Cloud Computing Security

Article · March 2020

CITATIONS
0

READS
79

1 author:

Pedro Brandão
Universidade de Évora
19 PUBLICATIONS **2** CITATIONS

SEE PROFILE

Cloud Computing Security

Pedro Ramos Brandao
Interdisciplinary Center for History, Cultures and Societies (UID/HIS/00057/2019)

Abstract
This work approaches security in Cloud Computing. Key aspects of cloud computing are developed. One will initially review the core concepts inherent in Cloud Computing, then the issues of security and privacy will be addressed. The relevant risks in Cloud Computing environments will be analysed, and some solutions for problem mitigation will be presented.

Keywords
Cloud Computing, Security, Privacy, Confidentiality.

I. Introduction

Cloud computing is a new computing model that allows the user to access a large number of applications and services from anywhere, regardless the platform, just having an access terminal connected to a platform with Cloud Computing [1].
The word suggests an idea of an unknown environment, to which we can only see the beginning and the end. For this reason, this expression has been well used regarding this new model, where in fact all infrastructure and computing resources are "hidden", the user only has access to a standard interface through which the whole range of applications and services are made available [1].
The cloud consists of a communications infrastructure composed of a set of hardware, software, interfaces, telecommunications networks, control and storage devices which allow the delivery of computing as a service [2].
To make this model possible, it's necessary to gather all applications and user data into large storage centers, known as data centers. Once assembled, users' infrastructure and applications are distributed in the form of services made available through the Internet [1].
Another important point for understanding this computing model refers to the participants of the cloud. These can be divided into three major groups: Service Provider, Programmer, and User. The provider is responsible for delivering, managing and monitoring the entire cloud infrastructure, ensuring the level of service and adequate security of data and applications. The programmer must be able to provide services to the end user, from the infrastructure provided by the service provider. While the end user is the consumer who will use the features offered by the cloud computing [1].
Cloud computing represents a new service model that can provide all kinds of data processing, infrastructure and data storage over the Internet, based on the user needs.
Information security is of the utmost importance, whether for companies or for the individual himself, at all times we are subject to threats, whether their natural causes or not, intentional or not. Insider information about third parties in the hands of malicious people may cause irreparable losses, conflicts, and may decide the future of one or more people. Information may decide things and as such keeping secrecy is critical if necessary.
In a common computational scope this care must be doubled. In the cloud computing environment where everything is kept on the Internet this concern needs to be even greater, because the risks and threats are even more constant. The main concerns regarding cloud computing with respect to security lie in two fundamental aspects: privacy and security.

II. Key Features

The convergence of a range of important technologies enables cloud computing to deliver services transparently to the user, among other functionality and features. Technologically the main relevant fields in this area are: hardware, with capacity for virtualization; Internet technologies such as Web 5.0, web services; systems management, such as independent computing and data centre automation; distributed computing, especially utility & grid Computing [3].
Taking into account that the focus of this work is not cloud computing, but security, we will not explain each of these technologies mentioned above. But we will give a brief description of the main features.

A. Elasticity

Cloud computing provides the illusion of infinite computational resources available for use. Therefore, users are expecting the cloud to be able to quickly deliver resources in any amount at any time. It is expected that the additional resources may be provided, possibly automatically, when the request for services increases.

B. Self-Service

The consumer of cloud computing services expects to acquire computing resources according to their need and instantly. To support this type of expectation, clouds must allow self-service access so that users can request, customize, pay for and use the desired services without human intervention.

C. Billing and Measurement of use

Since you have the option to request and use only the amount of resources and services that you deem necessary, services should be charged based on that use, such as by measuring the use of processors in hours. For this reason, clouds must implement resources that ensure an efficient commerce of services, such as adequate charging, accounting, billing, monitoring and optimization of use. This measurement of resource use should be done automatically and according to the different types of services offered (storage, processing, and bandwidth) and promptly replenished, allowing for greater commercial transparency [3].

D. Broad Network Access

The resources must be available through the network and accessible through standard mechanisms that allow them to be used by heterogeneous platforms, such as smartphones, laptops, PDAs, among others [4].

