Cloud Security

Bruno Arieira
a70565@alunos.uminho.pt

Daniel Vieira
a73974@alunos.uminho.pt

Cesário Perneta
a73883@alunos.uminho.pt

José Dias
a78494@alunos.uminho.pt

***Abstract*— This article was written in an attempt to approach cloud security theme. Cloud computing technology is a new concept of providing dramatically scalable and virtualized resources, bandwidth, software and hardware on demand to consumers. The main issue will revolve around its use as a secure source and the main responsible for security breaches in this area.**

Keywords-component; cloud; cyber-security; DDoS

I. Introduction

Considering that individual and organizational levels are increasingly changing to Cloud-Based Systems, the security of the Cloud, is a major issue to address, concerning the associated risks and how and who can cause attacks to it. Our objective is to find a way to prevent these attacks in order to provide security and data privacy to the target users on the cloud.

There have been more and more people and organizations using cloud as the main resource for data processing and storage. People that don't use the cloud, think about its future due to the lack of credibility and trust that can be deposited in its application. For example, if a major company decides to migrate all their data to the Cloud, including personal data from their employees, the first thing they should consider is studying the associated risks, to avoid the loss of data, due to an attack.

The world's leading organization dedicated to defining and raising awareness of the best practices that help ensuring a secure cloud computing environment, Cloud Security Alliance (CSA), has done a study named "Enterprise Resource Planning Applications and Cloud Adoption" about this. With this study, they found that 69% of organizations plan to migrate their data to the cloud and use major cloud infrastructure-as-a-service providers and 90% of the questioned say the applications they plan on migrating to the cloud are business-critical. In relation to the responsibility for cyberattacks in the cloud, 60% of participants of study, say they believe cloud services providers are responsible for the breaches, however 77% say it's the organization's responsibility to secure their applications.

In this article, we will begin to describe the work of Jay Heiser and Mark Nicolett in 2008 [1], that analyses the security risks of cloud computing and provides an evaluation of those risks.

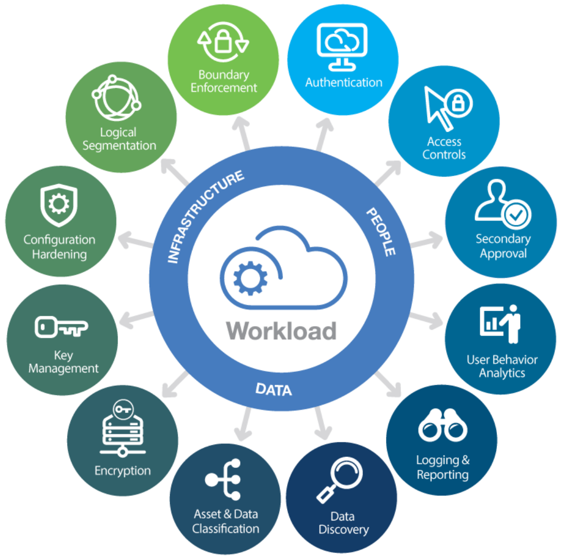


Figure 1. Cloud Computing Features

After that, we will approach an important vulnerability among several other vulnerabilities existing on the cloud and finally, we will compare the 2008 work with another by Huda Karajeh, Mahmoud Maqableh and Rae'd Masa'deh from 2016 [3], enabling us to compare and evaluate what has changed in these 8 years.

II. Related Work

We will address the differences and the evolution of security and the risks associated with the Could, between a period of 8years (from 2008 to 2016). Also, we will mention the work of Rashmi V. Deshmukh and Kailas K. Devadkar, about DDoS attacks, which are one of the main attacks and it is important to mention it [2]. This section is structured in subsections, corresponding to each article, where we describe them and do a critical analysis.

A. *Assessing the Security Risks of Cloud Computing*

The organizations that consider the use of Cloud-Based Systems, firstly should verify the use cases to check if they are acceptable and study its implied vulnerabilities, in order to get an idea of the consequences of this technology.

This research article was developed by a consulting company called GARTNER that analyses the security and implied risks in any cloud.

