

UNIT I - INTRODUCTION

Introduction: Business and IT Perspective.

- Businesses are looking for ways to deliver IT resources of their own for end-users - employees, partners and customers.

Cloud Computing is delivering IT-enabled services via the Internet that are built for the end users.

"It is the ability to deliver computing services over the Internet on demand on pay-as-you-go basis to the end users."

Cloud and Virtualization:

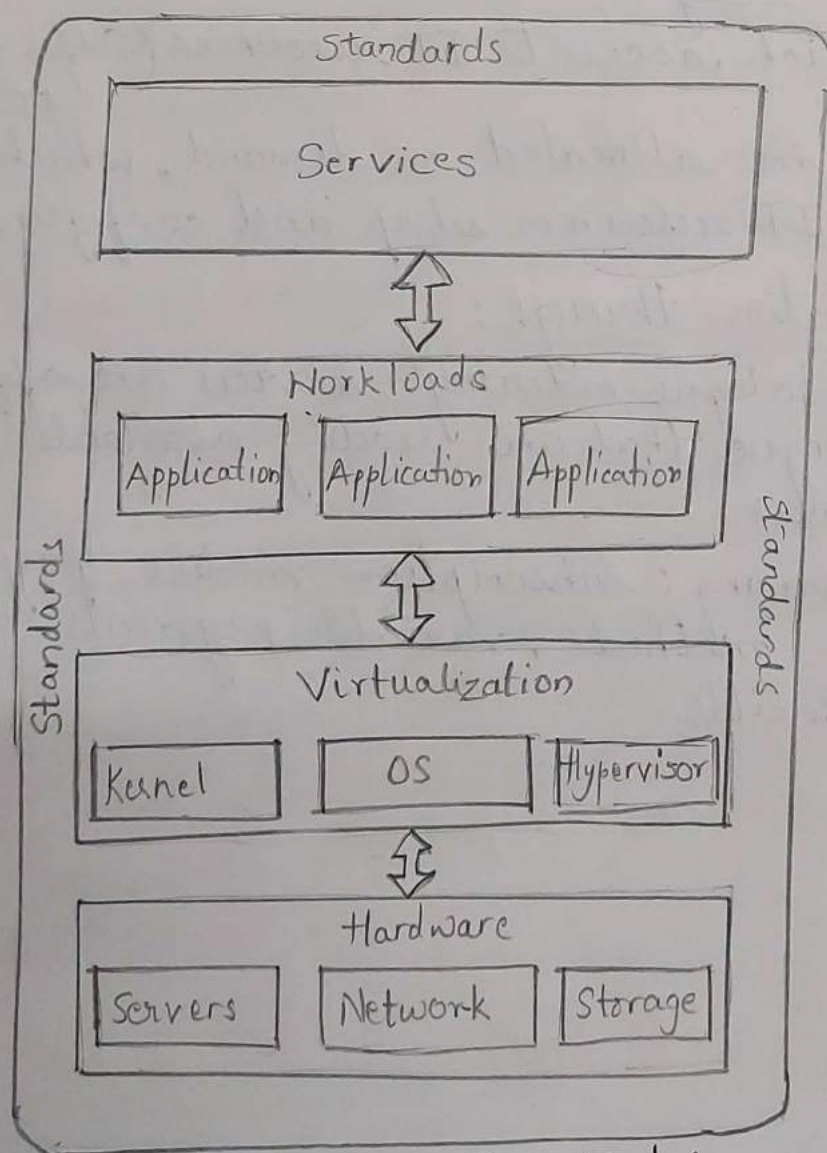


Fig.: Cloud Computing Model

- In cloud environment, people expect self-service, get started quickly, self-provisioning or rapid provisioning.
- The only way to get efficiency is by virtualizing, standardizing and automating. This brings down costs and improve services.
- The results include:

- Servers/storage:

IT resources from servers to storage, network and applications are pooled and virtualized to provide an implementation-independent, efficient infrastructure with scaling (meaning the ability to increase or decrease IT resources as needed to meet changing demand).

- Automation using:

- Point & click access to IT resources (Self-service portal).
- Resources are allocated on demand, which helps to reduce IT resources setup and configuration time.

