



BACHELOR OF COMPUTER APPLICATIONS SEMESTER 6

DCA3243 CLOUD COMPUTING

Unit 8

Information Storage in Cloud Computing

Table of Contents

SL No	Topic	Fig No / Table / Graph	SAQ / Activity	Page No
1	Introduction	-	-	3
1.1	Objectives	-	-	
2	Storage as a Service	1	1	4-8
3	Storage Providers	-	2	8-15
3.1	Amazon simple storage service	2	-	
3.2	Nirvanix	-	-	
3.3	Google bigtable datastore	-	-	
3.4	MobileMe	-	-	
3.5	Live mesh	-	-	
4	Cloud Data Security	-	3	16-20
5	Merits and Demerits of Cloud Storage	-	4	21-22
6	Summary	-	-	23
7	Terminal Questions	-	-	24
8	Answers	-	-	25

1. INTRODUCTION

Cloud storage is one of the prospective services that can be provided either to individuals or to organisations with the support of cloud computing models. It is the other form of networked online storage, which is quite different from the traditional storage method. This also represents the growth dimension of cloud technology towards business. Cloud Storage follows the disk storage that exists on offsite systems, usually maintained by a third party. Traditional media like flash drives and optical discs allow access to the end user directly, whereas PC and other devices have their own storage devices.

The data stored on the cloud is accessed only through network resources. Corporations traditionally own their own computer resources that can be accessed through their private network. With cloud storage, an organisation or an individual does not own hardware or specify the physical location of their data. Moreover, resources are virtualised in that the outward storage space does not specify an actual device. For example, the user may be provided with one terabyte storage volume in an actual disc drive, but originally, the data may be available on multiple drives and spread across many different locations. In this unit, we are going to discuss the services.

Provided by the cloud for storage, the list of cloud storage providers. We are also going to explore cloud data security and its merits and demerits.

1.1 Objectives

After studying this unit, you should be able to:

- ❖ *Explain the various cloud storage services.*
- ❖ *List the cloud storage providers in the market.*
- ❖ *Discuss cloud storage security.*
- ❖ *Clarify the merits and demerits of cloud storage.*

2. STORAGE AS A SERVICE

Storage as a Service is a business model in which a large company rents space in their storage infrastructure to a smaller company or individual. In the enterprise, SaaS vendors are targeting secondary storage applications by promoting SaaS as a convenient way to manage backups. Storage as a service is one of the important categories under cloud services. As the name indicates, it has the ability to provide leverage storage, which may be available or exist remotely. However, it is logically local to the application, which requires storage, as depicted in Figure 8.1. Storage as a service is considered to be one of the most important components of cloud computing, and it is very much influenced or supported by the other components of cloud computing.

