Cloud Computing Issues: A Possible Solution

Maddalena Castellani <castellani@triberticastellani.com>
MILANO, Italia

Roberto Giacobazzi <roberto.giacobazzi@univr.it>
VERONA, Italia

Cesare Triberti <triberti@triberticastellani.com>
MILANO, Italia

Abstract
While the current Pandemic has accelerated the strong link between IT and enterprise, it has also shown how current technology systems are increasingly at risk of cyberattacks.

In this article we will deal with Cloud Computing systems, whose use is increasingly central to enterprises, first analyzing the legal aspect within the larger set of outsourcing contracts, highlighting the strengths and weaknesses (especially regarding the need to comply with the rules provided by the GDPR), and then offer a possible technologically advanced solution (Homomorphic encryption) to the problem of data protection, confidentiality and security of data stored in systems based on the Cloud.

Keywords:
cloud computing; Outsourcing; Virtual Organization; Saas, Iaas; Daas; Privacy; GDPR; *homomorphic encryption*; cybersecurity; Cryptography; Man-At-The-End (MATE) attack; obfuscation

1. Cloud Computing, Outsourcing

The IT world is continuously evolving.

Its relationship with the business world has a twofold impact: on one hand, Information Technology allows economic relations to evolve, on the other, the business world is always looking for new technological solutions that allow continuous development and improvement.

An example of this is the increasing dissemination of software solutions in the marketplace: first through licensing and software development contracts, then through service contracts, spread around the world by the Internet[1].

In this continuously evolving world, the development of service contracts such as Outsourcing, Facility Management and Disaster Recovery fits perfectly with notions of Cloud Computing.

In the second part of this paper, we will examine the IT aspect of Cloud Computing and identify a possible solution to the problems raised in the first part, in which some of the legal risks of Cloud computing will be analyzed, focused mainly on security risks to data stored in Cloud-based systems.

The protection and confidentiality of data, as well as the need for companies to comply with the General Data Protection Regulation[2], has put the "privacy" issue squarely at the door of Cloud computing, due to the technological structure underpinning this service.

Great attention must be paid to the "privacy" risk since most online trials are now conducted on Cloud platforms.

Civil law, unlike common law, allows parties to stipulate contracts governed by the Italian Civil Code, which lays down precise rules for standard contracts. Non-standard contracts can also be stipulated, on condition that they comply with all the mandatory regulations[3].

IT contracts can be categorized both as typical (for example, software development and IT services) and atypical: in the latter case, the parties may use the principle of analogy, with software licenses as the template.

The codified system has also enabled the creation of a series of criminal laws against computer crimes, thereby overcoming the prohibition on the use of analogy in criminal cases.

Let us return to the central issue.

---

1 Cesare Triberti and Giuseppe Carrella, *Internet ,aspetti tecnici, tematiche sociali, incidenze giuridiche civili e penali*, (Edizioni Maros Milano (ITA), 2000).

2 European Parliament, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L199/1 (General Data Protection Regulation).

3 Art. 1322 c.c. (ITA) in <https://www.gazzettaufficiale.it/atto/serie_generale/caricaArticolo?art.progressivo=0&art.idArticolo=1322&art.versione=1&art.codiceRedazionale=042U0262&art.dataPubblicazioneGazzetta=1942-04-04&art.idGruppo=163&art.idSottoArticolo1=10&art.idSottoArticolo=1&art.flagTipoArticolo=2> accessed 1 August 2021.

Cloud computing is remarkably like an outsourcing contract, since it operates on the same technological and legal bases[4].

Outsourcing underpinned the spread of computer services throughout the industrial and commercial world, cutting labor costs (initially in the IT departments of the banking and assurance sector, then within big business).

This economic and technological boost paved the way for Cloud Computing.

There was a gradual transition from Grid systems to Cloud Computing, which is essentially an elaborate Grid system.

This is a complex infrastructure of dispersed computing power that was the driving force in the bulk processing of data.

This backstory and its parallel technological evolution are reflected in a single virtual computational system that offers the maximum potential in the use of shared applications, the concept behind the notion of the Virtual Organization.

A Virtual Organization is a set of human and technological resources that can best exploit this kind of asset sharing.

