SOCIETY FOR SCIENCE AND EDUCATION
UNITED KINGDOM

TMLAI TRANSACTIONS ON
MACHINE LEARNING AND ARTIFICIAL INTELLIGENCE

VOLUME 5 NO 4, 2017
ISSN 2054-7390

SAAS Cloud security : Attacks and Proposed Solutions

Sail Soufiane, Bouden Halima
Laboratoire d'informatique, Recherche opérationnelle et Statistique Appliquée LIROSA.
Abdelmalek Essaadi, Tétouan, Morocco
soufiane.sail@gmail.com; halima.bouden@gmail.com

ABSTRACT

Nowadays the Cloud has started to gain ground even in SMEs, in spite of that the Cloud is still unknown for several ... for others few reliable.

SaaS represents a promising technology, which grows each year rapidly. Only at the security level, there are many obstacles, and becomes a major problem against its adoption. For example the public cloud represents a huge risk since the data of several companies are stored at the same place, close to each other.

For this reason the security of transiting or stored data in the SaaS remains a challenge for providers in order to gain the confidence of the customers.

SAAS remains the target of several attacks, such as network attacks, etc., which aim to disrupt its operation. Therefore, it is essential to deal with these attacks, and tried to minimize vulnerability and adopt new security concepts.

Through this document, we are going to study the security of SaaS, We will try to find the burly and feeble points of the most famous clouds such as Google Amazon, Microsoft, and come out with Countermeasures and proposals solution.

Keywords: Cloud Computing, SaaS, Internet attacks, Data security, Vulnerability, Authentication.

1 Introduction

Cloud computing, or simply the cloud, is not a fashionable effect as we hear from time to time in the history of computing. It is an innovation that will profoundly change our relationship with new technologies. Now computers, software and network equipment are no longer products that we buy.These are services that we rent, and we can separate from them when we no longer need them. [1] The cloud offer several services. SaaS represents one of the services of this technology, where companies can use applications, without the need to buy them or worry about installation, operating system compatibility etc. A sector that continues to grow with a high level service and competition has begun to play in favor of the customer.In spite of these advantages, the security of the SaaS presents a great problem for the companies, on the level of Confidentiality, integrity, authentication, location of data etc.This represents amajor obstacle for this technology.This reflects the lack of user confidence in Software as a Service. In this document we will study the security of SaaS, and then in the second part we

DOI: 10.14738/tmlai.54.3194
Publication Date: 15th August, 2017
URL: http://dx.doi.org/10.14738/tmlai.54.3194

will do a comparison between Google Cloud, Amazon and Microsoft in terms of security, and finally see solutions that can be useful in securing the Cloud.

2 SAAS Security

As SaaS technology is one of the most widely used concepts in Cloud technology, it became the target of many attacks.Several security aspects in the SaaS are similar to the Web Service, since this technology requires only a web browser and internet in order to take full advantage of these services.In general, users do not dare to adopt such technology for fear of Attacks linked mainly to data security and more precisely to their confidentiality.

The most common problems with data security are data backup, data access, data storage locations, availability, authentication, and so on[2]. In the following table we summarize the different problems and the attacks of the cloud [Table 1].

2.1 Denial of Service (DoS) Attacks :

DoS is an attack that aims to make a service or resources unavailable to users for an indefinite period of time by flooding it with unnecessary packages.The main purpose of these attacks is to exhaust computer resources (CPU, network bandwidth) so that it renders services unavailable to users,The SaaS providers provided several services, if these services become inaccessible the customer will not be satisfiedwhich can have dangerous impacts. In a DDoS attack in general, the attacker typically disguises or "spoofs" the IP address section of a packet header in order to hide their identity from their victim.This makes it extremely difficult to track the source of the attack. [3]The DoS attack can use HTTP and XML to take down a server, this type of attack is called HX-Dos.

