A Survey on Security Issues and the Existing Solutions in Cloud Computing

Y. Ghebghoub, S. Oukid, and O. Boussaid

Abstract—Cloud Computing has been developed to deliver information technologies services on demand to organizations such as well as individual users, this technology is still in its early stages of development because it suffers from different security threats that prevent users trust it. In this paper, we identify different security problems existing in the cloud from several research papers and we show suggested solutions.

Index Terms—Cloud computing, security issues, threats, risks.

I. INTRODUCTION

Cloud Computing is a computer model that provides services in the form of on-demand services, it's accessible for everyone, everywhere and every time, including clouds referring to the internet and the web. Cloud computing is a concept still young but not so new that. Its early years in 1990, when the predicted mass adoption of grid computing, beyond only scientific computing applications. Basically, the principle is the same: it is thanks to technology virtualization pool of computing resources geographically dispersed to form a common virtual resource use "on demand". Found in cloud services, applications, processes all types, at least more customizable and that you can subscribe for free, without the need for other hardware resources that terminal (PC, phone or game console...) connected to the internet. This new technology suffers like all computer systems a serious problem that reduces trust between the client and the provider is the security.

In our paper, we focus on some papers that show different risks in the cloud and the different existing solutions that address these various problems. Our work is organized as follow: in the first and second sections, we will define cloud computing and its various models. In the third section, we related the services that inspired cloud computing, and in the forth section, we evocate the various advantages and disadvantages of this technology. Section five exposes some challenges facing the cloud and existing solutions. Finally, we conclude with a summary and a future proposal that will be our next work in this area.

II. THE DIFFERENT CATEGORIES OF CLOUD COMPUTING

A. The Public Cloud Computing

That are shared which anyone can access using an internet

Manuscript received March 6, 2013; revised July 7, 2013.

Y. Ghebghoub is with the University Saad Dahlab (e-mail: ghyasmine@hotmail.com).

S. Oukid is with the laboratory LRDSI Saad Dahleb University-Blida.

O. Boussaid is with the Institute of Communication of the University of Lyon 2, France.

connection and a credit card on a usage basis without subscription. So, these are virtualized infrastructure that shared by several users. It is easily accessible and managed from a self-service portal.

B. The Private Cloud Computing

A private cloud is one in which the services and infrastructure are maintained on a private network. Nevertheless, private cloud computing is unlike public cloud, owned and managed privately, and the access can be limited to a single business or a part of it. The private cloud computing may well seem safer in terms of security, stability, privacy and data persistence

C. The Hybrid or Mixed Cloud

It combines the use for the same company, a private cloud and a public cloud.

D. The Community Cloud

It is dedicated to a professional community that includes partners, subcontractors ... to work collaboratively on a project or a government cloud dedicated state institutions.

III. THE BENEFITS AND DISADVANTAGES OF CLOUD COMPUTING

A. The Benefits of Computing Cloud

Cloud computing offers the possibility of extending the information system of an enterprise at the request of the latter, according to the intended use. Services provided in the cloud are extensive. Particularly, the Company may benefit from the capacity of processing information, infrastructure, storage capacity and storage as well as computer applications.

B. The Disadvantages of Cloud Computing

Cloud computing seems to promise a great future. Many people or companies are against this notion, as the famous Richard Stallman (founder of the "Free Software Foundation") [1] who starts from cloud computing as a trap. The problem that comes up most is related security. How to guarantee the security of information stored in the cloud? More broadly Cloud Computing leads to the loss of control over the lifecycle of applications.

IV. MOTIVATION

Currently, security in information technology is considered as a key element. Hackers or the number of attackers are increased in order to address important data on the new technologies. Among them cloud computing, the technology that is being adopted by many companies due to industrial and commercial profits of cloud but the main

concern about these companies is the security of their data.

A. Problems of Security in the Cloud

In this study we classify security issues according to four categories of security, data security, logical security, physical security and administrative security.

1) Problems of data security

There are several studies that show the risks which threatened the security of the data stored in the cloud; we will show some in the next:

Kuyoro *et al.* [2] considered that security plays a very important role in cloud computing. They cited some problems such as security of data storage on a hard disk of another person, the loss of data and the problem of piracy; if hackers use thecloud services, they would offer free or at a cheaper price to fulfill their attacks.

Maheshwari and Pathak [3] have listed the various security challenges in cloud computing. They discussed the protection of data and that these data should mainly refer to the confidentiality, integrity and availability. They also identified problems of access users, the location and transmission of data which is secured by using IPSec (IP Security), SSL (Secure Socket Layer), but there still are some issues such as the speed and complexity of the input encoding.

Padia and Parekh [4] in their work showed various security issues, separating element by element. They began with problems related to data security from unauthorized access to data sources in an enterprise because the data is spread across different systems and they can be accessed by unauthorized persons.

