Cloud Security (22MCR16)

Module - 1

Cloud Computing Architectural Framework: Cloud Benefits, Business scenarios, Cloud Computing Evolution, cloud vocabulary, Essential Characteristics of Cloud Computing, Cloud deployment models, Cloud Service Models, Multi- Tenancy, Approaches to create a barrier between the Tenants, cloud computing vendors, Cloud Computing threats, Cloud Reference Model, The Cloud Cube Model, Security for Cloud Computing, How Security Gets Integrated.

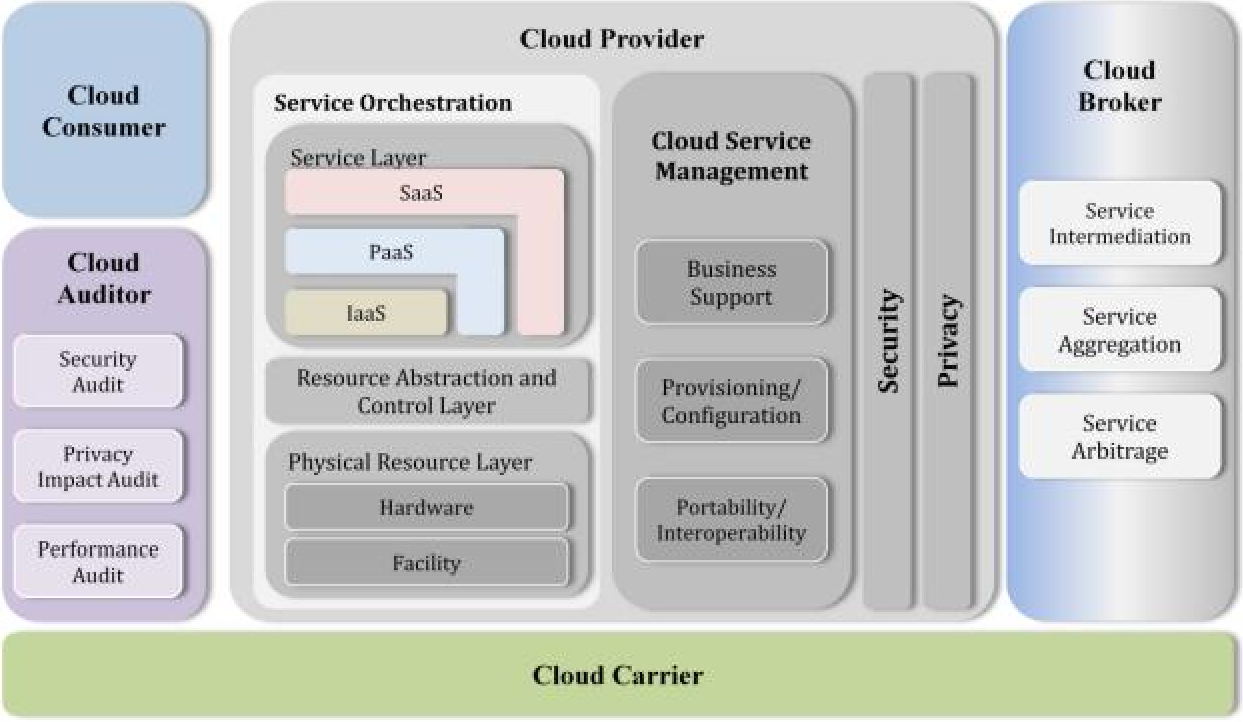
Questions

1. Define Cloud. Explain Cloud computing reference model.

The term cloud refers to a network or the internet. It is a technology that uses remote servers on the internet to store, manage, and access data online rather than local drives. The data can be anything such as files, images, documents, audio, video, and more.