Table 1:Different problems and attacks on the Cloud

Security Issues	Attack vectors	Attack types	Impacts
Virtualization level Security Issues	• Social engineering • Storage vulnerabilities • Datacentre vulnerabilities and Network • VM vulnerabilities, etc.	• DoS and DDos. • VM Escape. • HypervisorRootkit.	• Software interruption and modification (deletion) • Programming flaws
Application level Security Issues	• Session management and broken authentication • Security misconfiguration, etc.	• SQL injection attacks • Cross Site scripting and • Other application based attacks.	• Modification of data at rest and in transit • Confidentiality • Session hijacking
Network level Security Issues.	• Firewall misconfiguration, etc.	• DNS attacks • Sniffer attacks • Issues of reuse IP address • Network Sniffing, VoIP related attacks (e.g. VoIP phishing).	• Traffic flow analysis • Exposure in network
Physical level Security Issues	• Loss of Power and environmental control	• Phishing Attacks • Malware injection attack	• Limited access to data canters • Hardware modification and theft

2.2 Authentification issues

The primary purpose of authentication is to give access to the right users. Authentication is a weak point in Cloud services, and it is often targeted by attackers. Today, most user-centric services still use a simple authentication username and password, with the exception of some financial institutions that have deployed various forms of secondary authentication Site, virtual keyboards, shared secret questions, etc. to make it a bit more difficult for popular phishing attacks etc. [4]

The main authentication attacks include:

2.2.1 Man in the middle :

This attack is performed when an attacker places himself between two users. Whenever attackers can place themselves in the path of communication between two or more people, they may intercept and alter communications. [4]

2.2.2 Key logger :

A key logger sometimes called a keystroke logger, a key recorder, or a system monitor, is a hardware device or a small program that monitors each keystroke that a user types on the keyboard of a specific computer. As the user types, the device collect each keystroke and save it as text in its own miniature hard drive. [5]

2.2.3 Phishing / Ingénierie sociale :

This is an attack that aims to convince a user to reveal sensitive information (password or other sensitive information). Internet users often suffer from this attack, and since the cloud is web based, Cloud Clients are concerned as well. [2]

2.3 SQL Injection and Cross-Site Scripting :

The two most common threats that are used to steal user information from the Web application are sql-injection and cross-site scripting (XSS) by inserting malicious code into the Web application. Therefore, when users return data by using the text box on a Web page, hackers add special characters. The malicious code is inserted into a standard SQL code that alters the natures of the query.The attackers access a database and execute their own SQL command. That can be used to drill, modify, and delete the information. [6] Cross-site Scripting is one of the most common application layer hacking techniques that inject malicious scripts into web content. As the Cloud provides a shared environment, attackers attempt to insert malicious scripts such as JavaScript html and VBScriptinto the dynamic web application as a browser-side script to gather important information. [7]

2.4 Password reset attack :

In such an attack, the hacker attempts any possible combination of characters in order to find the password. Strong encryption can make data difficult to decipher but not indecipherable, since exploitation of large resources and techniques can make it possible.

2.4.1 Brute Force Attack :

In general users choose words or phrases easy as password, this facilitates the attack. Based on a list of word and phrase the attacker tries to guessed and found the right password.

2.4.2 Brute Forcing Session Identifiers :

In this attack, the hacker attempts to guess the session ID of the targeted victim, in order to succeed this attack the hacker needs a very powerful computer, which can be possible, if a hacker rents or buys a high-performance machine At Amazon for example.

2.5 Side Channel Attacks :

An attacker could attempt to compromise the cloud by placing a malicious virtual machine in the immediate vicinity of a target cloud server and then launching a lateral channel attack. Lateral channel attacks have emerged as a kind of an effective security threat targeting the implementation of cryptographic algorithm systems. The evaluation of the rigidity of a cryptographic system to Side channel attacks is therefore important for the secure concept of the systems. [8]

3 Google cloud vs Amazon vs Microsoft

Google nowadays is one of the world's leading in the cloud, offering several services, Google Drive, Dropbox (photos...), Gmail (emails) etc. This giant has gained the confidence of millions of users around the world, with its innovations, quality and especially security.

