What is Data Storage?

Data storage is a type of digital data storage where the data stores in the digital format and kept at the logical pools. The storage system completely maintains by the service provider. The storage services provided by them are available every time and can access remotely. The data stored is secured and can be accessed by few. The environment provided is secure and flexible the companies can buy or rent the storage and can allow an applicant to use it.

2. What is Cloud Storage?

Cloud storage is a service model in which the online data stores. The company that owns data stores and further maintained, managed, and secured by the[cloud provider](https://data-flair.training/blogs/cloud-service-providers-companies/)only. The cloud customer charge for their data storage on as you go basis which is monthly. Cloud storage has great benefits as it is easily accessible and reliable, it has rapid deployment along with flexible data backup and recovery options.

3. Types of Cloud Storage

* Public Cloud
* Private Cloud
* Hybrid Cloud

i. Public Cloud

[Public cloud](https://data-flair.training/blogs/what-is-public-cloud/) storage is basically compatible with unstructured data. It provides a multi-tenant storage environment. Here, the data store in multiple data centres and can access across multiple regions for continents. The cloud storage providers completely manage the public cloud storage.

ii. Private Cloud

[Private cloud](https://data-flair.training/blogs/private-cloud-tutorial/) is mostly compatible with the customers you need to customize their control over their data. Here, the enterprise and the cloud storage providers combine the data centre to serve the customer better.

iii. Hybrid Cloud

Hybrid cloud is a combination of private and publicl cloud which can modify as per the demand. It provides more flexibility to the customer and has more data deployment options. Hybrid cloud is suitable for both small and large sector organizations. It is accessible from anywhere and can provide numerous amount of benefits to the customer.

4. Advantages of Cloud Storage

* Cloud services are accessible from anywhere and can access anytime. This leads to the fact that [cloud storage](https://cloud.google.com/storage/) services are user-friendly and provides much flexibility to the customers.
* It secures as the data can store on the second party and third party server rather than using an external storage device. As the data stores at multiple places so there is no chance of data crash as it can retrieve from other places.
* Using cloud storage services is economical as the customer has to pay on pay as you go basis such that the customer is only charged for what they are used. Moreover, there are no upfront costs.
* Using cloud storage services eliminates the burden of maintaining the server as it is done by the Cloud Service Provider. This saves both cost and time.

5. Cloud Storage Risk

* Loss or damage of the data by the service provider
* Hacking or viruses which may affect the data can cause harm
* Unauthorized access
* Security not up to date

6. Infrastructure

Cloud storage has an infrastructure which bases on the principle of [virtualization in Cloud Computing](https://data-flair.training/blogs/virtualization-in-cloud-computing/). Virtualization eliminates the hardware by utilizing the single hardware and making many virtual separations of it. Its infrastructure is elastic, scalable, and multi-tenant. With the help of proper tools, the whole infrastructure can manage and information can store and retrieve easily.

With the help of ID and password, the whole content can retrieve from anywhere and at any time. In addition, there are proper security measures which authenticate the whole process of uploading and downloading. The applications here uses object storage protocol which is the reason the customers are backing up their data to the cloud.

7. What are the Precautions to Protect the Data?

Here, is a list of precautions which can use to protect the data:

* The processing of personal data should be secure even if the processing carry anywhere.
* The security provided should be of high level and there should be a proper agreement for that so that the data must remain secure.
* The functionality and the continuity of the service should maintain in a proper way.
* The data should be provision and the continuous monitoring should be done.

8. Data Protection Process

The process of data protection consists of various techniques such as backup, recovery, disaster recovery and, many others. One should keep in mind that if a vendor and the customer define issues and process it differently the service may not be as per the requirement.

The data which store in the drive should have a backup at several different places so that disaster takes place the data can retrieve from the different place.

There is a term business continuity which consists of operational recovery and disaster recovery the definition of operational recovery is that it pertains to recovers from a specific problem at the primary site the specific problem can be server, application, and failure of any disk.

There are very less amount of recovery events which caused by a disaster. However, most of them are operational recoveries.

9. Services Provided by Cloud Data Protection

* **Integrity-** Here the old version of data and this data are same. Several encryption measures are taken which are useful to secure the data from some illegal editing and corruption.
* **Infrastructure Security-** There are several methods which are taken to ensure the security of the cloud infrastructure and make it flexible for the customers.

