Cloud storage reduces IT spend, mobilizes workforces, enables huge cost—savings and maximizes accessibility to data from anywhere. But, is it really secure?
Table of Contents

1. Why do you need a Cloud Data Warehousing Service? ..................................................3

2. The minimum you should know about how cloud data storage works ......................5
   Basic cloud storage systems ...................................................................................5
   Redundancy fault tolerance ....................................................................................6
   Cloud Data Storage vs Traditional Digital Data storage, who wins? ........................7
   Flexibility and efficiency .......................................................................................7

3. Advantages of using Cloud Data Storage ..................................................................8

4. Disadvantages of using Cloud Data Storage ............................................................11

5. Cloud Storage Providers and the conditions and services they offer ......................14
   The big players in Cloud Storage .........................................................................14
   Is there anything to fear about as a Data Storage User? .......................................15
   Reliability and Security .........................................................................................15
   Cloud storage companies live and die by their reputation ....................................17

6. Security Systems offered by Cloud Storage Companies ........................................18
   Cloud Data Storage and Privacy Protection ..........................................................19
   Other Cloud Storage Services .............................................................................22

7. How to choose your Cloud Storage Provider ..........................................................24

8. How to protect your data yourself with SMiD .........................................................25
   SMiD is Simple, Flexible and Secure .....................................................................26

9. Contact Information ..................................................................................................27
   Company information ............................................................................................27
1. Why do you need a Cloud Data Warehousing Service?

The days of paper-based documents and administrative processes are gone. Administrative clerks and officials are no longer nailed to physical offices. Citizen service transactions and administrative processes now happen almost exclusively online or over the phone. This means that everyone in the sector has had to adapt to new ways of working in order to keep up with customer demand for more immediate and comprehensive service.

This digital evolution in administration has considerably increased the amount of data that needs to be stored. Data generated by social systems needs to be housed for long periods of time in order to comply with legislation and ensure that operations are sustainable. **This increasing need for data storage is posing a big problem** for enterprises, organizations, public and private institutions, governments, and even for individuals.

Societies have always amassed documents and invested in their archiving. **But the digital age has brought an intense proliferation of all kinds of data.** Every single second the world’s population is generating uncountable documents, photos, records, communications, and every imaginable kind of information.

The challenge is where to keep it all
Users are resorting to a range of solutions to this growing data storage challenge. Some invest in larger hard drives for their servers, others use external storage devices like thumb drives or compact discs, and some users, in desperation, may even delete whole folders to make space for new information.

But a new trend has taken the market by storm, offering massive storage of data at a low cost or sometimes for free. It is called 'cloud storage', and it is here to stay.

Image: cloudstoragecomparison.net
2. The minimum you should know about how cloud data storage works.

Cloud storage means that your data is kept in a remote database maintained by a third party, instead of on your computer's hard drive or other local storage infrastructure.

Access to your data is immediate via an Internet connection, yet the burden of keeping it secure and dealing with your increasing needs for storage is handled by the third party.

Cloud storage has become so popular that there are hundreds of solutions on the market, with more cropping up daily. Some are small operations that keep customer data in a single-room, while others fill warehouses with storage equipment. As end customer the difference you see is in the price, the storage limit, and speed of retrieval.

Basic cloud storage systems

The most basic cloud storage system is a single data server connected to the Internet. A client - that is, a computer subscribing to a cloud storage service - sends copies of its files over the Internet to the data server, which records the information. How and where the data is recorded is unknown to the end user. To access the cloud-stored data, the user accesses the remote cloud server through a Web-based interface. The server then either sends the files back to the client or allows the client to access and manipulate the files directly on the server.
Redundancy fault tolerance

In order to minimize risk, cloud storage systems usually rely on hundreds of data servers, storing client information on multiple machines at once. This is called redundancy.

Without sufficient redundancy, a cloud storage system cannot ensure clients that they will have immediate access to their information for as long as it is stored with the third party.

Most cloud provider systems store client data on multiple servers that use different power supplies, network connections, cooling services, etc. This is called fault tolerance, since it ensures that data remains intact even in the case of failure of one server. It is this feature that makes cloud storage unique from any other traditional digital office solution.

It is this feature what makes cloud storage unique from any other traditional digital office solution. It ensures that our data will be available.
Cloud Data Storage vs Traditional Digital Data storage, who wins?