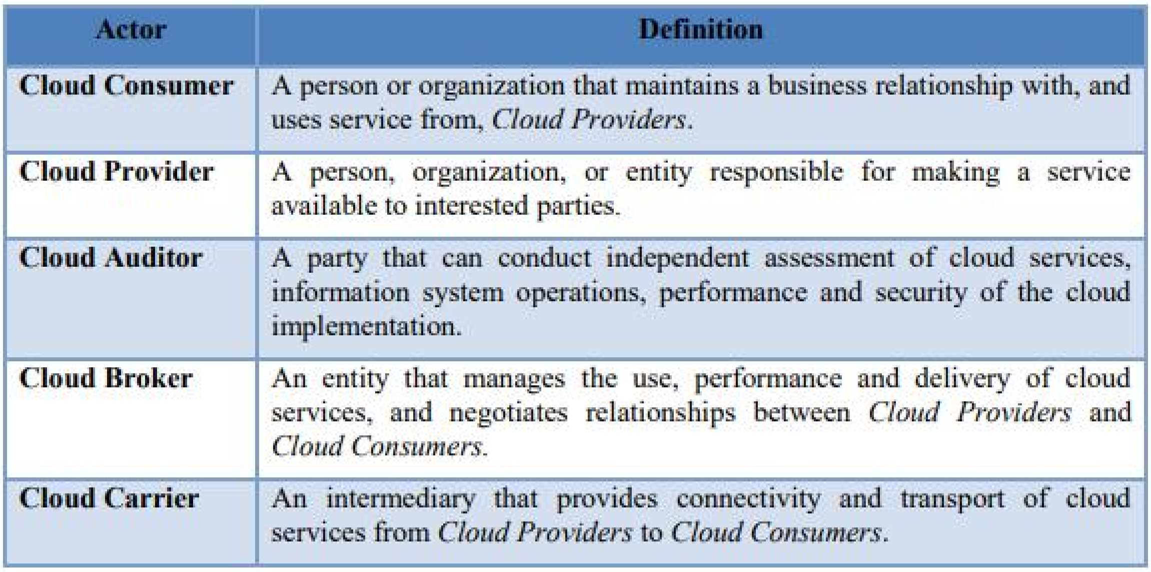
Cloud Reference Model

- Figure presents an overview of the NIST cloud computing reference architecture, which identifies the major actors, their activities and functions in cloud computing.
- The diagram depicts a generic high-level architecture and is intended to facilitate the understanding of the requirements, uses, characteristics and standards of cloud computing.



- As shown in Figure 1, the NIST cloud computing reference architecture defines five major actors: cloud consumer, cloud provider, cloud carrier, cloud auditor and cloud broker.

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



Actor	Definition
Cloud Consumer	A person or organization that maintains a business relationship with, and uses service from, *Cloud Providers*.
Cloud Provider	A person, organization, or entity responsible for making a service available to interested parties.
Cloud Auditor	A party that can conduct independent assessment of cloud services, information system operations, performance and security of the cloud implementation.
Cloud Broker	An entity that manages the use, performance and delivery of cloud services, and negotiates relationships between *Cloud Providers* and *Cloud Consumers*.
Cloud Carrier	An intermediary that provides connectivity and transport of cloud services from *Cloud Providers* to *Cloud Consumers*.

2. Explain characteristics and benefits of Cloud Computing.

Characteristics of cloud computing.

1) Multi-tenancy (multi sharing).
2) Massive Scalability.
3) Elasticity.
4) Pay as you go.
5) Self-Provisioning of services.

1. Multi tenancy (shared resources)

Unlike previous computing models, which assumed dedicated resources (i.e., computing facilities dedicated to a single user or owner), cloud computing is based on a business model in which resources are shared (i.e., multiple users use the same resource) at the network level, host level, and application level.

2. Massive scalability

Although organizations might have hundreds or thousands of systems, cloud computing provides the ability to scale to tens of thousands of systems, as well as the ability to massively scale bandwidth and storage space.

3. Elasticity

Users can rapidly increase and decrease their computing resources as needed, as well as release resources for other uses when they are no longer required.

4. Pay as you go

Users pay for only the resources they actually use and for only the time they require them.

5. Self-provisioning of resources

Users self-provision resources, such as additional systems (processing capability, software, storage) and network resources.

<u>Benefits of Cloud Computing</u>

Small Initial Investment and Low Ongoing Costs

- Public cloud computing can avoid capital expenditures because no hardware, software, or network devices need to be purchased.
- Cloud usage is billed on actual use only, and is therefore treated more as an expense. In turn, usage-based billing lowers the barrier to entry because the upfront costs are minimal.
- Depending on the contract being signed, most companies can terminate the contract as preferred; therefore, in times of hardship or escalating costs, cloud computing costs can be managed very efficiently.

Economies of Scale

- Most development projects have a sizing phase during which one attempts to calculate the storage, processing power, and memory requirements during development, testing, and production.
- It is often difficult to make accurate estimates; under- or overestimating these calculations is typical.
- The lead time for acquiring the equipment to support these estimates can sometimes be lengthy, thus adding to the time necessary to complete the project.
- With the flexibility that cloud computing solutions offer, companies can acquire computing and development services as needed and on demand, which means development projects are less at risk of missing deadlines and dealing with the unknown.

Open Standards

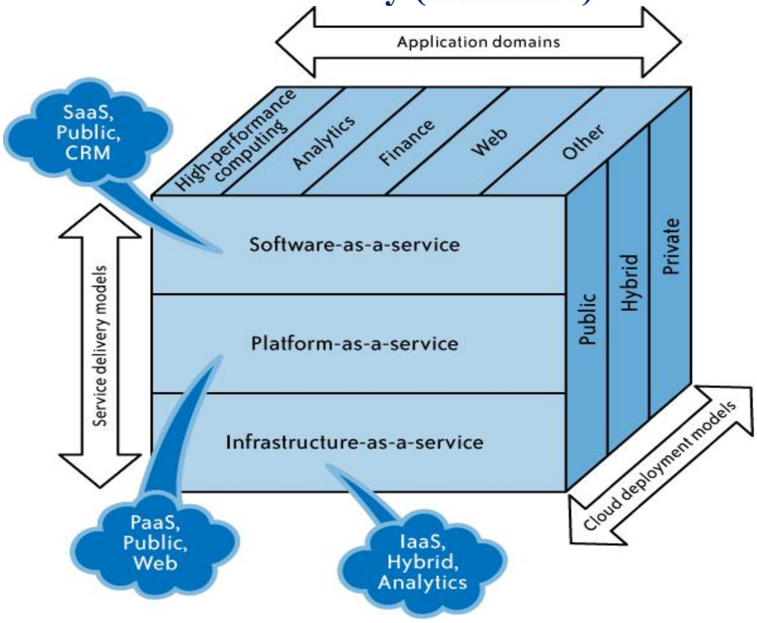
- Some capabilities in cloud computing are based on open standards for building a modular architecture that can grow rapidly and can change when required.
- Open source software is defined as computer software that is governed by a software license in the public domain, or that meets the definition of open source, which allows users to use, change, and improve the software.
- The flexibility to alter the source code is essential to allow for continued growth in the cloud solution.
- Open source software is the foundation of the cloud solution and is critical to its continued growth.