Usually, people easily join cloud services, because of the low associated costs, but they also must think about the risks involved as any externally provided service has, as well as some other unique risk challenges.

In another words, any organization that considers the use of any external service must evaluate the security and privacy risks, the advantageous and disadvantageous use cases and consider other alternative resources before going fully operational.

In the work referred [1], the following parameters were evaluated:

- **Privileged User Access:** The people who control the technology resources need to have privileged access to validate its performance, add and remove accesses, run administrative and maintenance tasks. Thus, it is required to give a higher level of confidence to the security on cloud technicians and work colleagues than to an employee with a short-lived contract with company.

- **Compliance:** Service providers must be subject to external audits and security certifications, to report to customers the specific controls that were evaluated. The cloud-computing provider that is not subject in this must advise the client that he can only use them for the most trivial of functions.

- **Data Location:** Due to an infrastructure that expands more and more each time it is very normal that you do not know in which country is the data stored. However, this is worrisome because of the country's national privacy regulations. Will providers be storing and processing data according to regulations? And in case of breaking the law, is it the provider that will assume the guilt?

- **Data Segregation:** The encryption of the stored data is more and more used and taken into consideration of the clients. The most likely failure is related to a flaw int the implementation which might have an exploitable weakness. Bearing this in mind, the encryption must be tested by experienced professionals. If the data is stored in encrypted form, then we must know who has access to the decryption keys and if it is possible that an authorized individual has to the company employees' data in case of an emergency.

- **Availability:** Reliability is one of the main advantages of the Cloud, but many offers based in cloud-services do not offer service-level commitments that are essential. The organizations must define service-level requirements for any IT workload and demand service-level agreements from the provider and ensure that the contract contains penalty clauses when service-level agreements are not met.

- **Recovery:** In case of an infrastructure failure or any sort of occurrence related with the cloud service it must have a recovery program to prevent loss of data. Thus, companies must know what would happen to the data and services if such problem occurs.

- **Investigative Support:** Internal investigations of inappropriate or illegal activity are very expensive and difficult to carry out. Cloud services are difficult to analyze because the services and client data can be dispersed between hosts and data centers in a constant state of changing. " If you cannot get a contractual commitment to support specific forms of investigation, along with evidence that the vendor has already successfully supported such activities, then your only safe assumption is that investigation and discovery requests will be impossible."

- **Viability:** Is necessary to ensure that the provider is safe, in other words, if the provider goes broke or if it is acquired it is necessary that the data is available in a format which is easier to import to any replacement application, showing their viability.

- **Support in Reducing Risk:** The specialized personnel in security network or administrators and managers, they shall inform the users and other employees of the company about the instructions in order to avoid phishing or malware attacks, in order to guarantee a secure use.

In order to evaluate the risks involved with cloud computing and cloud services there are a set of questions we must ask. For each question there is only one answer.

➢ "How qualified are the policymakers, architects, coders and operators to understand and reduce the risks of their offering?"

➢ "Accept whatever assurances the service provider offers."

Many companies or organizations do not have the internal capability or people that are competent enough (in the security level) to evaluate appropriately the security of an offering, therefore they are finding suppliers with more knowledge and security than they do.

➢ "What risk control processes and technical mechanisms are used?"

➢ "Evaluate the service provider in person."

If the organizations are concerned with the evaluations provided by their service providers, then they should be capable of evaluating the service themselves, but only if they have specialized personnel and the resources needed. However, such a method is highly inefficient. Usually the preferred method revolves around sending a third party to do the job.

- “What level of testing has been done to verify that the service and control processes are functioning as designed and to identify unanticipated vulnerabilities?”
- “Use a neutral third party to perform a security assessment.”

One company specialized in security can offer higher levels of strictness than almost anything else. One assessment firm can do a thorough risk analysis according to the needs of the client. The third party is less tendentious than the customer and specially less biased than the provider.