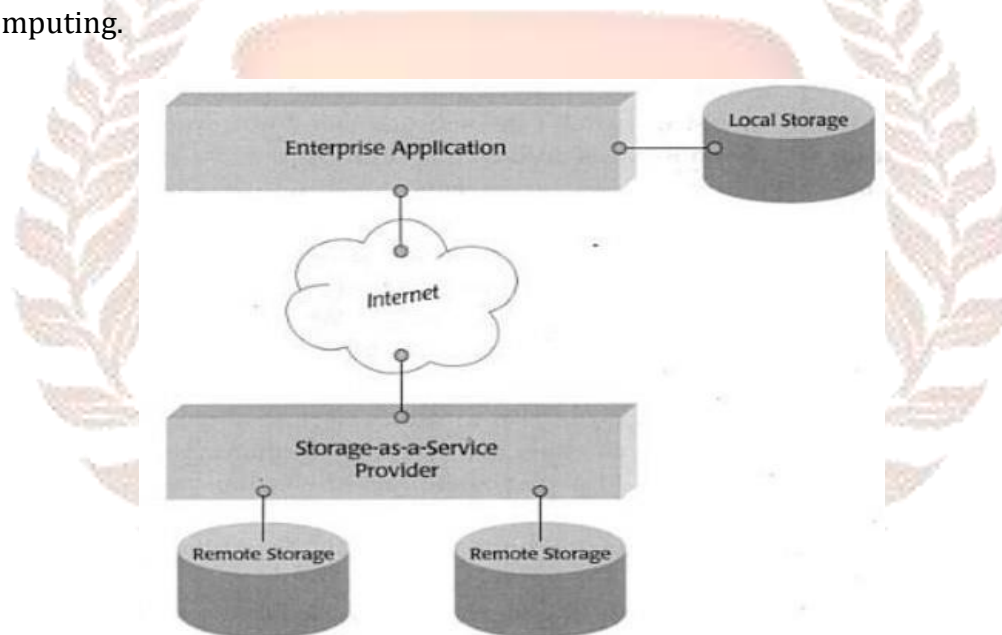


Fig: 8.1: Storage as a service allows to store remotely available locally

You may ask a question now that it is a waste to use the internet to access the disk, which is remotely available since the disk space is so cheap. One way this looks correct, but now we are going to discuss the core benefits of this remote disk access.

One important idea behind this is that you can expand the usage of disk space based on your need, and it is enough to pay for the amount that you utilise. This leads to the effective utilisation of disk as well as cost benefits. This cost benefit is purely applicable to those who are utilising more than 500 gigabytes either through direct access or by utilising the disk as if it were local to your client's computer.

The Backbone is SAN (Storage Area Networks):

A storage area network, or SAN, is a specialised, fast network that gives storage devices network access. Hosts, switches, storage components, and storage devices make up standard SAN configurations. These components are connected to one another via a range of technologies, topologies, and protocols. SANs may connect various locations.

Computer hard drives can only store a finite amount of data. When users run out of storage, they need to transfer files to an external storage device.

Traditionally, organisations built and maintained storage area networks (SANs) to archive data and files.

SANs are expensive to maintain, however, because as stored data grows, companies must invest in adding servers and infrastructure to accommodate increased demand.

This concept can also be utilised as a redundant backup for critical files. The next important advantage is that, as the user, you need not be involved in the maintenance of the hardware. During the shutdown of drives or devices, the replacement and repair processes are taken care of by the service providers. As users, we can stay away from such issues. Finally, storage as a service process provides you with disaster recovery support and getting back the deleted files or folders is also part of its service.

The service provider provides backup and restore file systems as per your requirements. There is no charge imposed to maintain the storage system, which will be taken care of by the service providers' officials internally. Looking at the other side of this process, there are some drawbacks also; as a user of the remote disk, you need to depend on internet support. If there is any problem with the network connectivity or network down, the user will have trouble accessing the disk.

There is no sense if there is a temporary loss of connection during your important mission. In many cases, those who leverage storage as a service are surprised to find that they cannot access their shared disk space when not connected to the internet. The next issue may be on the performance compared to on-premises storage, which is available physically near the application. When performance is the critical factor for the storage as the service, the user may not be interested in implementing this process. Performance is generally about half the

speed of the typical internet connection when compared with the local network. Of course, to compensate for this, one can use a faster connection, but again, it affects your cost calculation. The cost of the storage as a service can be high when compared with the on-premises solution. While SOA (Service Oriented Architecture) using cloud computing is cost-effective in some instances, it is not in many situations. The cost-effectiveness of cloud computing depends on the enterprise and domain. For example, a shared disk in storage as a service solution would be of high value for a virtual business with a

Cloud storage benefits include:

- Easy storing, accessing, and protecting your data via the internet.
- You can streamline work and outdated storage systems by uploading nearly any file and accessing it from multiple devices.
- You can also rest easy knowing all your important data is backed up in a safe, offsite location.
- This is especially useful in times of disaster recovery and if your hard drive lets you down.
- Reducing resources used to manage data is an additional benefit of online storage for businesses.