Sustainability

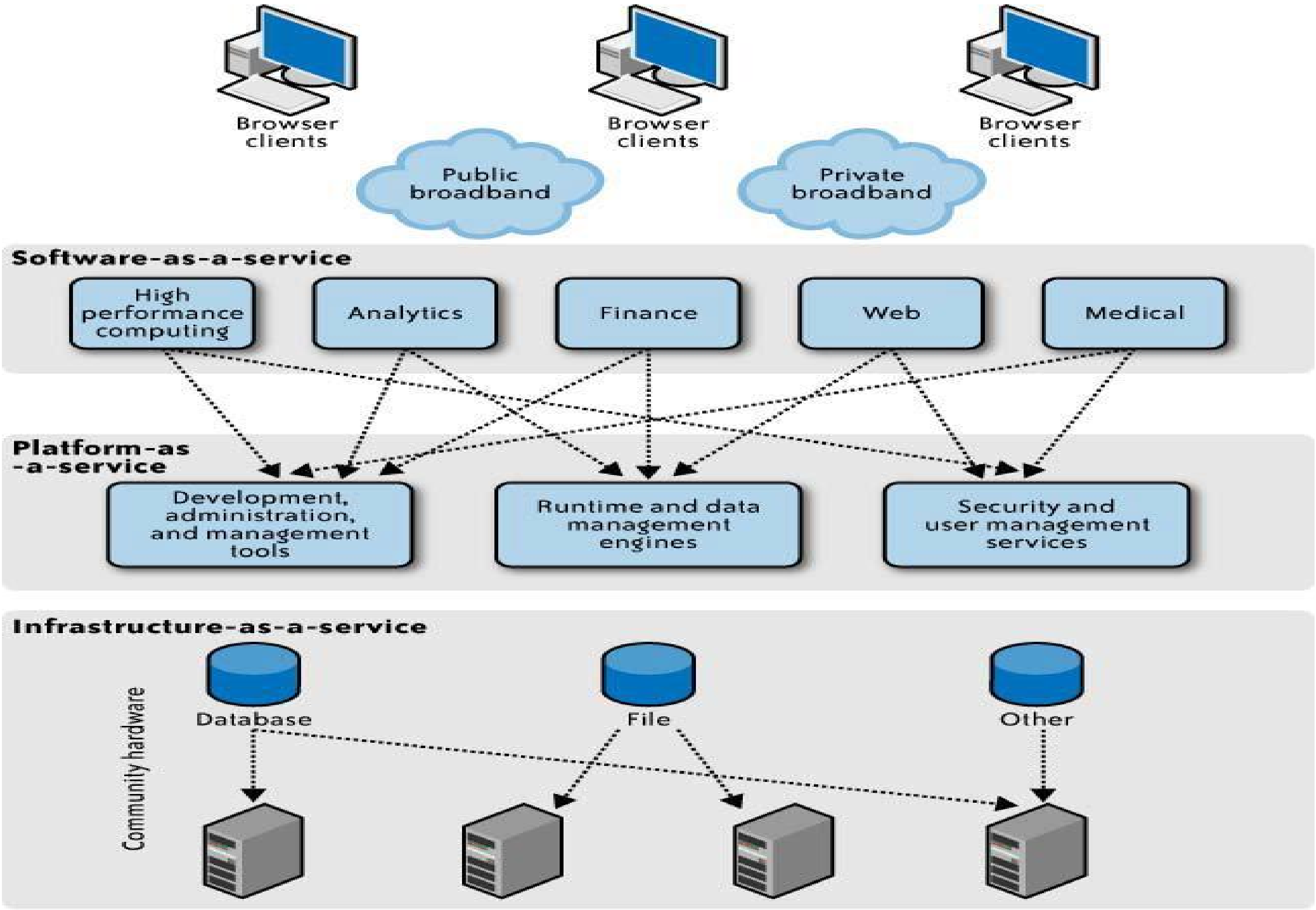
- Traditionally, companies have periodically struggled to maintain IT services due either to single points of failure in the network or to an inability to keep pace with business changes in both volume and the nature of transactions.
- Cloud computing allows companies to rely on the CSP to have limited points of failure, better resilience via clustering, and the ability to invest in state-of-the-art resilience solutions.