- Standardization through:

- Service catalogue ordering:- Services are offered from catalogue that are readily available on metered basis.
- Flexible pricing: Subscription models, pay-by-consumption methods, variable payments make IT services flexible.

Cloud Services Requirements:

- Cloud computing is considered as the next best solution for cost cutting in providing IT services.
- We need to decide the right workloads for the cloud.
- We require to understand which workloads ~~can~~ need vendor cloud and which needs to be onsite behind the organizational's firewall.
- Cloud service providers (vendors) must provide solutions that will provide dynamic infrastructure, which is required in cloud delivery.
- Along with workload solutions, it is required to deliver business outcomes to the clients.
- Any cloud computing service must offer the following advantages:
 - Any service management inside the cloud must provide visibility, control, automation across IT & business services.
 - It must accelerate standardization of services, supporting productivity & rapid client payback.
- Cloud providers can help clients to identify the right combination of public, private & hybrid models.
- Assistance should also include cloud strategy, cloud assessment, design and development of cloud roadmap.
- Clients must be encouraged to get started with a strategy and implement pilot deployment of a workload.

Cloud and Dynamic Infrastructure.

- Cloud is dynamic in nature because clients can access IT resources to deploy new applications, services or computing resources rapidly without re-engineering their entire infrastructure.

The following initiatives combines to provide cloud Dynamic Infrastructure :

- Service Management : Provide visibility, control, and automation across all the business & assets to deliver higher value services.
- Asset Management : Use of asset management sol^s to maximise the value of business assets.
- Virtualization and Consolidation : Reduces costs, improve responsiveness, fully utilize resources.
- Information Infrastructure : Helps in achieving information compliance, availability, retention, and security goals.
- Energy Efficiency : Addresses energy, environment, and sustainability challenges and opportunities.
- Security : Provide risk management, end-to-end industry customized governance.
- Resilience : Maintain business & IT operations continuously while adapting & responding to risks & opportunities.

Cloud Computing Characteristics:-

- The characteristics of a cloud are as follows:-
- Cloud computing uses commodity-based hardware and thus it can be replaced any time without affecting the cloud.
 - It uses commodity-based software container system. i.e. service can be moved from one cloud provider to any other cloud provider with no effect on the service.
 - Requires virtualization engine and an abstraction layer for the h/w, s/w and configuration of systems.
 - Multi-users where multiple users share the underlying infrastructure resources without compromising the privacy & security of their data.
 - Clouds implement 'pay-as-you-go' billing model
 - No lock-in of the resources and no up-front investment in procuring resources.
 - Scalable services are provided that deliver services expands and shrinks the resources automatically based on the business demands.

Cloud Computing Barriers:

Four major barriers are identified to large-scale adoption of cloud services.

- 1] Security:- Since most of the data exchange happens over Internet, IT security is handled by an external entity. Hence, data security is seen as higher risks.
- Another factor is, we have limited knowledge about the physical location of stored data
 - It is believed that multi-user platforms are less secure than single-user platforms.
 - Virtualization is relatively new technology
 - Monitoring the access to applications in the cloud have limited capabilities.

② Governance and regulatory compliance:

- Not all cloud service providers have well-defined service-level-agreements (SLAs) or SLAs that meet stricter standards.
- Recovery times are stated as 'as soon as possible' rather than a guaranteed no. of hours.
- Corrective measures are fairly minimal.
- From cloud service provider's point of view, it is impractical to meet all the requirements of individual customers.
- Overall performance of cloud service is dependent on the performance of components that is not in control of the customers & service providers (eg: n/w connection)

③ Integration and interoperability:

- Different businesses have different needs, Identifying & migrating appropriate applications to the cloud is made complicated due to the interdependencies among the applications.
- It also includes issues related to integrating legacy applications of cloud with new applications.
- It lacks standard interfaces or APIs.
- There are concerns regarding how different appl's, on different platforms, deployed at dispersed locations, can interact flawlessly & provide expected services.