Users can view all the resources and access modes, benefitting from a high standard of security and authentication.

These resources are integrated in a Database that does not depend on a central repository but is generated by a network of independent servers, which keep records of the transactions carried out and can aggregate this information in multiple ways.

The Grid coordinates and shares all the resources using different procedures and does not need centralized control.

It employs differentiated protocols able to guarantee users a quality service center (so-called QoS, quality of service)[5].

Users can make use of the different computing resources "on demand" and can access and manage reams of data, even if such data are distributed in different ways.

So the Grid is an ASP, Application Service Provider, the Service Level Agreement of which is contractually regulated both in terms of the services offered online, and the levels of management and security.

---

4 Triberti and Carrella (n 1) 132-139.

5 Yang Yong, Dumas-Menijvar Marlon, Garcia-Banuelos Luciano, Polyvyanyy Artem and Zhang Liang, 'Generalized aggregate Quality of Service computation for composite services' (2012) 85, 8 Journal of Systems and Software 1818-1830.

While there may be structural differences, it is but a short step from the Grid to Cloud Computing.

The National Institute of Standards and Technology (NIST) defines it as:

> "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.".

NIST offers five specific features of Cloud Computing, as follows[6]:

1. On-demand self-service.
2. Broad network access.
3. Resource pooling.
4. Rapid elasticity.
5. Measured service.

Here is a brief analysis.

On-demand self-service allows instant, automatic access to Cloud Computing resources without human interaction with the provider.

Broad Network Access makes possible the access and use of resources through the network (such as the Internet) using standard mechanisms compatible with uniform platforms, such as personal computers and intelligent telephony systems with their multiple applications.

Resource Pooling offers the possibility of placing the resources of a specific provider at the service of multiple users, taking advantage of the service's multi-tenancy and virtualization features, so that the consumer accesses them depending on specific needs.

Rapid Elasticity identifies the immediate flexibility in providing and releasing resources based on user demand. The consequence is that the requested resources are provided immediately, and without limitation on "consumption", multiplying in line with requirements.

Measured Service provides the Cloud system with the ability to control and make the best use of resources, delivering what each individual needs,

---

6 Eric Simmon, 'Evaluation on cloud computing servicesbased on NIST 800-145' (National Institute of standards and Technology (NIST), February 2018) 4 <https://doi.org/10.6028/NIST.SP.500-322> accessed 1 August 2021 , <https://www.nist.gov/system/files/documents/2017/05/31/evaluation_of_cloud_computing_services_based_on_nist_800-145_20170427clean.pdf> accessed 1 August 2021.

simultaneously measuring the use and cost, while increasing the service's transparency.

2. *Features of the Services*

All the services that can be delivered through Cloud Computing have been universally identified: increasing the possibility of new applications and improving the quality of the services.

Software-as-a-service (SaaS) is a software distribution model in which customers pay a periodic subscription or licensing fee and a third party, typically the software vendor, makes the application available over the internet. SaaS is one of the primary commercial applications of Cloud computing. In the SaaS model, rather than buying a physical copy of an application and installing it on a local server, the software vendor gives customers access to the application via the internet, hosting and maintaining it on their own servers.

What's more, any maintenance and troubleshooting of the underlying infrastructure remain the sole responsibility of the Software-as-a-Service provider, leaving the customer with more time to focus on strictly business-related matters. Another vital aspect of SaaS products is that they are constantly evolving and are regularly updated.

This category also includes the hardware (known as the Virtual Machine (VM)), consisting of large-scale servers.

With this service (anticipating the definition of Computer Service, the legal aspects of which will be examined below), a customer accessing the Cloud needs no technical knowledge or specific hardware/software resources.

It offers centralized access to an application via the Web.

Extensive IT knowledge or the downloading of updates or new files are not required since they are part of the contract.

A single application can operate with many users, maintaining the logical separation of each user's data.

Platform as a Service (PaaS) is a complete development environment hosted in the Cloud that enables application developers to create apps quickly and easily. It usually includes an Operating System, web server, tools, programming language, database, network, servers, storage and more. The PaaS provider hosts and maintains the system and may often construct its own solutions tailored to the unique needs of the customer. Users retain control of the applications and many providers offer pay-as-you-go and other online pricing models.

