the Internet and Gmail.

The Essential Characteristics of Cloud Computing are:

- On-demand self service
- Multi-tenancy and resource pooling
- Broad network access
- Rapid elasticity and scalability
- Resource pooling
- Measured and reporting service
- Automation
- Resilience
- Large Network Access
- Work from any location
- Comfortable payment structure
- Service Excellence
- Easy maintenance
- Flexibility
- Economical and Security



On-demand self-service

Cloud computing delivers on-demand service. It provides the feature of monitoring server uptime with computing capabilities to the end-users. Cloud computing provides pre-defined network storage that enables the end-users to monitor their computing capabilities. Cloud computing works on a self-service model.
They help end-users to make better decisions as they know how to use cloud computing services.

Multi-tenancy and resource pooling

One of the most important features of cloud technology is multi-tenancy. It can be defined as the software architecture that enables the single program instance to provide services to multiple end-users. This feature enables the usage of the same computing resources by multiple customers.

Broad network access

Cloud computing is achieved through standard computing mechanisms, and this feature helps promote heterogeneous thick and thin client platforms.
Examples of such platforms comprise mobile phones, laptops, dedicated workstations, and tablets. The capabilities are delivered across multiple networks. Cloud computing, therefore, helps break barriers and boundaries as they function across multiple geographies.

Rapid elasticity and scalability

The cloud computing capabilities can be released elastically. It enables you to scale the cloud computing services inward and outward, and it helps to be commensurate with the dynamic demand posted by the end-users.

Resource pooling

Cloud computing delivers affordable resource pooling solutions. With resource pooling, organizations can reduce substantial computing costs, and it helps in the dynamic pooling of resources that enable them to deliver computing services to several consumers.

Measured and reporting service

Cloud systems offer the metering capability to monitor, control, and optimize the usage of cloud resources. This feature can be defined as a measured service.
The metering capability is placed at some level of the abstraction of applicable services. Therefore, this feature enables transparency for both the provider of service and the consumer.

Automation

Through automation, IT teams and developers maintain and modify cloud services. When cloud infrastructure is in place, it ensures minimum interaction from humans. All the configurations are installed to ensure the monitoring and maintenance of cloud computing services, and such configurations are mostly automated. Therefore, automation in cloud computing facilitates the faster expansion of cloud services.

Resilience

Cloud computing delivers continuous server uptime, and hence it offers resilient services. It offers the capability to recover from any service interruption. The cloud service provider also develops strategies that boost disaster management, achieved by maintaining backup cloud nodes.

Large Network Access

Cloud computing is so versatile that it enables its users to access cloud services. These fundamental characteristics of Cloud Computing also enable them to upload data to the cloud from anywhere. For this, you need to have a decent internet connection and a robust device that helps make a connection to the cloud.

Work from any location

Cloud computing promotes the feature of remote working. It helps the end-user function, work, or deliver remote services from any location. Users are therefore able to access company data even on their smartphones or through laptops. It also enables users to connect with one another quickly.

Comfortable payment structure

Cloud computing offers a flexible payment structure that plays an important role in the cost-cutting of organizations. Pricing varies based on the features and functionalities chosen by a customer.
The payment options provided by the cloud service providers to the end-users are very simple and streamlined, which aides them in saving on substantial costs and time.

Service Excellence

Cloud computing delivers end-users with a wide range of services. The cloud service providers share end users' service level agreements with their clients.
It also provides documentation on how they would achieve continuous availability and bandwidth of their clients' services.

Easy maintenance

Easy maintenance is one of the critical features of cloud computing. The client is never involved in maintenance-related services. Its managed by the cloud computing provider. The maintenance services are so well planned that the downtime remains significantly low. Moreover, the cloud undergoes regular updates that help in capability optimization.

Flexibility

The end-users benefit from the flexibility offered by the cloud services when they host data in the dedicated cloud. This ensures that the end-users can do away from traditional hosting techniques wherein they had to change or switch the service providers more frequently.