④ Suitable workloads for cloud deployment:-

- Not every application is suitable candidate for moving to a cloud computing environment.
- Whether the appl^e is good fit on cloud depends on nature of business, characteristics and also technical aspects or its infrastr requirements

Cloud Adoption :-

- Cloud adoption is a strategic move by organisations of reducing costs, mitigating risks and achieving scalability of database capabilities.
- Organisations that go ahead with adopting cloud based technologies have to identify various security assessments.
- Based on various technical characteristics & compliances, organisations must decide on adopting the cloud services.
- Basically, cloud favours Web appl's and interactive appl's and services with low availability requirements & short life spans. Eg: Enterprise marketing campaigns need quick delivery of a promotion.
- Cloud suitable appl's are that are modular, isolated workloads, one-time batch processes, media distribution, packages like e-mail & collaborative business n/w's.
- Cloud suitable projects are R&D projects, prototyping of new appl's, designs models & those which scale horizontally on small servers - that is adding of more small servers rather than increasing single server's computational capacity.
- Appl's that need infrastr throughout the day, month or that have seasonal demands are more suitable for going onto cloud.
- Best examples in real world suitable for cloud are :
 - Small & medium businesses
 - Start-up companies

- Telecommunication sectors
- Education sector
- Clouds are not suitable for mission-critical & core businesses & their appl's, transaction processing that depend on data that are restricted to the organisation.
- Appl's that run $24 \times 7 \times 365$ with steady demand, those which consume significant memory, databases, are not suitable for cloud.
- Cloud is not suitable for appl's that scale vertically on single servers - that is, by increasing a server's computational capacity rather than adding more servers.
- Appl's that are static, which do not scale, not using true power of cloud aren't suitable.
- Appl's that use max. time of resources increase resource consumption and hence, the cost on cloud.
- Appl's that have sensitive data aren't meant for cloud as this environment is shared & multi-tenants.
- Licensing complexities occur when the terms & conditions of appl's to be moved over cloud do not meet the licensing docs of the legacy appl's.

UNIT-I Chapter-II

CLOUD DEPLOYMENT MODELS

⇒ Cloud Characteristics :

Cloud carries basic infrastructural characteristics that help in deploying cloud service in a fast and cost-effective way.

- 1] On-Demand Service
- 2] Ubiquitous Network Access
- 3] Location-Independent Resource Pooling (Multi-Tenant)
- 4] Rapid Elasticity.

On-Demand Service :

- A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without human interaction.

Ubiquitous Network Access :

- Heterogeneous client platforms or devices are able to make use of the services over the network & accessed through standard mechanisms.

Multi-Tenants

- Resources like storage, processing, memory, network bandwidth & virtual machines are pooled to serve many customers.
- These resources are assigned & re-assigned according to demand and also dynamically.
- Customers have no control or knowledge about the location about the services.

Rapid Elasticity

- Services available can be rapidly, flexibly setup (or provisioned), and automatically be allocated to quickly scale out and scale in.
- The services appear to be unlimited & can be purchased at any time to the customers.

⇒ Measured Service :-

- Cloud systems automatically control & optimize resource use by metering at some level of abstraction.
- Resource usage can be monitored, controlled and reported by providing transparency for both the provider and the consumer.
- The more standardization and virtualization you achieve within your infrastructure, greater the cost and expenditures. Hence, we need to address standardization and virtualization to reduce costs and also meet the dynamic needs of business.

Reasons why organisations are migrating to cloud computing

- To achieve flexibility and cost-reduction benefits
- To avoid vulnerability and delays that occur because of trial & error method.
- To augment limited in-house resources to smoothly migrate to cloud computing environment.

⇒ Cost Factor :

- One of the many reasons why cloud computing is popular is the cost aspect.
- By virtualization and standardization, we can deliver more services with few resources and drive up utilization.
- Automation reduces labour cost as cost benefit.
- Self-service plus standardization will lower operational costs, increase productivity and ensure better security.
- Self-service portal allows end consumers to only see services they are allowed.
- It helps them to initiate the process of getting services.
- At the infrastructure layer, virtualization helps in increasing the workloads & resource utilization.
- From the labor perspective, clients help themselves, less support is needed, hence reducing the cost for a dedicated team.
- In terms of automation, manual and repeatable tasks are computed on cloud and this reduces IT operations cost.

⇒ Benefits by adopting the cloud:

- 1] Self-service capability : This capability helps to be self-reliant.
 - Testing teams need not buy computing services as they can utilize same services over the cloud.
 - Reduces the procurement process and hence they can concentrate on the testing services & efforts.