Traditional digital data storage requires maintenance of hard disks, the electrical power necessary to keep them spinning, a safe risk-free physical space and a cooling system that prevents them from meltdowns. Security personnel must be hired to prevent unauthorized access to hard disks and technical staff to keep the storage system, redundant and consistently up and running so no files are lost or accessed by unauthorized parties.

Flexibility and efficiency

Cloud storage offers many advantages over traditional data storage. It is flexible, since it allows access to data from anywhere and it can expand as needs for storage grow. It is also extremely simple and cost-efficient, since there is no hardware to maintain, no staff to employ.

Using traditional or cloud storage is a matter of your company’s specific needs.

Keep on reading, we will discuss in detail advantages and disadvantages of both systems.
3. Advantages of using Cloud Data Storage

When it comes to storing data, cloud storage is quickly becoming the method of choice. Storing files remotely rather than locally provides an array of advantages for both home and professional users. Here are the top reasons to give up your external hard drive in favour of online storage services:

- **Cost** – Backing up your data is not always cheap, especially when you include the cost of any equipment needed to do so (external hard drives, backup tapes, etc.) and the cost of the time it takes to complete those routine backups. Online storage services reduce much of that cost providing ample storage space in the cloud for a low monthly fee.

- **Immateriality** – Cloud storage is invisible; with no physical presence, it does not take up valuable space at home or in the office.
SECURITY IN CLOUD STORAGE
Learning about Cloud Storage

- **Security** – Storing confidential or sensitive information in the cloud is often more secure than storing it locally, especially for businesses, because of its higher availability and fault tolerance.

- **Automation** – Online storage services make the tedious process of backing up easy to accomplish through automation. You simply select what and when you want to back up, and the service does the rest.

- **Accessibility** – With commercial providers you can access your account from any Internet connection, whether you are on a mobile browser or on your work computer.

- **File Syncing** – The very popular file syncing services ensure that your files are automatically updated across all your devices and that the latest version of a file saved on your laptop is available on your smartphone.

- **Information Sharing** – Some cloud storage providers include it as a service and, therefore, a file or even an entire folder with many documents can be shared with anyone by just a few clicks.

- **Collaboration** – Some online storage services that have full access to your information offer functionalities for collaboration purposes. They allow multiple people to edit and
collaborate on a single file or document, so you do not have to worry about tracking the latest version.

- **Added Protection** – Cloud storage serves as an added layer of data protection for your precious and irreplaceable files. Your information is kept in secure locations that are physically distant from your office.

- **Recovery** – In the event of catastrophic data loss of your local copies, your cloud service will have backups of all your original files, so you can restore them with some download time.

No matter what your storage needs may be, cloud storage service provides many and important advantages for storing both your home and professional files.
4. Disadvantages of using Cloud Data Storage

Like all new technologies, cloud computing has also its disadvantages. While these affect in general all users, private users or smaller companies are the ones who may feel slightly more disadvantaged than larger businesses.

- **Shared Information** – When you store information in a cloud storage provider, you provide it in clear and readable form. Sometimes, the transfer is done through encrypted communication tunnels (SSL), but it gets clear at the other end. This clear text transfer requires an absolute confidence on the provider, his installation, his security policies, and also his workers.

- **Non-Accountable Accesses** – Installations of your cloud storage provider are private installations that you cannot access and monitor. You always have to blindly trust your provider and you will never know whether any incident has exposed your information to non-authorized persons. This is especially true with public cloud storage providers and with those services that, in fact, are subcontracting with third parties that you do not even know.
Critical Dependency - If you do not store the same information in several really independent providers, the cloud storage user risks becoming a hostage of that provider in some circumstances.

Network Connections Dependency - Cloud storage needs active and efficient network connections to work. When the network is down, cloud services are down as well. When the network runs slowly, your services also run slowly, and your work is affected. Even if cloud computing providers take precautions to ensure that the network has a great uptime, the risk will always remain.

Connecting Peripherals - Connecting wireless devices can be difficult, especially when it comes to personal devices. Software incompatibilities are another problem.

Costs - When done on a small scale, cloud storage can be expensive and this is especially the case for small businesses. They might not be sure what service is best for their situation, so they have to try various offerings until they find the right one. However, in the long run, cloud storage is affordable, and in time one recuperates the money spent in the beginning.