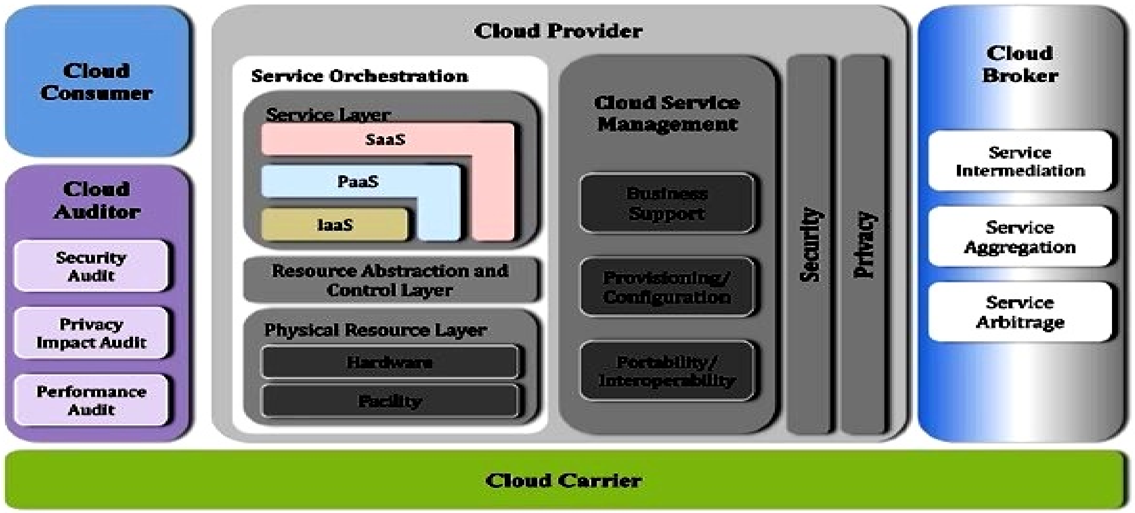
Economical and Security

This feature is one of the key aspects of cloud computing. It helps the big organizations to save a substantial amount on IT-related expenditure. You need to pay a small fee to the third-party providers to ensure that the cloud space is adequately administered and maintained. This also helps in boosting security in exchange for a nominal fee.

Availability

Cloud computing offers highly resilient services, and the cloud services are available for 24 x7 duration if the cloud resource faces downtime, the system recovers and starts within no time. While the cloud service makes a recovery, information stored in servers, networks, and databases remains to be secured. Since cloud services can be accessed from any geographical location, their services remain available most of the time.

Cloud Reference Architecture



These actors are listed below

- Cloud Consumer.
- Cloud Provider.
- Cloud Carrier.
- Cloud Auditor.
- Cloud Broker.

Each actor is an entity may be a person or an organization that participates in a transaction or process and/or performs tasks in cloud computing.

1. Cloud Consumer

- Cloud consumer is the main participants of cloud computing environment.
- A cloud consumer is a person or organization that use the cloud services such as SaaS, PaaS and IaaS.
- A cloud consumer browses the service catalog provided by a cloud provider, cloud consumer requests the appropriate service.
- Cloud provider sets up cloud environment for the service and make a contracts with the cloud consumer for the use of the service.
- Cloud consumers need cloud **Service Level Agreement(SLA**).

SLA act as a agreement for technical performance requirements provided by a cloud provider.

Some terms and conditions regarding the quality of service, security, remedies for performance failures are mentioned in the SLA.

Software as a service applications in the cloud are made accessible via a network to the SaaS consumers.

The consumers of SaaS may be a organizations that gives their employee with access to software applications, end users who directly use software applications, or it may be software application administrators who is responsible for configure applications on the software for the customers.

Platform as a service can also be employ by the consumer the tools to develop, test, deploy and manage the applications hosted in a cloud environment.

PaaS consumers can be application developers who design and implement application software in software company.

PaaS consumer may be application testers who run and test applications in cloud-based environments, application deployers who publish applications into the cloud,

PaaS may be a application administrators who configure and monitor application performance on a platform.

Cloud Consumers of Infrastructure as a service have access to different hardware resources like virtual computers, network devices such as router, storage media and other fundamental computing resource.

The consumers of Infrastructure as a service may be system developers, system administrators and IT managers who creates, install, manage and monitor the services for IT infrastructure operations.

Also Read – CPU Scheduling Criteria in OS

2. Cloud Provider

- A cloud provider is responsible for making a service available to the cloud consumer. Cloud provider may be a person , team or an organization.
- A Cloud Provider maintain and manages the different cloud computing services for the consumer and makes arrangement to deliver the cloud services to the Cloud Consumers suing network access or internet.

In context to **Software as a Service** Cloud provider is responsible for deploys, configuring, maintaining and updating the operation of the software applications on a cloud infrastructure so that the services are provisioned as per the required levels by the cloud consumers.

The major responsibilities of cloud provider in context to software as a service are to manage , control the applications and overall infrastructure.

In context to **Platform as a Service**, the Cloud Provider manages the computing infrastructure for the platform and runs the cloud software that provides the components of the platform. These components may be software execution stack, databases and some other components that act as middleware.

The PaaS Cloud Provider generally supports the development, deployment and management process of the Platform as a Service.

Some integrated tools like IDE, SDK, development version of cloud software, deployment and management are also the part of Platform as a Service.

Physical computing resources such as servers, networks, storage and hosting infrastructure are also maintain and manage by the cloud provider for the consumer of **Infrastructure as a Service**.