- ② Resource availability: Virtualization facilitates resource availability.
- It helps in tracking and use the resource pool to its maximum.
- ③ Operational efficiency:
- Template-based approach common to all teams, configurable appl^s, operating systems is more transparent.
 - This transparency can help the teams to understand the environment better and help in operational efficiency.
- ④ Hosted tools:
- The tools required are already hosted on cloud.
 - The developers and testers need not to install, configure, run or maintain tools on their system as they can log into the network maintaining these tools from any machine.

⇒ Cloud Deployment Models

Cloud delivery models can be briefly classified into following types:

1) Public: In this, the business rents the services that are required and pays for what is utilized on-demand.

- The resources (servers and storage) are owned & operated by a third-party cloud service provider and delivered over the internet.

Eg: Amazon Web Services (AWS)

Microsoft Azure

Google Cloud Platform etc.

2] Private: Private cloud refers to cloud deployment model operated exclusively to a single organization.
- It provides computing services to a private internal network (within the organisation) and selected users instead of public in general.
Example: HP Data centers, Elasta-private cloud, Ubuntu.

3] Hybrid: Enterprises deploy workloads in private IT environments or public clouds and move between them as computing needs and costs change.
- These give greater control over their private data.
- An organisation can store sensitive data on a private cloud and also on local datacenter and leverage the resource utilization in a robust way.

PUBLIC CLOUDS

- Offered by third-party providers
 - On-demand with the pay-as-you-use option
 - Multi-tenancy, resource pooling, service accounting
 - Enterprises are able to offload appl's to third-party service providers
 - Public cloud can be free or fairly inexpensive to use
 - User's data is not publically visible, vendors provide access control mechanism for their use.
- Examples of workloads on public clouds:
- 1) Web pages
 - 2) Public Wiki's and blogs
 - 3) Online storage solutions
 - 4) Online backup/restore solutions
 - 5) Jobs (tasks) with lower security constraints

Appl's not suitable on public clouds:

- 1) Workloads which are composed on other services
- 2) Workloads needing high-level accountability
- 3) Requiring high output online transaction processing
- 4) Workloads that depend on sensitive data.

PRIVATE CLOUDS:

- Clouds are deployed inside the company's firewall (on-premise) and run by on-site servers.
- Suitable when the traditional requirements, such as control, security and resiliency are of more importance by the organisation with restricted user access.

High "Cost of Privacy"

- As private clouds are implemented internal to an organisation, expenses are owned by them. Key benefits of cloud are not realised

1) Eliminating capital expenses and operating costs:-

H/w and s/w eliminates the pay-per-use potential, as there must be upfront purchases. The full cost of operations must be done by organisations.

2) Removing undifferentiated heavy lifting by offloading datacenter operations:

- Sometimes outside vendors are used offerings are utilized even though private cloud is deployed.
- In such cases, these costs might be justified if the benefits are larger.
- Private clouds provide more control over the information.

HYBRID CLOUDS:-

- A hybrid cloud is combination of an interoperating public & private cloud.
- Here, the consumers takes the insensitive/non-critical appl^s or information & compute on the public cloud while keeping all critical appl^s & information in control using private clouds.
- It offers the best of both cloud models — the scale & convenience of public cloud & control & ~~requisite~~ reliability of private cloud — and let them move between the two on basis of their needs.
- This model allows :-
 - 1) Elasticity, ability to scale capacity up & down
 - 2) Pay-as-you-go pricing.
 - 3) Network isolation & secure connectivity.
 - 4) Gradually move to public cloud, replicate an entire datacenter, or move anywhere.

★ Self-Study : Community clouds, Shared Private Cloud, Dedicated Private Cloud, Dynamic Private Cloud.

⇒ SECURITY IN A PUBLIC CLOUD :

Security concerned to be considered for the cloud deployment :

- 1) Mutli-Tendency : The cloud providers must build its security to meet the higher-risk requirements, so that the lower-risk clients get better security than they would have normally.

2) Security Review :- Security specialists who are able to identify the issues related to security must conduct regular audits, reviews & assessments for the security.

3) Mutual Risk :-

- Risks associated with each operator & service provider is mutual as they share the resources.
- Risk mitigation plan should be devised to suit the architecture of the cloud provider.

