International Journal on Data Science and Technology
2018; 4(1): 1-5
http://www.sciencepublishinggroup.com/j/ijdst
doi: 10.11648/j.ijdst.20180401.11
ISSN: 2472-2200 (Print); ISSN: 2472-2235 (Online)

The Importance of Authentication and Encryption in Cloud Computing Framework Security

Pedro Ramos Brandão

Interdisciplinary Center of History, Cultures and Societies, Évora University, Évora, Portugal

Email address:
pb@pbrandao.net

To cite this article:
Pedro Ramos Brandão. The Importance of Authentication and Encryption in Cloud Computing Framework Security. *International Journal on Data Science and Technology*. Vol. 4, No. 1, 2018, pp. 1-5. doi: 10.11648/j.ijdst.20180401.11

Received: March 18, 2018; **Accepted**: March 29, 2018; **Published**: April 20, 2018

Abstract: The issues of cybersecurity these days are extremely relevant. With the massive use of the Cloud Computing system, new concerns about the processes to provide this technology with security appeared. The Cloud Computing infrastructure is based on virtualization and distributed computing, often using the shared resource pooling system. For these scenarios, key issues are considered: authentication, and access control. These issues make relevant the following items: data security, regulatory data, privileged access and data recovery. The issue of security in cloud computing involves encryption, it is important to specify the advantages and disadvantages of symmetric encryption and asymmetric encryption. Parallel to this it is important to develop a set of policies for the creation of passwords and subsequent maintenance and alteration of them, as well as their security. the two mandatory pillars for security in Cloud Computing are encryption and a strong passwords policy.

Keywords: *Cloud Computing*, *Cybersecurity*, Cryptography, Passwords

1. Introduction

A good way to see cloud computing is a framework that already offers great value-added services, but is still in the state of full maturity, especially in security. As a new paradigm for computing, cloud computing presents challenges even if it offers advantages. Not all cloud deployment models (public, hybrid, private, and community) are appropriate for each service, each service customer, or all interested parties. Likewise, it is not cost effective for all cloud providers to implement high security or provide the same level of security. However, cloud computing is compelling, it is a growing trend in IT, and is forcing significant advances in supporting technologies such as security.

In this paper, are exposed some of the common security issues or prospective issues that adapt to cloud computing. Issues related to cloud architecture security will be addressed specifically**.**

2. Context

The act of protecting information and communication technologies (ICT) is called *cybersecurity*. This is a broad and unquestionably diffuse concept. Although *cybersecurity* may be a very useful term it's difficult to define it with absolute precision as it usually refers to one or more of the following aspects:

A set of activities as well as other measures designed to protect - computers, computer networks, software related to hardware, devices and the information they contain, and the way they communicate, including software and data, as well as other elements of cyberspace - from attacks, interruptions or other threats [1].

The status or quality of protection against such threats.

To the broad field of action aimed to implement and improve these activities, as well as the quality of protection.

The term *cybersecurity* is sometimes misused in public discussions, and mistaken for privacy, information sharing, intelligence gathering and surveillance. Let's see.

Privacy is related to an individual's ability to control third-party access to information about itself. A good *cybersecurity* can actually help protecting privacy in an electronic environment, but the information shared to aid in security efforts might sometimes contain personal information that, at

least some observers would consider as private. *Cybersecurity* may also be a means of protecting against unwanted surveillance and/ or obtaining data from an information system, usually a computer system. Paradoxically such activities may be useful in helping to put into effect such security. For instance, surveillance, in the form of monitoring the flow of information within a computer system, can be an important component of *cybersecurity*.

Companies as well as the general public have come to realize, albeit slowly, that cyber-crime is real and highly dangerous. Therefore, companies and corporations have taken some measures of perimeter defence of their systems. But nowadays, the question of security is no longer just related to the perimeter of defence to the exterior. Many technologies have been developed to mitigate cyber attacks but in parallel these attacks have become increasingly sophisticated.

