Introduction to Cloud Technology

Third Module: Chapter - Selecting Cloud Service Provider

Topics in this chapter

1. **Introduction**
2. **About Leading cloud Service Provider**
3. **Imp: Considerations for Selecting the cloud Solution**
4. **Standards and Best Practices**
5. **Understanding the best Practices**
6. **Practical Issues to be considered**

1. Considerations for Selecting The cloud Solution

1) Business Considerations
2) Data Safety and Security
3) Interoperability, portability and Integration
4) Service level considerations
5) Pricing and commercials
6) Hosting and geographical considerations
7) Contingency and recovery management
8) Ethical and legal considerations
9) Scalability and flexibility considerations

1) Business considerations

- ➔ Organisations move to the cloud to overcome many inefficiencies and achieve higher operational parameters.
- ➔ If cloud vendor focuses too much on technical outcomes, chances are that they may not understand the business need of an organisation, such a partnership that fails to deliver services to business objectives.
- ➔ Hence choose a Cloud Service Provider with vast experience and expertise in the same industry. Such cloud provider will provide the optimum results.

2) Data Safety and security

- ➔ One of the biggest concern of moving to cloud is the security of the data that resides in the infrastructure of the cloud service provider.
- ➔ Working with trusted cloud service provider is the key to manage various security issues that arise in the cloud.
- ➔ Organisation must consider the following parameters in choosing the cloud service vendor:
  - i. Regulatory Compliance

ii. Segregation of data in multitenant environments
iii. Data Recovery
iv. Access Privileges
v. Probability of data for business continuity
vi. Data Provenance
vii. Monitoring and Reporting
viii. Network Security
ix. Data Encryption

➔ Additional evaluation measures that reflect the unique demands of an organisation must also be considered while choosing the cloud service provider.

3) Interoperability, Portability and Integration

i. **Interoperability:** It the degree to which system or components work together without any fault.

➔ According to IEEE, It can be defined as the ability of two or more systems or applications to exchange information and mutually use the information that has been exchanged.

➔ Interoperability can be defined as the capability of diverse systems to understand the application and interfaces, authentications, data formats etc between public, private and hybrid clouds.

➔ It helps all systems to cooperate and interoperate all works.
Eg: Google Authentication, all user can login to Gmail from a particular device and can use all the Google Services like Playstore, Google Docs, Google Drive etc.

ii. **Portability :** The ability to move an entity(data or application) between different systems to be used on the target system. Eg: Data stored on the database used by many systems

➔ The syntax and **semantics** of the data are to be same for the ease of portability. Eg: XML is the common format used for data portability used by multiple systems.

➔ Application portability is the ability to transfer a particular application or its components between different cloud services. The application should be able to recompile and relink to ensure ease of portability. **API** (Application Program Interface)makes application portability easier.

iii. **Integration :** It lets developers and users integrate the various functionalities together.

➔ Eg: youtube API, which includes the building blocks for Analytics, Data Capture, Youtube Player etc. Any user with an embed link can easily integrate the Youtue Video in their website. It ports all the necessary data and the application across different hosting platforms.

4) Service Level Considerations

➔ To determine the service level of a cloud vendor, there are three factors to be considered are :
i. Availability

ii. Performance
iii. Reliability

➔ **Availability :** It is the determined by the number of 'nines' mentioned in the SLA. Cloud service provider guarantee uptime of 99.9 or 99.999% uptime for an entire year.

➔ **Reliability :** It is determined through its transparency in operations. The cloud contract must include information about frequency of backups, fault tolerance rate, provider response in case of outages, information about scheduled downtimes for maintenance tasks. Exact location of data center is not revealed, but country or region where the data reside must be known for regulatory and legal purposes.

5) Pricing structure and Commercial Consideration

➔ Pricing structure is the major deciding factors for start-ups.

➔ A transparent cost structure that includes both one-time cost as well as the ongoing cost must be presented by cloud service provider.