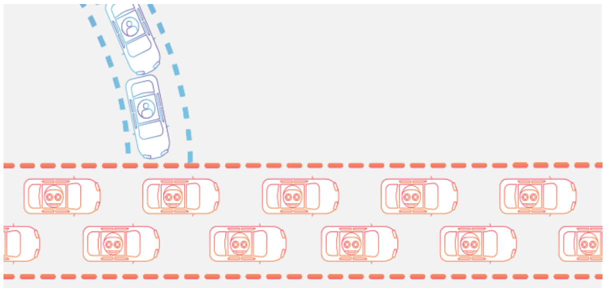
The offers in cloud-computing that include verifiable and specific information about the security and uptime are easier of evaluate, providing a competitive advantage. The best practices in cloud-computing will include high-level of transparence, but it is not yet clear enough how this transparency will show.

"Business units and IT organizations should evaluate the business benefits and risks of cloud-based products."

B. Understanding DDoS Attack & Its Effect In Cloud Environment

DDoS attacks are “major trouble to the availability” to Cloud Environment [2].

A DDoS attack is a malicious attempt to disrupt normal traffic of a targeted server, service or network. A DDoS attack is like a traffic jam clogging up the highway, this in turn makes it possible that the traffic will not arrive at the target.



There are two ways to affect the victims according to Rashmi V. Deshmukh. They are:

- Attackers can exploit any bug or weakness in the implementation in order to damage or disrupt.
- Some attacks use all bandwidth or resources of the victim’s system;

It is important that we understand what DDoS attacks are, for our own protection.

The attacker controls any machine that shows any exploitable vulnerability and uses that machine as an agent for the attack. Every agent is transformed into a bot. Many bots are called botnets so we can say that the attacker controls botnets.

When the IP address of the victim is targeted by the botnet, there will be a denial-of-service because each bot of botnet will respond to that IP address causing an overcrowding in the server or network.

This attack is possible because many people do not use security in their machines. Before DDoS attacks the attacker scans the whole network to find vulnerabilities. In those networks with vulnerabilities, the invader chooses a machine to make agents. These machines are called by *zombies* or bots.

It is difficult to find the attacker, because they are using false IP to hide themselves so they can use many ways like **Random Scan**, **Hitlist Scan**, **Permutation Scan**, **Divide and Conquer** and others.

Rashmi V. Deshmukh divides DDoS attacks in two types: one part revolves around **Bandwidth Depletion** and the other is about **Resources Depletion**.

The first type, **Bandwidth Depletion,** is the “type of attack that consumes the bandwidth of the victim or target system by flooding the unwanted traffic to prevent the legitimate traffic from reaching the victim network”.

In these attacks there are two types of attacks:

- **Flood attacks**: The invader sends a huge volume of traffic through zombies/bots. The effect of this attack is a saturated network and the victim’s access to Network slows down;
- **Amplification attacks**: The attacker sends many packets to a broadcast IP address in order to make the target system get malicious traffic;

The other type, **Resource Depletion,** is an attack where the goal is to exhaust the target system’s resources so that the users do not get service.

There are four types of attacks:

- **Protocol Exploit Attacks**: This attack consumes many resources from the victim in order to explore a feature of a protocol in the victim;
- **Malformed Packet Attacks**: It refers to packets with malicious information or data;
- **IP Address attack**: With the same source and destination IP address, this attack crashes the victim;
- **IP packet options attack**: This attack uses a feature of the IP packet so that they have an optional field with information. With this attack they put this field with bits to one just so that the victim spends time to processing the packet;

In order to prevent these, it is suggested that we use filters such as:

- Ingress filter: With this filter we don’t use packets with illegitimate IP address;

- Egress filter: The packets must have valid IP address in the network;
- Route based distributed packet filtering: Uses the “route information to filter the IP address spoofed packets”;
- Secure Overlay Services (SOS): This is an architecture that assumes that an incoming packet is just valid if it comes from legitimate servers;