The Cloud Provider implement the cloud software so that computing resources become available to the Cloud Consumer who use the infrastructure as service through a set of service interface and virtual network interfaces that helps in resource abstraction.

3. Cloud Auditor

A cloud auditor is a dedicated team of technically skilled person that can perform an independent examination or review of cloud service controls with the intent to express strength and weakness of the process and some suggestion or improvement.

Audits are performed to verify the standards of services after checking the evidence.

Major role of a cloud auditor is to evaluate the services provided by a cloud provider against the parameters such as security controls, privacy impact and performance etc.

To perform the audit of security a cloud auditor do the assessment of the security controls in the information system to determine the extent to which the controls are implemented accurately and operating as per expectation and producing the desired outcome with respect to the security requirements for the system.

Also Read – Smart Home Technology in India

4. Cloud Broker

Some time services integrations becomes more complex due to which it becomes difficult for the cloud consumer to manage the cloud service.

In such situation cloud consumer request cloud services from cloud broker. Cloud Broker acts as mediator between consumer and provider.

- A cloud broker manages the delivery of cloud services , their performance and use.
- A cloud broker negotiates relationships between cloud providers and cloud consumers.

In general, a cloud broker involves in three types of activities which are as follow

Service Intermediation

A cloud broker may enhances a given service by improving some specific capability and providing value-added services to cloud consumers.

The improvement may be related to managing the access to cloud services, identity management, performance reporting, enhanced security, etc.

Service Aggregation

Services aggregation can be seems as combining and integrating multiple services into one or some more new services.

The broker ensures the data movement between the cloud consumer and multiple cloud providers in secure manner.

A cloud broker also provides the data integration.

Service Arbitrage

Service arbitrage is very similar to service aggregation but there is a little bit difference also.

In service arbitrage the services to be aggregated are not fixed in advance.

In Service arbitrage a broker has the flexibility to select the services from multiple agencies.

The cloud broker, for example, can use a credit-scoring service to measure and select an agency with the best score.

5. Cloud Carrier

Cloud Carrier is another important actors in NIST cloud computing reference architecture.

- Role of cloud carrier is to provide the connectivity and transport of cloud services between cloud consumers and cloud providers.
- Cloud carriers provide access to consumers through **network**, telecommunication and other access devices.

For example- cloud consumers can obtain cloud services through network access devices, such as computers, laptops, mobile phones, mobile Internet devices.

Models of Cloud Services

The cloud servicing model mainly falls into 5 categories – Software as a service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), Identity as a Service (IDaaS), and Network as a Service (NaaS). Let's talk about each service model in detail.

Software as a Service (SaaS)

SaaS is identified as a software distribution model or a web platform on the Internet that offers clients access to cloud computing based on a subscription. Thus, came to be known as 'On-Demand Software' or 'Pay-You-Go-App'. The software will be distributed regularly like a service, rather than buying the solution once, like purchasing a product. Through SaaS providers, the customers get licensed services. SaaS is one of the fast-growing services and thus will shift to the role of active cloud service technology mandatory for all organizations and companies. Therefore, it is essential for both the users and buyers to understand the use and compatibility of SaaS.

Platform as a Service (PaaS)

PaaS is defined as a cloud computing platform built for programmers to create, test, run and control applications. It is mainly designed in a way that makes building websites or mobile applications easier and simpler for developers with no worries about fixing or handling the infrastructure required for development including the servers, data storage, networking, and databases. In PaaS, billing is charged only for platforms used by users for the length of time the services have been used. Unlike desktop solutions, you do not have to pay for any excessive activity. PaaS bears a striking resemblance to SaaS, except that SaaS easily distributes software through the internet, without having to purchase or maintain web development. As opposed to this, PaaS offers a platform for developing software delivered through the web. The point-and-click feature in PaaS enables non-programmers/ non-professionals to create web applications.

Infrastructure as a service (IaaS)

IaaS, otherwise known as Hardware as a Service (HaaS), is a computing infrastructure controlled through the Internet. One of the key benefits of using IaaS is that it allows consumers to eliminate the expense and complications in buying and controlling the physical servers. IaaS offers many ready-to-use features like the exact environment for development, personal networks, safe storage of data, performance tracking, etc. for the IT infrastructure of businesses. Companies do not have to develop and safeguard their own IT infrastructure, instead, they use third-party servers and cloud backup storage to completely strengthen the development process. Changing the infrastructure of your company to an IaaS solution can contribute to minimizing maintenance of local data centers, reducing costs on hardware, and achieving real-time business insights. IaaS Solutions also provides you with the flexibility to increase or decrease the scope of your IT resources as required. They help you get new applications faster and improve the reliability of your infrastructure.