3. With neat diagram, explain the cloud computing architecture.

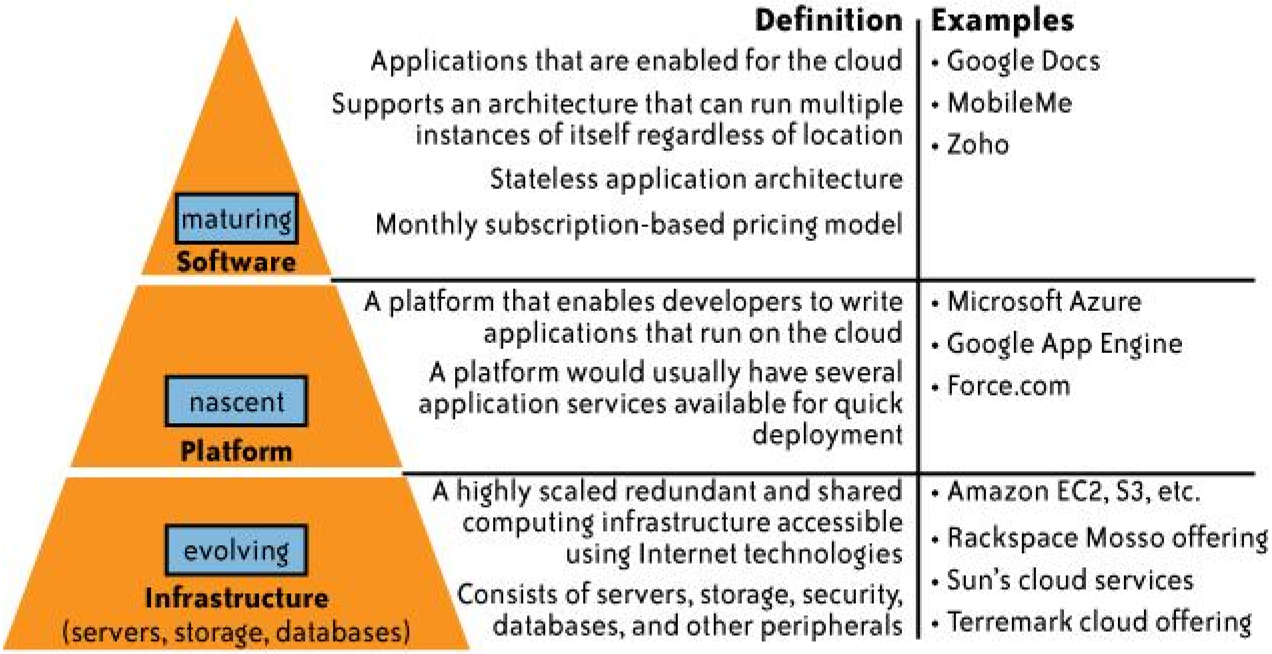
- A commonly agreed upon framework for describing cloud computing services goes by the acronym “SPI.” This acronym stands for the three major services provided through the cloud: software-as-a service (SaaS), platform-as-a-service (PaaS), and infrastructure-as-a-service (IaaS).
- Figure illustrates the relationship between services, uses, and types of clouds.



- Cloud computing isn’t so much a technology as it is the combination of many pre existing technologies.
- These technologies have matured at different rates and in different contexts, and were not designed as a coherent whole; however, they have come together to create a technical ecosystem for cloud computing.



4. Explain different types of clouds. OR Explain Cloud service models.



	Definition	Examples
maturing Software	Applications that are enabled for the cloud Supports an architecture that can run multiple instances of itself regardless of location Stateless application architecture Monthly subscription-based pricing model	• Google Docs • MobileMe • Zoho
nascent Platform	A platform that enables developers to write applications that run on the cloud A platform would usually have several application services available for quick deployment	• Microsoft Azure • Google App Engine • Force.com
evolving Infrastructure (servers, storage, databases)	A highly scaled redundant and shared computing infrastructure accessible using Internet technologies Consists of servers, storage, security, databases, and other peripherals	• Amazon EC2, S3, etc. • Rackspace Mosso offering • Sun's cloud services • Terremark cloud offering

While cloud-based software services are maturing, cloud platform and infrastructure offerings are still in their early stages

1) Software-as-a-service(SaaS).
2) Platform-as-a-service(PaaS).
3) Infrastructure-as-a-service(IaaS).

Software-as-a-service(SaaS)

- In a SaaS model, the customer does not purchase software, but rather rents it for use on a subscription or pay-per-use model (an operational expense, known as *OpEx*).
- In some cases, the service is free for limited use. Typically, the purchased service is complete from a hardware, software, and support perspective. The user accesses the service through any authorized device

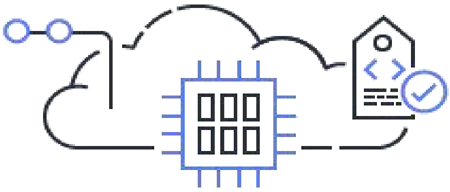
Key benefits of a SaaS model include the following:

- SaaS enables the organization to outsource the hosting and management of applications to a third party (software vendor and service provider) as a means of reducing the cost of application software licensing, servers, and other infrastructure and personnel required to host the application internally.
- SaaS enables software vendors to control and limit use, prohibits copying and distribution, and facilitates the control of all derivative versions of their software. SaaS centralized control often

allows the vendor or supplier to establish an ongoing revenue stream with multiple businesses and users without reloading software in each device in an organization.

- Applications delivery using the SaaS model typically uses the one-to-many delivery approach, with the Web as the infrastructure. An end user can access a SaaS application via a web browser; some SaaS vendors provide their own interface that is designed to support features that are unique to their applications.
- A typical SaaS deployment does not require any hardware and can run over the existing Internet access infrastructure. Sometimes changes to firewall rules and settings may be required to allow the SaaS application to run smoothly.
- Management of a SaaS application is supported by the vendor from the end user perspective, whereby a SaaS application can be configured using an API, but SaaS applications cannot be completely customized.