Cloud Storage Classes:

As an example -The Google Cloud Storage - Storage class has an impact on the object's accessibility and cost structure. An existing object's storage class can be updated by rewriting it or by using object lifecycle management.

Cloud storage can be broadly classified into two categories:

1. Unmanaged Cloud Storage
2. Managed Cloud Storage

Google Cloud Storage:

Google Cloud Storage is an enterprise public cloud storage platform that can house large unstructured data sets.

Google Cloud Storage customers access their data through a web browser or command-line interface. It provides unified object storage for live or archived data.

Objects stored in Google Cloud Storage are grouped into buckets. Buckets are containers within the cloud that can be individually assigned to storage classes.

Your objects can be stored in Google Cloud using the service known as cloud storage. A file in any format that makes up an object is an immutable piece of data. In bucket-style containers, you store items. Each bucket has a corresponding project, and you can organise your projects into groups called organisations.

Google Cloud Storage offers four storage classes:

1. Multi-Regional
2. Regional
3. Nearline and
4. Coldline

Google Cloud Storage System:

Large unstructured data sets can be stored on the public cloud storage platform for businesses called Google Cloud Storage. Companies might buy the storage for important or rarely used data.

The cloud storage system stores multiple copies of data on multiple servers at multiple locations.

If one system fails, then it is required only to change the pointer to the location where the object is stored.

Storage GRID:

It is a collection of software-defined object storage that covers several use cases in private, public, and hybrid multi-cloud systems.

1. Storage Area Network (SAN) is used to transfer data between a server and storage devices using fibre channels and switches.
2. Data is denoted by disk blocks. SAN uses SCSI, SATA protocols.
3. Network Attached Storage (NAS) uses files to store data blocks. Here, data is identified by file name as well as byte offset. Here, the file system is managed by the CPU and memory as Head Unit.

Distributed employee base. It would save on hardware maintenance and would provide easy and shared disk space as well.

SELF-ASSESSMENT QUESTIONS – 1

1. _____ is a business model in which a large company rents space for smaller companies.
2. Cloud storage service allows for the storage to be remotely made available locally state [True/False].
3. SOA Stands for. _____
 - a) Service Oriented Architecture
 - b) Servile Object Architecture
 - c) Storage Over Architecture
 - d) Storage Object Architecture

3. STORAGE PROVIDERS

If you see globally in cloud storage service, data is stored on hundreds of servers with redundancy. Here, the provider rents the storage to the client, and the cost is calculated on a cost-per-gigabyte or cost-per-transferred data basis.

The following are the popular service providers in the market.

- Google Docs
- Webmail providers (Gmail, Hotmail, yahoo)
- Youtube, Facebook, GoDaddy.
- Amazon Simple Storage Service (S3)
- Nirvanix
- Google Bigtable Datastore

There are **several different forms of services** that can be used in the cloud by CSPs, including.

- Software, often referred to as Software as a Service (SaaS).
- A computing platform for developing or hosting applications, known as Platform as a Service (PaaS)

- An entire networking or computing infrastructure, known as Infrastructure as a Service (IaaS).
- Rather than individuals and companies building their own infrastructure to support internal services and applications, the services can be purchased from the CSP, which provides the services to many customers from a shared infrastructure.

Functions of Cloud Storage Providers:

- Location of data centers
- Security
- Cost
- Performance
- Availability
- Integration
- Manageability
- Scalability
- Vendor lock-in potential

Cloud Storage Pricing:

- Cloud storage helps companies cut costs by eliminating in-house storage infrastructure.
- But cloud storage pricing models vary.
- Some cloud storage providers charge monthly the cost per gigabyte, while others charge fees based on stored capacity.
- Fees vary widely; you may pay \$1.99 or \$10 for 100 GB of storage monthly, based on the provider you choose.
- Additional fees for transferring data from your network to the fees based on the storage cloud are usually included in the overall service price.