With the proliferation of *Cloud Computing* systems, the question arises for entrepreneurs and the general public, whether they will be safer platforms than on-premise systems. The security technologies adopted and developed so far, for computer and electronic systems are also used in *Cloud Computing* platforms, nevertheless, *Cloud Computing* systems have other security systems and require a different approach.

In this work are exposed thus synthetically issues related to *cybersecurity* and applied to Cloud Computing.

3. Architecture Issues

The National Institute of Standars and Technology (NYST) defines cloud computing as an information technology model that conveniently enables, upon request, network access through resource sharing with configurable computing resources that can be rapidly deployed and delivered with minimal of effort or interaction by the supplier [2].

Operating safely and efficiently in cloud computing poses a major challenge in advanced planning. At a high level, we start with a data center that ensures the redundancy of Internet connections that allow connection to the services available. Access consists of the information technology frontier technology area (which can be defined by a set of systems and components that are subject to a single administrative control [3] and comprises a combination of network devices that enable secure communications. NIST defines it as the process of allocating information resources exclusively to an information system in which the security limit is defined for that same system [4]. In this perimeter we have an enormous amount of gears in physical supports and cabling following duly defined standards. An infrastructure is also needed to manage cloud computing and its resources while they are being made available. Each component (server, storage and network) requires a high degree of configurations. When we design this type of architecture and its planning, it is always in the perspective of a complex system, so we always consider all the processes and procedures necessary for operations, including security [5].

4. General Questions on Security in *Cloud Computing*

The term *Cloud Computing* comprises information technology IT services (such as infrastructures, platforms or applications) that can be organized and used over the Internet. The infrastructure on which *Cloud Computing* is built is a large scale distributed infrastructure, in which shared resource pooling is generally vitalized and the services offered in terms of virtual machines or deployment environment or software are distributed to customers. According to current requirements and workloads, Cloud Computing services can be dynamically scaled. As many features are used, they are measured and then the payment is made accordingly to the consumption of these features.

In fact, Cloud Computing provides a shared set of features, including data storage space, networking, computer processing power as well as specialized business and user applications. The actual storage location might be in a single storage environment or be replicated to multiple storage servers, based on the importance of the data. The storage model mechanism is based on four layers: a storage layer that stores the data, a basic layer of administration that ensures the security and stability of the storage itself, an application interface layer that provides the platform application service and an access layer that provides the access platform [6].

The main security challenges in Cloud Computing are as following:

Authentication: throughout Internet, data stored by the user is available to all unauthorized persons.

Access Control: in order to verify and promote authorized users only, Cloud Computing must have adequate and strong access control policies. Such services shall be adjustable, well planned, and their implementation properly supervised.

Policy Integration: there are many cloud computing providers, such as Amazon and Google. The number of conflicts between your policies and your clients' policies must be minimum, and both policies shall be close.

Services Administration: these different providers, such as Amazon and Google, establish information sharing agreements to increase the profitability of their businesses as well as of their technologies. Currently, there must be a division of these partnerships so that users get localized services easily and safer. Users shall be allowed to independently manage the different services provided by one and another entity and shall never mix the administration of Cloud Computing of two different entities.

As for key security issues specific to Cloud Computing, these are as following:

Data Security: data security mainly relates to confidentiality, integrity and availability. These are the main pillars, with regard to security, for this technology suppliers. As a general rule, security is first achieved with encryption.

Regulatory Complaint: customers are typically responsible for the security and integrity of their own data. They are also responsible for having their own systems updated. This fact requires compartmentalisation techniques between the

several customer's services and for such, security technologies of their own.

Data Locations: users probably will not know exactly where their data will be stored as well in which geographical location. As it is distributed computing and it's necessary to ensure its availability, geo redundancy plays a fundamental role in security.

Privileged User Acc**ess**: the type of credentials for accessing data is a security issue, hence users usually choose poor security passwords when allowed to.

Trust Issue: trust is a major issue in Cloud Computing. Users store their data in this type of system because of the confidence they have in this technology providers. Therefore, providers must keep systems highly robustness on safety, more than in conventional systems, hence if they lose consumer's confidence their business may run the risk of quickly collapsing.