The Platform-As-a-Service Model



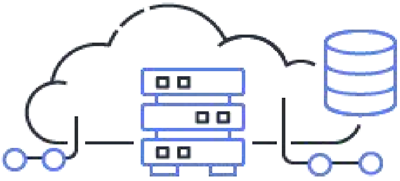
- In a platform-as-a-service (PaaS) model, the vendor offers a development environment to application developers, who develop applications and offer those services through the provider's platform.
- PaaS is a variation of SaaS whereby the development environment is offered as a service. The developers use the building blocks (e.g., predefined blocks of code) of the vendor's development environment to create their own applications.
- PaaS solutions are development platforms for which the development tool itself is hosted in the cloud and accessed through a browser. With PaaS, developers can often build web applications without installing any tools on their computer, and can then deploy those applications without any specialized system administration skills.
- PaaS is a variation of SaaS whereby the development environment is offered as a service.
- The developers use the building blocks (e.g., predefined blocks of code) of the vendor's development environment to create their own applications.
- PaaS solutions are development platforms for which the development tool itself is hosted in the cloud and accessed through a browser.
- With PaaS, developers can often build web applications without installing any tools on their computer, and can then deploy those applications without any specialized system administration skills.

At a minimum, a PaaS solution should include the following elements:

- A PaaS development studio solution should be browser-based.
- An end-to-end PaaS solution should provide a high-productivity integrated development environment (IDE) running on the actual target delivery platform so that debugging and test scenarios run in the same environment as production deployment.
- A PaaS solution should provide integration with external web services and databases.
- A PaaS solution must provide comprehensive monitoring of application and user activity, to help developers understand their applications and effect improvements.

- Scalability, reliability, and security should be built into a PaaS solution without requiring additional development, configuration, or other costs. Multi tenancy (the ability for an application to automatically partition state and data to service an arbitrary number of users) must be assumed without additional work of any sort.
- A PaaS solution must support both formal and on-demand collaboration throughout the entire
- software life cycle (development, testing, documentation, and operations), while maintaining the security of source code and associated intellectual property. A PaaS solution should support pay-as-you-go metered billing.

The Infrastructure-As-a-Service Model



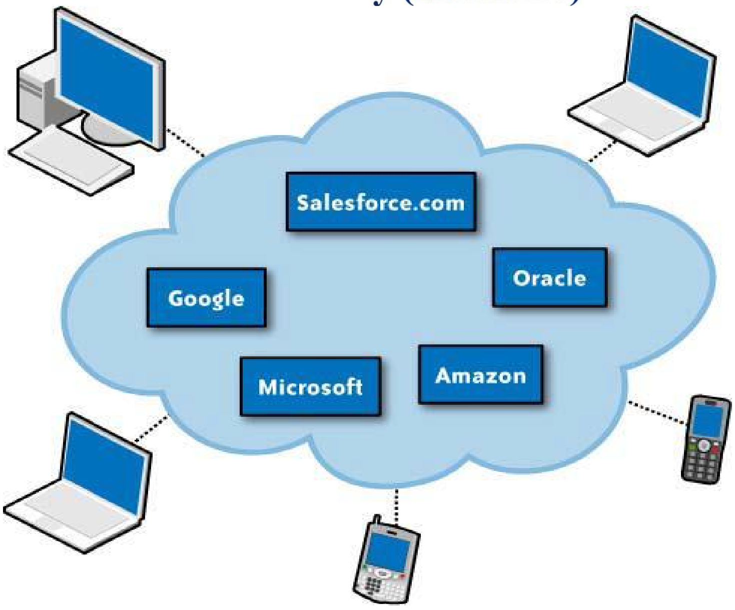
- The IaaS model is similar to utility computing, in which the basic idea is to offer computing services in the same way as utilities.
- That is, you pay for the amount of processing power, disk space, and so on that you actually consume.
- IaaS is typically a service associated with cloud computing and refers to online services that abstract the user from the details of infrastructure, including physical computing resources, location, data partitioning, scaling, security, backup, and so on.
- In cloud computing, the provider is in complete control of the infrastructure. Utility computing users, conversely, seek a service that allows them to deploy, manage, and scale online services using the provider’s resources and pay for resources the customer consumes.
- However, the customer wants to be in control of the geographic location of the infrastructure and what runs on each server.

5. Explain clouds deployment model.

Cloud Deployment Models

Public Clouds :

- Public clouds (or external clouds) describe cloud computing in the traditional mainstream sense, whereby resources are dynamically provisioned on a fine-grained, self-service basis over the Internet, via web applications or web services, from an off¬ site, third-party provider who shares resources and bills on a fine-grained, utility¬ computing basis.
- A public cloud is hosted, operated, and managed by a third-party vendor from one or more data centers. The service is offered to multiple customers (the cloud is offered to multiple tenants) over a common infrastructure; see Figure.
- In a public cloud, security management and day-to-day operations are relegated to the third party vendor, who is responsible for the public cloud service offering.
- Hence, the customer of the public cloud service offering has a low degree of control and oversight of the physical and logical security aspects of a private cloud.