E. Customization

In service to multiple users there is a great disparity between the needs of these, making essential the capacity of personalization of cloud resources. From infrastructure services, to platform services and software services.

III. Layered Architecture and Cloud Types

Cloud computing services are divided into three classes, which take into account the abstraction level of the feature provided and the service model of the provider. The level of abstraction may be

seen as an architecture layer where the services of the upper layers may be composed of the services of the lower layers. The three classes of service are named as follows: Infrastructure-as-a-service (IaaS), lower layer; Platform-as-Service (PaaS), intermediate layer; and Software-as-Service, top layer.

A. Infrastructure-as-Service - IaaS

In this class, infrastructure services are offered on demand, that is, virtualized hardware resources such as computing, storage and communication are offered. This type of service provides servers capable of running customized software and operating on different operating systems. It has an application that works as a single interface for infrastructure administration, promoting communication with hosts, switches, routers and support for the inclusion of new equipment. Because it's the lower layer, it's also responsible for providing the necessary infrastructure for the middle and upper layers.

B. Platform-as-Service - PaaS

This is the intermediate bed. It is offered as service, an environment in which the programmer may create and deploy applications without having to worry about how many processors or how much memory is being used to perform the task. Using the lower layer, it provides an infrastructure with a high level of integration compatible with various operating systems, programming languages and development environments.

C. Software-as-Service - PaaS

The highest layer of the cloud computing architecture is responsible for delivering end-to-end applications to the end user. This access is provided by the service providers through web portals, being completely transparent to the user, which allows the execution of programs that execute in the cloud from a local machine. To provide this transparency, SaaS uses the two lower layers, PaaS and IaaS.

IV. Implementation Models

The cloud implementation will depend on the need of the application to be offered and the type of service contract. Despite the appearance of services being publicly available, where any user has access to all types of cloud content, business models have promoted the development of implementation models that ensure an adequate level of control of the information to be made available and visibility in the cloud. Currently the implementation types are Public, Private, Community and Hybrid. In the public model the cloud is made available to the general public or to large industrial groups. The cloud implemented by a service provider, which must be able to guarantee its performance and security [4].

Private clouds are operated exclusively by an organization. The management of the network can be done by the organization itself or by third parties. If done by third parties, the infrastructure used belongs to the user, in this way, it is responsible for the control over the implementation of applications in the cloud [5].

The community model is characterized by the fact that the cloud infrastructure is shared by several organizations. And it supports a specific community which shares the same concerns as mission, security requirements, policy, and compliance considerations. It may be administered by organizations or by third parties and may exist locally or remotely [4].

In the hybrid cloud, the infrastructure is composed of two or more implementation models, each cloud remaining as a single entity, but united by the use of proprietary or standardized technology, ensuring data and application portability [4]. In case the hybrid cloud is made up of public and private cloud, it is characterized by the possibility of the private cloud having its resources expanded by reserving resources in a public cloud. This allows maintaining service levels even in case of rapid fluctuations in resource requirements. Another interesting feature is the use of it to perform periodic tasks which are more easily implemented in public clouds [5].

V. Advantages

Among the advantages of cloud computing there is the ability to access data and applications from anywhere, as long as there is a quality connection to the Internet, bringing mobility and flexibility to users. The payment-for-use model enables the user to pay only what he or she needs, avoiding wasted resources, and also thanks to scalability, it is possible to increase the availability of resources as the user verifies their need. This flexibility allows the risks related to infrastructure to be minimized because the company doesn't need to buy many physical resources and does not assume responsibility for the contracted infrastructure [5].

Other flexibilities consist of ease of use of services and resource sharing as well as reliability of services since the companies that offer the services are valued for their reputation, mainly for the ability to keep data secure through backup, encryption and strict access control.

Another great advantage is that companies which offer Cloud Computing ensure the contractual availability of information and services at 100%, that is, there will be no interruption of the flow of information or services.

VI. Disvantages

The main disadvantages of this technology are also key points for the its development, where it stands out:

Security: This is the most visible challenge to face because information that was previously stored locally will be located in the cloud in a physical location that is not accurate where it is or what types of data are being stored. The privacy and integrity of the information are then of paramount importance, as especially in public clouds there is a great exposure to attacks. Among the capabilities required to prevent information breaches are: data encryption, strict access control, and effective backup management [6].

