

Cloud computing or the data in the clouds

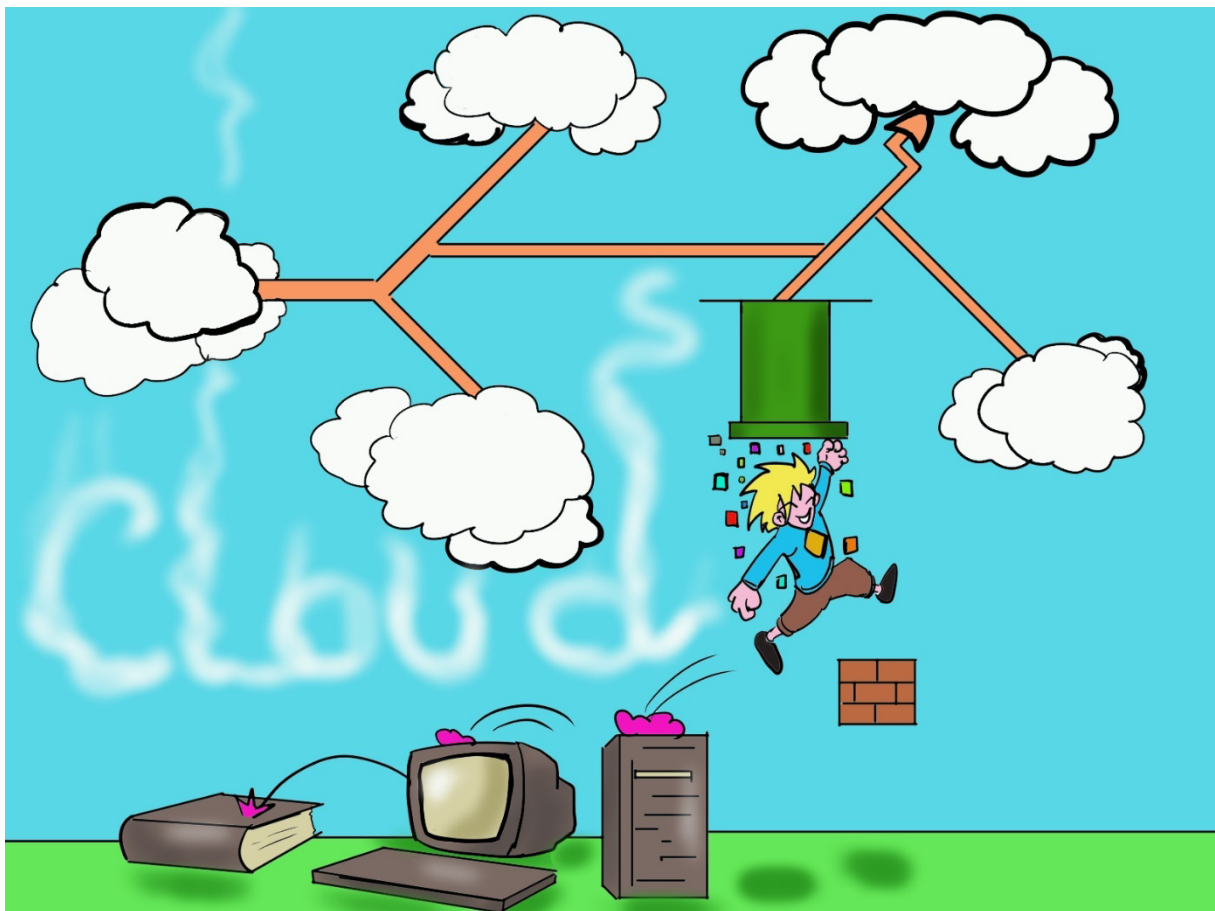
Translated into French as « *Informatique dans les nuages* », Cloud computing or Cloud is a system of storage and tools that has developed with the digitization of society and continues to grow.

It is as much about storing personal data as it is about using software or even gaming.

Initially reserved for professionals, this external network is now used by everyone, sometimes without even knowing it!

So when someone watches a video, on Netflix for example, the film is not usually downloaded to their tablet unless they request it. Instead, they access it via the broadcaster's cloud. The same applies to smartphone e-mail.

To access the cloud, the user needs an Internet connection and a software/application that enables data to be saved and consulted.



To give you a better understanding of this concept, this factsheet aims to present the Cloud with its main advantages and disadvantages, and to highlight the main questions it may raise in terms of data protection.



What is Cloud computing ?