Data Ownership - As one of the biggest issues that trouble cloud storage, data ownership is the major obstacle, especially if you have a great amount of data to deal with or if these data are sensible. There is no straightforward answer to the basic question of “who owns the data maintained by a cloud storage service, the uploader or the storage provider?” Cloud providers are used to establishing their own terms and conditions, which many times may seem arbitrary. Therefore, reading the small print is absolutely necessary when you deal with cloud storage providers, and especially with cloud hosting. Also note that, at times, you may not be allowed to upload a certain type of data.

No Hard Drive - For some users the lack of a hard drive is a neat advantage as this reduces costs and weight. For those who use (old) programs that need an attached hard drive, this may be a little unpleasant.
• **Security** - Although security in the cloud is generally good, there are still some serious security concerns. For instance, the interconnectedness of servers in the cloud may lead to a situation in which a hacker or an intelligence agency snoops the communications or breaches one system and then makes their way into other linked systems.

Many of the disadvantages of cloud computing are due to the fact that the technology is still relatively new. In other words, they will be addressed in time, as more and more users adopt cloud storage. **Nevertheless, no technology is perfect**, and cloud storage is no exception: when getting cloud services one should take into account all the possible disadvantages.
5. Cloud Storage Providers and the conditions and services they offer.

There are many cloud storage providers, and their numbers seem to increase every day. Not only are there a lot of companies competing to provide storage, but also the amount of storage each company offers to clients seems to grow regularly.

The big players in Cloud Storage

There are a few well-known companies that offer some form of cloud storage such as Google Docs; Web e-mail providers like Gmail, Hotmail and Yahoo Mail store e-mail messages on their own servers; sites like Flickr, Instagram and Picasa host millions of digital photographs; YouTube and Web site hosting companies like StartLogic, Hostmonster and GoDaddy store the files and data for client Web sites. And social networking sites like Facebook store pictures and other contents from their clients.

Other services are specialized in cloud storage. This is the case of Amazon Cloud Drive, Amazon S3, Google Drive, Box, Copy, Dropbox, MEGA, Microsoft OneDrive, among others. All of them offer cloud storage accounts that allow the user to upload and store files via a Web browser or through their file-sync desktop applications for PCs and laptops, or via specific Apps available in the Android and iOS market places.
Some services listed above are free. Others charge a flat fee for a certain amount of storage; and still others have a sliding scale depending on what the client needs. In general, the price for online storage has greatly decreased as more companies have entered the industry. Even many of the companies that charge for digital storage offer at least a certain amount of storage for free.

Is there anything to fear about as a Data Storage User?

The two biggest concerns about cloud storage are reliability and security.

Clients and general users are not likely to entrust their data to another company without a guarantee that:

1. They will be able to access their information whenever they want.
2. No one else will be able to get at it. Some user collectives, professionals, and even government officials in Public Administration are not allowed by law to do so.

Reliability and Security

In cloud storage services it is reasonable to worry that data saved in a remote storage system become vulnerable. There is always the possibility that a hacker will find a back door and access your data in the cloud; hackers could even steal the physical machines on which your data are stored. Even more, it is not difficult to imagine a disgruntled employee altering or destroying your data using his or her authorized credentials. In such
cases, **you are losing access to your data, but if they are encrypted, their confidentiality is protected.** Cloud storage companies invest a great deal of money in security measures to limit the possibility of data theft or corruption; however, if they fail, **you pay the consequences.**

Reliability is also a great concern, as important as security. An unstable cloud storage system is a serious risk if you put there the unique copy of your information. No one wants to save data to a failure-prone system or to trust a company that is not financially stable. While most cloud storage systems try to address this concern through redundancy techniques, there is still the possibility that an entire system could crash and leave clients with no way to access their saved data. The unique solution to face this risk is to use at least two different cloud storage providers that do not have anything in common (such as company, technology, geolocation, management, ownership, and legal system).

The best way to maximize reliability is to use two different completely independent cloud storage providers.
Cloud storage companies live and die by their reputation

It is in each company's best interests to provide the most secure and reliable service as possible. And they can do it better if they reduce the amount of risk that they assume. By working with encrypted data that they cannot decrypt, storage cloud providers can concentrate on providing file redundancy and integrity to assure their clients that no file will ever get lost or altered. If a company cannot meet these basic client expectations, it does not have much of a chance.
To secure data, most systems use a combination of techniques, including:

- **Authentication processes**, which identify authorized users, are represented by a user name and password.

- **Authorization practices**, where there are lists with users authorized to access the files stored on the cloud system. In many scenarios this authorization has to be multi-level to distinguish different functions and users.