Parakh and Kak [5] have shown that the traditional approach of security (explicit), whose data are stored on a single server and access to these data by a password, which is generally simple and memorable for most users, facilitated the attacks and intrusions on these data sources.

Karkouda *et al.* [6] treated in their work the security of the data warehouses stored in the cloud. They showed that reliance on providers is difficult to build with the traditional architecture of the cloud based on a single provider. This architecture threatens the confidentiality of customer data since they are hosted by a single provider of external risk operate [7].

Subashini, and Kavitha [8] consider that a multi-tenancy can cause problems in data security. This intrusion can be done either by hacking through the loop holes in the application or by injecting client code into the SaaS system. A client can write a masked code and inject into the application. If the application executes this code without verification, then there is a high potential of intrusion into other's data. They also spoke about data access and they considered that data access issue is mainly related to security policies provided to the users while accessing the data.

2) Problems of logic security

Subashini and Kavitha [8] considered that virtualization is one of the main components of a cloud. But this poses major security risks ensuring that different instances running on the same physical machine are isolated from each other is a major task of virtualization which is not met completely into day's scenario. The other issue is the control of administrator on host and guest operating systems. Current VMMs (Virtual

Machine Monitor) does not offer perfect isolation. Some vulnerability has been found in all virtualization software which can be exploited by malicious and local users to bypass certain security restrictions or gain privileges.

Arshad *et al.* [9] have focused their work on the risk of intrusion that threatens the cloud. They connects the severity of intrusions on virtual machines by factors such as the security requirements of the hosted application, the state of Service Level Agreement, the response time and the frequency of attacks on political of security.

Baniah and Brohi [10] spoke about virtual machines (VMs) that are managed by hypervisor in order to provide virtual memory as well as CPU (central processing unit) scheduling Policies to virtual machines. As the main source of hypervisor is managing a virtualized cloud platform, hackers are targeting it to access the virtual machine and the physical hardware, because hypervisor Resides Between virtual machine and hardware so attack on hypervisor can damage the VMs and hardware. In addition, co-location of multiple virtual machines increases the attack area and risk of virtual machine to compromised virtual machine. Intrusion detection and prevention systems must be able to detect malicious activity at the level of virtual machines, regardless of the location of the virtual machine virtualized cloud within the environment.

Bhadauria *et al.* [11] in cloud computing environment, the entire data resideover a set of networked resources, enabling the data to be accessed through virtual machines. Since these data centers may lie in any corner of the world beyond the reach and control of users. There are multifarious security and privacy challenges that need to be understood and taken care; they showed several risks that threaten the security of data in the cloud as SQL injection attacks, hidden field manipulation and distributed denial of service attacks.

3) Problems of administrative security

We mean by administrative problems all cases that affect the type of provider and the type of contract. There are certain authors who have spoken on this kind of problems.

Padia and Parekh [4] there may be a case that somecloud providers are not the authorized provider. They may be duplication of a Web page that already exists in order to trick and entice users into giving private or financial particulars or their passwords.

Finally, we summarized the problems that threaten the security of cloud computing on an unauthorized access to stored data, the risk of intrusion, loss of data, lack of trust between customer and supplier concern at confidentiality and availability of stored data, the poor use of services provided by malicious people, attacks on virtual machines and the type of provider and conditions of the signed contract.

B. Existing Solutions to Protect Cloud Computing

There are several works that propose solutions to some security issues that threaten cloud computing. These solutions are based on several techniques shown below.

1) Solutions based on cryptography

Sajithabanu *et al.* [12] propose a method to build a trusted computing environment for cloud computing system by providing secure cross platform into cloud computing system. The proposed Network consists of three backup sites for

recovery after disaster. The back up sites are located at remote location from the main server. If any one of the paths fails, it will use alternate path working. The encrypted file will be creating during back up sites and data's are compressed. The data will be decrypted during recovery operation. They proposed a cross-platform integration model by using secure communication via the internet and the utilization of a key for security. To encrypt the data SHA Hash Algorithm is used for compression, GZIP algorithm is used for symmetric splitting of files and SFSPL algorithm is implemented.

Ruj *et al.* [13] propose a new model for data storage and access in clouds, their scheme avoids storing multiple encrypted copies of the same data. In this framework, cloud stores encrypted data (without being able to decrypt them) in order to secure data storage. The main novelty of this model is addition of key distribution centers (KDCs). They propose DACC (Distributed Access Control in Clouds) algorithm by employing attribute-based encryption, where one or more KDCs distribute keys to data owners and users. KDC may provide access to particular fields in all records

Antony and Melvin [14] survey different encryption schemes used in clouds. Many encryption schemes like Attribute Based Encryption (ABE), key-policy attribute based encryption (KP-ABE), Ciphertext-Policy ABE (CP-ABE), CP-ASBE, hierarchical identity-based encryption (HIBE) are discussed in which all the schemes are concentrated on efficient access control. Finally it is concluded that HASBE scheme concluded the realization of scalable, flexible, and fine-grained access control in cloud computing.