This is a type of Cloud service that is particularly suitable for developing, managing and distributing applications.

By offering a platform equipped with all the necessary tools for the testing, development and deployment of applications in the same environment, PaaS eliminates the need to be concerned about anything other than development through the full underlying infrastructure, using the advantages of security, server software and backup, programming languages, libraries, services and dedicated tools, all developed by the provider.

Infrastructure as a service (IaaS) is a form of Cloud computing that provides virtual computing resources over the internet[7].

In the IaaS model, the Cloud provider manages IT infrastructures such as storage, server and networking resources, and delivers them to subscriber organizations via virtual machines accessible through the internet. IaaS offers many benefits for organizations, potentially making their work faster, easier, more flexible and cost efficient.

In an IaaS service model, a Cloud provider hosts the infrastructure components that are traditionally present in an in-house data center, including servers, storage and networking hardware, as well as the virtualization or hypervisor layer.

IaaS providers also supply a range of services to accompany the infrastructure components. These can include detailed billing, monitoring, access logs, security, load balancing,

clustering and storage resiliency, such as backup, replication and recovery.

These services are increasingly policy-driven, enabling IaaS users to implement greater levels of automation and orchestration for important infrastructure tasks. For example, a user can implement policies to drive load balancing in order to maintain application availability and performance.

Data Storage as a Service or DaaS (also known as Desktop as a Service) is directly related to the concept of virtualization on demand.

The service is based on the development of deduplication technologies that, in turn, deploy a hypervisor, that is, a particular technique of storing a computer's operating system configuration as if it were an image (snapshot) making it possible to issue the same type of configuration to one or more locations.

The data are made available via the Web and users can access them through any application, ensuring the best the provider can offer on the network, including storage, backup, and security systems. The customer

---

7 Xenofon Kontargirys, *IT laws in the era of cloud computing*, (Nomos, 2018).

does not have to pay the whole cost of a database license, only for what is used.

It is clear that the Cloud service features examined above have several points in common, like the ease of access, maintaining data separation even on a multiple-user service, cost savings for software supply and updating. These are borne by the provider, as well as the proper maintenance for remote access to services and the option of using services available on multiple Clouds.

They also differ, insofar as there is a Private Cloud and a Public Cloud.

With a Private Cloud, infrastructure use occurs only within a single operational structure/company that manages it directly or delegates management to a third party.

In the case of an in-house service, this means better use of the company's internal resources, the management of security and privacy of data and a reduction of costs compared to the use of a Public Cloud.

In-house management involves the configuration of servers in terms of hardware and software, plus the virtualization.

Conversely, in the Public Cloud, the Provider is responsible for the management and ownership of the entire structure, where they operate directly on the servers used by customers and manage the use of resources required by each client, providing them with ease of use and lower costs.

Finally, there is the Hybrid Cloud, a combination of private and public Clouds. The user can benefit from the greater flexibility of the Public Cloud, while maintaining their own data inside the company.

This type of solution demands a careful distribution of the different processing loads by combining the two architectures, private and public.

3. Advantages and Disadvantages of Cloud Computing

A special outsourcing contract with a supplier specialized in the management of computer resources via the Web means no costs for employees, hardware or software updates.

The costs and infrastructure remain the burden of the provider offering an on-demand service.

The individual contracts establish the appropriate clauses and the different costs of the service on a periodic basis or depending on use (on-demand).

They also offer peace of mind. The risk of interruptions due to system failures is non-existent since, even if a node fails, the service will still

be available and someone else will be worrying about maintenance and restoration costs.

The downside is the issue of the privacy and security of customer data, which requires careful risk assessment in the management and storage.

4. *Legal Aspects: Security and Risk in Cloud Computing*

In such a highly innovative and functional system, featuring a vast range of available services, the problem arises of guaranteeing the security and integrity of the data of customers or third parties.

So, what is Cloud Computing in the eyes of the law? This must be understood on order to allow users to take appropriate security measures to prevent breaches of network integrity and data security.

Under civil Italian law, the Cloud is a computer service contract (Outsourcing).