- **Encryption processes**, which use a complex algorithm to encode information so that a user needs to know and operate the proper encryption key to decode the encrypted files.

Authorization and encryption mechanisms are both responsible for protecting the privacy of your data and, by extension, your own privacy. If any of them fail, the whole system fails.

In particular, the **cryptographic algorithm** used has to be strong enough to assure that your potential attackers do not have access to the computer processing power required to discover the secret key needed to decrypt your information.
Information ownership in cloud storage services is equivalent to the knowledge of the secret cryptographic keys used to encrypt the files. **If the service provider knows the keys or can deduce them, encryption does not protect your privacy** and it is a waste of time and energy.

Encryption is only useful when you, and only you, know and control the cryptographic keys used to protect (cipher) your information.

But security by encryption also depends on how that process is done. If the cryptographic algorithm is run on computers such as those we use every day, unsuspected malware can also be installed and can spy the volatile memory assigned to the cryptographic processes. In such a case, the spying malware may see, copy, and exfiltrate the key, thus the entire secret is uncovered.

Encryption and decryption processes have to run on a dedicated computer whose software is properly certified, and it should remain in such state of grace all the time. These computers have to be operated following tight and simple enough procedures to assure that they do exactly what they are supposed to do and that no alien processes ruin their security.

**Cloud Data Storage and Privacy Protection**

Cloud storage is easy to come by; dozens of services offer you free space just for signing up. But which of those services are looking at the files you upload, and most importantly, which services encrypt your personal data in a way no one can look at them?
Privacy is even more important when it comes to cloud storage. You trust the service you sign up for to keep your files safe and secure and away from any prying eyes. Whether you use your cloud storage for your company’s critical information, your private data, multimedia, tax returns, backups, or whatever you want, it is very important to know that your provider is not rifling through your files. Even with a trustworthy provider, if their servers ever get hacked, you want to know that your private information and financial documents are safe.

Whether you want to protect your documents from potential thieves or want your files locked down in case your laptop or phone is lost or stolen, or you are concerned about the NSA spying activities, encrypting your documents is the only way to make sure you are the only person with access to them.

Your data may be hacked, if they are encrypted at least their confidentiality is protected.

With some providers (SpiderOak, Wuala, Tresorit and Mega) all your files are locally encrypted on your computer and then uploaded to the cloud servers; any changes you make to your files and folders are synced with the local decrypted versions before being secured and uploaded. In these software solutions, file encryption is user-controlled, which
means that the chosen password is king. As the encryption process takes place locally, the cloud provider has no way of knowing what is being stored. In these scenarios, your data is completely private because the user is the only person who knows what is being encrypted and transmitted, and the only unencrypted versions live on your local computer.

**Most cloud storage services that encrypt files use a key created by a key derivation algorithm that depends on your chosen password.**

This local encryption approach means that if you lose your password, the cloud storage provider cannot retrieve it, nor can he decrypt your locked files for you.

One important and critical disadvantage of these services is that:

**When you share a file with someone, the file gets unencrypted and stored in the cloud, so the provider can also access it without knowing the password.**

With software solutions of this kind, if the chosen password is secret and randomly generated, your information is protected against spy eyes outside your office, but this is not the case when passwords are chosen and used by human beings. Passwords chosen by human users can be sometimes quite easily guessed and be victims of dictionary attacks. **These software solutions do not protect your information stored in the cloud from attackers that can access, even temporally, the computer that encrypts and decrypts your files.**
Resident malware in those computers can spy the memory area assigned to the encrypting application process and steal the master key that protects all the files stored in the cloud. Since that moment, all your stored information is no longer exclusively yours; it has a new additional owner with the same empowerment as you have. If such security breach remains undetected, you will continue adding new files and information that will make that not-so-private cloud storage grow.

Finally, these software encryption solutions only protect the files that you backup in the cloud, but clear-text copies of all those files remain in all local synced computers. Anyone with physical access to the hard drives where those files are locally stored will be able to clone and steal that information.

Other Cloud Storage Services

Some big names in the cloud storage arena are not included above. That is not because they are insecure, or because they do not care about your privacy; it is just because they do not offer the tools or privacy promises that those above mentioned do. In the worst case, it is because they actually say outright that they scan your files “for content they
deem inappropriate”. If you insist on leaving your data with such providers, you should at least know what these providers’ privacy policy says.