Scalability is a key feature in cloud computing because applications for a cloud need to be scalable (or "elastic"). In this way the resources used can be changed according to the requests. For this to be possible, applications and their data must be sufficiently flexible. This task may not be simple and usually depends on implementation [7].

Interoperability is the factor in users' ability to run their programs and data across different clouds, so they are not restricted to a single cloud. This is a highly desirable feature in the cloud computing environment. Although many applications have tried to take this factor into account, there is a need to implement standards and interfaces to make this portability possible [8].

Reliability is related to the frequency with which the system fails and the impact of its failures (data loss or not). Applications developed for cloud computing must be reliable, that is, they must have an architecture that allows data to remain intact even if there are failures or errors in one or more servers or virtual machines on which those applications are running. This feature is related to the backup copy management policy [5].

Availability is a major concern because even Google systems, such as GMAIL, are unavailable, and even though the system is always online, the user always needs the Internet that is also a service that is not available to the level of a local area network. An alternative is to have more than one provider and thus more than one cloud, which would allow users to run their programs in another cloud while the other is offline. However, this alternative is not as simple as it requires interoperability between clouds [5].

VII. General IT Security

In order to understand IT security, we must first understand the three basic principles that guarantee it in a computerized environment, which is confidentiality, availability and integrity.

Confidentiality "is intended to protect information against unauthorized access by unauthorized persons or programs, while maintaining the confidentiality and privacy of their information" [9], i.e. in a computer environment, basically seeks to information from any person or program that is not allowed to access it.

Availability is the property that ensures that the information is always available for legitimate use, i.e. by those who are authorized by the owner of the information.

Integrity in a computing environment consists of the idea that information can not be altered or affected by users who do not have permission to do so.

The integrity of the information has as main objective the protection of the information against any type of alterations, without the authorization of the owner or other responsible for this information. [9]

This means that the information, when accessed, should be exactly as it was when it was last saved or opened, so steps must be taken to ensure that the information is not altered inappropriately or by persons who are not allowed to do so, in the same way that the content of the information must be protected not only while it is stored, but also during its processing avoiding losses of data in the event of any failure or break in the system.

Analysing all these principles is easy to see how they work together, complementing each other, trying to ensure that a system remains perfectly safe, but it is good to know that the level reached by each of these three aspects in an information technology environment, may vary according to your need for the business or service, where it will be employed and the value of the information that is intended to be preserved.

VIII. Risks and Threats

The biggest challenge facing cloud computing, especially for organizations, is security. To understand the potential security risks, they should make a thorough analysis of the cloud service that they will use. In the analysis process, the impacts generated should be evaluated if any of the security requirements already mentioned (confidentiality, integrity or availability) are compromised. And through this analysis, organizations can fully or partially move their processes or data to the cloud computing environment.

In order to evaluate the potential security risks in a cloud computing environment, it is necessary to understand the security risks of the three main models already described (Saas, PaaS and IaaS) of cloud computing deployment.

For the services provided by the IaaS, the main risks to be considered are those that concern the availability, in a way we can say that the IaaS is the base for the other environments because it provides the necessary capacity to carry out any other activity. "The IaaS level serves as the basis for the other service delivery models (PaaS and SaaS), and the lack of security at this level will certainly affect the models built on it." [10]

The IaaS offers the structural part and so it must take into account failures that can happen with your servers, network equipment and storage. Imagine if you are working on some document that is stored on a server that goes offline for any reason, whether it is a simple hardware failure or even a natural disaster where the server is stored, causing the server to stop functioning.

IaaS works with virtualization and this technology is used by different users, using different services with different needs in a single device, and can cause problems, since the virtual machines may not be fully prepared with regard to security [10].

A good example is the use of side-channel attacks where it is possible to perform a statistical analysis of the network traffic speed as the keys are typed, as well as the electromagnetic emanations of the screen, to determine what is being done in the machine [10].

Another very important factor to consider are attempts to steal credentials, where malicious people attempt to fraudulently obtain passwords of legitimate users of the system.