Private Clouds :

- Private clouds and internal clouds are terms used to describe offerings that emulate cloud computing on private networks.
- These (typically virtualization automation) products claim to deliver some benefits of cloud computing without the pitfalls, capitalizing on data security, corporate governance, and reliability concerns.
- Organizations must buy, build, and manage them and, as such, do not benefit from lower upfront capital costs and less hands-on management.
- The organizational customer for a private cloud is responsible for the operation of his private cloud.
- Private clouds differ from public clouds in that the network, computing, and storage infrastructure associated with private clouds is dedicated to a single organization and is not shared with any other organizations (i.e., the cloud is dedicated to a single organizational tenant). As such, a variety of private cloud patterns have emerged:

Dedicated

Private clouds hosted within a customer-owned data center or at a collocation facility, and operated by internal IT departments

Community

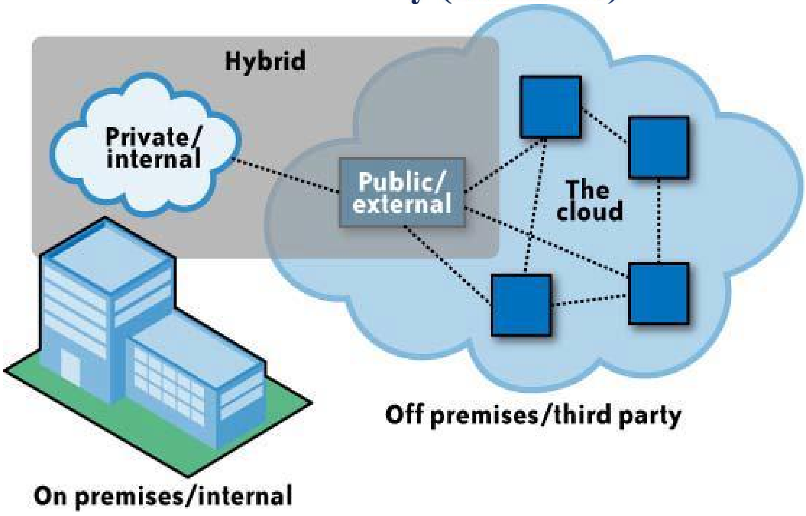
Private clouds located at the premises of a third party; owned, managed, and operated by a vendor who is bound by custom SLAs and contractual clauses with security and compliance requirements

Managed

Private cloud infrastructure owned by a customer and managed by a vendor

Hybrid Clouds :

- A hybrid cloud environment consisting of multiple internal and/or external providers is apossible deployment for organizations. With a hybrid cloud, organizations might run non-coreapplications in a public cloud, while maintaining core applications and sensitive data in-housein a private cloud (see Figure).



6. Explain Cloud Computing Threats.

Cloud Computing Threats

Security

- Because cloud computing represents a new computing model, there is a great deal of uncertainty about how security at all levels (e.g., network, host, application, and data levels) can be achieved.
- That uncertainty has consistently led information executives to state that security is their number one concern with cloud computing.

Privacy

- The ability of cloud computing to adequately address privacy regulations has been called into question.
- Organizations today face numerous different requirements attempting to protect the privacy of individuals' information, and it is not clear (i.e., not yet established) whether the cloud computing model provides adequate protection of such information, or whether organizations will be found in violation of regulations because of this new model.

Connectivity and Open Access

- The full potential of cloud computing depends on the availability of high-speed access to all. Such connectivity, rather like electricity availability, globally opens the possibility for industry and a new range of consumer products.
- Connectivity and open access to computing power and information availability through the cloud promotes another era of industrialization and the need for more sophisticated consumer products.

Reliability

- Enterprise applications are now so critical that they must be reliable and available to support 24/7 operations. In the event of failure or outages, contingency plans must take effect smoothly, and for disastrous or catastrophic failure, recovery plans must begin with minimum disruption.
- Additional costs may be associated with the required levels of reliability; however, the business can do only so much to mitigate risks and the cost of a failure. Establishing a track record of reliability will be a prerequisite for widespread adoption.

Interoperability

- The interoperability and portability of information between private clouds and public clouds are critical enablers for broad adoption of cloud computing by the enterprise.
- Many companies have made considerable progress toward standardizing their processes, data, and systems through implementation of ERPs.
- This process has been enabled by scalable infrastructures to create single instances, or highly integrated connections between instances, to manage the consistency of master and transaction data and produce reliable consolidated information.
- Even with these improved platforms, the speed at which businesses change may still outpace the ability of IT organizations to respond to these changes.
- SaaS applications delivered through the cloud provide a low-capital, fast-deployment option. Depending on the application, it is critical to integrate with traditional applications that may be resident in a separate cloud or on traditional technology.
- The standard for interoperability is either an enabler or a barrier to interoperability, and permits maintenance of the integrity and consistency of a company’s information and processes.