Data Recovery: it is defined as the process of restoring lost, corrupted or crashed data, and it's critical in Cloud Computing. However, as this technology is related to another, to virtualization, which provides highly sophisticated and reliable anti-failure systems, the issue of information retrieval becomes simpler in Cloud Computing than in conventional systems.

5. *Cloud Computing* Security

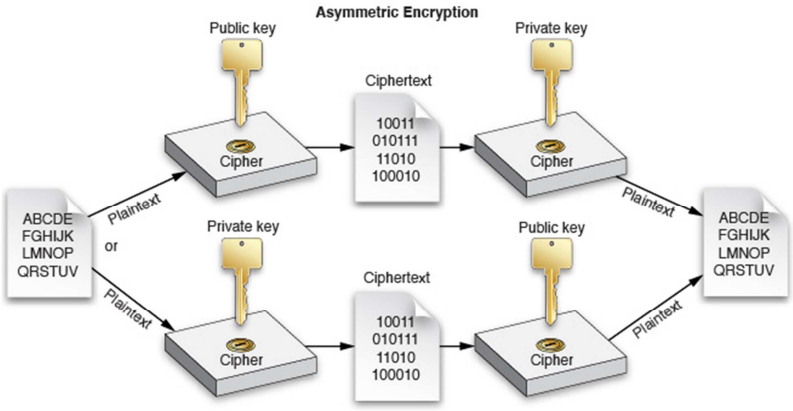
Cloud Computing encompasses applications, platforms as well as infrastructure segments. Each of these segments performs different operations and offers equally different products to companies and individuals around the world. Business package includes Software as a Service (SaaS), Applied Computing, Web Services, Platform as a Service (PaaS), Managed Service Provider (MSP), Service Commerce and Internet Integration. There are countless security issues, hence *Cloud Computing* comprises many technologies and includes networking, databases, operating systems, virtualization, scheduled resource, transaction management, load balancing, concurrency control, and memory management, whose security issues also apply to *Cloud Computing* itself. For instance, the network that interconnects computer systems needs to be safe and the mapping of virtual machines to physical machines must be safely performed. Data security also involves data encryption as well as ensuring that appropriate policies are applied to data sharing [7]. Nevertheless, there are even more security concerns in a *Cloud Computing* environment, such as following:

Access to servers and applications,
Data transfer;
Virtual machine security;
Network security;
Data security;
Private data;
Data integrity;
Data location;
Data availability;
Data segregation;
Security and compliance policy;
Patches management.

In order to implement *Cloud Computing* security, there are two major groups of primordial technologies: encryption, access control and firewalls accordingly to their specificity. [8]