In this context, one commonly used technique is phishing, where users are influenced to provide their account data. An example is the emails sent requesting the update of the profile for bank accounts, where the unwitting user ends up providing his bank details. There are also sites that are created in the same way as the legitimate ones in which the user inserts his information imagining that he is doing it in the original site, but ends up providing information and access to strangers.

IX. How to ensure safety?

Now let's give some examples and methods that can be used to minimize the risks in the cloud environment. Users, using the cloud service, are relying on all the data and information it produces to the service provider, so it is important that various measures and protection policies are adopted so that, in the event of any service information is not completely lost [10].

Privacy and information integrity are then of paramount importance, especially in public clouds where there is greater exposure to attacks. The capabilities required to prevent information breaches include: data encryption, strict access control, and an effective backup management system [11].

In the case of problems related to the availability of services, such as a failure or catastrophe, service providers should be prepared with contingency policies capable of making unavailability lasts for the shortest time possible, in more critical cases, and even completely imperceptible to users. In this sense, there are several contingency strategies, the two main ones being the Hot Sites and the Warm Site. The first is a strategy that is ready to be started as soon as some risk situation occurs and is related to the fault tolerance time of what is being protected, such as a database that can not go beyond a few seconds of unavailability, as they are sites equipped with facilities able to meet the needs of the company, while at the same time, a backup of the data is sent periodically to the Hot site ensuring data integrity [9].

The option "Warm site" is a strategy applied to objects that may remain in a time of greater unavailability, are places with a slightly smaller infrastructure, but not less able, because they can resume the services until 24 hours and also have data backup in a slightly longer period, this strategy can be used in email services, as they do not compromise business so intensely [9].

Authentication, authorization, and auditing of users within the cloud computing environment must have at least more than one technique capable of securing these three items, so it is possible

to greatly increase the chances of ensuring that who is accessing the services provided is really who "says" it is, and is authorized to access the files and services you select and what you do with them, "Authorization is the process of granting or denying rights to users or systems through the so-called lists Access Control Lists (ACL), defining which activities can be performed, [...]" [9].
Authentication is the means to make sure that the user or the remote object is actually who they are claiming to be. It is an essential security service because reliable authentication ensures access control, determines who is authorized to access information, allows audit paths and ensures the legitimacy of access.
There are three methods for user authentication: user and password, token or card, and retinal or fingerprint analysis. Combining all these methods makes it very difficult for malicious people to gain access to the cloud's resources by trying to pass themselves off to another user as they will rarely get two of that information they need to access.
A good policy to be able to provide access for each type of user is SSO (single sign on). SSO is a unique identifier provided to the user that contains all information pertaining to your user profile, that is, what it may and may not do and use within certain domains or, in other words, within the provider's network. service, this information is passed on to the identity server responsible for storing all these SSOs, access profiles, and access policy for each type of user and system resources, from there the identity federation server communicates with the server service provider, be it IaaS, SaaS or PaaS that identify what may be accessed and used by that SSO.
"To provide access to different levels of service, the consumer organization may use a Single Sign On (SSO) service that is part of a federation to authenticate users of the applications available in the cloud." [9]
This way it's possible to make user to enter his credentials only once, even having to use different resources of the cloud, simplifying access, since there is only one credential which can also guarantee greater authenticity and an easier audit of the same, since there is only one credential for all accesses.
To protect data transmitted while using cloud computing, cryptography techniques should be widely used, this technique consists of using algorithms to encrypt the data being transmitted, then encrypted data may be sent to the recipients who will need to know the key or the code used to decipher what was received.
Encryption represents a set of techniques that are used to keep information secure. These techniques consist of the use of encryption keys and algorithms. Knowing the key and the algorithm used it's possible to decipher the received message [9].
One way to ensure secure data transmission is to use a VPN (Virtual Private Network) which are cryptographic tunnels between two authorized points that can exchange information without any third-party interactions [9]. This is a virtual connection and therefore can not be "viewed" by users outside the tunnel, thus ensuring a higher level of privacy and data integrity.
In the VPN, the concept of tunnelling is used where the data packets to be transmitted go through an encryption process so that they are not decrypted in the event of an interception thereof and also by an encapsulation process receiving an additional header, this header contains the destination information within the tunnel and, upon reaching the destination, is removed, and the data packet is deciphered and addressed to its last destination.