Although the terms Cloud computing and Cloud are not yet uniformly defined, they do cover **all remote storage solutions**.

To put it plainly, the data or tools of a user or company (« *the customer* ») are no longer stored on his or her hard disk, but are available on remote servers accessible via the Internet.

These data are stored by IT infrastructures physically distant from those of the customer, in huge rooms known as « *data centers* ». These rooms, filled with powerful servers and computers, offer tools and/or **record, store, back up, protect and administer** all the data sent by everyone.

For the average person, the Cloud is therefore not physical but **virtual**, and corresponds to a **network of remote servers** scattered across the globe, but connected to each other and operating as a single system or network.

It takes its name from the English word for « *cloud* » because in the early 1990s, it was common practice to represent the Internet as a cloud in network diagrams.

As for the data stored in the Cloud, once connected to it, they can be accessed **anytime, anywhere, from any equipment** connected to the Internet.

Finally, it's important to note that some of the systems that use the Cloud, such as Google Drive or iCloud, are free, while others are not (Netflix or Disney+, for example).

What are the different types of Cloud?

There are four main types of Cloud.

The public Cloud	This is a Cloud deployment model where the IT resources do not belong to the end user but to a Cloud service provider, i.e. a company that offers infrastructure, platforms and/or software via a network. The Cloud service provider exploits these IT resources and shares them with a number of organizations and/or individuals. These resources, accessible via the Internet, are thus open to all and shared. However, the data and applications of each customer, i.e. anyone working in the Cloud, remain isolated and hidden from other Cloud customers.
-------------------------	---

	The supplier is responsible for maintaining the resources and guarantees availability, reliability and security through service level agreements. This is the most common model. Examples: AWS (Amazon Web Services), Microsoft Azure
The private Cloud	This is a model in which all resources are reserved via the Internet or an internal network for the exclusive use of a clearly defined group of users or entity. The resources are therefore inaccessible to any outsider. Private Cloud services are usually specially designed to meet customers' needs in terms of performance, storage capacity and network. Customers have the choice of hosting the private Cloud infrastructure directly on their own site (« <i>on-premise</i> ») or potentially in the supplier's data centre. Example: OVH
The hybrid Cloud	A hybrid Cloud combines several types of Cloud environments, including public and private Clouds, and may also include on-premises hosted infrastructures. For a Cloud to be truly hybrid, there must be a combination of at least 2 Cloud environments that exchange information with each other and run a uniform set of applications on behalf of a customer. Examples: - a combination of at least one private Cloud and one public Cloud; - a combination of at least two public Clouds; - a combination of at least two private Clouds.
The multi Cloud	In this model, customers run applications using Cloud services from at least two Cloud service providers to build, operate, access and secure applications consistently across all Clouds. This also minimizes dependency on any one supplier. Example : Anthos, the Google Cloud hybrid platform

How can the Cloud be used?

The Cloud makes it possible to provide a number of **services** (office tools, email, accounting, etc.) that can be defined according to the **roles** and **uses** of both the companies providing the service and those using it.

Traditionally, there are 3 main operating modes:

The IaaS mode (Infrastructure as a Service)

The Cloud makes it possible to implement a **virtual infrastructure** (server, virtualization layers, storage, networks) on which the user company can host operating systems, servers and application software.

The Cloud provider manages the **IT infrastructure alone**, while the customer manages the installation, configuration and updates of the operating system, middleware and applications, data, etc.

So only the **hardware infrastructure** is dematerialized.

Managed by the supplier	Virtualisation Servers Storage Network
Managed by the client	Data Applications Runtime environment Containers Operating system

The PaaS mode (Platform as a Service)

The Cloud makes it possible to implement a **platform for running software and applications**, on which the user company can install, configure and use the desired applications

With this solution, the supplier provides the **technical infrastructure** as well as a **set of integrated tools** for developing applications (operating system, database, etc.) and a web server. The customer focuses on developing the applications.

Managed by the supplier	Virtualisation Servers Storage Network Runtime environment Containers Operating system
Managed by the client	Data Applications

The SaaS mode (Software as a Service)

The Cloud provides the **software or application**, combining IaaS and PaaS services with installation, maintenance and configuration.

It's an interface that allows **the software to be used simply**, and requires no prior IT or technical knowledge.

