Cloud Computing

-**Benefits of Cloud Computing**
  - **1. Cost reduction**
  - **2. Scalability, availability and reliability**

-**Cloud Risks and Challenges**
  - **1. Vulnerability and security issues**
  - **2. Reduced operational governance control**
  - **3. Limited portability between cloud providers**
  - **4. Multi-regional compliance and legal issues**

- **Roles and Boundaries in Cloud Computing**

Benefits of Cloud Computing

Reduction in Initial IT Infrastructure Cost

- The immediate benefit of using Cloud is the reduction in initial cost.
- The initial costs include:
    1. Infrastructure costs:
        i. IT equipment
        ii. Software
        iii. Networking
        iv. Construction costs
        v. Installation costs

Benefits of Cloud Computing

- The infrastructure costs can be regarded as capital investments or ownership costs.
  - The cloud saves the initial upfront ownership costs.
  - The cloud offers affordable and attractive packages for services obtained in large volume.
  - The cloud reduces investment and proportional costs.

Benefits of Cloud Computing

- The cloud provider can increase the profit by increasing the resource utilization, using proven practices and by optimizing the cloud architecture.

- Common measurable benefits for the cloud consumers are:

  - Pay-as-you-go rental for short term usage

  - The availability of virtually unlimited resources on demand with negligible wait time for provisioning.

Cloud Computing

Increased Scalability, Availability and Reliability

Increased Scalability, Availability & Reliability

Increased scalability:

- The cloud can dynamically and instantly provide the computing resources.
- This provision can be on demand or as per user configuration.
- Similarly these IT resources can be released automatically or manually with the decrease in processing demand.
- This dynamic scalability avoids the over-provisioning and under-provisioning and the associated disadvantages.

Increased Scalability, Availability & Reliability

Availability:

- The availability of IT resources sometimes can be referred to profit and customer retention.
- If an IT resource becomes unavailable (such as a database dealing with clients' orders) then this may result in customer dissatisfaction and loss of business.

Increased Scalability, Availability & Reliability

Reliability:

- The reliability of IT resources is very important for continual business data processing and response time.
- The failure of any IT resource can be cause the collapse the IT system. For example failure of the Ethernet switch may crash a distributed application.

Increased Scalability, Availability & Reliability

- The modular structure and resource redundancy in cloud increases the availability and reliability. Cloud, on the other hand provides a guaranteed level of availability and reliability through a legal agreement called service level agreement (SLA) between the cloud provider and cloud user.

Increased Scalability, Availability & Reliability

- The recovery time after failure is the added penalty. It is the time when the system remains unavailable.

- The modular structure and resource redundancy in cloud increases the availability and reliability. It also improves the recovery time.

Cloud Computing

Challenges and Risks in Cloud Computing

Cloud Risks and Challenges

Vulnerability, security and trust issues

- The term *vulnerability* refers to a state of being attacked.
- Moving the business data to cloud can introduce vulnerabilities and security risks.

Cloud Risks and Challenges

- The term *security framework* refers to the procedures and practices for securing the resource such as data, network and IT infrastructure.

- Unless the cloud provider and cloud user are covered under same security framework, the vulnerabilities are unavoidable.

Cloud Risks and Challenges

- The cloud provider and user have to be in a *trust* relationship. The factors affecting the trust may include the following facts:
  - The data is being accessed remotely.
  - There are multiple users sharing the cloud based IT resources such as virtual storage.

Cloud Risks and Challenges

- The cloud provider has a privileged access to the users' data.

- The security of the data depends upon the security policies of the provider and the consumer.

Cloud Risks and Challenges

- There can be malicious consumers (human and automated) who can benefit from the security vulnerabilities of the cloud environment by stealing and/or damaging the business data.

Cloud Risks and Challenges

Reduced operational governance control:

- The cloud consumer gets a lesser privileged control over the resources leased from the cloud.
- There can be risks arising as to how the cloud provider manages the cloud.

Cloud Risks and Challenges

- An unreliable cloud provider may not abide by the guarantees offered in SLA of the cloud services. This will directly affect the quality of cloud consumer solutions (enterprise software) which rely upon these services.

Cloud Risks and Challenges

- The cloud consumer should keep track of actual level of service being provided by the cloud provider.

- The SLA violations can lead to penalties receivable from the cloud provider.

Cloud Risks and Challenges

Limited portability between cloud providers:

- Due to lack of industry standards for cloud computing, the public clouds environments remain proprietary to their providers.

Cloud Risks and Challenges

- It is quite challenging to move a custom-built software from one cloud to another if it has dependencies upon the proprietary environment (such as security framework) of the former cloud.

Cloud Risks and Challenges

Multi-regional compliance and legal issues:

- Cloud providers tend to set their data centers in regions favoring affordability and/or convenient. This may lead to legal issues for cloud provider as well as cloud consumers.

Cloud Risks and Challenges

- Some countries such as some UK laws require the personal data of UK citizens to be hosted inside UK.

- Thus a cloud provider with multi-regional data centers including UK, can not migrate the UK citizen's personal data outside UK.

