1.6. Design Challenges

Six open challenges in cloud architecture development

- Service Availability and Data Lock-in Problem.
- Data Privacy and Security.
- Unpredictable Performance and Bottlenecks.
- Distributed Storage and Wide Spread Bugs
- Cloud Scalability, Interoperability and Standardization.
- Software Licensing

Challenge 1: Service Availability and Data Lock-in Problem Service Availability

Service Availability in Cloud might be affected because of

- Single Point Failure Distributed
- Denial of Service
- Single Point Failure
  - Depending on single service provider might result in failure.
  - In case of single service providers, even if company has multiple data centers located in different geographic regions, it may have **common software infrastructure and accounting systems**.

Solution:

- Multiple cloud providers may provide more protection from failures and they provide High Availability (HA)
- Multiple cloud Providers will rescue the loss of all data.

Distributed Denial of service (DDoS) attacks.

- Cyber criminals, attack target websites and online services and makes services unavailable to users.
- DDoS tries to overwhelm (disturb) the services unavailable to user by having more traffic than the server or network can accommodate.

Solution:

- Some SaaS providers provide the opportunity to defend against DDoS attacks by using quick scale-ups.

Customers cannot easily extract their data and programs from one site to run on another.

Solution:

- Have standardization among service providers so that customers can deploy(install) services and data across multiple cloud providers.

Data Lock-in

- It is a situation in which a customer using service of a provider cannot be moved to another service provider because technologies used by a provider will be incompatible with other providers?
- This makes a customer dependent on a vendor for services and makes customer unable to use service of another vendor.

Solution:

- Have standardization (in technologies) among service providers so that customers can easily move from a service provider to another.

Challenge 2 : Data Privacy and Security Concerns

Cloud services are prone to attacks because they are accessed through internet. Security is given by Storing the encrypted data in to cloud.

- Firewalls, filters. Cloud environment attacks include
- Guest hopping
- Hijacking
- VM rootkits.

Guest Hopping: Virtual machine hyper jumping (VM jumping) is an attack method that exploits (make use of) hypervisor's weakness that allows a virtual machine (VM) to be accessed from another. Hijacking: Hijacking is a type of network security attack in which the attacker takes control of a communication.

VM Rootkit: is a collection of malicious (harmful) computer software, designed to enable access to a computer that is not otherwise allowed.

A **man-in-the-middle (MITM)** attack is a form of eavesdropping (Spy) where communication between two users is monitored and modified by an unauthorized party.

o Man-in-the-middle attack may take place **during VM migrations** [virtual machine (VM) migration - VM is moved from one physical host to another host].

Passive attacks steal sensitive data or passwords.

Active attacks may manipulate (control) kernel data structures which will cause major damage to cloud servers.

Challenge 3: Unpredictable Performance and Bottlenecks

- Multiple VMs can share CPUs and main memory in cloud computing, but I/O sharing is problematic.
- Internet applications continue to become more data- intensive (handles huge amount of data).
- Handling huge amount of data (data intensive) is a bottleneck in cloud environment.
- Weak Servers that does not provide data transfers properly must be removed from cloud environment

Challenge 4: Distributed Storage and Widespread Software Bugs

- The database is always growing in cloud applications.
- There is a need to create a storage system that meets this growth.
- This demands the design of efficient distributed SANs (Storage Area Network of Storage devices).
- Data centers must meet
  - Scalability
  - Data durability
  - HA(High Availability)
  - Data consistence
- Bug refers to errors in software.
- Debugging must be done in data centres.

Challenge 5: Cloud Scalability, Interoperability and Standardization Cloud Scalability

- Cloud resources are scalable.
- Cost increases when storage and network band width scaled (increased).

Interoperability

- Open Virtualization Format(OVF) describes an open, secure, portable, efficient, and extensible format for the packaging and distribution of VMs.
- OVF defines a transport mechanism for VM, which can be applied to different virtualization platforms.

Standardization

- Cloud standardization, should have ability for virtual machine to run on any virtual platform.

Challenge 6: Software Licensing and Reputation Sharing

- Cloud providers can use both pay-for-use and bulk-use licensing schemes to widen the business coverage.
- Cloud providers must create reputation-guarding services similar to the “trusted e-mail” services.
- Cloud providers want legal liability to remain with the customer, and vice versa.