Managed by the supplier	Data Applications Runtime environment Containers Operating system Virtualisation Servers Storage Network
--------------------------------	--

In a nutshell :

Operating modes	IaaS	PaaS	SaaS
Managed by the supplier	Virtualisation Servers Storage Network	Virtualisation Servers Storage Network Runtime environment Containers Operating system	Data Applications Runtime environment Containers Operating system Virtualisation Servers Storage Network
Managed by the client	Data Applications Runtime environment Containers Operating system	Data Applications	

What types of Cloud storage are available?

There are three of them:

- **object storage:** objects store unstructured data such as photos, videos, machine learning (ML) data, sensor data and audio files.

These data are stored by the objects in the format in which they arrive, enabling the metadata to be customized to make it easier to access and analyze the data.

Instead of being organized in hierarchical files or folders, objects are kept in secure compartments that offer virtually unlimited scalability.

- **File storage:** applications very often use file-based storage or file storage, which allows them to store data in a hierarchical folder and file format.
- **Block storage:** this is useful for enterprise applications such as databases or enterprise resource planning (ERP) systems, which often require dedicated, low-latency storage for each host.

Each block has its own unique identifier for fast storage and retrieval.

What are the advantages of the Cloud?

The benefits of the Cloud, for businesses and individuals alike, are numerous. These include

- **reduced costs:** organizations no longer need to purchase all the IT equipment that was once essential to their business, leading to a reduction in initial investment costs. They no longer have to obtain additional storage space or capital during peaks in activity.
What's more, the absence, in some models, of maintenance and a dedicated technical team means that savings can be made. Similarly, the subscription system allows customers to pay only for what they use.
- **flexibility and scalability of services:** depending on requirements, it is possible to increase or reduce the use of the IT resources on offer. What's more, Cloud-managed services are regularly updated.
- **virtually unlimited storage capacity:** providers are constantly **building** new data centres.
- **time savings:** the Cloud provider manages a number of constraints itself, such as maintenance, without the customer having to intervene.

- access to **very high** quality services without prohibitive costs.
- **easier data sharing**: any Cloud user can make their data available to one or more other Cloud users.
- **total accessibility**: applications are designed to be accessible anywhere, from any connected device;
- **data security**: the Cloud offers a higher level of security than a traditional system consisting of physical machines. Indeed, once the data are in the Cloud, a lost or stolen laptop is no longer a major concern.
What's more, storing data in the Cloud means you can always control where the data are stored, who can access them and what resources the customer consumes.
- **Business continuity**: data centres are highly secure, protecting data and guaranteeing business continuity. In the event of a disaster affecting the customer's premises (fire, for example), the data are no longer lost.

What are the disadvantages of the Cloud?

Despite its many advantages, Cloud Computing also has its drawbacks:

- **dependence on the Internet**: in the event of a breakdown, the entire activity of the organization is disrupted.
- **technical dependence on Cloud suppliers**: the organization may become dependent on the service offered by a supplier. What's more, the lack of interoperability between systems may prevent it from leaving its supplier.
- **loss of control** over the IT system: the organization no longer has complete control over the system, and the applications used may change at any time, in favour of others that are more efficient or better adapted to the provider's hardware.

What are the specific risks in terms of personal data protection?

As well as striking the necessary balance between the advantages and disadvantages of the Cloud from a practical point of view, we also need to consider the risks posed by this storage system in terms of protecting personal data.

Data lie at the very heart of the services offered by Cloud computing, and as with all IT projects, data security is analyzed in terms of data **availability, integrity and confidentiality**.

The main risks are as follows:

- **security risk:** even if the level of security offered by Cloud service providers is high, the risks of technical breakdowns and computer attacks cannot be ruled out, especially as the concentration of all data in one place is particularly tempting for hackers. The fact that data are transmitted over the Internet also increases the risks.
- **a risk of data loss** during backup or storage procedures.
- **a risk of data leakage and loss of confidentiality**, due to the number of existing servers and their relocation.
- **a risk of loss of control** (or sovereignty over the data), particularly as regards the location of the data and its subjection to the laws and regulations in force in the national territory where the servers are located (e.g. data placed in a Cloud, with servers based in the United States). In addition, many countries have put in place legislation or practices, such as the US Cloud Act, that allow them to access data hosted on Cloud services.

What is the Cloud Act?

The Cloud Act (Clarifying Lawful Overseas Use of Data Act) is an American law that allows the judicial authorities to access electronic data stored abroad by American companies, as part of criminal proceedings.

Under this law, it is therefore possible for the US government to access servers in Europe, and therefore in Monaco, as long as the company is American or has a business relationship with the United States.

