"Mircea cel Batran" Naval Academy Scientific Bulletin, Volume XIX – 2016 – Issue 2
The journal is indexed in: PROQUEST / DOAJ / Crossref / EBSCOhost / INDEX COPERNICUS / DRJI / OAJI / JOURNAL INDEX / I2OR / SCIENCE LIBRARY INDEX / Google Scholar / Academic Keys/ ROAD Open Access / Academic Resources / Scientific Indexing Services / SCIPIO / JIFACTOR

ABOUT ISSUES AND THREATS FOR CLOUD COMPUTING

Stefania Loredana NITA[1]
Marius Iulian MIHAILESCU[2]

[1]Integrated Systems Department, Institute for Computers, stefania.nita@itc.ro
[2]Department of IT&C, LUMINA – The University of South East Europe, marius.mihailescu@lumina.org

Abstract*: In the last few years, cloud computing has become more and more popular among small, middle and large companies because of more reasons. It provides different types of services, such as software applications, platforms and even infrastructures, through abstraction and virtualization, fact that brings to the companies many benefits. One of them is cost reduction because they do not need to buy servers, software products or licenses any more, and they pay just as they consume. On the other hand, the users are freed of the maintenance or upgrading, because this task become the responsibility of the cloud providers. Even if it is very powerful, still, cloud computing has some lacks. For example the security of the data: when the data are transmitted through systems which are not under the control of the user, the risk that data to be compromised is increased, especially the services inherit the vulnerabilities of the technology transformed in that service. In general, in providing of cloud computing services are involved third parties, fact that complicates the keeping of secured data. In this paper, we will identify and analyze the main issues of cloud computing and we will present the existing solutions to this issues.*

Key words: *cloud computing, security, services, software.*

I. Introduction

Cloud computing is a kind of computing based on sharing computing resources, so the applications are not handled on local servers or particular devices. Cloud computing shares some characteristics with grid computing.The purpose of the cloud is to use classical supercomputing power, or a power of computing of high-performance, for performing trillions of computations in a second for different types of applications, in order to providing individual information, for supplying data depositing. To accomplish this requests, cloud computing makes use of the networks from great clusters of servers, on which run computers with a technology of low-cost, having special links to propagate the processing of the data between them.

Cloud computing has become a trend technology among the companies, and not only. It provides an environment for files storing, applications and platforms storing and managing, an even the virtualized form of hardware. It is very important that all entities to be kept safety. Cloud computing security represents a suite of technologies and policies projected in order the data to be safe. In cloud computing the resources are shared, so it came up some worries, like privacy and data protection, the control of the accession, or identity management. The insurance of high level of security has become a major priority for many companies.

There are many benefits of using cloud computing, like costs reduction, the users are freed from the maintenance and administration of the applications, or servers, large power of computing. Besides the benefits are some lacks in cloud computing regarding the data security.

In the next section we will present some definitions of cloud computing and we will describe the cloud computing model services, in the third section we will describe the most frequent security issues of cloud computing. In the fourth section we will present some existing solution of the security issues from the domain literature.

II. Cloud computing

A. Definitions

In the last years, cloud computing has gained more and more importance, becoming an essential part of the technology. Cloud computing takes the technologies, services and applications and transform them into an on demand utility. The *cloud* word presents two important characteristics:

- *Virtualization*. The resources are shared and pooled, while the systems and depots could be provisioned on demand from a centralized infrastructure. In this case, the costs are evaluated on a measurable basis, the multi-tenancy is allowed and the resources are scalable.
- *Abstraction*. The details of the implementation are abstracted from the users or developers. The applications are running on unspecified

DOI: 10.21279/1454-864X-16-I2-075

physical systems, the data is stored in unknown locations, the administration of the systems is externalized and the access of the users to the resources is unlimited.

In 2011, The National Institute of Standards and Technology has defined the cloud computing as follows [1]:

"Cloud computing is a model for enabling ubiquitous, convenient, on - demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidlyprovisioned and released with minimalmanagement effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models."

On the other hand, in 2009, the Berkley researchers has characterized the cloud computing with three main elements [2]:

1. Cloud computing offers the delusion of unlimited resources accessible on request.
2. It exists the discharge of an up-front engagement by cloud.
3. The payment is proportional with the consumed resources, so the clients pay as they consume.

Besides these two definition, there is one more given by the Jericho Forums, which defines the cloud using the cube model (Figure 1), in which every dimension of the cube represents a characteristic of the cloud[3].

Some of the important vendors are Microsoft Azure, Amazon Web Services, or GoogleAppEngine.

Amazon Web Services is a complete, advanced cloud computing environment supplied by Amazon.com, offering a large variety of services on demand, which was released in 2006[4], [5].

