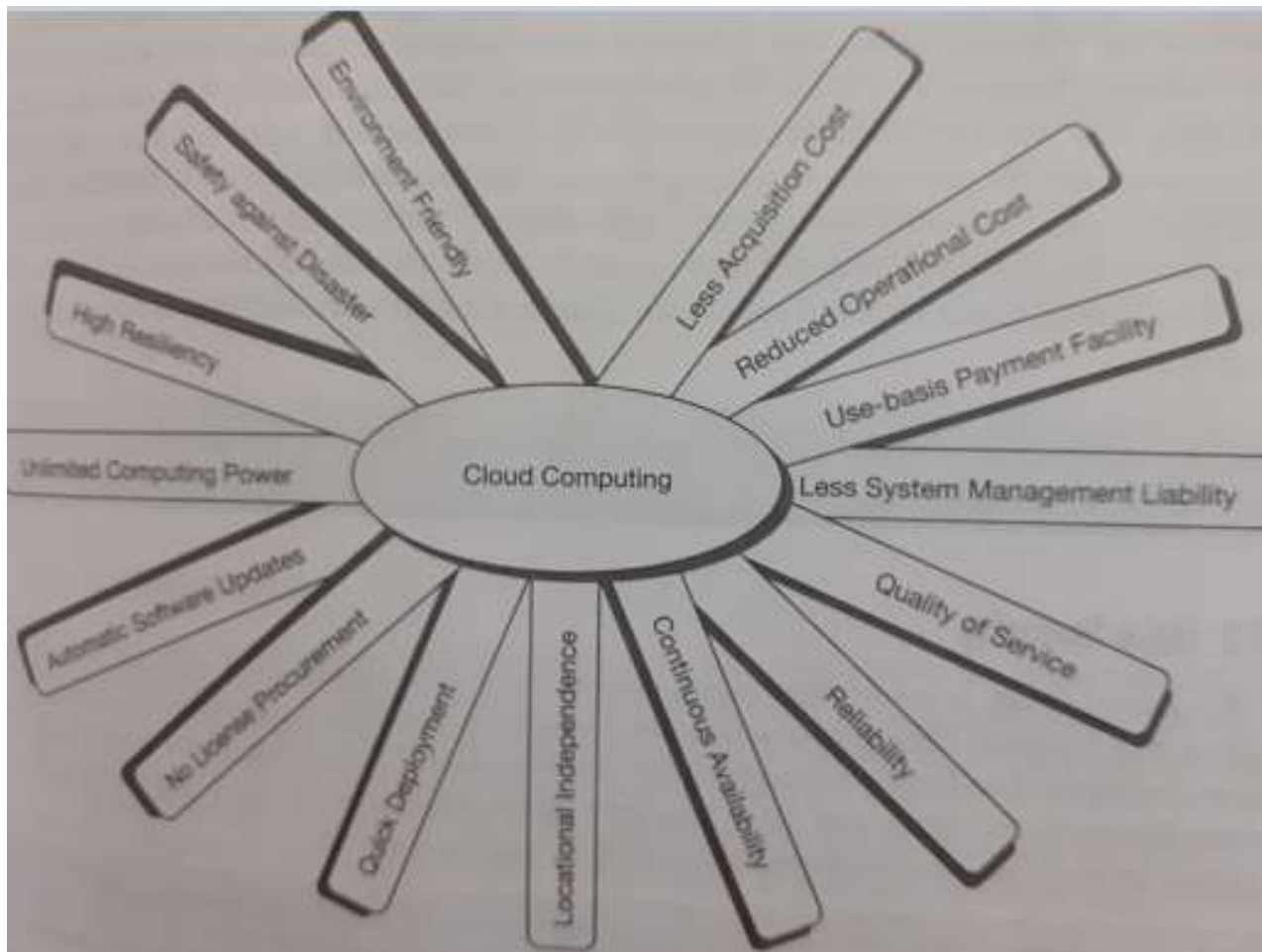


Benefits:



Quality of Service



- Everything in cloud computing is delivered as service
 - So quality of service is inevitable
 - QoS has multiple aspects such as:
 - Response time
 - Throughput
 - Availability
 - Reliability
 - Security
-
- You need cloud scalability to meet customer demand.
 - You need cloud reliability to ensure that your products and services work as expected.
 - You need cloud availability to ensure that customers can access your cloud services whenever they need to and from anywhere in the world.

What is reliability in cloud computing?

When you access an app or service in the cloud, you can reasonably expect that:

- The app or service is up and running.
- You can access what you need from any device at any time from any location.
- There will be no interruptions or downtime.
- Your connection is secure.
- You will be able to perform the tasks you need to get your job done.

Factors like these measure the reliability of your cloud offerings. In a perfect world, your system would be 100% reliable.