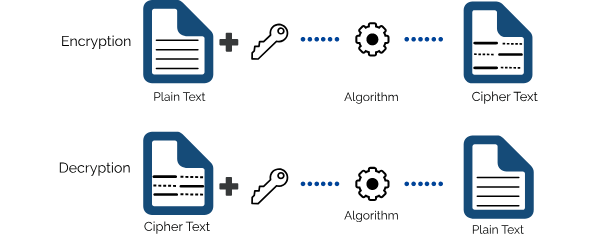
---------------------------------------------19/10/20

10. Encryption in Data Storage

There can be some hardships while implementing encryption. The problem can face due to key management and some other issues. Interview external encryption can cause hardships. These hardships are quite different for the hybrid cloud. As the handling encryption may not be an issue the issues will be when the customer will move to public cloud.

**What is encryption?**

In order to save private data from malicious attacks or hacks, encryption is used. This method is not new. In the past, kings used to send battle tactics to their soldiers using a coded language, readable only to his people. Encryption these days works with the same concept but the structure is different.  Now we use electronic devices to generate unique encryption algorithms to scramble our data. It is the method by which a plaintext or any type of data is encoded. The encoded data can only be decoded by the person who has the decryption key. This method keeps the data protected. The encrypted data is commonly referred to as the cipher text, while unencrypted data is called plain text.



**Types of data encryption:**

When it comes to encryption there are two major types: asymmetric encryption, also known as public-key encryption, and symmetric encryption.

**Symmetric-key encryption:**

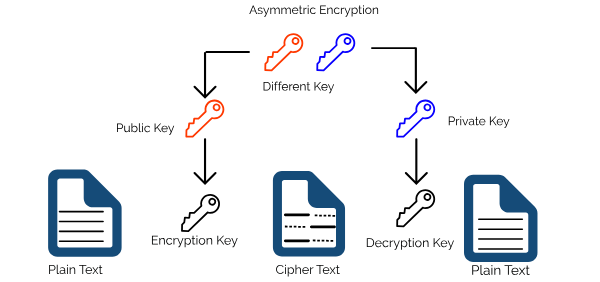
This type of encryption uses the **identical keys or the code**s for the computers involved in the message transmission. Each secret key’s data packet is self-encrypted. The symmetric encryption will be according to the Data Encryption Standard (DES), which uses a 56-bit key, although it is not considered to be attack-proof. The Advanced Encryption Standard (AES) is considered more reliable because it uses a 128-bit, a 192-bit or a 256-bit key.



**Asymmetric-key encryption:**

The asymmetric key encryption is also known to be the public key encryption uses private and public keys. The public key is shared with all the computers which want to connect with the user’s computer. Although the private matching key remains private to the user’s computers and it decrypts the message and makes it readable according to the public key encryption system. The keys are paired together but they are not identical. One key that is the public key can be shared with everyone and the other key is the private key that is kept in private.

For example the IT administrator who will encrypt the data will possess the two keys that locks the data. The public key will be available for anyone. The private key is kept private. The message which will be encrypted by the public key will be decrypted only by using the private key, while the message encrypted using the private key can be decrypted by using the public key. The process is called public key cryptography.



**Why and when is encryption used?**

Encryption is essential to ensure the security of sensitive information being transferred. It is the method that provides data security and end-to-end protection of data that is transmitted across the networks. It is used by organizations to ensure the data security of their data Organizations also use encryption to protect stored data on computers, servers and mobile devices like phones or tablets.

**How encryption works?**

Encrypted data is formed by using an encryption algorithm and an encryption key.  This process then generates the Cipher text (encrypted data) which can be viewed in the original form if it is decrypted with the correct encryption key.

Among the types of encryption, Symmetric key encryption is more mainstream; it uses Advanced Encryption Standard (AES) for encryption. If this data is transmitted, the sender has to provide the received with the decryption key.

The asymmetric cryptography uses the two different links which are linked with each other. The public key can be shared with everyone whereas, the private key will be kept secret. This attribute provides a method of assuring not only confidentiality, but also the integrity, authenticity and non-reputability of electronic communications and data at rest.

**Benefits of encryption:**

The primary function of encryption is to protect data which is stored on-premises (on a file server, NAS or SAN), or transmitted through internet or any other computer.

Encryption has the following key elements of security:

**These key elements of encryption leads to some amazing benefits:**

* **Protect Data:**

The data is protected through encryption. Suppose that the file is encrypted with 256-bit AES it will take a lifetime to crack the code.