Identity as a Service (IDaaS)

IDaaS (Identity as a Service) enables employee or consumer identity details management as a digital entity. This reduces the complexity in remembering and managing different usernames and passwords or deactivating the account and credentials when an employee leaves the organization. The main objective of an identity service is to make sure that the consumers are what they affirm to be and to provide them with the proper access at the exact time to any software application, files, or other resources. If the basic facilities are made on-site for this to happen, then the company needs to find out what to do each time a problem arises. Deploying a centralized cloud-based system developed by identity experts who have dealt with such problems before and resolved them for hundreds of companies is very simple.

Network as a Service (NaaS)

NaaS (Network as a Service) is a cloud service model that enables clients to directly gain access to the network infrastructure and is based on pay as you use model. It also allows networking services to be taken on lease from a cloud vendor rather than fixing their own network infrastructure by the customer. This service utilizes virtualized network infrastructure and gives safe network services to employees and clients. NaaS service providers always attempt to maintain and handle network resources in a way that reduces the workload of clients/employees. NaaS facilitate consumers to run their own networks with no maintenance on their own networking infrastructure. Similar to cloud services, NaaS providers operate networking activities with software and internet connection, thus enabling companies to establish their own networks with no hardware.

Cloud Deployment Model:

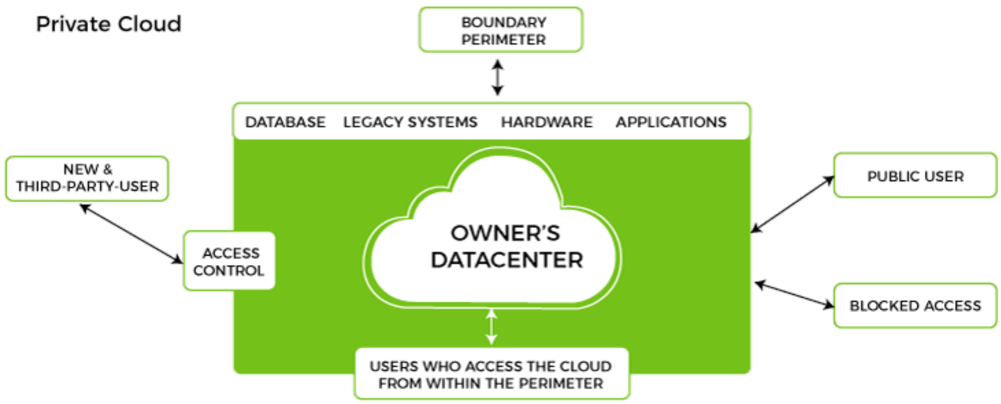
The cloud deployment model identifies the specific type of cloud environment based on ownership, scale, and access, as well as the cloud’s nature and purpose. The location of the servers you’re utilizing and who controls them are defined by a cloud deployment model. It specifies how your cloud infrastructure will look, what you can change, and whether you will be given services or will have to create everything yourself. Relationships between the the infrastructure and your users are also defined by cloud deployment types
Different types of cloud computing deployment models are:

- public
- private
- community
- hybrid

Private Cloud

Now that you understand what the public cloud could offer you, of course, you are keen to know what a private cloud can do. Companies that look for cost efficiency and greater control over data & resources will find the private cloud a more suitable choice.

It means that it will be integrated with your data center and managed by your IT team. Alternatively, you can also choose to host it externally. The private cloud offers bigger opportunities that help meet specific organizations' requirements when it comes to customization. It's also a wise choice for mission-critical processes that may have frequently changing requirements.



Benefits of Private Cloud

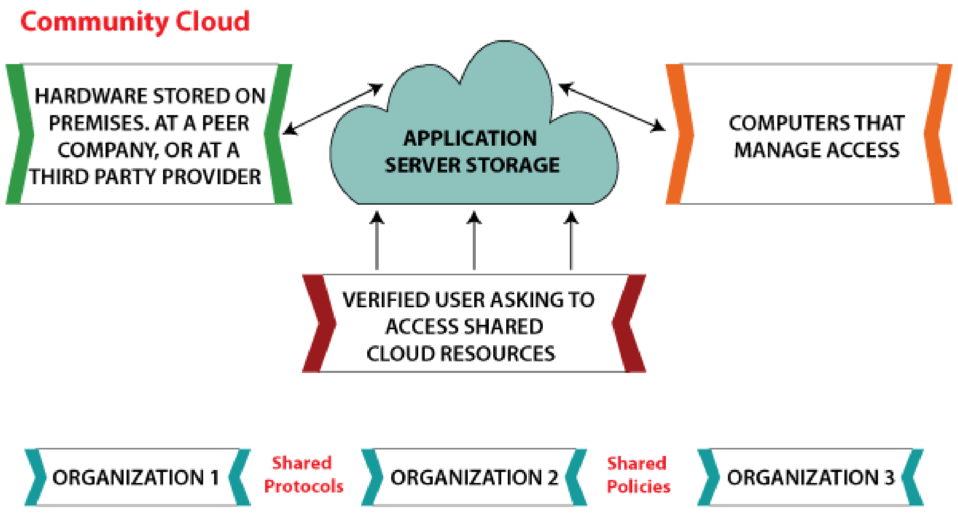
- Data Privacy - It is ideal for storing corporate data where only authorized personnel gets access
- Security - Segmentation of resources within the same Infrastructure can help with better access and higher levels of security.
- Supports Legacy Systems - This model supports legacy systems that cannot access the public cloud.