It is a procurement contract (art. 1655-1677 c.c.)[8], which can also be qualified as a "mixed" procurement contract, that is, it covers the service itself and supplementary software developments or additional applications, which have no effect on the legal definition.

All contracts involve a series of mutual guarantees between the client and the contractor, with prevalence given to the protection of the client. These guarantees established by the Civil Code "must" be specifically mentioned in the contract between the client and the Cloud provider.

In particular, all possible critical situations in the performance of the service must be regulated in detail.

There are “general contractual clauses” that are common to all IT contracts.

For example:

- Hardware Structure
- Software Structure
- Specialist Resources
- Limits on the Use of other Structures and/or Resources without Charge or a Reduction in the Quality of Service for the “User”.

8 Art. 1655 c.c. (ITA) in <https://www.gazzettaufficiale.it/atto/serie_generale/caricaArticolo?art.versione=1&art.idGruppo=208&art.flagTipoArticolo=2&art.codiceRedazionale=042U0262&art.idArticolo=1655&art.idSottoArticolo=1&art.idSottoArticolo1=10&art.dataPubblicazioneGazzetta=1942-04-04&art.progressivo=0> accessed 1 August 2021.

But there are also "special" clauses for the Cloud, designed to protect and guarantee this specific type of IT service. Firstly, risks may arise from specific criminal actions carried out by third parties against the customer's data and systems, the negative effects of which obviously extend to the Cloud provider.

The regulations on Computer Crimes are an example. They cover unauthorized access to a computer system or remaining on it without authorization, the damaging or extraction of data or the unlawful discovery of information, especially business information.

Special attention must be paid to the European Privacy Code and, in particular, to the regulations laid down by the GDPR, which governs the correct use of data and penalizes any behavior in breach of its provisions[9].

In summary, a list of critical issues is given below:

- the secure transfer of data from the customer to the Cloud;
- the secure management of data within the Cloud;
- the secure management, in accordance with agreed methods, of restoring data to the client;
- the coordination of data management, data transfer or sharing between different Clouds, particularly if they are located in distant geographical areas and subject to different jurisdictions;
- the accurate identification of each customer's data within the Cloud and the secure extraction of only the data required;
- the technological guarantee of interconnectivity related to the Virtual Network;
- problems of jurisdiction and applicable laws (divergent regulations between States and conflict between civil and common law) without precise contractual definition;
- the responsibilities of the Administrative Bodies of companies towards the shareholders for security breaches and consequent damage;
- the correct use of encryption as the primary guarantee against unlawful data access.

The foregoing highlights the need both for correct contractual management and technological advances, not only in the ordinary management phase of the Cloud, but also for the effective defense against cyberattacks, given that the pervasiveness of Cloud-based IT systems is now well established.

9 Kontargirys(n 7) 181.

5. A Possible Solution

As mentioned above, every Cloud-based system needs secure data management on the part of Cloud providers and the problem of privacy protection lies with them. These issues are impeding the deployment of Cloud services when large volumes of sensitive data are involved. The ultimate frontier of data security and privacy for Cloud computing is represented by *homomorphic encryption*. Homomorphic encryption is intended to solve the problem of malicious misuse of data in remotely executed algorithms, such as the Cloud. In a Man-At-The-End (MATE) attack scenario[10], the security, the integrity, and in particular the privacy of sensible can be compromised. A MATE attack scenario is characterized by two parties, say Alice and Bob, that are supposed to cooperate in order to achieve a given result. In this scenario, we may assume Alice to be a trusted entity, while no trust can be ensured for the case of Bob. In our setting, Alice can be a user of a Cloud service and Bob can be the Cloud service itself, here specified by a set of functionalities that operate on Alice' data in order to produce a result that can be useful for Alice. A MATE attack holds when Bob intentionally, or because he has been hacked, performs a malicious misuse of Alice' data, with the specific intent of breaking privacy and integrity constraints on the information provided by Alice. Here Bob' Cloud service corresponds to perform some operation op on Alice' private (or partially private) data set D. Examples are the analysis of financial data to evaluate specific assets, or a machine learning-based analysis of a CT Scan image for specific medical diagnosis. In a Cloud computing environment we can imagine that the operation op will be performed remotely on the Cloud servers under the control of Bob' Could algorithms. Alice, who can be a trusted financial advisor or an MD at your trusted medical center, provides the data D to the Cloud (Bob) and receives back an analysis. If this protocol has been attacked in a MATE attack, an adversary (e.g., Bob or a hacker) gains the control of Alice' private data at the Cloud level. This could violate the privacy and integrity of Alice' medical records and other sensitive personal data. On a larger scale, this phenomenon could cripple a national infrastructure and national security.