In this section, we will focus on a few popular storage providers and their services.

3.1 Amazon Simple Storage Service

Amazon s3 Simple storage service is an online storage web service provided by AWS (Amazon Web Services). It supports storage through web service interfaces. “Amazon

launched S3, its first publicly available web service, in the United States in March 2006 and in Europe in November 2007”.

Amazon S3 is the storage for the internet. Using this, you can store and retrieve any amount of data at any time and anywhere on the web. This concept is achieved with the help of the AWS management console web interface. The complete task of AWS management is shown in Figure 8.2



Fig: 8.2: AWS management console task

Amazon s3 objects are comprised of files and metadata that describe the files here; the data are stored in the form of objects inside the buckets. To store an object in Amazon S3, upload the file which you need to store to a bucket. When you upload a file, you can set permissions on the object as well as any metadata. When you want to upload a file to Amazon s3, it needs to be stored in the bucket. While uploading the object, you can set permissions to the concerned object. Here, the buckets act as containers; you can have one or more buckets with access control.

A bucket can be stored in one of several regions. You can choose a region in order to optimise for latency, minimise costs, or address regulatory requirements. Amazon S3 is currently available in the US Standard, US West (Oregon), US West (Northern California), EU (Ireland), Asia Pacific (Singapore), Asia Pacific (Tokyo), South America (Sao Paulo), and GovCloud (US) Regions. The US Standard region automatically routes requests to facilities in Northern Virginia or the Pacific Northwest through network maps.

Objects stored in a particular region never leave the current region unless it is explicitly transferred. Objects can be set either private or public, and individual users can be given access rights or permission. Data is secured from unauthorised access with the proper authenticated mechanism. Encrypted forms of uploading and downloading data provide proper security. Its flexibility supports adding protocol or functional layers, and the default download protocol is HTTP.

3.2 Nirvanix

It is a “provider of enterprise-class cloud storage services with headquarters in San Diego, California, United States. The company deals with public, hybrid and private cloud storage services, all with usage-based pricing and accessible via HTTP using the Nirvanix Web Services API”.

Nirvanix announced that the National Geographic Society has moved its backup and archival of large unstructured multi-media files to the Nirvanix Cloud Storage Network to take advantage of the economic and on-demand quick benefits that the cloud brings. With the growth of their unstructured

For content files, the National Geographic Society needed an alternative to the traditional approach of continually buying physical storage capacity for their archival needs. With the Nirvanix CloudNAS Gateway, they were able to encrypt data both in flight and at rest, as well as securely transfer data to any of Nirvanix's eight globally distributed cloud storage data centres. The following are some of the key features of the Nirvanix Cloud Storage Network:

- 24x7 monitoring with mobile and e-mail alerts to system administration staff for all processes.
- Automatic intrusion detection and monitoring
- SSL support for data to/from the Cloud Storage Network
- Robust encryption support for data uploads
- Strong password authentication
- De-identified physical file architecture requiring a 3-step key to link files to users.
- Token-based authentication with server-side session management
- Stringent enforcement of information security policy
- RAID 6 data storage at single or multiple nodes
- Checksum error checking and internal integrity checks

3.3 Google Bigtable Datastore

It is not so easy to design highly scalable and data-intensive applications to design. If you've ever used hardware or software load balancing, you must have experienced the users may be interacting with many web and database servers. The user's request may not necessarily be serviced by the same server that handled his previous request. These servers may be

available in different data centres or perhaps in different countries, requiring you to implement processes to keep your data secure, safe and synchronised. The hardware and software required to scale your application

It can also be complex and expensive and may even dictate that you outsource or hire dedicated resources.