- The UK citizen is legally bound to keep the personal data on clouds hosted in UK only.

Cloud Risks and Challenges

- Some countries such as USA allows government agencies' access to data hosted inside USA.

- Despite that the owners of this data are neither residing inside nor the citizens of USA, but still their data is accessible by the USA government agencies if hosted inside USA.

Cloud Computing

Roles and Boundaries in Cloud Computing

Roles and Boundaries in Clouds

- Cloud provider: The organization that provides the IT resources.

- Responsible for providing IT resources as per SLA.

- Also performs the management and administrative tasks to assure flawless provisioning of cloud services.

Roles and Boundaries in Clouds

- A cloud provider usually owns the IT resources of the cloud.

- It is also possible that the cloud provider resells the cloud services leased from another cloud providers.

Roles and Boundaries in Clouds

- Cloud consumer: The organization or individual who has contracted with cloud provider to lease/rent the cloud IT-resources through user interface and/or through software API calls.

- In the later case, a cloud consumer uses a *cloud service consumer* (a software program) to interact/use a cloud service.

Roles and Boundaries in Clouds

- Cloud Service Owner: Is the one who owns the cloud service. Can be:
  - Cloud consumer: If the deployed service is on leased IT-resources.
  - Cloud provider: If the cloud provider has deployed the service on cloud IT-resources.
- A cloud service owner may not be the owner of the cloud IT-resource.

END

Roles and Boundaries in Clouds

- Cloud Resource Administrator: This role is responsible for administering the cloud resources (including cloud services).

Roles and Boundaries in Clouds

- Cloud resource administrator can be:
  - Cloud consumer (as cloud service owner)
  - Cloud provider (when the service resides inside the cloud)
  - Third party contracted to administer a cloud service

Roles and Boundaries in Clouds

- Additional roles:
- Cloud Auditor: Provides an unbiased assessment of trust building features of the cloud. These include the security, privacy impact and performance of the cloud. The cloud consumer may rely upon the cloud audit report for choosing a cloud.

Roles and Boundaries in Clouds

- Cloud Broker: A party that provides mediation services to cloud providers (seller) and cloud consumers (buyer) for the purchasing of cloud services.
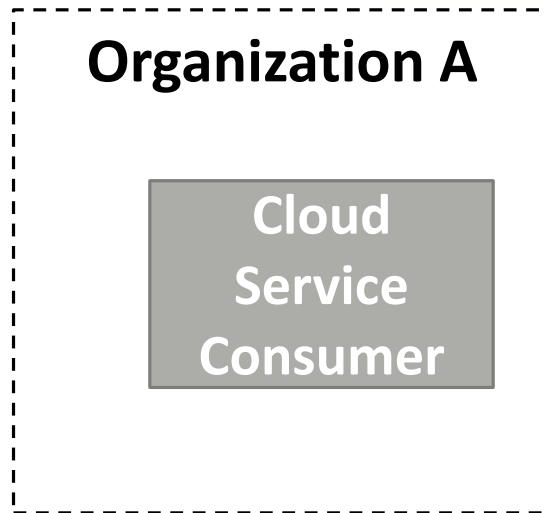
Roles and Boundaries in Clouds

- Cloud Carrier: The party responsible for providing connectivity between cloud provider and cloud consumer. The ISPs can be assumed as cloud carriers.

- The cloud provider and cloud carrier are in legal agreement (SLA) to assure a certain level of connectivity and network security.
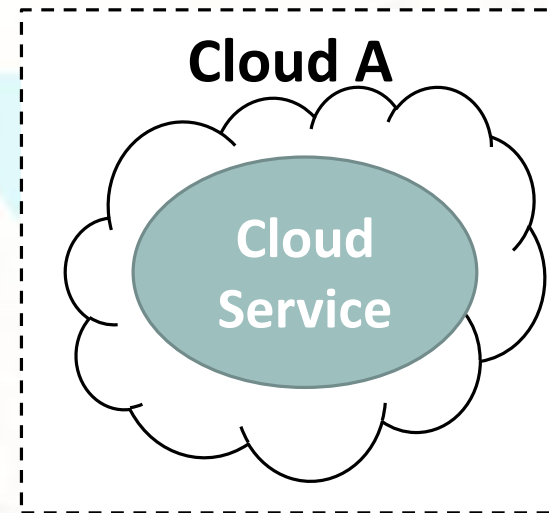
END

Roles and Boundaries in Clouds

- Organizational boundary: This is a boundary of ownership ad governance of IT assets of an organization.

- Similarly, the cloud has its organizational boundary.

Roles and Boundaries in Clouds

Organization A

Cloud Service Consumer

Cloud A

Cloud Service

Organizational boundary

Organizational boundary

Roles and Boundaries in Clouds

- Trust boundary: When an organization takes the role of cloud consumer, then it has to extend its trust boundary to include the cloud resources.

- A trust boundary represents a border around trusted IT-resources.

Roles and Boundaries in Clouds

Trust boundary

Organization A

Cloud Service Consumer

Cloud A

Cloud Service

Organizational boundary

Organizational boundary