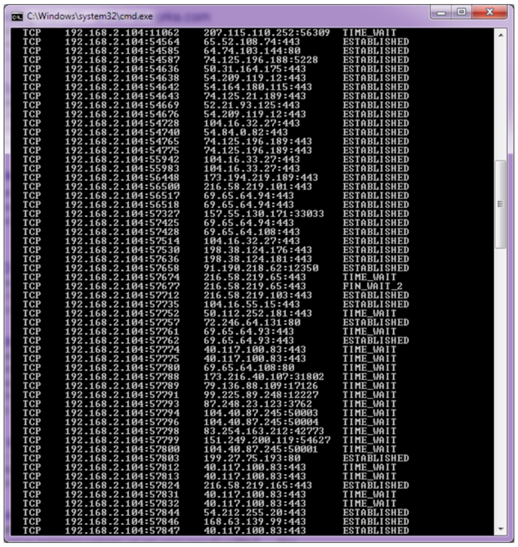
These suggestions are very good to follow although we have more:

- ➢ Buy more bandwidth: The goal of DDoS attacks is to overlap the bandwidth so if it is not too expensive then it is better to buy more;
- ➢ Share y our server in many datacenters with a good balancing system to distribute traffic between them. The datacenters are connected to different networks and there are no obvious network bottlenecks or points that can fail. This is good because if one server is attacked and if the others are in another place, it is very difficult to attack the others;
- ➢ We can configure our router to reject ICMP packets or stop DNS responses from outside of the network;

“The intrusion detection system helps the victim to avoid the propagation of DDoS attacks and prevents it from crashing”.

We must detect the intrusion and we can do it using some strategies:

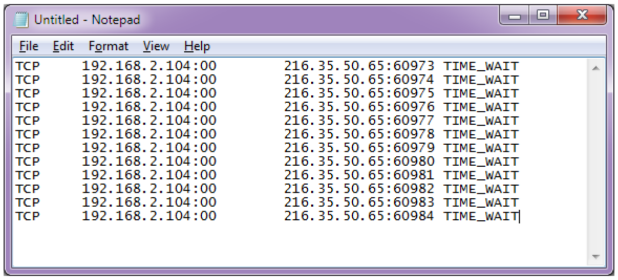
- **Anomaly detection:** We detect attacks using previously detected normal system’s values and compare them with the current values to see if there are some strange behaviors.
- ❖ We must analyze the IP packet and in one small step we can see if we are attacked or not. Using terminal, we can digit “-netstat -an” and the result must be something like this:



```
TCP    192.168.2.104:11062    207.115.110.252:56309  TIME_WAIT
TCP    192.168.2.104:54564    65.52.108.74:443       ESTABLISHED
TCP    192.168.2.104:54585    64.74.103.144:80       ESTABLISHED
TCP    192.168.2.104:54587    74.125.196.188:5228    ESTABLISHED
TCP    192.168.2.104:54636    50.31.164.175:443      ESTABLISHED
TCP    192.168.2.104:54638    54.209.119.12:443      ESTABLISHED
TCP    192.168.2.104:54642    54.164.180.115:443     ESTABLISHED
TCP    192.168.2.104:54643    74.125.21.189:443      ESTABLISHED
TCP    192.168.2.104:54669    52.21.93.125:443       ESTABLISHED
TCP    192.168.2.104:54676    54.209.119.12:443      ESTABLISHED
TCP    192.168.2.104:54728    104.16.32.27:443       ESTABLISHED
TCP    192.168.2.104:54740    54.84.0.82:443         ESTABLISHED
TCP    192.168.2.104:54765    74.125.196.189:443     ESTABLISHED
TCP    192.168.2.104:54775    74.125.196.189:443     ESTABLISHED
TCP    192.168.2.104:55942    104.16.33.27:443       ESTABLISHED
TCP    192.168.2.104:55983    104.16.33.27:443       ESTABLISHED
TCP    192.168.2.104:56448    173.194.219.189:443    ESTABLISHED
TCP    192.168.2.104:56500    216.58.219.101:443     ESTABLISHED
TCP    192.168.2.104:56517    69.65.64.94:443        ESTABLISHED
TCP    192.168.2.104:56518    69.65.64.94:443        ESTABLISHED
TCP    192.168.2.104:57327    157.55.130.171:33033   ESTABLISHED
TCP    192.168.2.104:57425    69.65.64.94:443        ESTABLISHED
TCP    192.168.2.104:57428    69.65.64.108:443       ESTABLISHED
TCP    192.168.2.104:57514    104.16.32.27:443       ESTABLISHED
TCP    192.168.2.104:57530    198.38.124.176:443     ESTABLISHED
TCP    192.168.2.104:57636    198.38.124.181:443     ESTABLISHED
TCP    192.168.2.104:57658    91.190.218.62:12350    ESTABLISHED
TCP    192.168.2.104:57674    216.58.219.65:443      TIME_WAIT
TCP    192.168.2.104:57677    216.58.219.65:443      FIN_WAIT_2
TCP    192.168.2.104:57712    216.58.219.103:443     ESTABLISHED
TCP    192.168.2.104:57735    104.16.55.15:443       ESTABLISHED
TCP    192.168.2.104:57752    50.112.252.181:443     TIME_WAIT
TCP    192.168.2.104:57757    72.246.64.131:80       ESTABLISHED
TCP    192.168.2.104:57761    69.65.64.93:443        TIME_WAIT
TCP    192.168.2.104:57762    69.65.64.93:443        ESTABLISHED
TCP    192.168.2.104:57774    40.117.100.83:443      TIME_WAIT
TCP    192.168.2.104:57775    40.117.100.83:443      TIME_WAIT
TCP    192.168.2.104:57780    69.65.64.108:80        TIME_WAIT
TCP    192.168.2.104:57788    173.216.40.107:31802   TIME_WAIT
TCP    192.168.2.104:57789    79.136.88.109:17126    TIME_WAIT
TCP    192.168.2.104:57791    99.225.89.248:12227    TIME_WAIT
TCP    192.168.2.104:57793    87.248.23.123:3762     TIME_WAIT
TCP    192.168.2.104:57794    104.40.87.245:50003    TIME_WAIT
TCP    192.168.2.104:57796    104.40.87.245:50004    TIME_WAIT
TCP    192.168.2.104:57798    83.254.163.212:42773   TIME_WAIT
TCP    192.168.2.104:57799    151.249.200.119:54627  TIME_WAIT
TCP    192.168.2.104:57800    104.40.87.245:50001    TIME_WAIT
TCP    192.168.2.104:57803    199.27.75.193:80       ESTABLISHED
TCP    192.168.2.104:57812    40.117.100.83:443      TIME_WAIT
TCP    192.168.2.104:57813    40.117.100.83:443      TIME_WAIT
TCP    192.168.2.104:57824    216.58.219.165:443     ESTABLISHED
TCP    192.168.2.104:57831    40.117.100.83:443      TIME_WAIT
TCP    192.168.2.104:57832    40.117.100.83:443      TIME_WAIT
TCP    192.168.2.104:57844    54.212.255.20:443      ESTABLISHED
TCP    192.168.2.104:57846    168.63.139.99:443      ESTABLISHED
TCP    192.168.2.104:57847    40.117.100.83:443      ESTABLISHED
```

The image shows what a server would like. We can see many IP connected to specified ports.

In DDoS attacks, the output is like this:



```
TCP     192.168.2.104:00        216.35.50.65:60973 TIME_WAIT
TCP     192.168.2.104:00        216.35.50.65:60974 TIME_WAIT
TCP     192.168.2.104:00        216.35.50.65:60975 TIME_WAIT
TCP     192.168.2.104:00        216.35.50.65:60976 TIME_WAIT
TCP     192.168.2.104:00        216.35.50.65:60977 TIME_WAIT
TCP     192.168.2.104:00        216.35.50.65:60978 TIME_WAIT
TCP     192.168.2.104:00        216.35.50.65:60979 TIME_WAIT
TCP     192.168.2.104:00        216.35.50.65:60980 TIME_WAIT
TCP     192.168.2.104:00        216.35.50.65:60981 TIME_WAIT
TCP     192.168.2.104:00        216.35.50.65:60982 TIME_WAIT
TCP     192.168.2.104:00        216.35.50.65:60983 TIME_WAIT
TCP     192.168.2.104:00        216.35.50.65:60984 TIME_WAIT
```

We know that it is not a terminal’s output, it is a simulation but what we can show is that there are some differences. One of those is that the IP is the same and it is connected to specific ports.