Limitations of Private Cloud

- Higher Cost - With the benefits you get, the investment will also be larger than the public cloud. Here, you will pay for software, hardware, and resources for staff and training.
- Fixed Scalability - The hardware you choose will accordingly help you scale in a certain direction
- High Maintenance - Since it is managed in-house, the maintenance costs also increase.

Community Cloud

The community cloud operates in a way that is similar to the public cloud. There's just one difference - it allows access to only a specific set of users who share common objectives and use cases. This type of deployment model of cloud computing is managed and hosted internally or by a third-party vendor. However, you can also choose a combination of all three.


Community Cloud
HARDWARE STORED ON PREMISES, AT A PEER COMPANY, OR AT A THIRD PARTY PROVIDER
APPLICATION SERVER STORAGE
COMPUTERS THAT MANAGE ACCESS
VERIFIED USER ASKING TO ACCESS SHARED CLOUD RESOURCES
ORGANIZATION 1
Shared Protocols
ORGANIZATION 2
Shared Policies
ORGANIZATION 3

Benefits of Community Cloud

- Smaller Investment - A community cloud is much cheaper than the private & public cloud and provides great performance
- Setup Benefits - The protocols and configuration of a community cloud must align with industry standards, allowing customers to work much more efficiently.

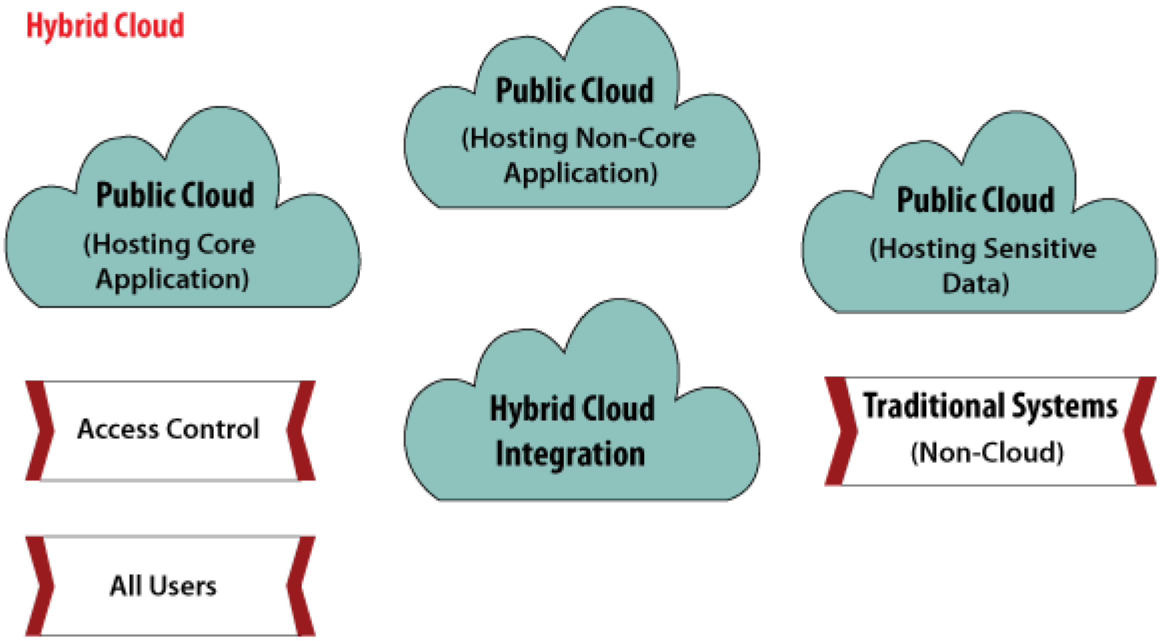
Limitations of Community Cloud

- Shared Resources - Due to restricted bandwidth and storage capacity, community resources often pose challenges.
- Not as Popular - Since this is a recently introduced model, it is not that popular or available across industries

Hybrid Cloud

As the name suggests, a hybrid cloud is a combination of two or more cloud architectures. While each model in the hybrid cloud functions differently, it is all part of the same architecture. Further, as part of this deployment of the cloud computing model, the internal or external providers can offer resources.