A study published in August 2022 by the Dutch Ministry of Justice concluded that European entities can be subject to this extraterritorial law even if their registered office is not in the United States, as long as they use American technologies

It even states that the Cloud Act also applies when a European Cloud provider uses American hardware or software.

- a risk of data being **transferred to a country that does not have an adequate level of protection**, subject by law to certain rules such as the implementation of appropriate guarantees (e.g. signature and implementation by data exporting and importing entities of the European Commission's standard contractual clauses) or, in rare cases, prior authorization from the APDP.

[For more information, refer to the factsheet **Data transfers outside the Principality : scenarios to consider**]

What measures should be taken to secure the Cloud?

While there is no such thing as zero risk, there are a number of measures that can be taken to protect data in the Cloud, taking into account factors such as the type and sensitivity of the data to be protected.

The main measures are as follows:

Cloud configuration

A large number of data breaches in the cloud are due to basic vulnerabilities, such as configuration errors.

To reduce these errors, it is important to:

- change the **default settings set in their original state**;
- **never leave a cloud storage bucket (container) open**;
- use the **security commands** offered by the service provider.

Securing accounts

To prevent malicious software from infiltrating operating systems, **anti-virus and anti-malware software** must be installed and regularly updated.

Similarly, **all devices used** to access data in the Cloud must be **secure**, including smartphones and tablets. Indeed, if data are synchronized on several devices, the risk of one of them being compromised and affecting the others increases.

Configuring access to data

Not everyone within an organization is necessarily entitled to access all the information available in the Cloud. It is therefore important for IT teams to ensure that administrator privileges are only accessible to those who really need them, and that these administrators' accounts are properly secured.

Similarly, it is important to ensure that access to data is **restricted to duly authorized users only**, and that these access permissions are removed or modified as soon as users are no longer authorized to access a resource because they have left the organization or changed functions.

Securing access to accounts

Passwords used to access accounts must be secure. **Unique and complex passwords** should be used, which should be **renewed regularly**, and **multi-factor authentication** should be used to provide an additional barrier in the event of the password being divulged.



Using a password manager can be a good idea if you want to assign separate, complex passwords to each application, database and service, without having to remember them all.

Encrypting data

Because they move from one storage location to another, data hosted in the Cloud are more likely to be intercepted. To make them less vulnerable, different encryption methods can be used to ensure that communications cannot be accessed by outsiders at any time without the encryption key:

- **end-to-end encryption** of all data uploaded to the Cloud (recommended for financial, confidential or commercially sensitive information);
- **encryption of all communications** with the Cloud;
- **encryption of particularly sensitive data**, such as account identifiers.



If possible, it is strongly recommended that you use **your own encryption keys** and not those of the service provider. It is also very important to manage encryption keys **safely and securely**. It is therefore advisable to store them carefully outside the Cloud, within the organization itself. You might also consider **updating them regularly**.

Installing security updates

Cyber criminals are always on the lookout for vulnerabilities, so it is always a good idea to install security updates and patches as quickly as possible.

Checking the security of the Cloud service provider

With the use of Cloud computing, cybersecurity is no longer the sole responsibility of the customer, but also depends on the service provider. It is therefore important to ask yourself the following questions before choosing your supplier:

- Are external security audits carried out regularly?
- Are customer data logically segmented and stored separately?
- Can the data be encrypted? Are they encrypted? Which parts are encrypted?
- What policies are applied to the storage of customer data?
- Are data properly deleted when a service is exited from Cloud?
- How are access rights controlled?

You should also read the supplier's terms and conditions of use (T&Cs) carefully, and check in particular that data are not stored on servers located in countries that do not offer an adequate level of protection.

Putting in place internal procedures

It is also advisable to establish internal security policies dedicated to the Cloud, as well as providing awareness training for employees.

What is a sovereign cloud?
Growing concern in Europe about the increasing dependence of businesses and institutions on large American Cloud providers is prompting many countries to promote « <i>trusted Clouds</i> », using the technology of the American giants but operated by European companies, in data centres located in Europe. The Sovereign Cloud is therefore a deployment model in which the hosting and all the processing carried out on data by a Cloud service are physically carried out within the limits of national territory by an entity governed by national law and in application of national laws and standards, in order to preserve the security and confidentiality of these data. As a result, in 2021, the Principality of Monaco launched its own sovereign Cloud, which currently relies on two data centres on national territory and a backup data centre in Luxembourg.