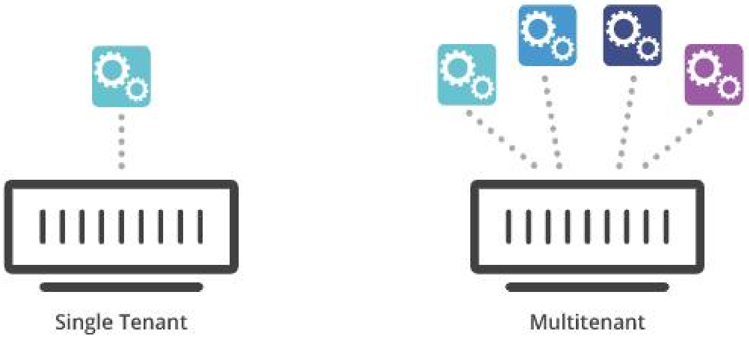
Economic Value

- The growth of cloud computing is predicated on the return on investment that accrues. It seems intuitive that by sharing resources to smooth out peaks, paying only for what is used, and cutting upfront capital investment in deploying IT solutions, the economic value will be there.
- There will be a need to carefully balance all costs and benefits associated with cloud computing—in both the short and long terms. Hidden costs could include support, disaster recovery, application modification, and data loss insurance.

7. Explain Multi-tenancy in cloud Computing.

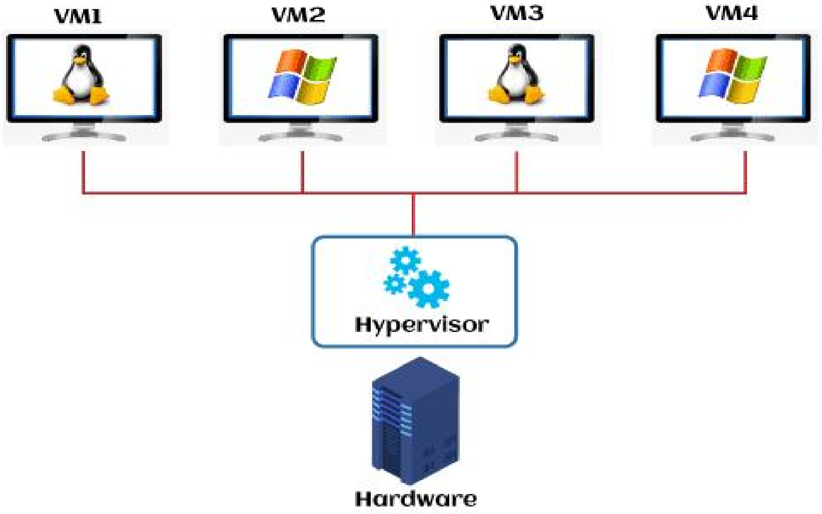
Multi-tenancy in cloud computing

- In cloud computing, multi tenancy means that multiple customers of a cloud vendor are using the same computing resources.
- Despite the fact that they share resources, cloud customers aren't aware of each other, and their data is kept totally separate.
- Multi tenancy is a crucial component of cloud computing; without it, cloud services would be far less practical.
- Multi-tenant architecture is a feature in many types of public cloud computing, including IaaS, PaaS, SaaS, containers, and server less computing.



Two Approaches on Multi-Tenancy in the Cloud

1) Hypervisor level Isolation



- Hypervisor is a very low-level layer of software that maps the physical machine to a virtualized machine on which a regular OS runs on.
- When the regular OS issue system calls to the VM, it is intercepted by the Hypervisor which maps to the underlying hardware.
- The hypervisor also provides some traditional OS functions such as process scheduling to determine which VM to run. Hypervisor can be considered to be a very lean OS that sits very close to the bare hardware.
- Since Hypervisor focus on low-level system level primitives, it provides the cleanest separation and hence lessen security concerns.
- On the other hand, by intercepting at the lowest layer, Hypervisor retain the familiar machine model that existing system/network admin are familiar with.
- Since Application is now completely agnostic to the presence of Hypervisor, this minimize the change required to move existing apps into the cloud and makes cloud adoption easier.
- Of course, the downside is that virtualization introduce a certain % of overhead. And the tenant still need to pay for the smallest VM even none of its user is using it.