Google Drive is one of Google's services, oriented data storage remotely. It is used to synchronize between a PC and the Cloud. [9] Google Drive is not mountable as a network drive, is not accessible via FTP or another open protocol, which limits network attacks of this kind.

But Concerns about Google Drive are usually related to legitimate security. Of course, like any cloud-based storage system, users are under the mercy of servers. The worst nightmare that can happen to a user is seeing the servers breaking down (Google is not immune to this, such a breakdown has already been reported before), which will cost a lot for Google and its Loyal customers. This is why reliability is an important issue.

Except that at this level Google has a rather good technical infrastructure, since it has expertise in this area that few other companies can match, as to the availability and speed of servers are almost exemplary.

One of the security measures adopted by this company to limit human error, which can be committed by the user, retention of deleted files for 30 days, which can be very useful,

The data is stored and fragmented, with a randomly chosen file name and encrypted.In spite of the progress it has made, it remains often under criticism, as only the data transiting and stored in the servers are encrypted, since Google does not offer the possibility of encrypting locally via a private key and chosen by the user, So Google is able to decrypt without user intervention. To catch up with competitors Google has just launched an encryption key management service (KMS) after a delay of two years in front of Amazon, this tool provides developers with a solution to manage encryption keys.

Recently a Google search team had tried to develop their own encryption algorithm, but there is no evidence that it will be adopted, at least in the near future. [10]

The security side then represents a greater brake at Google. For example, in order to connect to the storage space, we can use our Google account, gathering a username and password for two different services can cause serious and catastrophic damage, since if the user leaves Gmail account for example opened or the window of its browser without disconnecting, anyone can easily access and see all the files stored. Google's advice regarding this topic remains basics, they basically consist of using a strong password, and logging out when finished etc.

Finally, this American giant, where the majority of its servers found it on American soil, must satisfy the requests of access of the American authorities according to the terms of Patriot Act; it means that they must communicate the information which is entrusted to them to the United States intelligence agencies. This puts users' privacy at risk. Google goes beyond that, since it states in their terms of use that they are entitled to use user’s data, for a service improvement, a deliberately vague definition, which does not show the limits of use of those information.

On the other side of the competition, Amazon, another giant that has made fascinating progress, by dominating this market far ahead of Google and Oracle. It has achieved spectacular revenues. But Amazon is not immune from criticism, especially when it concerns the security of its cloud; with a high number of breakdowns compared to others. Protection systems have proved several times their inability to cope Attacks. Despite that progress has been done in order to improve their services and minimize vulnerabilities.

The Amazon Cloud is the source on which several services are based, so the reliability of the Amazon infrastructure is no longer to be demonstrated. The performance of Amazon Cloud Drive is also excellent.

However, Amazon is one of the worst providers in terms of the confidentiality of the data entrusted to it. The data is not encrypted locally and is stored in clear text on the servers. Encryption occurs only to protect data during transfer. Fortunately, there are third-party services offering to encrypt data before sending to Amazon Cloud Drive. [9]

Often Amazon is blamed for dealing with the security of these infrastructures more than web applications, causing flaws related to attacks like XSS and SQL Injection, to catch up, the company has tried to put up a layer of Security that will limit such fails, except that it did not give the desired results, since not so long ago Hackers were able to recover several password users, a blow that brought the company to adopt a method of double identification. Today plus your email and password Amazon will ask you to enter a special code (sent by SMS) in order to better secure accounts, a procedure that can protect more.

Amazon had also removed the local applications that allowed the connection to the data, and it limited itself from the website, meaning that to access its storage space the user is obliged to pass through the website.

Moreover, since Amazon is a company under American law, hosting on American soil, the data are also submitted to the Patriot Act, as for its competitor Google.