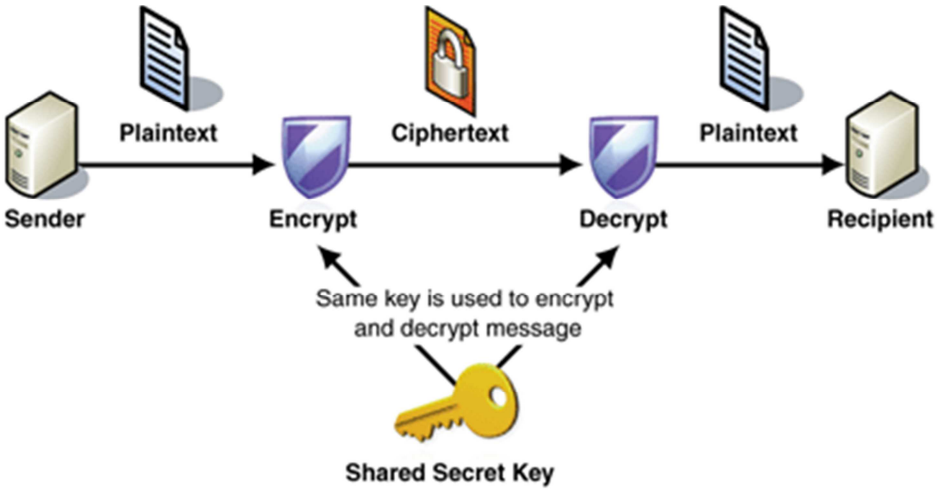
5.1. Data Encryption

Consists of a technology for the security of information, which serves to protect data, whether in motion or at rest. Security may vary in complexity from the simple (easy to manage, low cost, and frankly not very secure) to the highly secure level (very complex, costly to manage, and very restrictive in terms of access). Web service API's that are used to access a *Cloud Computing* platform provide SSL encryption for safer access, and this is generally considered as a standard. Once the information reaches its destination, it's decrypted (or not in some cases) and stored. Nowadays, it is advised that all information, whether in transit or stored in *Cloud Computing* shall be encrypted, but through the asymmetric system (Figure 1). In this system, there are two encryption keys, one to encrypt data and another to decrypt it, and thus the encryption key never circulates over the Internet, unlike symmetric encryption that uses the same key to encrypt and decrypt data (Figure 2). This solution is characterized by being faster in processing, but it does require the key to circulate over the Internet.



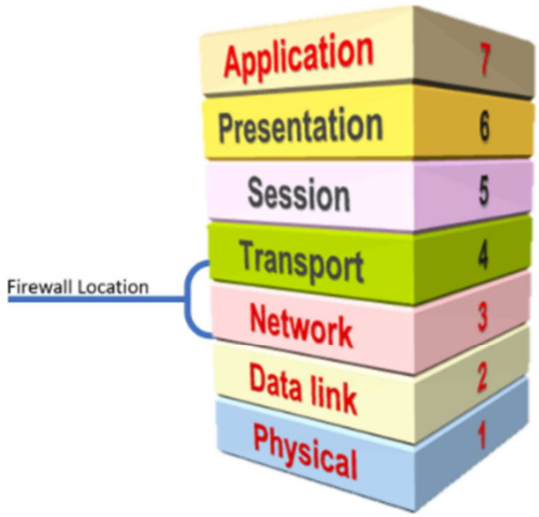
Source: MIT

Figure 1. *Asymmetric cryptography.*



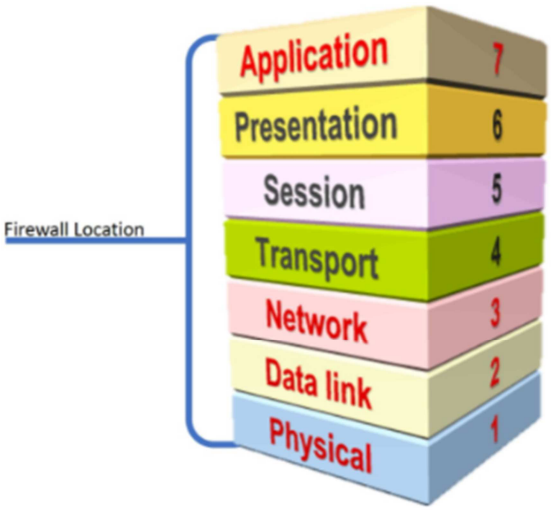
Source: MIT

Figure 2. *Symmetric cryptography.*



Source: MIT

Figure 3. *Two-layer firewall.*



Source: MIT.

Figure 4. *Seven-layer firewall.*

In data encryption (symmetric as well as in asymmetric) firewall systems only monitor two layers of the OSI model, the Transport layer and the Network layer (Figure 3). As for Firewall systems used in *Cloud Computing* and virtual machines, those shall monitor all layers of that model: Physical, Data Link, Network, Transport, Session, Presentation and Applicability (Figure 4). Only this way one can determine total data content, and not merely the origin and destination of the IP addresses and ports used, as well as if whether data transported are effectively indicated for a particular port or application [9].

The issue of authentication and authorization is very important in *Cloud Computing* security, because data access is layered and the required passwords are various. In this context, password creation policy acquires special relevance.

The proposal is a password template, developed by the Author, and currently being tested in the curricular part of a post-graduation in Virtualization and *Cloud Computing* at ISTEC - Institute of Advanced Technologies, in Lisbon, but which also incorporating Microsoft's recommendations for strong password creation in Active Directory.