2) Solutions based on data partitioning scheme

Parakh and Kak [5] considered that the traditional approach to securing data is to store and back it up on a single server and allows the access upon the use of passwords that are needed to be frequently changed. However, there is a tendency among users to keep passwords simple and memorable leading to the possibility of brute force attacks. Therefore, they prefer to use an algorithm for online data storage and number theory. The idea is to divide the data into K parts $d = d_1, d_2, d_3, \dots, d_k$. This division is made with the separation algorithm to the data stored on servers later randomly selected denoted $S = S_1, S_2, S_3, \dots, S_m$ with $m > k$. Data is partitioned on different servers so they are implicitly secured and they do not need to be encrypted partitions because they do not show the same information.

Karkouda *et al.* [6] proposed a way to protect data warehouses, to limit risks in cloud computing and to provide confidentiality and availability of data. The proposal is to split each data stored in the warehouse on several cloud providers through the sharing secret algorithm (Shamir 1979). Algorithm secret sharing shares the data tuples from several suppliers. The way of distributing data allows in one hand to store at each part of the provider information, they are then not understandable and not exploitable by a malicious user in the case of intrusion and secondly not to depend on one provider.

3) Solutions based on machine learning

Arshad and al. [9] focused on such challenge intrusion severity analysis. In particular, we highlight the significance of intrusion severity analysis for the overall security of clouds. Additionally, we present a novel method to address this

challenge in accordance with the specific requirements of clouds for intrusion severity analysis. They proposed to solve the severity problem by treating it as a problem of classification. Furthermore, machine learning techniques have been used to perform this classification. In this frame, the unsupervised learning techniques are usually more suitable for offline analysis as the classifications tend to change over the length of analysis data sets. The goal of a classifier is to build a model of class distribution in terms of the quantified characteristics of the constituent objects of the data set. In more formal terms, let $Z = \{(d_1, c_1), (d_2, c_2), \dots, (d_n, c_n)\}$ be a data set where $d_i \in D$, which represents the individual data items, and $c_i \in C$, which represents the class to which the particular data item belongs. In this case, a classifier h is a function such that $h: D \rightarrow Y$ i.e. it defines a mapping between a data item and its class based on some attributes. Consider an application Z with certain security characteristics Noted by X . The severity S of an intrusion I on the application Z is a function of the intrusion and the security characteristics f the victim application. This can be formally described as below:

$$S = f(I, X) \quad (1)$$

The output for function (1) can be defined as below:

$$S = f(I, X) \{c\}$$

where c is an entity in set, C is representing possible levels of severity.

4) Solutions based on multi agent system

Talib [7] describes an approach that allows us to build a security cloud platform using multi-agent system architecture to facilitate security of cloud data storage. This architecture tends to use specialized autonomous agents for specific security services and allows agents to interact and to facilitate security of Cloud Data Storage (CDS). They describe an approach that allows us to build a security cloud platform. The framework proposed has been built by using two layers; the functionality of those layers can be summarized as follows:

Agent layer has one agent called the User Interface Agent. He acts as an effective bridge between the user and the rest of the agents

Cloud Data Storage layer has two different network entities that can be identified as follows: cloud users which has data to be stored in the cloud and rely on the cloud for data computation. Cloud security platform has significant resources expertise in building and managing distributed cloud data storage servers, owns and operates live cloud computing systems.

V. CONCLUSION AND FUTURE WORK

In this paper, we present an overview of cloud computing which became used from individuals and institutions alike, and we underscored one of the most important problems in cloud: it is the security. There are several threats to the protection of cloud and detracts the trust between the user and the provider including unauthorized

access, data loss, poor use of services provided by the cloud, the bad and the different hardware hacker attacks and intrusion.

To make this technology more secure, researchers have proposed several security solutions that are based on several ways as cryptography and other.

As we mentioned earlier, the cloud has several security problems among accessible by "anyone" who exposes the cloud to several threats such as unauthorized access to data sources, data theft and intrusions.

In the future, we propose a solution to control the user access to data sources stored in the private cloud by using two important security policy role based access control (RBAC) and multilevel. We propose to incorporate a framework between the client and the cloud; sharing the network into three parts (client control framework, cloud).

This layer controls user access through RBAC model that shares the users according to roles whose role is so abstract function in an organization and for each role are associated privileges which are a set of rights to duties can be achieved by each part. And thanks to the multi-level policy is associated to each role a level of security to provide confidentiality and integrity of data stored in the cloud and protect against unauthorized access.

