Architectural Design Challenges

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

o Depending on single service provider might result in failure.

o In case of single service providers, even if company has multiple data centres located in different geographic regions, it may have **common software infrastructure and accounting systems**.

Solution:

o Multiple cloud providers may provide more protection from failures and they provide High Availability (HA)

o Multiple cloud Providers will rescue the loss of all data.

Distributed Denial of service (DDoS) attacks.

o Cyber criminals, attack target websites and online services and makes services unavailable to users.

o DDoS tries to overwhelm (disturb) the services unavailable to user by having more traffic than the server or network can accommodate.

Solution:

o 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:

o 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:

o 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

o Storing the encrypted data in to cloud.

o Firewalls, filters.

- Cloud environment attacks include

o Guest hopping

o Hijacking

o 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 enableaccess to a computer that is not otherwise allowed.
- A **man-in-the-middle (MITM)** attack is a form of eavesdroppping(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 centres must meet

o Scalability

o Data durability

o HA(High Availability)

o 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 bandwidth 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, that 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.

3.6. Cloud Storage

- Storing your data on the storage of a cloud service provider rather than on a local system.
- Data stored on the cloud are accessed through Internet.
- Cloud Service Provider provides Storage as a Service

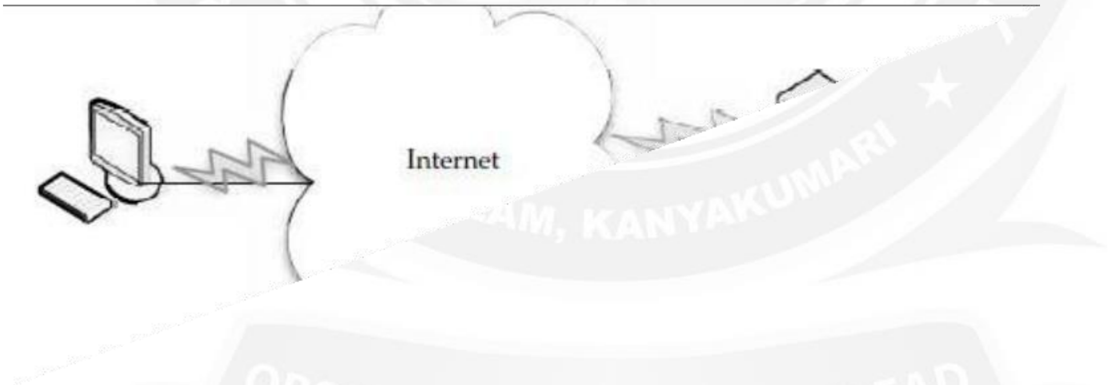
3.6.1 Storage as a Service

- Third-party provider rents space on their storage to cloud users.
- Customers move to cloud storage when they lack in budget for having their own storage.
- Storage service providers takes the responsibility of taking current backup, replication, and disaster recovery needs.
- Small and medium-sized businesses can make use of Cloud Storage
- Storage is rented from the provider using a

o cost-per-gigabyte-stored **(or)**

o cost-per-data-transferred

- The end user doesn’t have to pay for infrastructure (resources), they have to pay only for how much they transfer and save on the provider’s storage.



5.2 Providers

- Google Docs allows users to upload documents, spreadsheets, and presentations to Google’s data servers.
- Those files can then be edited using a Google application.
- Web email providers like Gmail, Hotmail, and Yahoo! Mail, store email messages on their own servers.
- Users can access their email from computers and other devices connected to the Internet.
- Flicker and Picasa host millions of digital photographs, Users can create their own online photo albums.

- YouTube hosts millions of user-uploaded video files.
- Hostmonster and GoDaddy store files and data for many client web sites.
- Facebook and MySpace are social networking sites and allow members to post pictures and other content. That content is stored on the company’s servers.
- MediaMax and Strongspace offer storage space for any kind of digital data.

3.6.2 Data Security

- To secure data, most systems use a combination of techniques:

o Encryption

o Authentication

o Authorization

Encryption

o Algorithms are used to encode information. To decode the information keys are required.

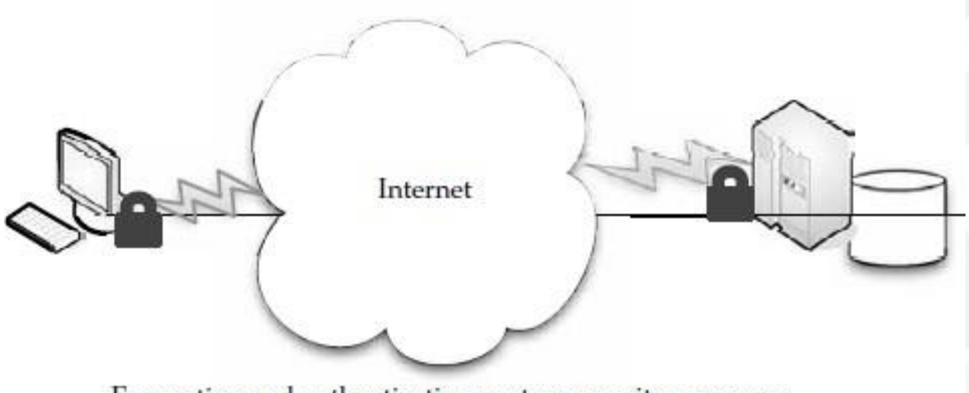
Authentication processes

o This requires a user to create a name and password.

Authorization practices

o The client lists the people who are authorized to access information stored on the cloud system.

If information stored on the cloud, the head of the IT department might have complete and free access to everything.



Encryption and authentication are two security measures you can use to keep your data safe on a cloud storage provider.

Reliability

- Service Providers gives reliability for data through redundancy (maintaining multiple copies of data).

Reputation is important to cloud storage providers. If there is a perception that the provider is unreliable, they won’t have many clients.

Advantages

- Cloud storage providers balance server loads.
- Move data among various datacenters, ensuring that information is stored close and thereby available quickly to where it is used.
- It allows to protect the data in case there's a disaster.
- Some products are agent-based and the application automatically transfers information to the cloud via FTP

Cautions

- Don't commit everything to the cloud, but use it for a few, noncritical purposes.
- Large enterprises might have difficulty with vendors like Google or Amazon.
- Forced to rewrite solutions for their applications.
- Lack of portability.

Theft (Disadvantage)

- User data could be stolen or viewed by those who are not authorized to see it.
- Whenever user data is let out of their own datacenter, risk trouble occurs from a security point of view.
- If user store data on the cloud, make sure user encrypts data and secures data transit with technologies like SSL.