Let's understand the hybrid model better. A company with critical data will prefer storing on a private cloud, while less sensitive data can be stored on a public cloud. The hybrid cloud is also frequently used for 'cloud bursting'. It means, supposes an organization runs an application on-premises, but due to heavy load, it can burst into the public cloud.



Benefits of Hybrid Cloud

- Cost-Effectiveness - The overall cost of a hybrid solution decreases since it majorly uses the public cloud to store data.
- Security - Since data is properly segmented, the chances of data theft from attackers are significantly reduced.
- Flexibility - With higher levels of flexibility, businesses can create custom solutions that fit their exact requirements

Limitations of Hybrid Cloud

- Complexity - It is complex setting up a hybrid cloud since it needs to integrate two or more cloud architectures
- Specific Use Case - This model makes more sense for organizations that have multiple use cases or need to separate critical and sensitive data

UNIT-2

Cloud Computing Software Security Fundamentals

cloud security objectives: Assuring the confidentiality, integrity, and availability of information resources.

Confidentiality – ensuring privacy is a crucial data security objective. Confidentiality involves restricting data only to those who need access to it. Encryption and setting passwords are ways to ensure confidentiality security measures are met.
Integrity – making sure that the data in an organization's possession is accurate, reliable and secured against unauthorized changes, tampering, destruction or loss.
Availability – private information is available for anyone who is authorized to access it, such as when a customer requests to view his or her profile.

Cloud Security Services :

1. **Identity and Access Management** should provide controls for assured identities and access management. **Identity and access management** includes people, processes and systems that are used to manage access to enterprise resources by assuring the identity of an entity is verified and is granted the correct level of access based on this assured identity. Audit logs of activity such as successful and failed authentication and access attempts should be kept by the application/solution.
2. **Data Loss Prevention** is the monitoring, protecting and verifying the security of data at rest, in motion and in use in the cloud and on-premises. **Data loss prevention** services offer protection of data usually by running as some sort of client on desktops/servers and running rules around what can be done. Within the cloud, data loss prevention services could be offered as something that is provided as part of the build, such that all servers built for that client get the data loss prevention software installed with an agreed set of rules deployed.
3. **Web Security** is real-time protection offered either on-premise through software/appliance installation or via the cloud by proxying or redirecting web traffic to the cloud provider. This provides an added layer of protection on top of things like AV to prevent malware from entering the enterprise via activities such as web browsing. Policy rules around the types of web access and the times this is acceptable also can be enforced via these **web security** technologies.
4. **E-mail Security** should provide control over inbound and outbound e-mail, thereby protecting the organization from phishing and malicious attachments, enforcing corporate policies such as acceptable use and spam and providing business continuity options. The solution should allow for policy-based encryption of e-mails as well as integrating with various e-mail server offerings. Digital signatures enabling identification and non-repudiation are features of many cloud e-mail security solutions.
5. **Security Assessments** are third-party audits of cloud services or **assessments** of on-premises systems based on industry standards. Traditional security assessments for infrastructure and applications and compliance audits are well defined and supported by multiple standards such as NIST, ISO and CIS. A relatively mature toolset exists, and a number of tools have been implemented using the SaaS delivery model. In the SaaS delivery model, subscribers get the typical benefits of this cloud computing variant elasticity, negligible setup time, low administration overhead and pay-per-use with low initial investments.
6. **Intrusion Management** is the process of using pattern recognition to detect and react to statistically unusual events. This may include reconfiguring system components in real time to stop/prevent an intrusion. The methods of intrusion detection, prevention

and response in physical environments are mature; however, the growth of virtualization and massive multi-tenancy is creating new targets for intrusion and raises many questions about the implementation of the same protection in cloud environments.

7. **Security Information and Event Management** systems accept log and event information. This information is then correlated and analyzed to provide real-time reporting and alerting on incidents/events that may require intervention. The logs are likely to be kept in a manner that prevents tampering to enable their use as evidence in any investigations.
8. **Encryption** systems typically consist of algorithms that are computationally difficult or infeasible to break, along with the processes and procedures to manage **encryption** and decryption, hashing, digital signatures, certificate generation and renewal and key exchange.
9. **Business Continuity and Disaster Recovery** are the measures designed and implemented to ensure operational resiliency in the event of any service interruptions. **Business continuity and disaster recovery** provides flexible and reliable failover for required services in the event of any service interruptions, including those caused by natural or man-made disasters or disruptions. Cloud-centric business continuity and disaster recovery makes use of the cloud's flexibility to minimize cost and maximize benefits.
10. **Network Security** consists of security services that allocate access, distribute, monitor and protect the underlying resource services. Architecturally, **network security** provides services that address security controls at the network in aggregate or specifically addressed at the individual network of each underlying resource. In a cloud/virtual environment, network security is likely to be provided by virtual devices alongside traditional physical devices
11.

principles of a cloud security architecture

The architecture of a cloud security system should account for tools, policies and processes needed to safeguard cloud resources against security threats. Among its core principles, it should include:

1. **Security by design** – cloud architecture design should implement security controls that are not vulnerable to security misconfigurations. For example, if a cloud storage container holds sensitive data, external access should be locked, and there should be no way for an administrator to open access to the public Internet.
2. **Visibility** – many organizations use multi-cloud and hybrid-cloud deployments that traditional security solutions fail to protect. An effective

strategy accounts for both the tools and the processes to maintain visibility throughout an organization’s complete cloud-based infrastructure.