Finally with regard to Microsoft and its One Drive, it does not do better than the others. It is true that the transiting data is protected via SSL, and we can opt for two-factor authentication, except that once on the server the data are stored in clear, only professionals with a contract One Drive Enterprise have the chance to see their data stored encrypt.

Worse than that Microsoft reserves the right to remove some content that is contrary to the terms of use of its service, which means that customer data are analyzed.

Microsoft does not escape the Patriot Act law same like Google and Amazon.

4 Proposition and Solution :

The following key security features should be carefully considered as an integral part of the SaaS application development and deployment processes FIG1:

- Data security.
- Network security.
- Location of data.
- Data Integrity.
- Segregation of data.
- Access to data.
- Authentication and authorization.
- Data confidentiality.
- Web application security.
- Availability.
- Backup.
- Identity management and connection process. [11]

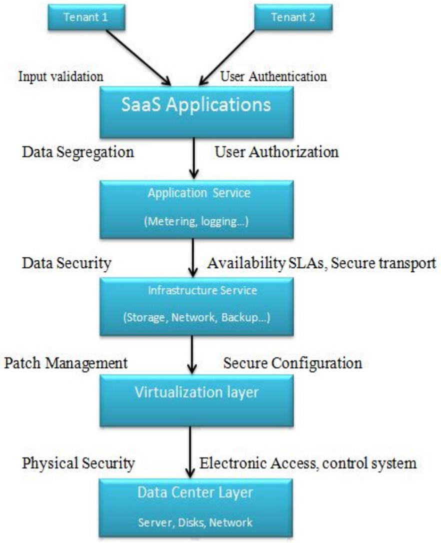


Figure 1:Different security layer in the SaaS

4.1 Network security and data integrity (transport):

SSL or Secure Socket Layer is a protocol to secure communication between two computers. This solution can solve problems related to the transport of information between a client and a server.

This system allows securing any protocol of the TCP / IP. Based on two protocols, that allows total security of the data transiting. If we use 128 bits - SSL we will have a total of 2 ^ 128 key combination possibility, which will be very difficult for a hacker to get to decrypt it, the SSL provided another version of 256bits even more secure. This one will be quite complicated for a hacker, and easy to deal with a brute force attack.

The notion of certificate (CA's Certificate Authorities) in the SSL during an SSL negotiation is considered as the guarantor, in order to clearly identify the server with which we communicate. The Cloud server first sends the credentials to the client when it connects and then sends a copy of its SSL certificate. The owner verifies the certificate and then sends a message to the server and the server sends a digitally signed acknowledgment to start an encrypted SSL session to transfer the data between the browser and the server in encrypted mode. [12]

4.2 Data Storage :

The layered approach to secure data storage is given in FIG 2.

Where the first layer allows a secure authentication of the person, then the second layer will allow the anonymization of the person's data. Third step concerns the encryption of the data, so that finally they will be classified in order to well manipulate the data, and guarantee a high security.

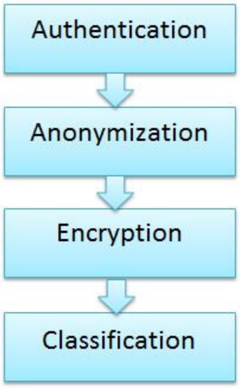


Figure 2: Proposed security model.

4.2.1 Authentication:

An effective average of authentication is OTP (one time password) which is a valid password only for a session or transaction. OTP is like a validation system that provides an extra layer of security. It is automatically generated by a pre-calculated method, which will eliminate some of the shortcomings associated to static passwords such as password longevity, password simplicity, and brute force attack. OTPs are generated on the server side and sent to the user using a telecommunication channel. [13]

Clouds cannot be accessed without the right combination of user name, user password, and one-time password. OTP generated must be difficult to estimate, retrieve, or trace by hackers. [14]

Several elements can be used to generate a single-use password that is difficult to guess. [13]