X. Robust Security Implementation Models

A. Cryptographic Search

Cryptographic Search (Searchable Encryption) is a technique that provides search capabilities in encrypted data without requiring the encryption key. This technique uses two parts: a client and a server that stores an encrypted D database, where the client has a Q access key and uses it to obtain the query result Q (D) without revealing the text and the result of the query to the server. An access key is a set of codewords that are related to keywords associated with the records of the searched table in the database. The query returns the records in which there is a match between the words of the access key Q and the words of the records in the table [12].
As an example of a scenario of use of encrypted search, suppose that a given
client wants to store his encrypted medical data in a database in the cloud so that he may selectively retrieve the records. The client associates a set of keywords for each table record, for example type of disease. To use the cryptographic search, the client encrypts the set of keywords that are associated with the records in the table. Records of medical data are also encrypted using some standard encryption template. Keywords and medical data are stored in a table in the database. To query the records that are associated with the word "diabetes," the client creates a Q query key using the word "diabetes" and sends the query to the server, which checks each keyword in the table to select the records where it exists the query key and the keyword "diabetes", returning those records to the client, if they exist. In this case, the server gets information on which records were returned but learn nothing about the contents of these records.
Cryptographic search schemes may use cryptographic schemes based on symmetric key or asymmetric key. Public-key schemas are suitable for multi-user attributes, in which any client can encrypt the data using public parameters, but only one user can query the data. In the symmetric key scheme, only the owner of the secret key can create the keywords [12].

B. Provate Information Retrieval

To protect the standard privacy of data access, each data access operation must be hidden so that anyone who is "watching" the transaction does not get any meaningful information. PIR - Private Information Retrieval is an unencrypted public database query technique with protection against user access privacy breach. An access privacy violation occurs when, in addition to having access to the properties of aggregated statistical data, the cloud provider may, with high probability of success, know certain private information about the user from stored encrypted data [13].
PIR protocols allow clients to retrieve information from public or private databases without revealing to the database servers which records are retrieved. In protecting the content of queries, PIRs may protect important domains of applications such as patent databases, pharmaceutical databases, online censuses, location-based services and online behavioral analysis for advertising on the network [13].
A PIR scheme models the database as a binary string x = x1, x2, x3, ..., xn of size n. Identical copies of this string are stored in k servers, where $k \geq 2$. Users have an index i (an integer between 1 and n) and are interested in obtaining the bit value xi make random queries to the servers and get answers with which may compute bit xi. The queries performed on the servers are distributed regardless

of the value of i so that the servers do not obtain any information about i. Queries do not necessarily retrieve a particular bit or sets of bits. They may define functions computed by the servers, for example, a query can specify a set of indexes between 1 and n and the server response can be the XOR of the bits that have these indexes.

The most relevant parameter in PIR schemes is the complexity of communication between the user and servers. The most efficient protocols for communication with two servers have O (n 1 3) communication complexity. Because PIR schemes use unencrypted data, they are not suitable for use in unreliable cloud environments [13].

C. SMC-Secure Multiparty Computation

SMC (Secure Multiparty Computation) is a distributed data processing technique, with privacy guarantee. At SMC, a group of stakeholders wishes to evaluate some function of common interest to the group and for that it processes individual private data without revealing this data to each other. Only the function output is available to all parties. Collaborative data processing is often required in a cloud environment. In distributed processing, parties may be passive opponents who attempt to obtain "extra" information about the data from other parties [14].

In this method, each client Ci has a private input xi, and all clients compute a public function f (x1, x2, x3, ..., xn) without revealing xi to others, except what can be derived from the input or output function [14].

