Cloud Computing Security

Alexander Souza – ID G00317835 – Student at GMIT- Galway-Mayo Institute of Technology

***Abstract* — Due to the potential of the cloud for the various IT services, there is a growing concern over security. In this article the various situations in which users are most concerned will be presented, while also addressing some of the most common problems. After analysing the various types of problems, we can also present possible solutions. To better understand these problems, you will be shown some attack surfaces, and alerts for some classic problems.**

Keywords—cloud; users; services; problems

I. Introduction

Cloud computing is a recent subject that will modify the concept of computing and the way people use computers. It uses much of the functions of local computers for cloud-connected servers. This cloud delivers computing resources such as processing and storage, adding benefits to users and businesses, reducing risk, utilizing the better infrastructure and reduces the need for specialized manpower, leaving this to cloud service providers. This assignment raises issues around stability and security in cloud computing.

We will explore issues regarding security and privacy by identifying key issues that can affect cloud services and solutions, showing inconveniences with multi-user hosting on the same physical machine and the sharing of computing resources among them, let's approach choice solutions that a customer can choose to protect himself. To better understand cloud computing we will define the different models. Let's identify key players in the cloud infrastructure, definitions and concepts, issues and security implications, and their solutions with examples.

II. Definition And Architectures

The cloud definitions that are most commonly used by companies in the area, were created by the organization NIST (National Institute of Standards and Technology) in 2011 [1]. According to this organization, the cloud has a number of characteristics. It should be a self-consumable service, network-accessible, resource pooling, have fast elasticity and should be a measured service. The agency also defined three more infrastructure models in the cloud:

- **Software as a Service (SaaS):** Of the three models, this is the simplest and the most used. SaaS is a form of software distribution, in which the provider is responsible for all the structure necessary to make the system available and the customer is only responsible for using the software and its configuration. The services are accessed by several clients through an interface that communicates through the Internet. This way you can avoid maintenance and support costs as the software runs in the cloud [11]. Example: Google Docs.

- **Platform as a Service (PaaS):** PaaS is a computing platform consisting of a hosting service and software implementation supported by the service provider. Thanks to PaaS, the programs do not have to be installed on users' machines, thus not imposing restrictions on the software and hardware configurations that each user has, i.e. the client does not need to control the technical structure of the cloud such as the network, operating system, or storage. They only control the software [11]. Example: Windows Azure.
- **Infrastructure as a Service (IaaS):** Infrastructure services typically make computing, storage, and network resources available through virtualization over the Internet. IaaS becomes particularly useful because the associated cost is defined by the number of resources that are used, that is, the user acquires elasticity in the configuration that he needs, thus, avoiding wasted resources [11]. Example: Amazon EC2.

Four types of implementations of the cloud have been introduced in order to protect sensitive data in the cloud, so that users cannot access certain resources.

- **Private Cloud**: This is done only for a single user (a company or organization for example). The physical infrastructure used belongs to the organization or to a provider that manages it, and there is complete control by the organization in relation to the applications that are implemented and executed in the cloud. This type of cloud provides greater security and transparency but requires a larger investment.
- **Public Cloud**: Infrastructure in the public cloud belongs to the provider, and services are available over a public network to multiple users. It has a low cost and is very scalable.
- **Community Cloud**: The community cloud infrastructure belongs to and is shared by several organizations being targeted to a specific community that shares the same concerns, characteristics or interests.

- **Hybrid Cloud**: The hybrid cloud is the composition of the public and private models. In this type of cloud, a private cloud can use the resources on a public cloud.

III. Interveners

Considering cloud administration is not physical, the user data will be totally on the side of the provider, leading to security issues:

- **Cloud Provider:** Is the entity that provides and distributes cloud infrastructures;
- **Service Provider:** Is the entity that uses the cloud infrastructure to deliver applications and services to end users;
- **Service Consumer:** Is the entity that uses the services hosted on the cloud infrastructure;

Each of these stakeholders play an important role in the cloud, particularly relating to both security and private data. [2] To combat this type of problem, some security is introduced through the **SLA (Service Level Agreement)** [10]**,** which is a legal agreement that must be discussed, negotiated and accepted by all the stakeholders of the cloud before the purchase/use of the service. The content of this document should address and identify all aspects of the system, such as customer needs, define required services, simplify complex issues, reduce conflict areas, balance customer expectations, assurances, and system security. [3] Since each service available by the cloud may have different types of infrastructure, the realization of an agreement does not follow any standards, which means that each provider makes its SLA according to the customers or the services that it has.

IV. Access Interfaces

Since the user does not have physical control over the cloud, they need an interface to be able to access it through the Internet. It is critical that there are robust security mechanisms within this interface when accessing the cloud, using a SOAP-based web service (Simple Object Access Protocol) or through a REST web application [4]. For SOAP-based web services, security is ensured through the use of X.509 certificates and XML signatures. For services based on REST web applications, security is obtained through authentication using a password. Whether in services using SOAP or services using REST, it is essential that the connection is over HTTPS. Virtualization is essential for there to be clouds. Through virtualization, a system is highly scalable, which did not happen before its appearance - physical servers connected through VLANs were used [5].

V. Attack Surfaces

Identifying and analyzing the different attack surfaces of a system is a very important exercise that must be performed by both users and the service provider, so it will be easier to select and identify problems in the cloud infrastructure/system. As we have seen previously, the cloud is defined primarily by three different classes: users, services, and service providers. Each of these classes create interaction pairs. Through this scheme mounted at the expense of the three classes identified, it is easier to expose the different attack surfaces that a cloud computing system has.