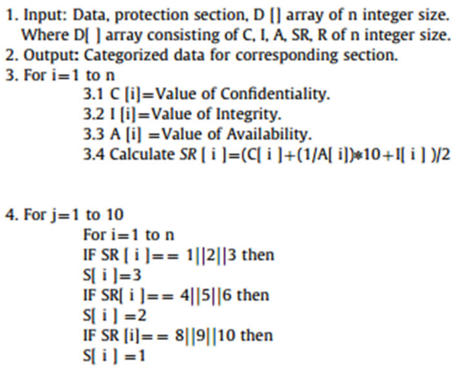
4.2.2 Encryption and Anonymization:

Since the data is no longer stored on the client side, and since the cloud is based on resource sharing technology, this sharing makes the exact location of user data impossible to determine. That does generate problem of security and accessibility. [16]

Encryption has become a necessity for the customer to protect his data. To increase the security level of data in the public cloud, it is important to encrypt them using anonymization with backups and audits. [17]Anonymization can be defined as the operation of deleting all the information that directly or indirectly identifies an individual [18] contained in a document or a database. This will make it very difficult to re-identify the persons or entities concerned.

4.2.3 Classification:

In order to better manipulate, and limit the leakage of the data, a method of classification of the data is adopted. This classification is generated by an algorithm that calculates the degree of sensitivity of data, based on 3 criteria (Confidentiality, Integrity, Availability) Fig3. Once the calculation is done, we classify our data according to 3 categories. Public, private, access limited. [19]



```
1. Input: Data, protection section, D [] array of n integer size.
   Where D[ ] array consisting of C, I, A, SR, R of n integer size.
2. Output: Categorized data for corresponding section.
3. For i=1 to n
            3.1 C [i]=Value of Confidentiality.
            3.2 I [i]=Value of Integrity.
            3.3 A [i] =Value of Availability.
            3.4 Calculate SR [ i ]=(C[ i ]+(1/A[ i])*10+I[ i ] )/2


4. For j=1 to 10
            For i=1 to n
            IF SR [ i ]== 1||2||3 then
            S[ i ]=3
            IF SR[ i ]== 4||5||6 then
            S[ i ] =2
            IF SR [i]== 8||9||10 then
            S[ i ] =1
```

Figure 3: Classification algorithm.

The result of our calculation will allow us to classify our data, a result Sr = 1 || 2 || 3 will classify our data in the category (high sensitivity) where access is limited, if Sr = 4 || 5 || 6 data will be placed in the private (private) category, otherwise the data will be stored in the public part.

This classification makes it possible to better manipulate our data and to reinforce security. Fig4

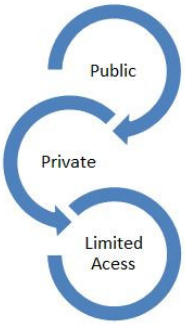


Figure 4: The different levels of classificatio

4.3 Location of data and Confidentiality:

In the Cloud and SaaS, users do not know where their data is stored; problem arises, when these data are stored in countries where laws allow governmental or other organizations to access these data. For example, the United States. To solve this problem, the service provider must immigrate to a country where the laws do not permit any private data access. A secure SaaS model must be able to provide reliability to the client on the location of the data.

4.4 Availability:

Service availability is one of the strengths of the cloud service, but at the security level, it is one of the biggest problems, the unavailability of a service for some time, can cost a lot for a customer. This customer whowant to have a service available at any time. The DoSs attack is an example of attacks that aims to make a service or resource unavailable to users by sending useless messages.

In order to identify these messages, we propose the SOTA method which is based on the DPM algorithm [21] [22] (DPM's role is to mark the ID field and the reserved FLAG in the IP header). SOTA, which is a web service security application, its objective is to apply the traceability of SOA approach. In order to identify the false identities of the messages, since the objective of the X-DoS, and DX-DoS and hidden the true identity of the attacker.