5.2. Phase 1: Creating Passwords

All passwords must be reasonably complex and difficult to guess by unauthorized persons. For instance, organizations employees shall choose passwords of at least eight characters in length, that contain a combination of upper-case and lower-case letters, numbers and punctuation marks or other special characters. These requirements shall be applied with specific software whenever possible.

In addition to meeting these requirements, users shall also use common sense when choosing passwords. They must avoid easy to violate basic combinations, such as "password", "password1" and "Pa $$ w0rd" which are equally bad in terms of security.

A password must be unique, and with meaning only to the user who chooses it. This means that words taken from a dictionary, common phrases and consecutive equal names shall be avoided. A recommended method for choosing a strong yet

easy-to-remember password is to choose a phrase, include your initials and replace some of those letters with numbers and other characters, as well as mixing the upper-case letters. For instance, with the phrase "This may be a way to remember" you can create the following password: "TmB0WTr!".

Users shall choose unique passwords for all accounts of the company or institution in which they work and can't use a password that they are already using for a personal account.

All passwords shall be frequently changed, as frequently as required accordingly to account in question (personal or professional, for instance). This requirement will be applied using the computer software whenever possible.

If the security of a password raises doubts - for instance, if it appears to you that an unauthorized person has logged into your account - the password must be changed immediately.

Default passwords - such as those created for new users, or those that protect new systems when they are initially configured - shall be changed as soon as possible.

5.3. Phase 2: Password Protection

Users shall never share their passwords with others in the company, including co-workers, managers, administrative assistants, IT staff, etc. All those who need access to a system will receive their unique password.

Users shall never share their passwords with third parties, including those who claim to be representatives of a business partner or mandated by an administrator, with a legitimate need to access the system.

Users shall take measures to prevent phishing attacks as well as other hacking attempts to steal passwords and sensitive information. All users shall receive training on how to recognize these attacks.

Users shall refrain from typing passwords on any type of media or keeping them on their workstations. These shall only be stored in user's memory.

Users must not use word-processing software or other such tools to help store and memorize them.

6. Conclusion

Cloud Computing security uses some general principles of *cybersecurity*, but in addition, it also requires specific mechanisms based on other improved technologies, and/ or already used in conventional security systems.

The two basic and essential pillars of *Cloud Computing* security are the encryption of the structure and all information (at origin, transport and data final storage) as well as the compliance with high security robustness principles by systems that allow authentication and authorization. These two principles, on their own, endow the structures with a high level of security [10].

Lastly, we emphasize that we did not interconnect these issues with the concepts of high redundancy or anti-failure mechanisms, hence they are related to other area than *cybersecurity* [11].

References

[1] E. FISCHER, "Cybersecurity Issues and Challenges," Congressional Research Service, Washington, 2016.

[2] H. SINGH, "A Review of Cloud Computing Security Issues," International Journal of Advances in Engineering and Technology, vol. 8, 2015.

[3] M. PATRA, "Cloud Computing," IRACST, vol. 1, 2011.

[4] S. SAPATAPATHY, "Cloud Computing: Security," IRACST, vol. 1, 2011.

[5] K. HAMLEN, "Security Issues for Cloud Computing," Journal of University of Texas, vol. 6, 2010.

[6] G. MELL, "The NIST Definition of Cloud Computing version 15," National Institute of Standars and technology, Information Technology Laboratory, USA, 2009.

[7] E. SIRON, Hyper-V Security, USA: PACKT, 2014.

[8] H. SWANSON, "NIST Special Publication 800-18 - Guideline for Developing Security Plans for Federal Information Systems," US Department of Commerce, USA, 2006.

[9] V. WINKLER, Securing The Cloud, USA: Syngress, 2011.

[10] J. DOHERTY, SDN and NFV, Indiana - USA: Pearson, 2016.

[11] A. FERREIRA, Introdução ao Cloud Computing, Lisbon - Portugal: FCA, 2015.