Asstands on the official web site [6]:"*Microsoft Azure is a growing collection of integrated cloud services—analytics, computing, database, mobile, networking, storage, and web—for moving faster, achieving more, and saving money."*

Google AppEngine represents a platform, which allows the build of scalable web application and mobile backend and supplies built-in services or APIs. The scaling of the applications is done automatically. After uploading the code, Google manages the application's availability, without server's provision or maintenance being the task of the user[7].

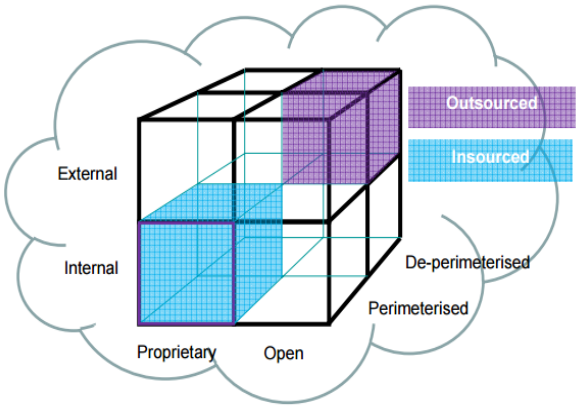

Figure 1. The cube model presented in [3]

B. Service models of cloud computing

Software as a Service (SaaS)**.** In Software as a Service model, the users have access to software applications and databases. SaaS is also known as on demand software, and the estimated costs is computed following the principle payment/consume, being a model of software implementation through which the provider is licensing an application in order to be used as on demand service. The application could be accessed by the users on different devices, using an easy to use interface. SaaS eliminate the link between machines and solutions, fact that allows the users to license only that resources they need. Using Saas, the operational costs for IT are eliminated, because the cloud provider maintains everything regarding applications. Some examples of SaaS are: GoogleApps, Oracle On Demand, SalesForce.net, SQL Azure etc[8].

Platform as a Service (PaaS). In Platform as a Service (PaaS) model, the providers offers solutions for advanced development, but also applications host. Paas is addressed to the companies which could develop and host the own solutions based on demand in order to accomplish the requests from third parties or internal requests. The cloud providers offers a computational platform, which includes an operating system, execution environment for programming languages, web servers and databases. So, the user could develop and implement applications on the cloud infrastructure, using programming languages and tools ensured by the provider. There is no need to imply other software or hardware components, fact that reduces the costs. The resources are automatically scaled, so they not need to be manually allocated. Also, the administration and

DOI: 10.21279/1454-864X-16-I2-075

the control of the cloud infrastructure which comprises networks, servers or operating systems not the user's task, but to the cloud provider task[8]. Instead, the user have full control over developed applications. Examples of Paas are Google AppEngine, Windows Azure Platform, Force.com etc.

Infrastructure as a Service. The Infrastructure as a Service model is used by the institutions which want to externalize all infrastructure, including servers, storage environments, networks. This is also known as Hardware as a Service. In the IaaS model with minimal functionalities, a provider rents a technological infrastructure, so virtual servers on remote, which could replace the IT systems from the company's headquarters or which could be used together with the existing systems[8]. The cloud provider owns the equipment and is responsible with the host, administration and maintenance of it. The user in not implied in controlling the cloud infrastructure, but controls the operating system, storage environment, implemented applications and limited the user controls the network components. Examples of IaaS are: Amazon Elastic Compute Cloud (EC2), Eucalyptus, GoGrid etc.

These three service models are known as SPI model for cloud computing. Are more service models, but these are incorporated by the SPI model. Another types of services are: Storage as a Service (StaaS), Identity as a Service (IaaS), Compilance as a Service (CaaS) etc.

III. Security threats of cloud computing

Data breaching is the process through which the data is viewed unauthorized or illegally, or accessed or retrieved by a malicious user, application or service. This issue is created for stealing or publishing the data on an unsafe or illegal location. In 2015, were many data braches, including attacks on companies of health care, information security, banks, universities.An example is Premera BlueCross BlueShield, a health care company, which have announced in March 2015 that in January 2015 were affected almost 11.2 million subscribers and few entities that works with this company. Thus, names, bank account information, addresses, and many others data have been compromised[9].

Exploiting system vulnerabilities.Even if exploiting the system vulnerabilities is not a new technique for compromising the data, it have become a real problem, because different institutions distribute some types of data between them, creating a new point of attack. Luckily, these could be avoided with simple IT processes, like frequent vulnerabilities scanning, and other basic processes.

Shared resources.The layers of cloud computing are applications on the top, then platforms, and then infrastructures. All of these could share the same memory. If a vulnerability appears in one of the layers, all of them could be affected, because the shared memory could be affected and it will result a chain of vulnerabilities [10].