The App Engine datastore provides distribution, replication, and load-balancing services behind the scenes, which helps you focus only on implementing business logic. (GFS). Bigtable is a highly distributed and scalable service for storing App Engine's datastore. It is driven mainly by two Google services, Bigtable and Google File System, and it manages structured data. It was designed to scale to an extremely large size with petabytes of data across thousands of clustered commodity servers. It is the same service that Google uses for over 60 of its own projects, including web indexing, Google Finance, and Google Earth. The first thing which you can observe in Bigtable is that it is not a relational database. Bigtable uses a non-relationship object model to store entities and supports you in creating simple, fast, and scalable applications.

These unique characteristics imply a different way of designing and managing data to take advantage of the ability to scale automatically. In particular, the App Engine Datastore differs from a traditional relational in the following important ways:

- The App Engine Datastore is designed to scale, allowing applications to maintain high performance as they receive more traffic:
 - Datastore writes scale by automatically allocating data as necessary.
 - Datastore reads scale because the only queries supported are those whose performance scales with the size of the result set (as opposed to the data set). This means that a query whose result set contains 100 entities performs the same whether it searches over a hundred entities or a million. This property is the key reason some types of queries are not supported.
- Because pre-built indexes serve all queries on App Engine, the types of query that can be executed are more restrictive than those allowed on a relational database with SQL. In particular, the following are not supported:
 - Join operations.

- Inequality filtering on multiple properties
- Filtering of data based on results of a sub-query.
- Unlike traditional relational databases, the App Engine Datastore doesn't require entities of the same kind to have a consistent property set (although you can choose to enforce such a requirement in your own

Application code). It is not currently possible for a query to return only a subset of the result entities' properties.

For more in-depth information about the design of the Datastore, read our series of articles on Mastering the Datastore.

3.4 Live mesh

Live Mesh is Microsoft's "software-plus-services" platform and experience that enables PCs and other devices to be aware of each other through the internet, enabling individuals and organisations to manage, access, and share their files and applications seamlessly on the web and across their world of devices. Live Mesh has the following components.

- A platform that defines and models a user's digital relationships among devices, data, applications, and people made available to developers through an open data model and protocols.
- A cloud service providing an implementation of the platform hosted in Microsoft data centres.
- Software is a client implementation of the platform that enables local applications to run offline and interact seamlessly with the cloud.
- A platform experience that exposes the key benefits of the platform for bringing together a user's devices, files and applications, and social graph with news feeds across all of these.

Live Mesh is essentially a desktop in the cloud. Through Mesh, you can store files online to access them from any computer. You can also sync local files or folders stored on any PC, so those files appear in your Mesh and on any machines, you include in the sync.

To use Live Mesh, first go to the Live Mesh Web site and sign in with your Windows Live account. After accepting the terms of the software agreement, you'll see the Device window,

which displays an icon to your Live Desktop and an option to add devices you wish to sync. Your first step should be to connect to the Desktop, where you can access the “Get Started” help information and create a new folder to store the files you wish to upload.

By creating folders, you can use Live Mesh as a traditional online file storage site. To do that, double-click on the Create new folder icon and name the folder. After you open your new folder, you can now upload files, either one at a time by browsing to or typing their local path or several in one shot by dragging and dropping them onto the folder window. (Note that before you can drag and drop, you first must install a Live Desktop plug-in. For now, the drag-and-drop method works only in Internet Explorer.)

You can display the folders on your desktop as icons or in detail mode. You can also turn on a navigation pane so you see your folder tree on the left and a file list on the right. A Media Viewer can play certain audio and video content, such as WMA and WMV files, within Live Mesh. Double-clicking on most files and documents, however, prompts you to open them in their native applications, which need to be installed locally.

Though Live Mesh can serve as a simple online storage site, I find the tool most useful for its synchronisation capabilities. By adding computers to your Live Mesh network, you can sync folders and files between your Live Desktop and your PCs. Those of us who juggle more than one desktop or notebook can use Live Mesh to sync documents, browser favourites and other files across machines.

3.5 Terremark Worldwide, Inc.

It is a subsidiary of IBM, a company that offers IT services. The company, with its headquarters in Miami, Florida, operates data centres across the US, Europe, and Latin America. It provided managed hosting, colocation, disaster recovery, data storage, and cloud computing services.

