ISM Unit 5

⑥ Characteristics of Cloud Computing:

→ On demand self services: The cloud computing service does not require any human administrators. Users themselves are able to manage cloud resources as needed.

→ Broad Network Access: The computing services are generally provided over standard networks and heterogeneous devices.

→ Rapid Elasticity: The computing services should have IT resources that are able to scale in and out quickly and on as needed basis.

→ Resource pooling: The IT resources present are shared across multiple applications. Multiple clients are provided service from the same physical resource.

→ Measured service: The resource utilization is tracked for each application. Done for various reasons like effective use of resources.

→ Easy Maintenance: The services are effortlessly maintained. The downtime sometimes remains low or absolutely zero. The resources undergo several updates. Updates are more viable and perform quicker than previous versions.

→ Scalability: It enables cost-effective running of workloads.

→ Economical: Helps in reducing IT expenditure of the organizations.

→ Security: Creates a copy of the data that is stored to prevent any form of data loss.

→ Remote working: Users can work from any location.

④ Cloud Service Models:

→ Classified primarily into 3 models according to NIST:
(a) Infrastructure-as-a-Service (IaaS)
(b) Platform-as-a-service (PaaS)
(c) Software-as-a-service (SaaS)

(a) Infrastructure-as-a-Service(IaaS): eg: Amazon Elastic Compute Cloud. (Amazon EC2)
→ Also known as Hardware as a Service (HaaS)
→ Allows customers to outsource their IT infrastructures.
→ Clients can dynamically scale the configuration to meet changing requirements and are billed only for the services actually used.
→ IaaS eliminates the need for every organization to maintain their IT infrastructure.
→ Offered in 3 models: public, private and hybrid.
public - Infrastructure resides at cloud computing platform vendor's data center
private - Infrastructure resides at customer premise.
hybrid - Combination of both in which the customer selects the best.

(b) Platform-as-a-Service (PaaS): eg: Google App Engine, Microsoft Windows Azure.
→ Provides a runtime environment.
→ Allows programmers to easily create, test, run and deploy web applications.
→ back-end stability is managed by cloud service providers, so the end users do not need to worry about managing the infrastructure.
→ PaaS provides: ① Programming languages.
② Application frameworks
③ Databases.
④ Other tools required to develop, test and deploy the applications.
→ lower risk, scalability.

(c). Software-as-a-service (SaaS): Eg. EMC Mozy.
→ Also known as On-Demand Software.
→ Provides various business-services to start-up the business.
→ Provides software for document management.
→ Social Networking service providers use SaaS for their convenience.
→ Used to handle the unpredictable number of users and load as e-mail services.
→ It is easy to buy.
→ Services are offered as a one-to-many model. Single instance of application is shared by multiple users.
→ Requires less Hardware.
→ Low-maintenance.
→ No particular hardware / software versions required.

(10). Cloud Deployment Models:

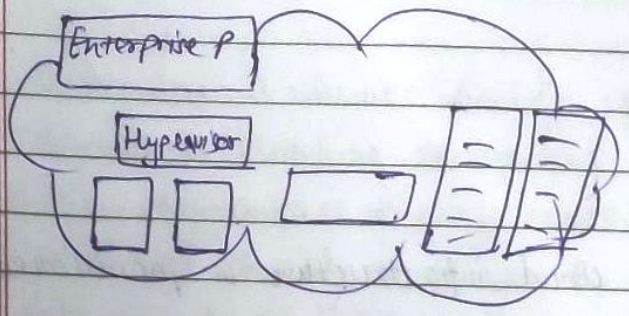
4 deployment Models according to NIST:
(a) public
(b). private
(c). community
(d). hybrid.

(a). public cloud model: The cloud infrastructure is provisioned for open use by general public.
→ It may be owned, managed and operated by a business, academic or government organization.
→ Consumers use the cloud services offered by the providers via internet and pay the required charges.
→ Low capital cost, enormous stability.
→ Popular Public cloud service providers are Amazon, Google and Salesforce.com.

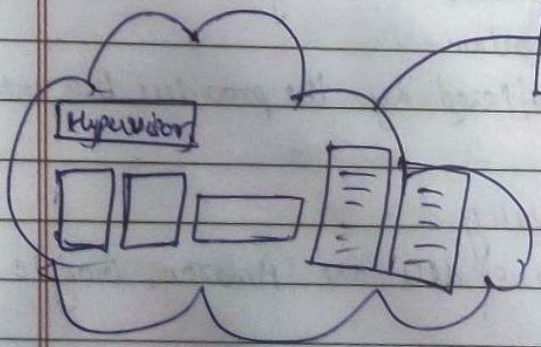
(2) Private Cloud Model: → The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers.
→ It may be owned, managed and operated by the organization, a third party or some combination of them.
→ two variations: (i) On premises
(ii) Off Premises.