D. Decomposition Anonymity

Encryption is a useful tool for protecting the confidentiality of sensitive data. When data is encrypted, conducting queries becomes a challenge. Thus, while data encryption provides confidentiality, encrypted data is much less convenient to use than decrypted data. [15]

When used with relational databases, encryption creates two major problems. The first problem is that relational databases require that the data types be defined prior to their storage. The second problem is that queries or functions cannot be performed over encrypted data. You cannot evaluate date ranges or make value comparisons on encrypted data. Index structures cannot be used either. In addition, cryptographic-based methods need to include key generation and distribution strategies. However, there are several disadvantages related to the management of cryptographic keys, such as:

- The need to store keys for as long as data remain encrypted.
- The allocation or revocation of keys for access to data by users.
- The need to keep multiple encrypted copies of the same file for access multi-user using public-key [15].

Thus, new techniques to ensure the privacy of cloud-stored data, which are not cryptographic-based, become necessary in a variety of application scenarios. In this way, I present a strategy to preserve the privacy of data stored in the cloud, called "decomposition," which uses decomposition and dispersion of files to separate data into unrecognizable parts and store them on distributed servers in the cloud. In addition, the proposed approach does not encrypt the data to be stored and processed in the cloud [16].

The "decomposition" technique extracts information from the data files on quantity, quality and measure. Data files are considered objects. Each object has three characteristics that determine it: quality, quantity and measure. In a data file, quality is represented by the 256 possible combinations of the 8 bits that make up the bytes that form the file. The quantity is the number of times that each byte is found in the file and the measure is the order in which the bytes are arranged in the file. In a 256-byte file where only the bytes representing the letters "A", "B", "C" and "D" occur in equal proportion, for example:

Archive: "ABCDABCDABCDABCDABCDABCDABCD... ABCD"(256 bytes)
Quantity: 64(A), 64(B), 64(C) ,64(D)
Quality: A, B, C, D

Measure: A (1º,5º,9º,13º...253º), B (2º,6º,10º,14º...,254º), C (3º,7º,11º,15º...,255º), D(4º,8º,12º,16º,256º) [16]

The following are the steps that make up the "decomposition" technique:

1. The decomposition algorithm reads 256-byte sequences from the data file. I will from now on refer to this set of bytes as I-Object [16].
2. The algorithm extracts the I-Object quality, quantity and measure information, storing this information in two arrays with a size of 256 elements each: The Quantity-Quality integer array [256] and the character array Measure [256]. I will refer to these arrays as vectors hereafter [16].
3. The Quantity-Quality vector [256] will store, for each of the different bytes existing in the I-Object, the number of times this byte is found in the I-Object. For example, if the byte 000011112 = 1510 is present 20 times in the I-Object, the Quantity-Quality [15] item will be equal to 20. If byte 1510 is not present, the value of the Quantity-Quality item [15] will be zero [16].
4. For each item of the Quantity-Quality vector, the decomposition algorithm converts the value of the item in a sequence of bits '1', if the element of the vector is greater than zero. Example: Quantity-Quality [25] =3 ⇒ VectorBits [25] = '111'. If the element of the Quantity-Quality vector is equal to zero, the VectorBits will not store any value [16].
5. The items in the VectorBits are concatenated as follows: VectorBits [0] + '0' + VectorBits [1] + '0' +, ... + '0' + VectorBits [255], producing a vector of 512 elements, which is used as input in a function that reads the vector into 8-item sequences and converts to the corresponding ASCII representation, creating a 64-byte sequence, which is written to the quantity-quality.dec file. Ex: '01000001' is converted to the letter 'A' [16].
6. The measured character vector [256] will store, for each element of the Quantity-Quality vector [256]> 0, the order in which the bytes appear in the I-Object. The position of the bytes will vary from 0 to 255, representing the 1st to the 256th byte contained in the data block. The vector will use the decimal value of the byte to represent the values of the positions of the I-Object bytes. Table 2.18 shows an example in which byte-1 occurs 3 times and byte-3 occurs 1 time in the I-Object and there is no occurrence of bytes 0, 2, and 255. The measured vector [256] is recorded in the file measure. dec [16-17].