➔ The pricing depends on different factors like security level, storage space etc.

➔ It must be flexible and must not carry any hidden costs.

➔ Review about previous prices of different organisations will help to understand the details of cost structure.

6) Hosting considerations

➔ Organisations must pick choose the cloud vendor based on their hosting expertise and ensure that it matched with the cloud requirements.

➔ Eg: A large or medium based enterprise moving into infrastructure to the cloud, can consider AWS(Amazon Web Services) as the best provider in the market space.

7) Geographical considerations

➔ Cloud Service provider carries the data across multiple locations in various geographic regions to mitigate risk such as localised outages, service latency and increased cost.

➔ Enterprise must know about the different locations of their data as the laws governing the storage and use of data vary with different locations.

➔ Violating the regulatory requirements can cause serious threats to data security.

➔ Organisations that wish to limit the geographic location must choose the cloud service provider accordingly.

➔ Contractual agreement and pre-engagement scrutinising are common measures to limit the geographic boundaries.

8) Contingency and Recovery Management

➔ The cloud vendor must be able to provide various data protection solutions in detail.

➔ Disaster Recovery(DR) measures must be implemented by the client organisation.

➔ The client must understand the DR features offered by cloud vendor and vendor's backup capabilities.

➔ Other factors to consider while choosing the Cloud service provider are :

i. DR Contingencies
ii. Location of the data center
iii. Recovery destination
iv. Data center features

9) Ethical and Legal considerations

➔ The cloud service provider and client(cloud consumer) must maintain a smooth relationship with the service provider and must ensure there is no financial loss in the form of legal penalties.

10) Scalability and Flexibility Considerations

➔ With the growth of organisations the cloud service provider must be able to scale up to accommodate the storage requirements and add new users into the system with no difficulty.

➔ The services must also be able to scale down resources when not in use.

➔ Dynamic Scaling makes business highly agile in competitive environment.

➔ Choosing right cloud service provider with a large range of options to security, performance, who can customise its needs and pay the cost of usage.

2. Standards and Best Practices

➔ With Standard practices have proved to mitigate risks and enhance the chances of cloud success.

Cloud computing Standards Organisations

➔ Cloud computing standard organisations are dedicated to address carious standards issues that arise in any cloud environment.

➔ They have defined guidelines and best practices to help interoperability and portability of data and applications.

➔ Examples of well known organisations are:

i. National Institute of Standards and Technology (NIST)
ii. Cloud Security Alliance
iii. Open Grid Forum (OGF)
iv. The Object Management Group (OMG)
v. Cloud Computing Interoperability forum (CCIF)
vi. Distributed Management Task Force (DMTF)
vii. Storage Networking Industry Association(SNIA)
viii. Open cloud Consortium(OCC)

3. Understanding Best Practices

i. Choose the right cloud service provider

➔ Choose the right vendor based on the availability, performance and security measures accordingly.

ii. Adopt a phased-in approach

➔ Organisations share their right of control over their data with the cloud vendors.

➔ In Phased-in approach, the organisation moves the data to the cloud only in parts rather than the whole thing into the cloud.

iii. Leverage the goodness of the cloud with creativity

➔ Cloud offers flexibility and scalability to enterprises. Organisation must be leverages the power of cloud to derive the best benefits.

iv. Audit to ensure better security in the cloud

➔ Regular assessment of problems, compliance of policies set earlier and identification of required upgrades must be performed to endure the highest level of security for the cloud system. Audit tools are used to perform this.

v. Keep data closer to lower latency and costs.

➔ Placing data as close as possible to the compute and processing resources reduces latency and shipping cost.

➔ It reduces the amount organisations need to pay for the bandwidth used in the cloud.

4. Practical Issues to be Considered

1. Proper negotiation of SLA.
2. Vendor Lock-in
3. Change in Organisational culture
4. Compliance and security of data
5. Commercial implication of shipping large volumes of data
6. Integration of the cloud into the existing system.

****