(i) On-premises: → also known as internal cloud.
→ Hosted by an organization within its own data-centers.
→ Best suited for organizations that require complete control over their applications, infrastructure and security mechanisms.

(ii) Off-premises: → Externally hosted private cloud.
→ Hosted external to an organization and managed by third party organization.
→ Full guarantee of privacy and confidentiality.

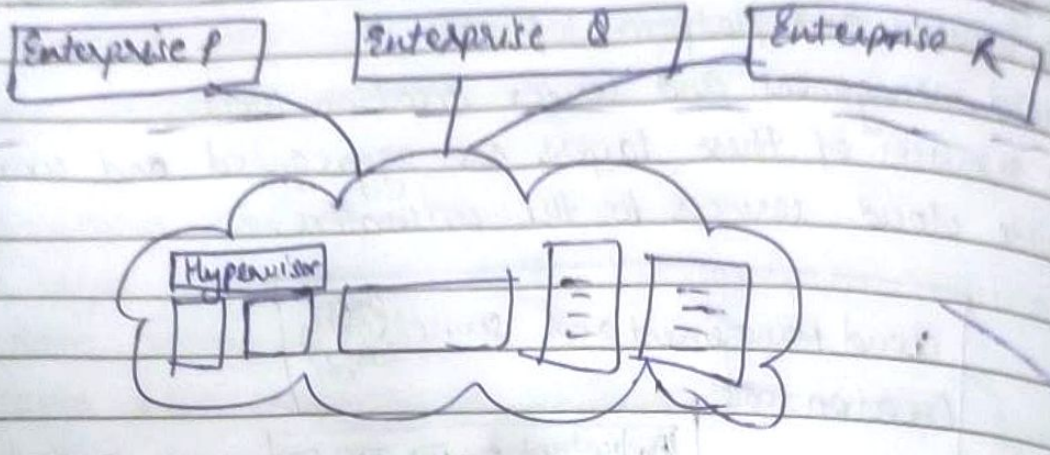


On-premise Private Cloud.

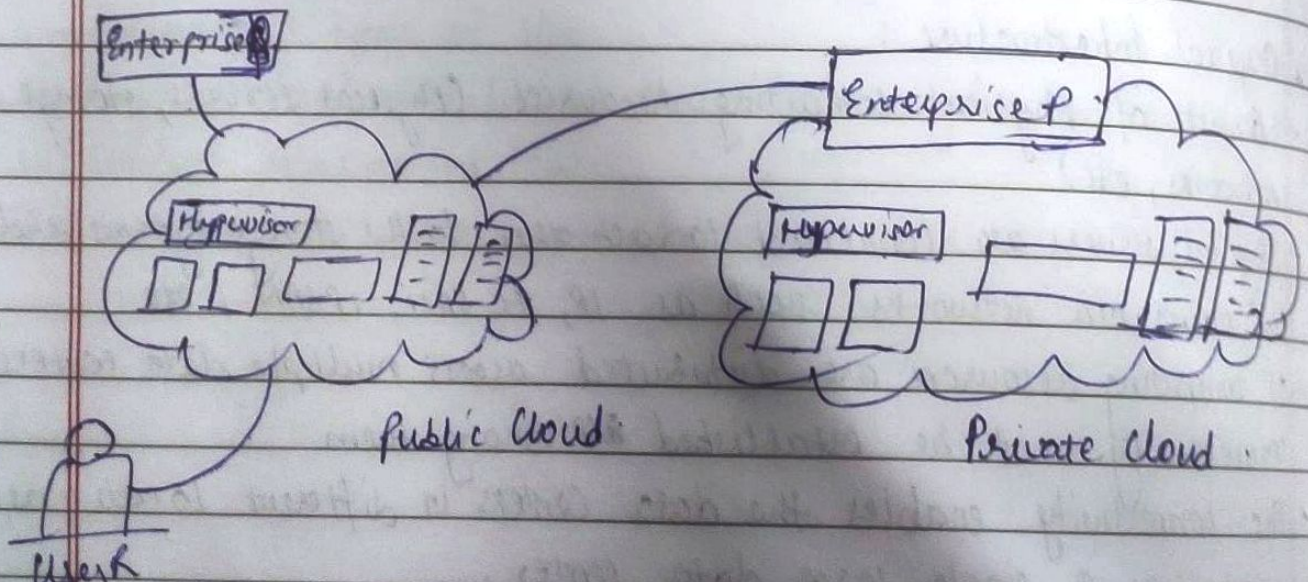


Off-premise Private Cloud.