The files measured.dec and quantity-quality.dec are stored in different cloud providers. In this case, each of the files is insufficient to rebuild the original file. For example, assuming that the provider

who owns the quantity-quality.dec file would attempt to rebuild a 256-byte block of the original file [18-19].
Using the raw-force method to attempt to reconstruct the 256-byte sequence of an I-Object, the probability of the provider finding the correct sequence of bytes, knowing the quantity and quality is a repeated permutation P of 256 elements: Prob = 1/P256 n1, n2, n3..., where n1, n2, n3 ... are the quantity and quality items known. For an I-Object with only 1 byte of quality or quantity, the probability is 1/256. For an I-Object with 2 different bytes, the probability is approximately 1/1076 [19] [20].
As the quantity of quantity items or quality increases, the probability of finding byte order tends to zero. With 10 different bytes in the I-Object, the probability already reaches 1/10256. For the cloud provider that stores the file measure.dec, that is, the order in which the bytes are arranged in the block, the probability of recomposition of the I-Object using gross force is 1/256, that is, approximately
1/10506. The larger the file, the greater the difficulty of the attacker to rebuild it [21].
The advantages of this technique over conventional techniques that use cryptography to ensure confidentiality of data stored in the cloud are as follows [22]:
1. No use of cryptographic keys.
(i) Applicability of the technique for SaaS, PaaS and IaaS solutions without any changes in user application interfaces.

2. The technique may be applied to any format of stored data (data and programs).

3. There is no maximum limitation on the file size to be anonymised.

The solution supports purging of cloud data, since files made available at distinct providers do not reveal information about the original data. If the user leaves the cloud, the data can be considered automatically expunged.

XI. Conclusion

In order to have a minimum of security in Cloud Computing systems we must use an encryption system, if it is not possible, we should use a data dispersion model.
In addition to this primary information security issue we must also take into account the following points:

A. Access Control

With so much ease of access by so many people, you have to create good control methods. In addition to knowing exactly who is allowed to see what, you also need to know if all used appliances are properly insured.
It's important to create strong, different passwords for each user that change frequently. We must be agile in excluding users who are no longer part of the company or organization.

B. Investing in user Awareness

It is of the utmost importance that everyone knows the importance of keeping data protected. An investment should be made in the training of user safety.

This can be done through workshops with best practice tips, with messages reminding them of the importance of not opening suspicious links and even courses on information security.
Small practices like leaving machines locked when you leave the table and being aware of antivirus updates can make a lot of difference.

C. Do Backups

It is never too much to remember that all care is little when you think of data, whether they are in the cloud or not. So, it is important to always have a second, and even third, backup of the information.
This backup can also be in the cloud, but on a server other than the main one already used.

D. Use of Encryption

Data in the cloud can only be accessed by people who have a password to access it. But even with all the precautions with regard to security, but there may still be leaks of information.
That's why cryptography is so important. So even if someone can get to the information, they will not be able to decipher them unless they have the key to it.

References

[1] SILVA, F. H. R.,"A study on the benefits and security risks of using Cloud Computing; 2010 15f", Scientific article of conclusion of course presented at the University Centre Augusto Motta, UNISUAM-RJ.
[2] HURWITZ, Judith; BLOOR, Robin; KAUFMAN, Marcia; HALPER, Fern,"Cloud Computing for Dummies", 1. ed Indiana, U.S.: Wiley Publishing, Inc; 2010. pp. 336.
[3] BUYYA, Rajkumar; BROBERG, James; GOSCINSKI, Andrzej,"Cloud Computing – Principles and Paradigms", 1. Ed New Jersey, U.S.: John Wiley & Sons, Inc. 2011. pp. 664.
[4] MELL, Peter; GRANCE, Timothy,"The NIST Definition of Cloud Computing (Draft)", January 2011. [Online] Available: http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800- 145_cloud-definition.pdf.
[5] CHIRIGATI, Fernando Seabra,"Cloud Computing", Rio de Janeiro, RJ. 2009. [Online] Available: <http://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2009_2/seabr a/.
[6] KAUFMAN, L. M. Data,"Security in the World of Cloud Computing", IEEE Security and Privacy, 7(4): pp. 61-64, 2009
[7] SUN MICROSYSTEMS, INC.,"Introduction to Cloud Computing Architecture", White Paper, 1st edition, 2009a.
[8] DIKAIAKOS, M. D.; PALLIS, G.; KATSAROS, D.; MEHRA, P.; VAKALI, A.,"Cloud Computing – Distributed Internet Computing for IT and Scientific Research", IEEE Internet Computing, 13(5): pp. 10-13, 2009.
[9] MOURATO, Joao Carlos Gomes,"Security of Information Systems", 2008. 10 f. Article (Degree in Informatics Engineering) - School of Technology and Management - Polytechnic Institute of Portalegre, Portalegre, 2008.
[10] MARCON, Arlindo; LAUREANO, Marcos; SANTIN, Altair; MAZIERO, Carlos,"Aspects of Security and Privacy in Cloud Computing Environments", [Online] Available: http://professor.ufabc.edu.br/~joao.kleinschmidt/aulas/seg2011/nuvem.pdf
[11] NOGUEIRA, Matheus Cadori; PEZZI, Daniel da Cunha, "Computing Now is in the Clouds", [Online] Available: http://www.inst-informatica.pt/servicos/informacao-e-documentacao/dossiers-tematicos/teste-dossier-tematico-no-7-cloud-computing/tendencias/a-computacao-agora-e-nas-nuvens