* **Security available on multiple devices:**

Accessibility and device independency is a crucial part of most enterprise environments. Encryption removes the risk of data breach and unauthorized access. It ensures that the data remains secure regardless of the device on which it is stored and accessed.

* **Secure Transmission:**

During transmission the data is secured through encryption. Encryption techniques like E2E will ensure data remains protected.

* **Integrity:**

Integrity ensures that the contents of the message or data are not changed since it was sent.

* **Confidentiality:**

Encryption prevents unauthorized access to data, maintaining confidentiality. This can be done by monitoring the flow of decryption keys.

* **Data Integrity:**

The lack of protection measures result in data leakage or a data breach; this in turn results in reputation damage and sometimes substantial financial repercussions.

Encryption technology prevents data breaches and deliver enhanced data integrity.

* **Ensure Compliance:**

Most compliance regulations observe strict policies pertaining to data security. Encryption technology plays a vital role in delivering data protection and enabling organizations to remain compliant.

------------------------------------------------------------------------------------------------20/10/20

**What is storage encryption?**

* Storage encryption means the use of encryption/decryption for backed-up and archived data, both in transit and on storage media. All products of StoneFly deliver encryption to facilitate data security.

# Data encryption options

Cloud Storage always encrypts your data on the server side, before it is written to disk, at no additional charge. Besides this [standard, Google-managed behavior](https://cloud.google.com/storage/docs/encryption/default-keys), there are additional ways to encrypt your data when using Cloud Storage. Below is a summary of the encryption options available to you:

* Server-side encryption: encryption that occurs after Cloud Storage receives your data, but before the data is written to disk and stored.
  + [***Customer-supplied encryption keys***](https://cloud.google.com/storage/docs/encryption/customer-supplied-keys): You can create and manage your own encryption keys. These keys act as an additional encryption layer on top of the standard Cloud Storage encryption.
  + [***Customer-managed encryption keys***](https://cloud.google.com/storage/docs/encryption/customer-managed-keys): You can manage your encryption keys, which are generated for you by Cloud Key Management Service. These keys act as an additional encryption layer on top of the standard Cloud Storage encryption.
* [***Client-side encryption***](https://cloud.google.com/storage/docs/encryption/client-side-keys): encryption that occurs before data is sent to Cloud Storage. Such data arrives at Cloud Storage already encrypted but also undergoes server-side encryption.

**TYPES OF ENCRYPTION IN CLOUD STORAGE**

* Volume-based encryption : Volume encryption works either by encrypting an entire hard disk partition (C:, D:, etc) or by creating an encrypted container file. This container, often several gigabytes in size, is internally encrypted by a piece of software that also makes the container appear as a drive letter or folder. Files saved in that special location are automatically encrypted and added to the container.
* Application specific encryption : allows organizations to **encrypt** entire files or **specific** fields of data at the **application** level, before it is stored.
* File encryption : File encryption refers to encrypting data stored on disk on a file-by-file basis. In either case, the goal is to prevent unauthorized persons from opening and reading files that are stored on the disk. Support for disk/file encryption can be built into an operating system or file system.
* Disk encryption is a technology which protects information by converting it into unreadable code that cannot be deciphered easily by unauthorized people. Disk encryption uses [disk encryption software](https://en.wikipedia.org/wiki/Disk_encryption_software) or [hardware](https://en.wikipedia.org/wiki/Disk_encryption_hardware) to [encrypt](https://en.wikipedia.org/wiki/Encryption) every [bit](https://en.wikipedia.org/wiki/Bit) of data that goes on a [disk](https://en.wikipedia.org/wiki/Disk_storage) or disk [volume](https://en.wikipedia.org/wiki/Volume_(computing)). It is used to prevent unauthorized access to data storage.

11. Data Loss Prevention

There are sensitive data which must monitor with the help of tools and it must confirm that the data recognized by the data based on string matching.

Data loss prevention (DLP) is a process for protecting sensitive data at rest, in-transit, and on endpoints to reduce the likelihood of data theft or unauthorized exposure. DLP solutions aim to prevent sensitive data and confidential information from being stored, used, or transferred insecurely.

DLP required for a number of technologies and many processes to become effective there should be a policy through which the creation and implementation of infrastructure will work to push the policy to monitor.

DLP this tool should also inspect traffic on network traffic and critical host system alike..