Several solutions have been put forward in Computer Science (CS) to overcome MATE attacks. It is clear the difference between a MATE attack

10 Christian Collberg, Jack Davidson, Roberto Giacobazzi, Yuan Gu, Amir Herzberg, and Fei-Yue Wang, 'Towards Digital Asset Protection' (2011) 26(6)IEEE Intelligent Systems 8-13.

and a Man-In-The-Middle (MITM) attack. In the latter a standard encryption mechanism can be extremely effecting to protect all communications between Alice and Bob. In MITM attacks, both parties Alice and Bob are trusted entities and only the communication has to be protected, while in MATE attacks it is one of the two parties of the protocol that can be untrusted. Code/Data obfuscation, white-box cryptography and (fully) homomorphic encryption are solutions designed specifically in order to solve the problems of privacy and integrity in MATE attacks.

Code/Data obfuscation and White-Box Cryptography are partial solutions to this problem[11]. In code/data obfuscation and white-box cryptography, the structure of our asset is intentionally morphed in order to maintain the sensible information secret and protected. This can be performed easily and usefully in many contexts, such as in code protection against reverse engineering or for hiding cryptographic keys for protecting digital assets (e.g., DRM in music, video etc). This technology has a major drawback: the information that is made secret cannot be used by the third party, e.g., the Cloud, simply because the same existence of this information is hidden to the Cloud.

In a (fully) homomorphic encryption (FHE) mechanism[12], the operation op operates homomorphically with respect to the primitives of encryption Enc_k and decryption Dec_k for some private key k, if the following equation holds for any possible (private) data set D:

$Dec_k(op(Enc_k(D))) = op(D)$.

In a sentence: the operation op can operate on encrypted (hence protected) data set D producing a cyphertext that, once decrypted (e.g., by a private key) results in the correct application of the operation op to D. FHE enables the design of programs for any desirable functionality, which can run on encrypted inputs and produce an encryption of the expected result. The key point is that the private key k is unknown to the operation op. Therefore, such programs never really decrypt their inputs, i.e., they never reveal to the untrusted user the private data set D and can therefore run by any untrusted party without compromising privacy, security or integrity. This *magical* mechanism is reality and several solutions are known in this field with an endless effort by scientists and engineers to make it available

11 Obfuscation: Finn Brunton and Helen Nissenbaum, *A User's Guide for Privacy and Protest* (MIT Press 2015).

12 Craig Gentry, 'Fully Homomorphic Encryption Using Ideal Lattices' (the 41st ACM Symposium on Theory of Computing (STOC) 2009).

as service to users[13]. Two are the main issue of FHE: *Scalability* and *expressivity*. Scalability means that the current technology can handle relatively small amounts of data with e relatively high computational effort. While scalability can be overcome by the advancements of the technology or by weakening the FHE paradigm, by restricting the full privacy only to portions of the data set D, the expressivity issue is more fundamental. We know that we can implement any Boolean circuit in FHE, but can we imagine to run in FHE any program? Namely can we imagine of having a FHE interpreter that can run an arbitrary program? If we impose limitations on the way programs run (e.g., in the amount of memory used or computational time complexity) the answer is yes. It is still not clear whether a FHE system can run an arbitrary program. This means that, while Alice can keep secret her data set D to Bob, yet achieving the desired result op(D) but computed by Bob on $Enc_k(D)$, hence without knowing D, if D is itself a software component and the operation op that Bob is required to perform is just its remote execution, then it is not clear whether Bob can provide this service in FHE for all programs D. Therefore, while data protection can be and will eventually be protected by FHE, the protection of software assets is way more complex and probably impossible.

13 Homomorphic Encryption Standardization: <https://homomorphicencryption.org> accessed 1 Auugust 2021.