VI. Safety Problems

The biggest disadvantage known in the use of cloud computing and which most inhibits the expansion and adoption of cloud computing by companies is undoubtedly the possibility of being attacked and weak security measures. In order to enrich the concept of cloud computing and appease security disruptions, several research groups and organizations, as well as government agencies, have carried out various studies to identify gaps and security issues in order to develop new skills and techniques for each of these problems. In recent years, several attacks and various information leaks have been reported, and in many of them, a common thought has been observed that went through the initial blame of cloud systems. Each of these attacks has been studied in order to determine if this attack was actually due to a security breach in the cloud or if it is simply an attack using traditional strategies which exploit web application problems, for example, brute force attacks.

A. Traditional Security Issues

Sometimes certain security issues such as data leakage from cloud clients are initially attributed to defects in cloud systems but later it comes to be found that these problems are just traditional/classic problems of data security in digital systems such as Phishing [6]. There are several examples of these. In 2014 several celebrity photos that were in their backup account on Apple iCloud were published on the Web [7]. Initially the problem was attributed to a security breach in the Cloud, however, later, due to investigations conducted by Apple, it was determined that the problem was not due to some weakness of its cloud, but rather to a traditional web-based attack in using the brute force technique to get the username and passwords of these celebrity accounts in the "Find My Phone" system of Apple. In this way the hacker obtained the credentials to access the system that stored the photos of the victims. Another example of a problem that was not related to a cloud server crash was the case involving the photo leak of the SnapChat mobile application, which says it does not save content shared by clients on its servers. The service provider denied blaming this attack and blaming a third party (SnapSaved) for storing the photos and content of its clients through an API, which later became pirated, making the content available to the public. This process of identifying the true problem and the true culprit is very important because it helps in future investigations and taxonomies in the problems of the cloud, causing the systems of the cloud to become increasingly robust and resistant against attacks. This benefits both the users as well as the service providers.

VII. Safety Solutions

The evolution of the use of cloud computing, and the consequent need for protection, led to the creation of some security solutions, either hardware or software that aimed to protect the different organizations to the maximum, making them feel confident in the use of cloud computing, so that data of extreme importance is not exposed [8].

A. *Data Protection*

Since the customer using cloud computing will always be dependent on the provider, they will need a means to separate them and make their data inaccessible, or at least illegible, to third parties.

As such, encryption and data encryption techniques have emerged, increasing the security of a client, causing their data not to be read by attackers, thus protecting and maintaining the integrity of an organization [9].

VIII. Conclusion

Cloud computing has been increasing exponentially in recent years, enabling organizations to achieve greater performance and lower costs in hardware.

Throughout this article, we discussed the basic security aspects and issues that can arise in cloud computing. The biggest obstacle an organization can encounter in cloud computing is the issue of security. Privacy and data integrity are the keys to the discussion. Because data is not physically stored on the premises of the organization and accessed via the Internet, it becomes vulnerable to malicious agents. However, you can get around these obstacles by following security solutions. As expected, no solution or security system can be given as guaranteed, because sooner or later some entity will be able to compromise that system. The fact that there is currently no generic standard for cloud infrastructures and services makes the implementation of standards and protocol security techniques difficult because what for a mount becomes relatively safe and effective for a different assembly can lead to the opposite happening. It is with conviction that we can say that even with the adversities referred to in this article, the future of cloud computing will be promising and long-lasting.

References

[1] Grance, Peter Mell and Timothy, "The nist definition of cloud computing," 2011.

[2] Mohamed Al Morsy, John Grundy and Ingo Müller, "An Analysis of The Cloud Computing Security Problem," Sydney, Australia, 30th Nov 2010..

[3] Balachandra Reddy Kandukuri, Ramakrishna Paturi V., Atanu Rakshit, "Cloud Security Issues," *SCC '09 Proceedings of the 2009 IEEE International Conference on Services Computing,* September 21 - 25, 2009.

[4] Juraj Somorovsky, Mario Heiderich, Meiko Jensen, Jörg Schwenk, "All Your Clouds are Belong to us – Security Analysis of," 2011.

[5] M. N. J. V. S. K. D. zur Muehlen, "Developing web services choreography standards—the case of REST vs. SOAP," July 2005.

[6] Yousra Abdul Alsahib S.Aldeena, MazleenaSalleha, YazanAljeroudib, "An innovative privacy preserving technique for incremental datasets on cloud computing," vol. 62, pp. 107-116, August 2016.

[7] Iyengar, Rishi, Time.com,, "Apple to Strengthen Security After iCloud Nude Celebrity Photos Leak," 2014.

[8] Jakóbik, Agnieszka - Grzonka, Daniel - Palmieri, Francesco, "Non-deterministic security driven meta scheduler for distributed cloud organizations," 2016.

[9] Geong Sen Poh1 - Baskaran, Vishnu Monn2 - Ji-Jian Chin2 - Mohamad, Moesfa Soeheila1 - Kay Win Lee1 - Maniam, Dharmadharshni1 - Z'aba, Muhammad Reza3 , "Searchable Data Vault: Encrypted Queries in Secure Distributed Cloud Storage.," 2017.

[10] RAJAVEL, Rajkumar1, - THANGARATHINAM, Mala1, "ADSLANF: A negotiation framework for cloud management systems using a bulk negotiation behavioral learning approach.," vol. Vol. 25, no. Issue 1, pp. p563-590, 28p, 2017.

[11] Subhankar Dhar, "From outsourcing to Cloud computing: evolution of IT services," vol. Vol. 35, no. Issue 8, pp. pp. 664-675., 2012.