Encrypting cloud storage

What is this document?

This document will show you how you can encrypt cloud storage yourself, rather than relying on the cloud storage to do it for you.

Use symmetric cryptography (AES256, etc)

There are different ways to use AES256 for encryption. Particularly, this is symmetric and has a password on it.

Encrypt a file online

The best website to do this is using hat.sh which encrypts files that you enter. This can be done with a public private keypare.
All you have to do is choose your files, upload, password set or public key, then you're good to go. Just make sure you save the password in a safe place.

Mobile device

In some cases, you may be able to encrypt files using your android device or iphone.
One way to do this is to use secret space encrypter (SSE)
While it does require some configurwation, you will be able to encrypt separate files/directories and upload those encrypted files/directories wherever you want.
Note:
For all file types: i recommend AES256 encryption.
There are different ones, like blowfish448, shacal, etc.
Note:
For the apple app store, if you want the full version of the products, you have to pay for it.
https://apple.co/3PEitmq
Lighter versions are available for free.
See this link on paranoia works for more information
Nevertheless, it gets the job done, as you can encrypt files, and even decrypt them.

Windows

https://paranoiaworks.mobi/download/

You can make encrypted versions of files using veracrypt.fr
It's for all OSes, but veracrypt works.

Online encryption services (not recommended)

Some of these services will do the encryption for you.
One of those services is axcrypt. They will provide you convenience as you don't have to do the encryption yourself, however, they will also be doing the encryption, even if the encryption keys are storedo n your device. Even if google doesn't have your data, there's a chance that the encryption provider may have your data.
You shuold always do it yourself.

Note

For linux servers, some applications will encrypt the backups for you. For example, cloudron has the option to, while sending your backups to the cloud, encrypting the files as it does so with AES256 with a password you select.
Encrypted files in .enc format will use .enc.
For example: example.tar.gz.enc
Additionally, some cloud services, for example, AWS, will have tools to encrypt your files at the client side.
see : AWS S3 client side encryption tool

PGP encryption.

The best way to do encryption is to use asymmetric encryption, like PGP
The reason is because you are using public key cryptography. There is no brute forcing a key, unless they have the device with that key.
Without it, they cannot access your data and it is encrypted.
It is also commonly used to encrypt emails.

Android

On android, there is openkeychain

This is an encryption tool on android that allows you to encrypt files without a nother computer, and securely.

Windows

Gpg4win

Linux

For linux there is the gnu privacy guard
It should be mentioned that GnuPG can do encryption using AES with a password, but the default method is to use PGP.

What about encryption at rest or serverside encryption?

This is not enough. Server side encryption and encryption at rest means that hackers may not be able to see your data.
However, even if outsiders can't see it, employees of your cloud provider may stil be able to see it, as they have the keys to that server side and encryption at rest.
Client side encryption means that, you, encrypt your own data, with noone able to access it as long as your device is secured. Only you have the encryption keys to your files.
There is also another benefit of encryption: your files cannot be decrypted without the key or password. This means that if you get subpoenaed for any reason, the cloud storage provider cannot decrypt your files..
Only you get to decrypt your own files.

The absolutely best solution

The absolutely best solution is to use nextcloud
You can run your own instance, and turn on encryption for your instence.
For more information: see Enable End-to-End Encryption Between Nextcloud and Your Desktop Client
While server side encryption isn't necisarily recommended only, the benefit is at least if you have to stick with server side, you have your own keys, stored on your own server as long as you don't get hacked.
As long as your server doesn't get hacked, you are good.
Still, when possible, end to end encryption is still recommended when possible.

So what can i do with these encrypted files?

You can store the encrypted versions of the files in google drive, microsoft onedrive, cloudflare r2, or even a public network, as long as you do not store the original (decrypted) version of the file.