Enterprises can choose to burst onto a public cloud using Terremark's new private cloud solution.

SELF-ASSESSMENT QUESTIONS – 2

4. In storage service cost for the client is calculated on cost per _____.
5. _____ is the first publicly available web service in the United States in March 2006
 - a) GoDaddy
 - b) Amazon web services
 - c) Nirvanix
 - d) Google Docs
6. Nirvanix has strong password authentication state [True/False]
7. The App Engine datastore provides, _____ and _____ services behind the scenes.
8. MobileMe is a subscription-based service by the company.
 - a) Cisco
 - b) Google
 - c) apple
 - d) IBM



4. CLOUD DATA SECURITY

Cloud providers identified the concern of cloud security and worked hard to address the issues. It is becoming one of the big challenges for cloud providers; soon, cloud security may reach the level of its own set-up security. The cloud provider needs to enforce strict security policies to impose additional trust for the clients. Military-grade security systems use special-purpose security hardware with great standards. Now, the same technology is extended to cloud computing technology called trusted computing.

Data security refers to the process of protecting data from unauthorised access and data corruption throughout its lifecycle.

Cloud data security consists of a set of policies, controls, procedures, and technologies that work together to protect data in the cloud.

The technology, policies, services, and security measures that guard against loss, leakage, or misuse of any form of data stored in the cloud via breaches, exfiltration, and unauthorised access are referred to as cloud data security.

These security measures are configured to protect cloud data, support regulatory compliance, and protect customers' privacy, as well as set authentication rules for individual users and devices.

From authenticating access to filtering traffic, cloud security can be configured to the exact needs of the business.

And because these rules can be configured and managed in one place, administration overheads are reduced, and IT teams are empowered to focus on other areas of the business.

Cloud Storage Protection Basics:

- A starting point for any cloud storage security initiative is to understand how data is stored in the cloud.
- At the most basic level, clouds rely on logical pools to store data across multiple servers.
- A storage service provider operates these systems off-premises and connects the entire environment through a control node.

- This control makes it possible for a person with an Internet connection to access files on demand.
- Such flexibility is increasingly critical as organisations look to become more agile and flexible.

To secure cloud-based apps, systems, the data they contain, and user access, an organisation must apply a variety of technological solutions, policies, and practices.

In the cloud computing environment, the security of data becomes serious because the data is in different places, even all over the globe.

Data security and privacy protection are the two main factors of user's concerns about cloud technology.

Data security and privacy protection issues are relevant to both hardware and software in cloud architecture.

Cloud computing environment provides two basic types of functions:

1. Computing: the supply of computing services via the Internet (the "cloud"), including servers, storage, databases, networking, software, analytics, and intelligence. This enables speedier innovation, adaptable resources, and scale economies.
2. Data storage: Digital data is saved on servers located off-site in a kind of computer data storage known as cloud storage.

Securing data at rest: Cryptographic encryption is certainly the best practice, and in many U.S. states and countries worldwide, it is the law for the cloud provider to secure data at rest. Now, hard drive manufacturers are shipping self-encrypting drives that support trusted storage standards. These drives build encryption hardware into the drive, providing automated encryption with performance impact or minimal cost. Software encryption can also be used; since the encryption key can be copied off the machine without detection, it is considered as less secure.

Securing data in transit: During transit, data encryption techniques can be used. Apart from this authentication and integrity protection, it ensures whether the data reaches the addressed customer with any modification in the data. Well-established protocols such as

SSL/TLS support to achieve the above task. But here, one more tricky and challenging job is authentication.

Authentication: It is one of the very basic actions for accessing data by allowing only authorised people. In the cloud environment, access control and authentication are more important than ever since the cloud, and all of its data are accessible to anyone over the Internet.