Virtualization[13]. Virtualization brings a large range of vulnerabilities. It brings new occasions for malicious users, because of the extra layer, which needs to be secured. The vulnerable virtualization points are: the hypervisor, public virtual machine image repository, virtual machine rollback and life cycle, and virtual networks. The hypervisor of cloud computing is the program which allows to many virtual machines to use the same resources. If it is compromised, then all virtual machines could be compromised. The public virtual machine image repository is the software which contains configuration files for all virtual machines of the system, so they have a fundamental role in the cloud computing security. The virtual machines could be returned to a previous state, but returning to a previous state it is possible to be again vulnerable to a security issue already resolved.Also, the virtual machines have a life cycle undeterministic, so they could be suspended, turned on or off, facts that could influence the other virtual machine behavior. Virtual networks enlarge the virtual machine communication, fact that gives new opportunities of attacks.

IV. Existing techniques and solutions

*Homomorphic encryption*represents an encryption method in which the cipher texts can be operated with particular operation by a party which have access to it[10]. These operations are the equivalent operation over the plain text. Simple homomorphic encryption allows a single operation over the plaintext to have a corresponding operation over the cipher text in the presented context. Let's say the encrypted text c_1 is obtained using a public key*pk* from the message m_1, and the encrypted text c_2 is obtained using the same key, from message m_2[10]:

$$c_1 = encryption(pk, m_1) \quad (1)$$

and

$$c_2 = encryption(pk, m_2) \quad (2)$$

If we multiply the c_1 and c_2, at decryption of the result we obtain the same result if we multiply the m_1 and m_2. For s_k being the decryption key, we obtain[10]:

DOI: 10.21279/1454-864X-16-I2-075

$$m_1 \times m_2 = decryption(sk, c_1 \times c_2) \quad (3)$$

Fully homomorphic encryption is stronger than the above operations. Instead having just one operations, we have a corresponding operation applied on encrypted text of the operation applied on the plain text. In other words, every program has an equivalent program, which performs of cipher texts. If *p* is the program and the *p'* is the corresponding program over encrypted text, we have:

$$p(m_1, \ldots, m_n) = decryption\left(sk, p'(pk, c_1, \ldots, c_n)\right). \quad (4)$$

where $c_i = encryption(pk, m_i)$ and $encryption/decryption$ represents fully homomorphic encryption scheme[10].
Homomorphic encryption represents one of the most powerful encryption techniques, which have applications in cloud computing.

Another powerful techniques are Crypto Cloud Computing (CCC)[11] and Digital signatures[12].
In the following, we present some solution proposed in the domain literature.

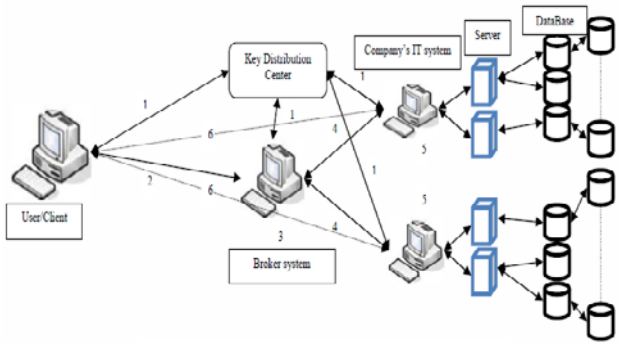

Figure 2. The architecture proposed in [14]

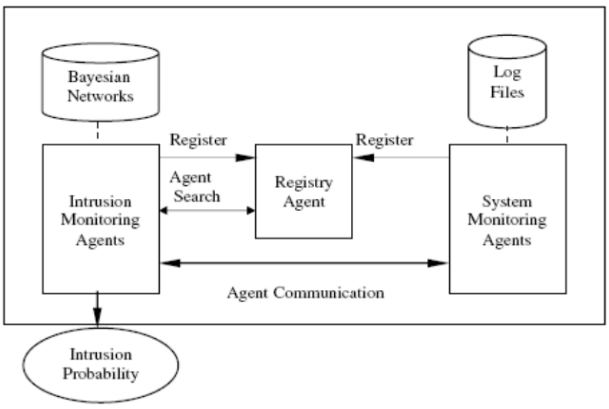

Figure 3. The architecture proposed in [15]