- ❖ We can analyze packets and if there are some anomalies, we must filter the packets using the router
- ❖ If the first victim is attacked and to prevent it from spreading to the neighbors, we can use **D-Ward**. It is a DDoS defense system that autonomously detects and stop attacks. This system offers good service to legitimate traffic even during an attack, but in same time it reduces DDoS traffic.
- ❖ We can use a **MULTOPS.** It is a data structure and if there’s an IP address of a system that participated in DDoS attack, it will block the IP address.
- ❖ Create a database of well-known signatures or patterns to exploit. If some pattern has been detected, DDoS are reported.

After a DDoS attack is detected we must block the attack and follow the tracks in order to catch the attacker.

C. *Privacy and Security Issues of Cloud Computing Environment*

This work [3] was used in order to understand how technology specialist’s advice the clients that think about migrating to cloud services, relatively to associated risks and parameters to evaluate, implied in the security.

Cloud-computing has many problems, related to security and loss of control, that can affect its adoption and development. According to this article, "Extensive testing showed that single security method does not provide a secure environment in cloud computing and they suggest combining more than one method to provide a comprehensive security model."

This work also focuses in the classification of cloud computing according to the service type of subscriber:

- Software as a Service (SaaS), where the service provider hosts the application, which enables users to connect and use applications through a web browser which in turn reduces control over the application configuration settings;
- Platform as a Service (PaaS), is a complete environment of development and implementation on the cloud, with resources that make everything available, in other words, provides a subscriber a platform as a service to deploy their applications on the cloud infrastructure while maintaining control over they application;
- Infrastructure as a Service (IaaS), service model that delivers computer infrastructure on an outsourced basis to support enterprise operations. This model in turn offers the subscriber control over other resources such as the database and other computing resources.

The cloud-computing environment has continually grown, where an increasingly number of people and organizations keep migrating. This generates more concerns because it increases the need there is for more security.

Providing a stable and secure environment in the private cloud is easy because the data is protected by a firewall, and not available to external public. For the public cloud it is not so simple because the data is in the internet and there are no firewalls. Thus, it is a very hard and complex task to provide the same level of security.

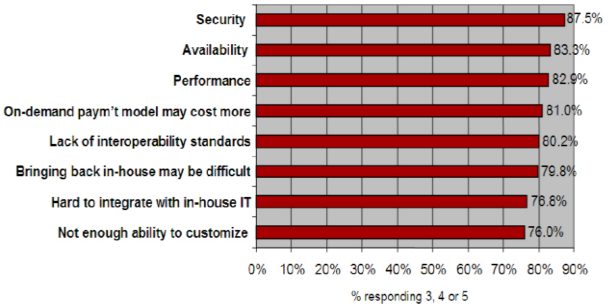


Figure 2. Cloud-computing challenges

"Security issue has a big concern in cloud computing due to its nature of virtualization, elasticity, scalability, and ubiquity of the data; in which a cloud system needs more security protection from intentionally changes and must be protected to be accessed from unauthorized people."

In order to migrate, we must think about the consequences that can come with the migration.

There are some features that we must have to migrate:

- **Trust:** The client and Cloud Enterprise must trust each other. The client must trust in the Enterprise, without even suspecting that there will be errors in the future. In public Clouds, the control of the Cloud is granted by the Client and the effect of this is reducing the potential risk. In private cloud, data, processes and applications are owned and managed by the infrastructures.
- **Availability:** It is the ability of the cloud to retrieve the needed data at any time. The enterprises need to have a service that they can use at any moment and the Cloud must do it.
- **Integrity:** This is extremely important. The system must guarantee that the data are not modified without authorization, or, just by the people who have authorization to do so
- **Authentication/Authorization**: Authentication refers to the process that is used to prove the users claimed identity while they are trying to access any system. Authorization is the process that is used by the system in order to identify the functions and actions they authenticated user is permitted to and access depending of their authorization
- **Confidentiality:** Cloud computing is based on sharing the same resources by multiple users at different levels and must have confidentiality to save sensitive data that must be protected. It can do it using an encryption technique.