12. Cloud storage  Architecture

**Cloud** storage is a model of [computer data storage](https://en.wikipedia.org/wiki/Computer_data_storage) in which the [digital data](https://en.wikipedia.org/wiki/Digital_data) is stored in logical [pools](https://en.wikipedia.org/wiki/Pool_(computer_science)), said to be on "the cloud". The [physical storage](https://en.wikipedia.org/wiki/Storage_virtualization) spans multiple [servers](https://en.wikipedia.org/wiki/Server_(computing)) (sometimes in multiple locations), and the physical environment is typically owned and managed by a [hosting](https://en.wikipedia.org/wiki/Internet_hosting_service) company. These cloud storage providers are responsible for keeping the data [available](https://en.wikipedia.org/wiki/Availability) and [accessible](https://en.wikipedia.org/wiki/Data_access), and the physical environment protected and running. People and organizations buy or lease storage capacity from the providers to store user, organization, or application data.

Cloud storage services may be accessed through a [colocated](https://en.wikipedia.org/wiki/Colocation_centre" \o "Colocation centre) [cloud computing](https://en.wikipedia.org/wiki/Cloud_computing) service, a [web service](https://en.wikipedia.org/wiki/Web_service) [application programming interface](https://en.wikipedia.org/wiki/Application_programming_interface) (API) or by applications that utilize the API, such as [cloud desktop](https://en.wikipedia.org/wiki/Cloud_desktop) storage, a [cloud storage gateway](https://en.wikipedia.org/wiki/Cloud_storage_gateway) or [Web](https://en.wikipedia.org/wiki/World_Wide_Web)-based [content management systems](https://en.wikipedia.org/wiki/Content_management_system).

Cloud computing is believed to have been invented by [Joseph Carl Robnett Licklider](https://en.wikipedia.org/wiki/Joseph_Carl_Robnett_Licklider) in the 1960s with his work on [ARPANET](https://en.wikipedia.org/wiki/ARPANET) to connect people and data from anywhere at any time.[[1]](https://en.wikipedia.org/wiki/Cloud_storage#cite_note-origin-1)

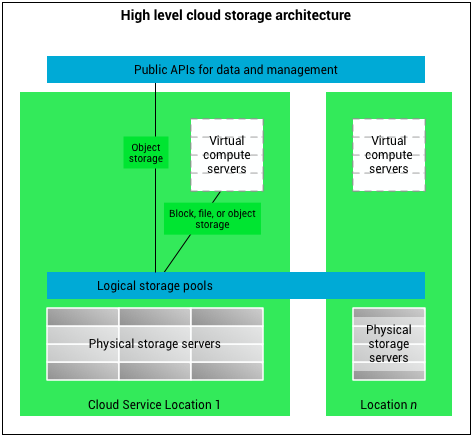
In 1983, [CompuServe](https://en.wikipedia.org/wiki/CompuServe) offered its consumer users a small amount of disk space that could be used to store any files they chose to upload.[[2]](https://en.wikipedia.org/wiki/Cloud_storage#cite_note-2)

In 1994, [AT&T](https://en.wikipedia.org/wiki/AT%26T) launched PersonaLink Services, an online platform for personal and business communication and entrepreneurship. The storage was one of the first to be all web-based, and referenced in their commercials as, "you can think of our electronic meeting place as the cloud."[[3]](https://en.wikipedia.org/wiki/Cloud_storage#cite_note-3)

[Amazon Web Services](https://en.wikipedia.org/wiki/Amazon_Web_Services) introduced their cloud storage service [AWS S3](https://en.wikipedia.org/wiki/AWS_S3) in 2006, and has gained widespread recognition and adoption as the storage supplier to popular services such as [SmugMug](https://en.wikipedia.org/wiki/SmugMug" \o "SmugMug), [Dropbox](https://en.wikipedia.org/wiki/Dropbox_(service)" \o "Dropbox (service)), and [Pinterest](https://en.wikipedia.org/wiki/Pinterest" \o "Pinterest).

In 2005, [Box](https://en.wikipedia.org/wiki/Box_(company)) announced an online file sharing and personal cloud content management service for businesses.[[4]](https://en.wikipedia.org/wiki/Cloud_storage#cite_note-4)

-------------------------------------------------------------------------------------------------------------------------------21/10/20



Cloud storage is based on highly virtualized infrastructure and is like broader [cloud computing](https://en.wikipedia.org/wiki/Cloud_computing) in terms of interfaces, near-instant elasticity and [scalability](https://en.wikipedia.org/wiki/Scalability), [multi-tenancy](https://en.wikipedia.org/wiki/Multi-tenancy), and [metered](https://en.wikipedia.org/wiki/Metered) resources. Cloud storage services can be utilized from an off-premises service ([Amazon S3](https://en.wikipedia.org/wiki/Amazon_S3)) or deployed on-premises (ViON Capacity Services).[[5]](https://en.wikipedia.org/wiki/Cloud_storage#cite_note-5)

Cloud storage typically refers to a hosted [object storage](https://en.wikipedia.org/wiki/Object_storage) service, but the term has broadened to include other types of data storage that are now available as a service, like block storage.