3. **Unified management** – security teams are often overworked and understaffed, and so cloud security solutions must provide unified management interfaces. Teams must be able to centrally manage a wide range of cloud security solutions from one pane of glass.
4. **Network security** – the cloud uses a shared responsibility model, and the organization is responsible for securing traffic flows to and from cloud resources, and between the public cloud and on-premise networks. Segmenting networks is also important to limit an attacker’s ability to move laterally once they have gained access to a network.
5. **Agility** – the cloud fosters development and deployment of new solutions. Security should not inhibit this agility. Organizations can use cloud-native security solutions that integrate seamlessly into the agile development lifecycle.
6. **Automation** – automation is critical to swift provisioning and updating of security controls in a cloud environment. It can also help identify and remediate misconfigurations and other security gaps in real time.
7. **Compliance** – regulations and standards like GDPR, CCPA, and PCI/DSS protect both data and processes in the cloud. Organizations can leverage cloud provider solutions, but will often need third party solutions to manage compliance across multiple cloud providers.

SECURITY CONCERNS:

1. **Network Availability** The value of cloud computing can only be realized when your network connectivity and bandwidth meet your minimum needs: The cloud must be available whenever you need it. If it is not, then the consequences are no different than a denial-of-service situation
2. **Cloud Provider Viability** Since cloud providers are relatively new to the business, there are questions about provider viability and commitment. This concern deepens when a provider requires tenants to use proprietary interfaces, thus leading to tenant lock-in.
3. **Disaster Recovery and Business Continuity** Tenants and users require confidence that their operations and services will continue if the cloud provider’s production environment is subject to a disaster.
4. **Security Incidents** Tenants and users need to be appropriately informed by the provider when an incident occurs. Tenants or users may require provider support to respond to audit or assessment findings. Also, a provider may not offer sufficient support to tenants or users for resolving investigations.
5. **Transparency** When a cloud provider does not expose details of their internal policy or technology implementation, tenants or users must trust the cloud provider’s security claims. Even so, tenants and users require some transparency by providers as to provider cloud security, privacy, and how incidents are managed.

6. **New Risks, New Vulnerabilities** There is some concern that cloud computing brings new classes of risks and vulnerabilities. Although we can postulate various hypothetical new risks, actual exploits will largely be a function of a provider's implementation. Although all software, hardware, and networking equipment are subject to unearthing of new vulnerabilities, by applying layered security and well-conceived operational processes, a cloud may be protected from common types of attack even if some of its components are inherently vulnerable.
7. **Loss of Physical Control** Since tenants and users lose physical control over their data and applications, this results in a range of concerns:
   * Privacy and Data With public or community clouds, data may not remain in the same system, raising multiple legal concerns. •

   * Control over Data User or organization data may be comingled in various ways with data belonging to others.

   * A tenant administrator has limited control scope and accountability within a Public infrastructure-as-a-service (IaaS) implementation, and even less with a platform-as-a-service (PaaS) one. Tenants need confidence that the provider will offer appropriate control, while recognizing that tenants will simply need to adapt their expectations for how much control is reasonable within these models.

How Do You Calculate Risk Tolerance?

Knowing an organization's risk tolerance aids in planning its risk management plan, and influences how resources are invested. For example, if an organization's risk tolerance is low, it will invest more heavily in information security controls to protect sensitive and confidential data.

Factors Influencing Risk Tolerance

Several factors have inevitable repercussions on the risk tolerance of the companies, and these vary according to the business objectives of each.

Establish a Timeline

Each investor should make investment choices based on their time horizon. Over the long term, the market trends up. However, there is a higher risk of volatility in the short term. For example, an individual who intends to withdraw their money in 15 years can take more risk than someone who needs cash in five years.

Likewise, an organization may be in an economic or financial situation where it is more focused on liquidity. In this case, the company's risk tolerance will be low, and the investment strategy will be more conservative.

Dimensions of Your Portfolio

The greater the portfolio’s size and diversity, the more risk-tolerant it is. A $50 million portfolio allows an investor to assume greater risk, and therefore to consider more diverse opportunities, than a $5 million portfolio. Compared to a smaller portfolio, the percentage loss in a more extensive portfolio is substantially less.