[12] Aggarwal, C. C. (2005),"On k-anonymity and the curse of dimensionality", In Proceedings of the 31st international conference on Very large data bases, pp. 901–909. VLDB Endowment.
[13] Aggarwal, C. C., Philip, S. Y.,"A condensation approach to privacy preserving data mining", pp. 183–199. Springer, 2004.
[14] CAMENISCH, J., Fischer-Hübner, S., Rannenberg, K., "Privacy and identity management for life. Springer", 2011.
[15] Cao, J., Karras, P.,"Publishing microdata with a robust privacy guarantee", Proc. VLDB Endow., 5(11): pp. 1388–1399, 2012.
[16] Chen, K., Liu, L.,"Privacy preserving data classification with rotation perturbation", In Proceedings of the Fifth IEEE International Conference on Data Mining, pp. 589–592. IEEE Computer Society.
[17] Chor, B., Kushilevitz, E., Goldreich, O., Sudan, M. (1998),"Private information retrieval. Journal of the ACM (JACM)", 45(6), pp. 965–981. [Clarke 1999] Clarke, R. (1999). Introduction to dataveillance and information privacy, and definition of terms.
[18] Domingo-Ferrer, J.,"A survey of inference control methods for privacy-preserving data mining, pp. 53–80. Springer, 2008.
[19] Duncan, G. T., Keller-McNulty, S. A., Stokes, S. L., "Disclosure risk vs. data utility: The ru confidentiality map", In Chance. Citeseer, 2001.
[20] Fung, B. C., Wang, K., Fu, A. W.-C., Yu, P. S.," Introduction to Privacy-Preserving Data Publishing: Concepts and Techniques", Chapman-Hall, 2010.
[21] Fung, B. C. M., Ke, W., Yu, P. S.,"Anonymizing classification data for privacy preservation", Knowledge and Data Engineering, IEEE Transactions on, 19(5), pp. 711– 725, 2007.
[22] Gionis, A., Mazza, A., Tassa, T.,"k-anonymization revisited", In Data Engineering, 2008. ICDE 2008. IEEE 24th International Conference on, pp. 744–753. IEEE, 2008.

Pedro Ramos Brandao, Integrated Researcher Doctorate of CIDHEUS - University of Évora, PhD in Information Sciences by the Évora University and PhD in Contemporary Political History by ISCTE; Master in Institutional and Political History by ISCTE, Degree in Multimedia Engineering from ISTEC and Degree of History from Lisbon University Lusíada. President of the ISTEC Scientific Council. Coordinator of the ISTEC Post-Graduation Department. ISTEC - Director of the degree in Computer Science. Coordinator of the End of Degree Project in Computer Science - ISTEC. Professor Coordinator at ISTEC. Director of Kriativ-Tech Magazine - Scientific journal with arbitration. Reviewer in "International Journal of Information and Communication Sciences - USA" ISSN:2575-1719; Scientific Committee Member of International Conference on Virtual and Networked Organizations Emergent Technologies and Tools (http://2100projects.org/conferences/vinorg18/committees.htm)