Service Level Agreement, SLA



- ❑ The SLA is a contract negotiated and agreed between a customer and a service provider
- ❑ Service provider is required to execute service requests from a customer within negotiated quality of service requirements for a given price
- ❑ Due to variable load, dynamically provisioning computing resources to meet an SLA and allow for an optimum resource utilization will not be an easy task

What is Cloud Resiliency?

Cloud resiliency is the term used to describe the **ability of a server, storage system, data server, or entire network to both recover and continue operations without systems connected** to the network going down, stopping their function, or losing their operational capabilities.

What is cloud disaster recovery?

Cloud disaster recovery (CDR) is a cloud-based managed service that helps you quickly recover your organization's critical systems after a disaster and provides you remote access to your systems in a secure virtual environment.

When it comes to traditional DR, managing a secondary data center can be time consuming and costly. Cloud disaster recovery has changed everything when it comes to traditional DR by eliminating the need for traditional infrastructure and significantly reducing downtime. IT departments can now harness the power of the cloud for immediate spin-up and fail over. This creates faster recovery times at a fraction of the cost.

How does cloud disaster recovery work?

Cloud disaster recovery takes a very different approach than traditional DR. Instead of loading the servers with the OS and application software and patching to the last configuration used in production, cloud disaster recovery encapsulates the entire server, which includes the operating system, applications, patches, and data into a single software bundle or virtual server. The virtual server is then copied or backed up to an offsite data center or spun up on a virtual host in

minutes. Since the virtual server is not dependent on hardware, the operating system, applications, patches, and data can be migrated from one data center to another much faster than traditional DR approaches.

Challenges:

Limited Portability

Inter-operability

Data Security

Reduced control over governance

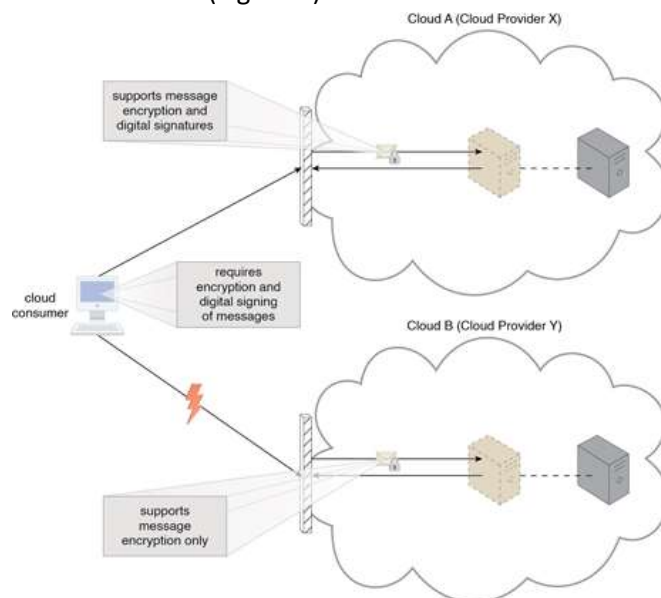
Regional compliance and legal issues

Bandwidth cost

Limited Portability Between Cloud Providers

Due to a lack of established industry standards within the cloud computing industry, public clouds are commonly proprietary to various extents. For cloud consumers that have custom-built solutions with dependencies on these proprietary environments, it can be challenging to move from one cloud provider to another.

Portability is a measure used to determine the impact of moving cloud consumer IT resources and data between clouds (Figure 1).



Interoperability is the ability of two or more systems or applications to exchange information and to mutually use the information that has been exchanged.

Cloud interoperability is the ability of a customer's system to interact with a cloud service or the ability for one cloud service to interact with other cloud services by exchanging information according to a prescribed method to obtain predictable results.

Bandwidth cost

If the customer's application is only sending data and consuming bandwidth 12 hours a day — all of its users are in North America — during 20 business days, that means that the customer is effectively using 1.85 megabits per second of bandwidth during the month (200 gigabytes per month divided by the sum of 20 days times 12 hours in a day times 60 minutes an hour times 60 seconds per minute). Put another way, the customer's \$30 per month equates to a bandwidth charge of \$16.20 per megabit (\$30 divided by 1.85 megabits per second).

Cloud service providers buy a lot of bandwidth to provide access to the Internet. My market research (albeit not exhaustive) puts the current price per megabit of bandwidth for a large cloud provider at around \$8. That means that for the 1.85 megabits per second that the customer uses, Azure effectively pays \$14.81 to its bandwidth provider and keeps \$15.91, or 51 percent gross profit — not a bad profit margin on a commodity business like bandwidth. To be fair, other cloud service providers, like Amazon (s amzn) and Rackspace, (s rax) charge similar or higher bandwidth fees and likely make similar gross profits

References

- *Cloud Computing*, Sandeep Bhowmik
- *Internet*
- The Hidden Cost of the Cloud: Bandwidth Charges
 - <https://gigaom.com/2009/07/17/the-hidden-cost-of-the-cloud-bandwidth-charges/#:~:text=Cloud%20service%20providers%20buy%20a,cloud%20provider%20at%20around%20%248>.