© Community cloud → The cloud infrastructure is provisioned for special use by a specific community of consumers from organizations.
→ May be owned/managed/operated by one or more of organizations in the community, a third party or some combination of them
→ may exist on or off premises.

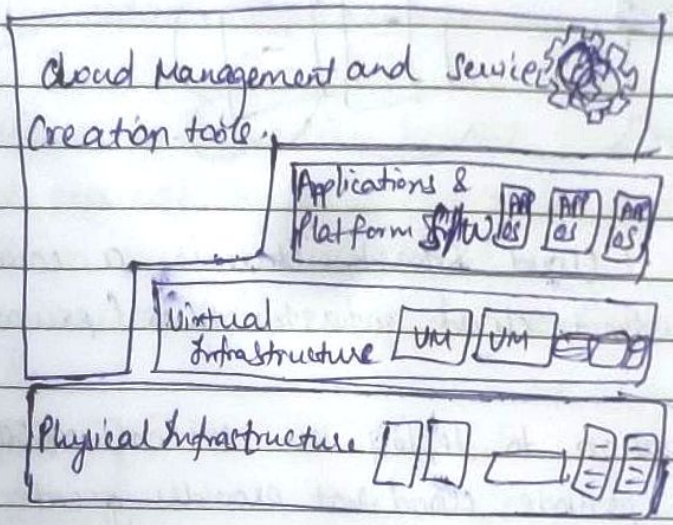


② Hybrid Cloud : → Cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community or public).
→ Allows an organization to deploy less critical applications
→ Data remains on private cloud that provides greater security



① Cloud Computing Infrastructure:

→ Collection of HW and SW that enables the 5 essential characteristics of cloud computing.
→ Usually consists of the following layers:
(a) Physical Infrastructure
(b) Virtual Infrastructure
(c) Applications and platform software.
(d) Cloud management and service creation tools.
→ The resources of these layers are aggregated and coordinated to provide cloud services to the consumers.



(a) Physical Infrastructure:
→ Consists of physical computing resources. (Physical servers, storage systems, networks, etc).
→ Physical servers are connected to each other, to the storage systems and to the clients via networks such as IP, FC SAN, IP SAN, etc.
→ If computing resources are distributed across multiple data centers, connectivity must be established among them.
→ The connectivity enables the data centers in different locations to work as a single large data center.

① Virtual Infrastructure:
→ On top of physical infrastructure.
→ Enables some of cloud characteristics such as resource pooling and rapid elasticity.
→ Helps to reduce cost
→ Better efficiency and optimization.
→ Provides a consolidated view of resource capacity
→ Consolidated resources are managed as a single entity called resource pool.

② Applications and Platform Software:
→ This layer includes a suite of business applications and platform software.
→ Platform s/w provides the environment on which business applications run.
→ for SaaS, both the application and platform s/w are provided by cloud service providers.
→ In case of PaaS, only platform service is provided by cloud service providers.

③ Cloud Management and service Creation tools:
→ Includes 3 types of s/w.
(i) Physical and virtual infrastructure management s/w.
(ii) Unified Management s/w.
(iii) User-access management software.

(12) Cloud Challenges:

- Challenges for consumers:
  - → Business-critical data requires protection and continuous monitoring of its access.
  - → Consumers might not be willing to transfer control of their business-critical data to cloud.
  - → Consumers may or may not know in which country their data is stored.
  - → Some cloud service providers allow consumers to select the location.
  - → Mismatch b/w hypervisors.
  - → difficulty for consumers to change their cloud service provider.

- Challenges for providers:
  - → Cloud service providers must ensure that they have adequate resources to provide the required levels of services.
  - → It is a challenge for cloud service providers to estimate the actual cost of providing the services.
  - → Some of the software vendors offer standardized cloud licenses at a higher price compared to traditional licensing models.

(13) Cloud enabling Technologies:

(a). Grid Computing
(b). Utility Computing
(c). Virtualization
(d). Service-Oriented Architecture.