Objectives

Individuals have different financial goals and investment objectives. For many people, financial planning isn’t only about accumulating as much money as possible. Some investment decisions relate to the types of businesses an investor wants to support and less about expected returns. As a result, each person’s risk tolerance will vary depending on their personal interests and goals.

An organization with a digital transformation and cybersecurity strategy may invest heavily in new technology and will not experience high investment returns in the short term. Then again, these investment decisions aren’t meant to generate an immediate return; instead, they are driven by business objectives, long-term operational efficiencies, and avoidance of security risks.

Level of Investor Confidence

Each investor approaches risk uniquely. Some investors are naturally more willing to take risks than others. On the other hand, market volatility can be exceedingly distressing for risk-averse investors. As a result, risk tolerance is closely tied to an investor’s comfort level when taking risks.

Age

On average, young individuals should be able to take greater risks than older folks. This is because young individuals have the ability to make more money while simultaneously having more time to deal with market volatility.

Types of Risk Tolerance

Different types of risk tolerance help financial advisers, investors, and organizations determine the types of investments that are suitable for their financial situation and comfort level. These are divided into three categories: aggressive, moderate, and conservative.

Aggressive

Investors who take aggressive risks are (hopefully) well-versed in the market and are willing to take substantial chances in the pursuit of large rewards. In addition, such investors are accustomed to experiencing significant portfolio volatility. Typically, aggressive investors are wealthy, experienced, and have a diverse portfolio.

They choose asset types such as stocks with dynamic price movement. Because of the amount of risk they take, they benefit from higher returns when the market is performing well. Likewise, they may suffer significant losses when the market is underperforming. They do not panic-sell during market downturns since they are accustomed to daily market volatility.

Moderate

Moderate risk investors are less risk-tolerant than aggressive risk investors. They take some risk and often specify a maximum loss percentage. They invest in a variety of asset classes, both risky and safe. When the market is doing well, they earn less than aggressive investors but do not lose as much when it is down.

Conservative

Conservative investors take the least amount of risk in the market. They avoid hazardous assets in favor of ones they believe are the safest. They place a higher value on liquidity and preventing losses than on gaining profits. As a result, they typically invest in asset types with less volatility such as government bonds, where their capital is secured.

Legal and Regulatory Issues:

Cloud computing is here to stay, all thanks to its several benefits. When connected to the right cloud infrastructure, you can save costs and enjoy broad network access and rapid elasticity.

While it is easy to be clouded by the benefits of cloud computing, you must also consider some legal issues. Doing so would ensure that you make an informed decision, especially in your choice of Cloud Service Provider (CSP). Plus, you can adequately protect yourself from the adverse effects of these legal issues in cloud computing. Today, I’ll be discussing some of the issues you need to look out for.

Data Protection

Data protection is one of the most critical legal issues you must consider when using the cloud for your operations. It is especially important if your business includes handling the personal data of individuals in any form. There are data protection regulations with strict provisions on how you handle the personal data of individuals.

Under most of these regulations, including the General Data Protection Regulation, which deals with handling data of EU citizens, you can't just export citizens' personal data to the cloud without obtaining the necessary consent. You must also comply with the data protection standards as stipulated by these regulations. Failure to do so would attract strict sanctions.

You need to understand what the law says about data protection in your jurisdictions.

Data Privacy and Security

Another essential legal issue in cloud computing that you should pay attention to is data privacy and security. If a third party receives unauthorized access to private information about your clients, it can damageyour company's reputation. Your business risks losing sensitive and corporate confidential information in the case of a security breach. You may also have to compensate your customer for violating their data privacy, which would cost your business a lot.

Make sure you engage a CSP that would offer you the highest privacy and security standard possible. You should also ensure that there are necessary firewalls to prevent a security breach.

Data Ownership (Intellectual Property Rights)

It is safe to assume that you own all the rights to data sent to the cloud by your company. However, it is advisable that your Service Level Agreement (SLA) with the CSP expressly indicates that your company has full rights to the data stored in the cloud and can retrieve it whenever you want. It is also essential to have these provisions in place, especially concerning data generated inside the cloud. The CSP may want to claim newly generated data because it was generated in the cloud through a data analytics solution.

Let the SLA provide that data generated in and out of the cloud by your company belongs to your company.

Jurisdiction Issues

The issue of differences in laws applicable across different jurisdictions is one of the legal issues in cloud computing. For instance, the government can require CSPs to disclose client data in some jurisdictions. However, in some other jurisdictions, there is express protection for data stored in the cloud, and in those jurisdictions, governments cannot access it without following due process.

You may want your SLA to contain express provisions that the CSP can only hold your data in specific jurisdictions.