REFERENCES

- [1] Laboratoire de recherche xbrainlab, Le Cloud Computing : Réelle révolution ou simple évolution, *Livre blanc*, 2011.
- [2] S.O. Kuyoro, F. Ibikunle, and O. Awodele, "Cloud Computing Security Issues and Challenges," *International Journal of Computer Networks*, vol. 3, issue 5, pp. 247-255, 2011.
- [3] R. Maheshwari and S. Pathak, "A Proposed Secure Framework for Safe Data Transmission, in Private Cloud," *International Journal of Recent Technology and Engineering*, vol. 1, issue 1, pp. 78-82, April 2012.
- [4] N. Padia and M. Parekh, "Cloud Computing Security Issues, in Enterprise Architecture and Its Solutions," *International Journal of Computer Application*, vol. 2, issue 1, pp. 149-155, December 2011.
- [5] A. Parakh and S. Kak, "Online data storage using implicit security," *Information Sciences*, vol. 179, pp. 3323-3331, 24 May 2009.
- [6] K. Karkouda, N. Harbi, J. Darmont, and G. Gavin, "Confidentialité et disponibilité des données entreposées dans les nuages," in *Proc. 9^{ème} atelier Fouille de données complexes (FDC 12)*, pp. 1-14, 2012.
- [7] A. Talib, "Security Framework of Cloud Data Storage Based on Multi Agent System Architecture: Semantic Literature," *Computer and Information Science*, Published by Canadian Center of Science and Education, vol. 3, pp. 175-186, November 2010.
- [8] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *Journal of Network and Computer Applications*, vol. 34, pp. 1-11, 2011.
- [9] J. Arshad, P. Townend, and J. Xu, *A Novel Intrusion Severity Analysis Approach for Clouds*, School of Computing, University of Leeds, Leeds, LS2 9JT, UK, pp. 1-13, 2011.
- [10] M. Adib Bamiah and S. Nawaz Brohi, "Seven Deadly Threats and Vulnerabilities in Cloud Computing," *International Journal of*

Advanced Engineering Sciences and Technologies, vol. 09, pp. 087-090, 2011.

- [11] R. Bhadauria, R. Chaki, N. Chaki, and S. Sanya, "A Survey on Security Issues in Cloud Computing," *IEEE Communications Surveys and Tutorials*, pp. 1-15, 2011.
- [12] S. Sajithabanu and E. G. P. Raj, "Data Storage Security in Cloud," *International Journal of Computer Science and Technology*, vol. 2, issue 4, pp. 437-440, Oct. -December 2011.
- [13] S. Ruj, A. Nayak, and V. Stojmenovic, "DACC: Distributed Access Control in Clouds," in *Proc. International Joint Conference of IEEE TrustCom-11/IEEE ICSS-11/FCST-11*, pp. 91-98, 2011.
- [14] N. Antony and A. A. R. Melvin, "A Survey on Encryption Schemes in the Clouds for Access Control," *International Journal of Computer Science and Management Research*, issn 2278-733x, vol. 1, Issue 5, pp. 1135-1139, December 2012.

Yasmina Ghebhoub was born on 1986 in Algeria. She received the Bachelor degree in natural science and life, Blida in June 2004 then the Diploma Degree in Computer Science in 2007, Master Degree in Computer Science: Software Engineering in 2009 from Saad Dahleb University-Blida. She is a temporary teacher of computer science at the University Saad Dahlab. She is currently a Ph.D. student in the Department of Computer Science. Her research interests include security of Data Warehouses, Security on cloud.

Saliha Oukid is Vice Rector for External Relations of Saad Dahlab University, Blida, Algeria. She is a lecturer Class A and director of laboratory LRDSI Saad Dahleb University-Blida. Her research interests include Machine learning, Biocomputing, Data mining, Data Warehouses, Decision Support Systems.

Omar Boussaid is a full professor in computer science at the Institute of Communication of the University of Lyon 2, France. He received his Ph.D. degree in computer science from the University of Lyon 1, France in 1988. He received the accreditation to supervise research in 2006 at the University Lumière Lyon 2.

Since 1995, he is the director of the Master Computer Science Engineering for Decision and Economic Evaluation of the University of Lyon 2. He is the director of the Department of Computer Science and Statistics. He was a head of the Decision Support Databases research group within the ERIC Laboratory, during March 2008 to October 2010.

His main research subjects are data warehousing, multidimensional databases and OLAP. His current research concerns complex data warehousing and mining, XML warehousing, combination of OLAP with data mining and information retrieval, the use of ontologies within complex data warehousing, social OLAP with the detection and analysis of communities, data warehouses and OLAP on the cloud, using the MapReduce paradigm and NoSQL databases to create OLAP cubes in the cloud environment.