(a). Grid Computing:
→ form of distributed computing that enables the resources of numerous heterogeneous computers in a N/w to work together on a single task at the same time.
→ Enables parallel computing and is best for large workloads.

(b). Utility Computing:
→ Service provider makes computing resources available to the customers, as required and charges them based on usage.
→ Similar to other utility resources such as electricity where charges are based on consumption.

(c) Virtualization:
→ Technique that abstracts physical characteristics of IT resources from the resource users.
→ Enables the resources to be viewed and managed as a pool and lets users to create virtual resources from the pool.
→ Provides better flexibility.
→ Optimize resource utilization and delivering resources more efficiently.

(d). Service Oriented Architecture (SOA):
→ Provides a set of services that can communicate with each other.
→ These services work together to perform some activity or simply pass data among services.

13.8 Cloud Adoption Considerations

Organizations that decide to adopt cloud computing always face this question: "How does the cloud fit the organization's environment?" Most organizations are not ready to abandon their existing IT investments to move all their business processes to the cloud at once. Instead, they need to consider various factors

before moving their business processes to the cloud. Even individuals seeking to use cloud services need to understand some cloud adoption considerations. Following are some key considerations for cloud adoption:

- **Selection of a deployment model:** Risk versus convenience is a key consideration for deciding on a cloud adoption strategy. This consideration also forms the basis for choosing the right cloud deployment model. A public cloud is usually preferred by individuals and start-up businesses. For them, the cost reduction offered by the public cloud outweighs the security or availability risks in the cloud. Small- and medium-sized businesses (SMBs) have a moderate customer base, and any anomaly in customer data and service levels might impact their business. Therefore, they may not be willing to deploy their tier 1 applications, such as Online Transaction Processing (OLTP), in the public cloud. A hybrid cloud model fits in this case. The tier 1applications should run on the private cloud, whereas less critical applications such as backup, archive, and testing can be deployed in the public cloud. Enterprises typically have a strong customer base worldwide. They usually enforce strict security policies to safeguard critical customer data. Because they are financially capable, they might prefer building their own private clouds.
- **Application suitability:** Not all applications are good candidates for a public cloud. This may be due to the incompatibility between the cloud platform software and the consumer applications, or maybe the organization plans to move a legacy application to the cloud. Proprietary and mission-critical applications are core and essential to the business. They are usually designed, developed, and maintained in-house. These applications often provide competitive advantages. Due to high security risk, organizations are unlikely to move these applications to the public cloud. These applications are good candidate for an on-premise private cloud. Nonproprietary and nonmission critical applications are suitable for deployment in the public cloud. If an application workload is network traffic-intensive, its performance might not be optimal if deployed in the public cloud. Also if the application communicates with other data center resources or applications, it might experience performance issues.
- **Financial advantage:** A careful analysis of financial benefits provides a clear picture about the cost-savings in adopting the cloud. The analysis should compare both the Total Cost of Ownership (TCO) and the Return on Investment (ROI) in the cloud and noncloud environment and identify the potential cost benefit. While calculating TCO and ROI, organizations and individuals should consider the expenditure to deploy and maintain their own infrastructure versus cloud-adoption costs. While calculating the expenditures for owning infrastructure resources, organizations should include both the capital expenditure (CAPEX) and operation expenditure

(OPEX). The CAPEX includes the cost of servers, storage, OS, application, network equipment, real estate, and so on. The OPEX includes the cost incurred for power and cooling, personnel, maintenance, backup, and so on. These expenditures should be compared with the operation cost incurred in adopting cloud computing. The cloud adoption cost includes the cost of migrating to the cloud, cost to ensure compliance and security, and usage or subscription fees. Moving applications to the cloud reduces CAPEX, except when the cloud is built on-premise.

- **Selection of a cloud service provider:** The selection of the provider is important for a public cloud. Consumers need to find out how long and how well the provider has been delivering the services. They also need to determine how easy it is to add or terminate cloud services with the service provider. The consumer should know how easy it is to move to another provider, when required. They must assess how the provider fulfills the security, legal, and privacy requirements. They should also check whether the provider offers good customer service support.
- **Service-level agreement (SLA):** Cloud service providers typically mention quality of service (QoS) attributes such as throughput and uptime, along with cloud services. The QoS attributes are generally part of an SLA, which is the service contract between the provider and the consumers. The SLA serves as the foundation for the expected level of service between the consumer and the provider. Before adopting the cloud services, consumers should check whether the QoS attributes meet their requirements.