The TPM can easily provide stronger authentication than usernames and passwords. TCG's IF-MAP standard allows for real-time communication between the customer and the cloud provider about authorised users and other security issues. A customer's identity management system will immediately inform the cloud providers about the fired or reassigned users. This helps the user's cloud access to update accordingly to revoke the unauthorised. If such user tries to access, they can be immediately disconnected. Trusted Computing enables authentication of client PCs and other devices, which is also a critical process to ensure security in cloud computing.

Separation between customers: One of the most important cloud concerns is separation between a cloud provider's users to avoid accidental or intentional access to delicate information. Cloud providers would use virtual machines to separate customers. TCG technologies can provide significant security improvements for VM and virtual network separation.

In addition, the TPM can provide hardware-based verification of hypervisor and VM integrity. The TNC standards and architecture can provide robust security and network separation.

Cloud legal and regulatory issues: Cloud providers need to have legal and regulatory experts to check whether they have sufficient regulatory policies and procedures. These personnel need to verify whether these practices are effectively implemented for their adequacy. The issues that need attention are compliance, data security and export, data retention and destruction, auditing, and legal discovery. In the areas of data retention and deletion, Trusted Storage and TPM access techniques can play a key role in limiting access to data.

Incident response: As part of expecting the unexpected, customers need to plan for the possibility of cloud provider security breaches or user misbehaviour. An automated response or at least an automated notification is the best solution. TCG's IF-MAP (Metadata Access Protocol) specification enables the integration of different security systems and provides real-time notification of incidents and user misbehaviour.

Data Integrity:

- Verifying the integrity of data in the cloud remotely is the prerequisite to deploying applications.
- Bowers et al. proposed a theoretical framework, "Proofs of Retrievability," to realise remote data integrity checking by combining error correction code and spot-checking.
- The HAIL system employs the POR mechanism to examine how data is stored across many clouds. It can verify the redundancy of copies and perform availability and integrity checks.
- Schiffman et al. proposed a trusted platform module (TPM) remote checking to check the data integrity remotely.

The Techniques to Implement Data Integrity:

- Homomorphic Encryption
- Encrypted Search and Database
- Distributive Storage
- Hybrid Technique
- Data Concealment
- Deletion Confirmation

Identity Management in the cloud:

The word "identity management" (IM) refers to the information system employed by the company. This provides authentication, privileges, authorisation, and roles of the enterprise boundaries while also representing the systematic management of any single identity.

Cloud computing provides a platform for a wide range of Internet-based services.

But besides its advantages, it also increases the security threat when a trusted third party is involved.

By involving a trusted third party, there is a chance of heterogeneity of users, which affects security in the cloud.

A possible solution to this problem could be to use a trusted third-party independent approach for Identity Management to use identity data on untrusted hosts.

Different levels of protection can be used to prevent data leakage and privacy loss in the cloud.

SELF-ASSESSMENT QUESTIONS - 3

9. _____ It is an international standard having high-security components in computers.
- a) Trusted networks connect.
 - b) Trusted storage
 - c) Trusted platform module
 - d) None of the above

5. MERITS AND DEMERITS OF CLOUD STORAGE

There are several advantages of the cloud storage model compared to networked online storage and individual storage. The data stored in the end-user device cannot be accessed easily by others, whereas the cloud storage data is with a third party. In cloud storage, since it is with a third party, they are more prone to loss or theft. Networked storage devices address those problems, but they still require both human and physical resources that an individual or a corporation may not possess. For example, creating a redundant storage array and backing it up is outside the skill set of most people, while building and maintaining a data centre is beyond the core capabilities of most organisations. It is a wise decision to choose cloud storage since it is more efficient and scalable than calculating the

Storage is required to store the data, and purchasing is required for this purpose. At the same time, cloud users need to pay only for what they want or for the quantity they utilise. Cloud storage is a feasible solution that can grow instinctively to meet increased demand. This also focuses on the economy of scale when many individuals and organisations decide to store their data on the same systems, which are managed by a single provider.