Dropbox, Google, and Amazon say they will only dig into your files if someone tips them off to illegal or copyrighted material, or if law enforcement comes knocking. All three will insist on seeing a North American court order before investigating or turning over any data to the authorities. In principle, they would not shutter your account because they found something they did not like. On the other end is Microsoft’s OneDrive that scans its users’ files looking for illegal or malicious contents, but Microsoft is not alone here. Apple reserves the right to scan your files stored in Apple’s iCloud as well.

All cloud storage services have privacy policies which you must read before signing up. All of them will respond to court orders issued in their countries, but those storing encrypted data do not even know what there is on their servers, much less how to decrypt them, so they physically cannot give them to someone who comes asking for them.

If you still want to use those providers, add some encryption using a third party software tool to encrypt your data locally. For example, you can use TrueCrypt, Boxcryptor, Viivo or EnCifra Box, which are fully compatible with Dropbox, Google Drive, OneDrive, and others.

Software encryption tools are not safer than the computer they are run on (malware is widely spread), but using them is better than no encryption at all.
7. How to choose your Cloud Storage Provider

Finally the really important question is how to choose your ideal cloud storage provider. Summarizing the previous chapters:

1. Cloud storage or traditional storage? Consider the pros and cons.
2. Ask yourself: do you need free storage or can you afford to pay. How much can you pay?
3. Check the (online) reputation of your possible cloud storage providers.
4. What security measures does the company offer? What redundancy techniques do they use?
5. What level of security does the provider offer? Only authentication by name and password? Authorisation lists? Encryption?
6. Where does data encryption take place? Does the provider have access to the encryption key?
7. Do you need and could you afford the use of a second independent cloud provider to be perfectly safe?
8. Do you need to share files with others?
9. Read the small print before signing.
10. Be sure to meet the legal requirements of your country concerning data storage.

If you carefully follow this advice you have good chances to succeed. However, there is an even better way to storage in the cloud without any risk:

Encrypt your data yourself and the only thing you must care about is to choose a provider with a high reliability.
SECURITY IN CLOUD STORAGE
SMiD makes every Cloud your own Private Cloud

8. How to protect your data yourself with SMiD

The most secure cloud storage solution is the one over which you have complete control.

That is exactly what SMiD makes for you. Using cloud storage inherently means giving your files—encrypted or otherwise—to someone else, so it is better if you do not need to trust him.

SMiD Devices: The solutions that give you exclusive control over your Cloud Store Data

You just have to choose the right cloud storage provider(s) and take security matters into your own hands.

SMiD solutions are completely plug & play data protection devices designed even for SMBs or company departments.

They automatically encrypt the information and store it where you want. They work with up to 7 different cloud providers, allowing having an automatic and private backup outside the office (or inside if you need).
Strong encryption keys are generated into each device and never go outside; they are always under the information owner control.

No one will ever see what you store in the cloud. The key to SMiD security is not just its deep round-the-clock encryption, but its absolute inability to be accessed by anyone else.

Get all the benefits of cloud storage – flexibility, cost-savings, scalability, convenience – while ensuring your data remains 100% safe and confidential, round-the-clock.

SMiD is Simple, Flexible and Secure

- Compatible with local and cloud storage. Storage provider Independence. Private & automatic cloud backup
- No local risk of unwanted access, theft, loss or disaster
- No client software installation required
- Encryption keys exclusively under the user control. Only the user can turn the device on with his startup key. Client-side encrypted data storage
- Security independent of passwords or passphrases. Long, internally-generated, random cryptographic keys.
- Cryptolocker and other ransomware protection
- Any infrastructure or operating system
- Legal compliance
9. Contact Information

Valle Fernández, CEO

Tel +34 915 466 856
valle.fernandez@smidcloud.com

“Everything we design is deeply based on research. We stay up-to-date on the latest and greatest IT innovations, and take our time to perfect and assure that our solutions have the right functionalities the customer needs.”

Company information

SMiDCloud is a technology company that creates innovative cybersecurity solutions that effectively ensure the security and privacy of information stored both in the cloud and locally.

SMiD Cloud’s team designed SMiD to provide the market with the first device capable of managing information security automatically and transparently for users. Users select any cloud storage provider to be managed with their SMiD device, and SMiD renders all data completely unreadable to anyone but the user. It removes risk and complication from the cloud storage equation.

SMiD Cloud delivers cybersecurity solutions that are designed to meet the needs of different kinds of cloud storage users – from home-based professionals, to law firms, to high-security corporate departments with stringent data protection policies.