4) Employee Physical screening :-

- Contract employees background verification should be done by a third party for cloud service provider.
- Service providers must publish its policy to all employees, this establishes the trust between the user & the service provider.

5) Multi-Geographical Datacenters :-

- Cloud datacenters are distributed and hence less prone to disasters.
- But, it is important that providers test their disaster recovery option as they are heavily tied with SLA's & penalties.
- They must check & test with mock drills for failover.

6) Physical security :-

- Physical threats are another factor to be analyzed when opting cloud services.
- Components such as biometric access, surveillance cameras, logbook, escorts, automatic alarms are installed in datacentres.

7) Regulations :

- All cloud service providers should have a special team for any incident based response that is based on the policies and regulations.
- These regulations & policies should be shared with the customers.

8) Programming Conventions :

- Cloud providers might use their own s/w's that may be prone to security threats & bugs.
- It is recommended that they use secure coding and programming practises.
- It should be written based on standards that are well documented, reviewed, accepted & adhered.

9) Data Control

- Data and information are at greatest risk in today's scenario.
- Cloud service providers should be able to adhere to the guidelines laid by region or agency.
- There should be strong encryption mechanism for the in-flight data.
- Cloud provider must maintain the security incident policy.

* Self-Study : Public v/s Private v/s Hybrid cloud

⇒ Cloud Infrastructure Self-Service



7) Regulations :

- All cloud service providers should have a special team for any incident based response that is based on the policies and regulations.
- These regulations & policies should be shared with the customers.

8) Programming Conventions :

- Cloud providers might use their own s/w.s that may be prone to security threats & bugs.
- It is recommended that they use secure coding and programming practises.
- It should be written based on standards that are well documented, reviewed, accepted & adhered.

9) Data Control

- Data and information are at greatest risk in today's scenario.
- Cloud service providers should be able to adhere to the guidelines laid by region or agency.
- There should be strong encryption mechanism for the in-flight data.
- Cloud provider must maintain the security incident policy.

* Self-Study : Public v/s Private v/s Hybrid cloud

⇒ Cloud Infrastructure Self-Service

- The cloud infrastructure has to be provisioned & paid up-front in private clouds.
- Self-service provisioning of infrastructure capacity is only possible up to a point in private clouds. ⇒

- SLA's and contractual terms and conditions are negotiable between the cloud vendors & the customers to meet specific requirements.
- The sensitive data and information stay behind the organisation's firewall.
- There is no best model or right model for any organisation. It depends on the use, policies, applⁿ behaviour, location, govt. regulations and compliances.
- Public clouds can be good option for the testing and development cloud as the provisioning requirement in the development & test environment is very rapid & for shorter period.
- Cloud computing employs a structured technique to leverage IT industry best practises.
- Infrastructure Strategy and Planning Features:-
 - There are three major features:
 - 1) Evaluation to know the gaps, readiness & strengths of the existing environment.
 - 2) Development of the value proposition for cloud computing in the enterprise.
 - 3) Strategy, planning, and roadmap to successfully implement the selected cloud delivery model.
- Cloud architected solⁿs have introduced new characteristics like scalability and consistent delivery.
- Helps reduce cost investment and operational cost with meeting the high SLAs.

* Cloud Computing Steps :

The process from virtualization to cloud computing has following steps:

1) Stage 1 :- Server Virtualization :

- Companies usually start virtualization as a consolidated attempt.
- The main aim is to reduce capital expenses such as server, storage and networks, reducing energy costs, and avoiding datacenter build out or more.

2) Stage 2 : Distributed Virtualization :

- Once the companies achieve capital expense improvements, they next focus on elasticity, operational improvements, rapidity & organizing downtime more efficiently.

3) Stage 3 : Private Cloud :

- Once the processes are designed and standards are in place to enable broad automation, the company is ready to look at introducing self-service capabilities.

4) Stage 4 : Hybrid Cloud :

- Private clouds are not only the answer to any enterprise.
- Self-service portals & interface introduced by private clouds should enable the IT enterprises to leverage public cloud services without affecting end users.

5) Stage 5: Public Cloud

- Some companies use public clouds services first, and use their experience & lessons to establish private clouds for their enterprises.
- Hence, virtualization is not the must thing to establish cloud in their companies.