There are many investigations on how the best security for Cloud Computing would be. Lombardi and Di Pietro, in 2011, proposed a system to increase security, called Advanced Cloud Protection System (ACPS). With this system there are notifications about any violation of security to Management layer. They tested the system against various attacks and the performance was very good. This result showed that ACPS was effective in the Cloud System.

Another alternative to security is a system, called Hidden Markov Model (HMM), that detects any type of security breach in the cloud computing network. In this system the administrator is using the network filter to monitor subscriber behavior and he is notified when any event starts.

This system is very good. It can detect any violation even if the invader logs in with a valid username and password.

Multi-Clouds Service Model is another alternative to provide more security in a Cloud. This model is based on multiple service providers and the results are very good when compared with a single service provider.

Organization for Economic Cooperation and Development (OCDE) established that accountability is one the mechanisms that is used to provide a trustworthy computing environment by improving the data at different levels.

"Accountability is defined as a commitment of the organization for accepting actor of the host for the personal data that are entrusted in the computing environment from the collection time until when it is destroyed".

III. Proposed Solution

The Cloud Computing has become increasingly popular recently with many companies and other parties considering the move, so it is necessary that this technology evolves for it to be safer.

Hospitals in lack of light are supported by generators to avoid any damage on patients. To avoid DDoS attacks, we must use the same idea but using bandwidth. If the traffic is too much or it has exceeded a value chosen by the network administrator or other parameters that the same administrator wants, the network should use the extra bandwidth to avoid attacks or find a way to improve the traffic of the network.

Cloud computing is a complicated nature of service provision chains, but we must try to check if the security is broken or not. A suggestion is the creation of an independent association, like FMI, where every country in the world will provide for the costs and this association will have authority to investigate any enterprises of Cloud Service. We think that the countries must pay in order to protect their citizens. We live in time where data is everything. Due to this migration we don't know where our data is and as such, we need an independent association to maintain and regulate. An association that verifies if the rules are followed.

IV. Findings and Conclusions

Developing this article made us see the high level of security implied and the challenges involved with cloud-computing services.

It's of the utmost importance that each company which desires the adoption of cloud services pays attention to the risks of security as to avoid devastating situations. As the name suggests, the implementation and operational details, such as location, are irrelevant, which is a wonderful efficiency, but not beneficial due to the problems of security. One revealing thing for us was the fact of the cloud subscribers prefer to use the company or private systems rather than cloud system, as they fell much more positive towards security and privacy issues.

"Nowadays, cloud computing cannot replace completely the traditional computing due to the problems in the different deployment models as several large enterprises and government do not accepted it fully."

References

[1] H. Jay and N. Mark and I. N. Sneddon, "Assessing the Security Risks of Cloud Computing," ID Number: G00157782, June 2008.

[2] D. V. Rashmi and D. K. Kailas, "Understanding DDoS Attack & Its Effect In Cloud Environment," Sardar Patel Institute of Technology, University Of Mumbai, India, 2015.

[3] K. Huda, M. Mahmoud and M. Rae'd, "Privacy and Security Issues of Cloud Computing Environment," in University of Jordan, June 2016.

[4] https://www.esecurityplanet.com/network-security/how-to-prevent-ddos-attacks.html?fbclid=IwAR0UKOWP89kdhDa8DlamMA7RtVF2Teye7cHjnrRdYG-TSoSdKgoXMw40wY0

[5] https://www.loggly.com/blog/how-to-detect-and-analyze-ddos-attacks-using-log-analysis/?fbclid=IwAR38ugfaeHmmQMhQ4HsGP780OZHGlOhletXGLCArT2vt0sTAmfHF9gpdriA