Each packet entering the router will be marked. The marked packet will not change during its passage through the network. The DPM is applied to the SOTA Framework, placing the Service Oriented Trace back Mark (SOTM) mark in the web service message. The true identity of a package is stored in the SOTM and placed inside the SOAP (web service). Like DPM, in SOTM the tags do not change during the transit in the network. SOTM is composed of an XML tag and placed in the SOAP header. When discovering an X-DoS or DX-DoS attack, SOTM can be used to identify the true source of fake messages.SOTA only offers the ability to identify fake messages that aims to disrupt a server by flooding it with unnecessary messages to exhaust it. The direct elimination of a message from an X-DoS and DX-Dos attack will be supported by the Cloud Protector. [20] Which is a Neural Network (Neural Network), who allows X-DoS messages to be detected and filtered. A neural network is a set of connected units composed of input and output layers. In a neural network, the threshold logic unit (TLU) is used. The TLU inserts the input objects into an array of quantities and additions to each other, to see if they are above fixed threshold or not.

Other solutions proposed to limit the impact of network attacks (Dos, DDos etc.). The IDS which is a set of software and hardware components that primarily aims to detect and analyze any attack attempt. NIDS analyzes the network to detect attacks based on a comparison between the analysis and the standards. And HIDS which is more interested in the machine than the network. It analyzes in real time the flows related to a machine.

The combination of these two will have a positive effect, if they are properly configured.

The life cycle of a package in such a model is simple:

Once the packet arrives at the firewall it will be analyzed based on the configuration, if it is invalid it will be blocked otherwise it will be processed by our IDS (NIDS & HIDS) Based on defined standards and configurations. If the system will recognize the packet as innocent it will redirect to the requested Cloud service, otherwise the system will trigger the alarm and it will notify the cloud administrator. All the packets received from same IP will be deleted, and the system will immigrate to another more secure virtual machine, and we will inform the firewall of the new configurations that it must take into consideration. [23]

4.5 Application security:

In security, humans remain the weak point; some mistakes committed can be fatal. Those errors that can be formatted in bad configuration as they may be related to programming the application and codes.Such errors are catastrophic, since they open the doors to hackers to harm the system; SQL Injection XSS etc. are all attacks that are based on flaws in a code.This is why application security tests are very important before commissioning.

Web Application Security Scanner is software that performs automatic tests on an application and identifies security vulnerabilities. The scanners do not act on source code, but they only perform functional tests and try to find security vulnerabilities. We can find several types of analyzer, whether open source or paid, for example Grabber, Wapiti, Zed Attack Proxy etc. [24]

5 Conclusion

As already mentioned in this document, the SaaS and the Cloud in general offers great advantages for companies, at the technologic level, cost, flexibility and ease of use etc.

Only the obstacles that limit the adoption of this technology are numerous, and security comes at the top of these obstacles. Since some practices can seriously harm the operation of the Cloud. For example collecting all the data from the different clients in one location puts all data at risk.

The flexibility and ease of adapting SaaS to data access policies in an enterprise is paramount, it will protect data, and ensure the integrity and confidentiality of data.

A SaaS must be reliable, to convince a user, whose only concern is whether his data is secure or not.

In this document, we tried to deal with some of the attacks that target SaaS, offering some solutions that can ensure data security, such as SSL which is one of the best solutions to protect the circulating data, CTB which allows Identifying incoming packets to protect against DoS attacks, or the data encryption and classification model, which will help secure the stored data.

REFERENCE

[1] Emile Yaogo« Le cloudcomputing : L'informatique comme l'électricité ou l'eau que nous consommons ».http://www.faso-tic.net/spip.php?article415&rubrique1 29décembre 2016.