Merits:

- It is possible to access the data from any location where you have an internet facility with that system.
- Implementation can be simple.
- It is easy and efficient to expand the service based on the organisation's needs.
- Various parties can be permitted to access your data.
- There's no need to physically manage storage (fix bad disks, backup data) if the storage is bundled as an outsourced managed service.

Demerits:

Having difficulty accessing your data can be unsatisfying for the individual or to an organisation and losing it altogether can be tragic. At the same time, most individuals and organisations lack the skills and resources to store and maintain their data properly. For these reasons, cloud storage services are now being used by everyone, from individual users to large corporations.

- Performance can be affected by traffic on the internet. The access speed of the remote storage will never match with local access.
- Security is a very challenging concern. When a company's sensitive data is transported over an insecure network such as the Internet, there's a possible risk of exposure. But even a corporate network has its own risks. Rigorous security practices may reduce this problem.
- There is a chance for a dramatic price hike if the usage is not monitored carefully. Out of sight should not be out of mind; Cloud Storage needs to be proactively supervised.

The experience of Signal Creek technology, a cloud storage support provider in the market, is shared as "Based on our experience at Signal Creek with a range of our partners, the state of Cloud Storage today seems most advantageous to smaller businesses, as opposed to the larger organisations we typically work with. With the heavy demands of large

Enterprise storage and archiving, Cloud Storage isn't a clear choice for large organisations with enormous amounts of data, or heavy data security and compliance requirements".

SELF-ASSESSMENT QUESTIONS - 4

10. Implementation of cloud storage is very difficult. [True/False]

6. SUMMARY

- It is discussed that cloud storage is the other form of networked online storage, which is quite different from the traditional storage method.
- Storage as a Service is a business model in which a large company rents space in their storage infrastructure to a smaller company or individual.
- cloud storage service data is stored on hundreds of servers, and the provider rents the storage to the client, and the cost is calculated on a cost per gigabyte.
- Popular cloud storage providers are Google Docs, Amazon Simple Storage (s3), Nirvanix and Google Bigtable Datastore, Live Mesh and Mobilmex, which are discussed in this unit.
- Regarding cloud security, the cloud providers are very concerned about identifying the issues and working hard to address them.
- Finally, we are concluding with a discussion of the Merits and demerits of cloud storage.

7. TERMINAL QUESTIONS

1. Explain the concept of storage as a service.
2. List and explain the cloud storage providers.
3. Explain the issues involved in cloud security and how to overcome them.
4. Discuss the merits and demerits of cloud storage.

8. ANSWERS

Self-Assessment Questions

1. Storage as a Service
2. True
3. a. Service Oriented Architecture
4. gigabyte.
5. b. Amazon web services
6. True
7. distribution, replication, and load-balancing
8. b. apple
9. Trusted networks connect.
10. False

Terminal Questions

1. Storage as a Service is a business model in which a large company rents space in their storage infrastructure to a smaller company or individual; for details, refer to section 8.2.
2. Cloud storage service data is stored on hundreds of servers with redundancy. Here, the provider rents the storage to the client, and the cost is calculated on a cost per gigabyte; for details, refer to section 8.3.
3. In cloud storage, security is one of the challenging factors that the cloud provider needs to focus on and address. For details, refer to section 8.4.
4. As we know, cloud computing is one of the recent and growing technologies for the computing process. It has its own merits and demerits. For details, refer to section 8.5.

9 REFERENCES

E-Reference

- <https://developers.google.com/appengine/docs/python/datastore/overview>
- <http://www.ctoedge.com/content/how-google-app-engine-datastore-works>
- <http://www.ijorcs.org/uploads/ijorcs/secure-data-storage-in-cloud-computing1317065261.pdf>
- http://www.trustedcomputinggroup.org/files/resource_files/1F4DEE3D-1A4B-B294-20Whitepaper_July29.2010.pdf