Object storage services like [Amazon S3](https://en.wikipedia.org/wiki/Amazon_S3), [Oracle Cloud Storage](https://en.wikipedia.org/wiki/Oracle_Cloud#Infrastructure_as_a_Service_(IaaS)) and [Microsoft Azure](https://en.wikipedia.org/wiki/Microsoft_Azure) Storage, object storage software like [Openstack Swift](https://en.wikipedia.org/wiki/OpenStack" \l "Object_Storage_(Swift)" \o "OpenStack), object storage systems like [EMC Atmos](https://en.wikipedia.org/wiki/EMC_Atmos), EMC ECS and Hitachi Content Platform, and distributed storage research projects like OceanStore[[6]](https://en.wikipedia.org/wiki/Cloud_storage" \l "cite_note-oceanstore-6) and VISION Cloud[[7]](https://en.wikipedia.org/wiki/Cloud_storage#cite_note-7) are all examples of storage that can be hosted and deployed with cloud storage characteristics.

Cloud storage is

Made up of many distributed resources, but still acts as one, either in a [federated](https://en.wikipedia.org/wiki/Federation_(information_technology))[[8]](https://en.wikipedia.org/wiki/Cloud_storage#cite_note-8) or a [cooperative storage cloud](https://en.wikipedia.org/wiki/Cooperative_storage_cloud) architecture

* Highly fault tolerant through redundancy and distribution of data
* Highly durable through the creation of versioned copies
* Typically [eventually consistent](https://en.wikipedia.org/wiki/Eventual_consistency) with regard to data replicas[[9]](https://en.wikipedia.org/wiki/Cloud_storage#cite_note-9)

Advantages

* Companies need only pay for the storage they actually use, typically an average of consumption during a month.[[10]](https://en.wikipedia.org/wiki/Cloud_storage#cite_note-zdnet-10) This does not mean that cloud storage is less expensive, only that it incurs operating expenses rather than capital expenses.
* Businesses using cloud storage can cut their energy consumption by up to 70% making them a more green business.[[11]](https://en.wikipedia.org/wiki/Cloud_storage#cite_note-11)
* Organizations can choose between off-premises and on-premises cloud storage options, or a mixture of the two options, depending on relevant decision criteria that is complementary to initial direct cost savings potential; for instance, continuity of operations (COOP), disaster recovery (DR), security (PII, HIPAA, SARBOX, IA/CND), and records retention laws, regulations, and policies.[[12]](https://en.wikipedia.org/wiki/Cloud_storage#cite_note-12)
* Storage availability and [data protection](https://en.wikipedia.org/wiki/Data_protection) is intrinsic to object storage architecture, so depending on the application, the additional technology, effort and cost to add availability and protection can be eliminated.[[13]](https://en.wikipedia.org/wiki/Cloud_storage#cite_note-13)
* Storage maintenance tasks, such as purchasing additional storage capacity, are offloaded to the responsibility of a service provider.[[10]](https://en.wikipedia.org/wiki/Cloud_storage#cite_note-zdnet-10)
* Cloud storage provides users with immediate access to a broad range of resources and applications hosted in the infrastructure of another organization via a web service interface.[[14]](https://en.wikipedia.org/wiki/Cloud_storage#cite_note-14)
* Cloud storage can be used for copying [virtual machine images](https://en.wikipedia.org/wiki/Virtual_machine_image) from the cloud to on-premises locations or to import a virtual machine image from an on-premises location to the cloud image library. In addition, cloud storage can be used to move virtual machine images between user accounts or between data centers.[[15]](https://en.wikipedia.org/wiki/Cloud_storage#cite_note-15)
* Cloud storage can be used as natural disaster proof backup, as normally there are 2 or 3 different backup servers located in different places around the globe.
* Cloud storage can be mapped as a local drive with the WebDAV protocol. It can function as a central file server for organizations with multiple office locations.