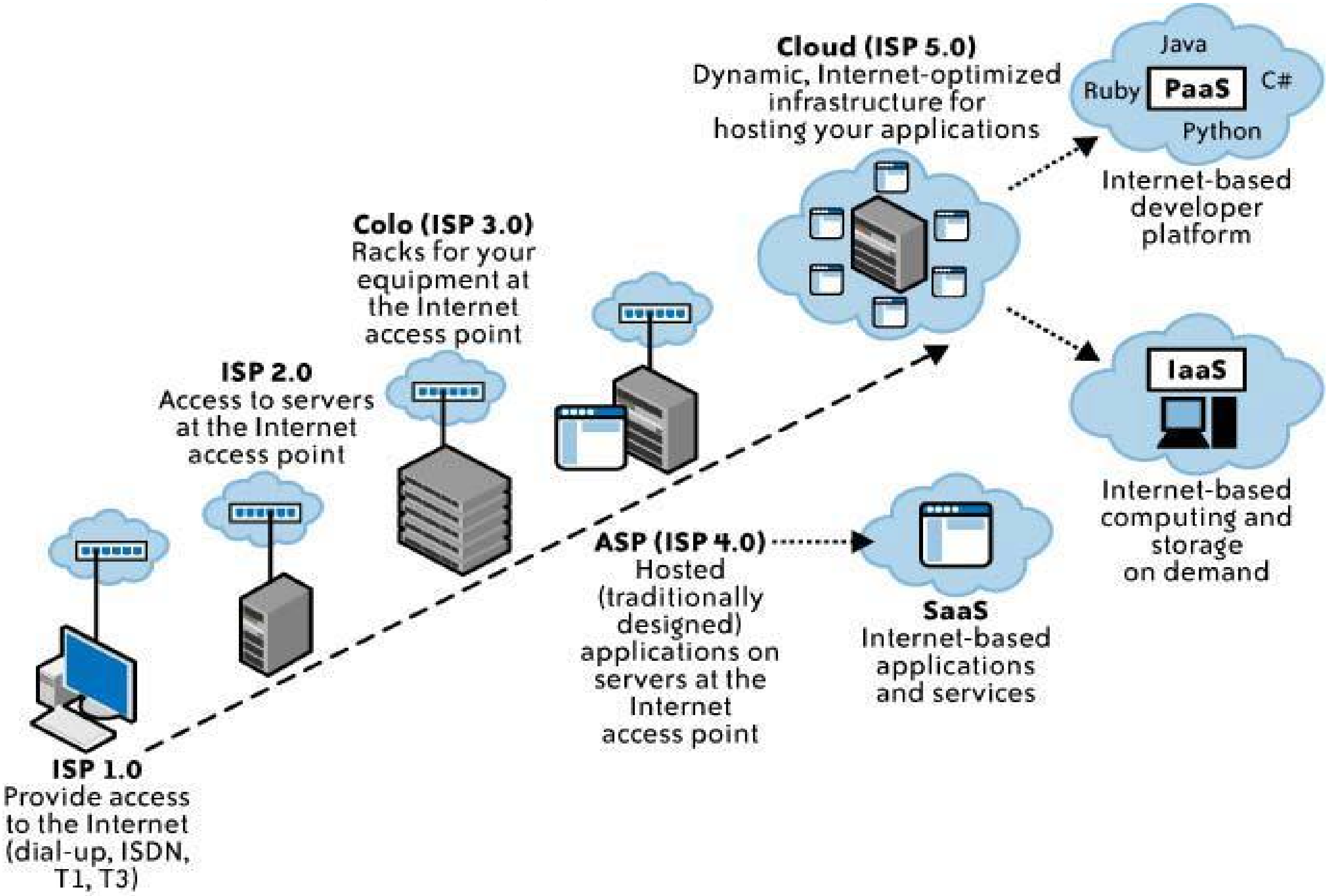
2) DB level Isolation :

- if tenants are running the same kind of application, the only difference is the data each tenant store. Why can't we just introduce an extra attribute "tenantId" in every table and then append a "where tenantId = $thisTenantId" in every query

- In other words, add some hidden column and modify each submitted query.
- In additional, the cloud provider usually need to re-architect the underlying data layer and move to a distributed and partitioned DB.
- Some of the more sophisticate providers also need to invest in developing intelligent data placement algorithm based on workload patterns.
- In this approach, the degree of isolating is as good as the rewritten query.
- The advantage of DB level isolation is there is no VM overhead and there is no minimum charge to the tenant.

8. Explain Evolution Of Cloud Computing.

The Evolution of Cloud Computing


Cloud (ISP 5.0)
Dynamic, Internet-optimized infrastructure for hosting your applications
Java
Ruby
PaaS
C#
Python
Internet-based developer platform
IaaS
Internet-based computing and storage on demand
Colo (ISP 3.0)
Racks for your equipment at the Internet access point
ISP 2.0
Access to servers at the Internet access point
ASP (ISP 4.0)
Hosted (traditionally designed) applications on servers at the Internet access point
SaaS
Internet-based applications and services
ISP 1.0
Provide access to the Internet (dial-up, ISDN, T1, T3)

- Figure 1-2 displays cloud computing and cloud service providers (CSPs) as extensions of the Internet service provider (ISP) model.
- In the beginning (ISP 1.0), ISPs quickly proliferated to provide access to the Internet for organizations and individuals.
- These early ISPs merely provided Internet connectivity for users and small businesses, often over dial-up telephone service.
- As access to the Internet became a commodity, ISPs consolidated and searched for other value-added services, such as providing access to email and to servers at their facilities (ISP 2.0).
- This version quickly led to specialized facilities for hosting organizations' (customers') servers, along with the infrastructure to support them and the applications running on them. These specialized facilities are known as collocation facilities (ISP 3.0).

- Those facilities are “a type of data center where multiple customers locate network, server, and storage gear and interconnect to a variety of telecommunications and other network service provider(s) with a minimum of cost and complexity.
- As collocation facilities proliferated and became commoditized, the next step in the evolution was the formation of application service providers (ASPs), which focused on a higher value-added service of providing specialized applications for organizations, and not just the computing infrastructure (ISP 4.0).
- ASPs typically owned and operated the software application(s) they provided, as well as the necessary infrastructure.
- Although ASPs might appear similar to a service delivery model of cloud computing that is referred to as software-as-a-service (SaaS), there is an important difference in how these services are provided, and in the business model.
- Although ASPs usually provided services to multiple customers (just as SaaS providers do today), they did so through dedicated infrastructures. That is, each customer had its own dedicated instance of an application, and that instance usually ran on a dedicated host or server.
- The important difference between SaaS providers and ASPs is that SaaS providers offer access to applications on a shared, not dedicated, infrastructure.