[2] Salman Iqbal, Miss Laiha Mat Kiah, BabakDhaghighi, MuzammilHussain, Suleman khan, Muhammad Khurram Khan, Kim-Kwang Raymond Choo. On Cloud Security Attacks: A taxonomy and Intrusion Detection and Prevention as a Service. 2016

[3] I. Mettildha Mary, P.V.Kavitha, Priyadharshini M, Vigneshwer S Ramana. Secure Cloud ComputingEnvironmentagainst DDOS and EDOS Attacks. 2014

[4] Ajey Singh, Dr. ManeeshShrivastava. Overview of Attacks on Cloud Computing. 2014

[5] Margaret Rouse. http://searchmidmarketsecurity.techtarget.com/definition/keylogger

[6] Bhadauria, R., Al., A survey on security issues in cloud computing. 2011

[7] Rodero-Merino, L. et Am., Building safe Pass clouds: A survey on security in the multitenant software platforms. Computer & security, 2012.31(1): p 96-108

[8] Qiasi Luo1 and Yunsi Fei2. Algorithmic Collision Analysis for Evaluating Cryptographic System and Side-Channel Attacks", International Symposium on H/w – Oriented Security and Trust, 2011

[9] Matthieu Lamelot, Stockage en ligne : lequel choisir ? , http://www.tomshardware.fr/articles/comparatif-stockage-cloud,2-2332.html 7 Novembre 2016

[10] VALENTIN BLANCHOT Une IA de Google a créé son propre cryptage de données. https://siecledigital.fr/2016/11/03/intelligence-artificielle-google-cryptage-donnees/ 3 Novembre 2016.

[11] S. Subashini, V. Kavitha, A Survey on Security Issues in service delivery models of cloud computing. 2011

[12] Sandeep K. Sood, A combined approach to ensure data security in cloud computing.

[13] : Al Haddad Zayed, Hanoune Mostafa, MamouniAbdelazize, « Cloud Computing et sécurité : Approches et solutions. Décembre 2015.

[14] Balakrishnan.S, Saranya.G, Shobana.S, and Karthikeyan.S, « Introducing Effecyive Third Party Auditing (TPA) for Data Storage Security in cloud » Int. J.Comput.SciEnceTechnol, vol. 2 Jun 2011.

[15] F. Aloul, S. Zahidi, and W. El-Hajj, « Two factor authentification using mobile phones, » in Computer Systems and Applications, 2009 AICCSA 2009. IEEE/ACS InternationalConference on, 2009, pp. 641-644.

[16] E. M. Mohamed, H.S Abdelkader, and El-Etriby, « Enhaced data security model for cloud computing, » in Informatics and Systems (INFOS), 2012 8th International Conference on, 2012, pp. CC-12.

[17] Insitute of Electrical abdEkectronics Engineers, Ed., « Enhancing Data Security during Transit in Public Cloud , » Int.J. Eng. Innov. Technol. IJEIT, vol.3 ,Jul. 2013.

[18] « la protection des données personnelles dans l'open data : une exigence et une opportunité. » [online]. Available :http://www.senat.fr/rap/r13-469/r13-4697.html. [Accessed : 08-jul-2015].

[19] SagarTirdkar, YazadBaldawala, SagarUlane, Ashok Jori. Improved 3-Dimensional Security in Cloud Computing. International Journal of Computer Trends and Technology (IJCTT°- volume 9 number 5. 2014.

[20] AmanSagar, Bineet Kumar Joshi and NishantMathur. A study of distributed denial of service attack in cloud computing (DDOS). 2013.

[21] Belenky A, Ansari N. Tracing multiple attackers with deterministic packet marking (DPM). In : Proceedings of IEEE Pacific Rim conference on communications, computers and signal processing, vol , 2003 p.49-52.

[22] Ashley Chonka, Yang Xiang, Wanlei Zhou, AlessioBonti. Cloud Security defence to protect cloud computing against HTTP-DOS and XML-DOS attacks. 2010

[23] Omar Achbarou, My Ahmed El kiram, Salim El Bouanani, Securing Cloud Computing from different Attaks Using Intrusion Detection Systems.

[24] Ashley Chonka, Yang Xiang, Wanlei Zhou, AlessioBonti. Cloud Security defence to protect cloud computing against HTTP-DOS and XML-DOS attacks. 2010