In [14], the authors have proposed an interesting solution based on encrypting and fuzzy logic with a trust model. In the Figure 2 is presented the architecture proposed in[14]. It works as follows [14]: the first step is to introduce a broker system among various companies that will be used for showing the trust valuables of various companies (which will be computed and saved on the broker system) and for establishment of a connection among the clients and the companies selected by the clients. Next, the firms should notify the broker system on the upgraded data of the trusted valuables, and then, these values will be updated by the broker system for the companies on the proper site in order to be seen by the next customer. Another important thing in this approach is that the companies keep data about the levels of the servers and database which will be used in order to rate these two components of the company for giving higher performance services for customers and users. The data of the companies could be encrypted using AES, and the keys are kept on the principal system. For a comprehensive description, see[14].
Another approach regarding security in cloud computing is the intrusion detection system (IDS) based on Bayesian networks and multiply sectioned Bayesian networks (MSBNs) [15]. The authors present a system (Figure 3) for intrusion detecting which has three purposes:

1. Detecting of the intrusions through local monitoring and distributing the own estimation convictions of the agents for a collaborative detecting;
2. The undermined hosts are identified and isolated using a distributed relied framework;
3. The performance of the detection is increased and false positives are decreased.

In [16] it is proposed a protocol for secured computations, called SecCloud, that is the first protocol which links secure storage and secure computation for cloud, as the authors have mentioned. Another proposal is an experimental cloud computing environment, called SecHDFS, used in order to test SecCloud. Also, the authors have introduced two concepts, *Secure Computation Confidence* and *Secure Storage Confidence*, which determines how secure the computations and the storages are.

DOI: 10.21279/1454-864X-16-I2-075

CONCLUSIONS

As cloud computing is more and more adopted by different companies, we need to find the security issues and also we need to find solutions to them. We have seen that cloud computing have different definitions, but its purpose is always the same, indifferent of definitions. It provides powerful service models, which could be secured using techniques like homomorphic encryption or crypto cloud computing. Further, we have seen that there are more security issues, many of them becoming from virtualization, others inherited from the core applications and we have mentioned a few solutions from the domain literature.

BIBLIOGRAPHY

[1] Peter Mell, Timothy Grance, *The Nist Definition of Cloud Computing*, NIST Special Publication 800-145, September 2011.

[2] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, MateiZaharia, *Above the Clouds: A Berkeley View of Cloud Computing*, Technical Report No. UCB/EECS-2009-28, February 10, 2009.

[3] *Cloud Cube Model: Selecting Cloud Formations for Secure Collaboration*, 2009, https://collaboration.opengroup.org/jericho/cloud_cube_model_v1.0.pdf

[4] *Amazon Web Services (AWS),* http://whatis.techtarget.com/definition/Amazon-Web-Services-AWS

[5] *Amazon Web Services,* https://en.wikipedia.org/wiki/Amazon_Web_Services

[6] *Microsoft Azure*, https://azure.microsoft.com/en-us/overview/what-is-azure/

[7] *Google Cloud Platform*, https://cloud.google.com/appengine/

[8] Hoang T. Dinh, Chonho Lee, DusitNiyato, Ping Wang. *A survey of mobile cloud computing: architecture, applications, and approaches*, Wireless communications and mobile computing, 2013, 13.18: 1587-1611.

[9] Sarah Kuradra. *The 10 Biggest Data Breaches Of 2015 (So Far)*, 2015, http://www.crn.com/slide-shows/security/300077563/the-10-biggest-data-breaches-of-2015-so-far.htm/pgno/0/3

[10] Mark D. Ryan.*Cloud computing security: The scientific challenge, and a survey of solutions*, Journal of Systems and Software, 2013, 86.9: 2263-2268.

[11] Marius I. Mihailescu. Stefania L. Nita. *Software engineering and applied cryptography in cloud computing and big data*, International Journal on"Technical and Physical Problems of Engineering" (IJTPE), 2015, 24.7:47-52

[12] PrashantREWAGAD,Yogita PAWAR. *Use of digital signature with diffiehellman key exchange and AES encryption algorithm to enhance data security in cloud computing,* In: Communication Systems and Network Technologies (CSNT), 2013 International Conference on. IEEE, 2013. p. 437-439.

[13] Keiko Hashizume, David G. Rosado, Eduardo Fernández-Medina, Eduardo B. Fernandez. *An analysis of security issues for cloud computing*, Journal of Internet Services and Applications, 2013, 4.1: 1-13.

[14] Kawser W. Nafi, Tonny S.Kar, Amjad Md. Hossain, M. M. A. Hashem. *A New Trusted and Secured E-commerce Architeture for Cloud Computing*, Informatics, Electronics & Vision (ICIEV), 2013 International Conference on. IEEE, 2013, pp. 1-6.

[15] Jaydip Sen, *A Robust and Fault-Tolerant Distributed Intrusion Detection System*, Parallel Distributed and Grid Computing (PDGC), 2010 1st International Conference on. IEEE, 2010, pp. 123-128.

[16] Lifei Wei, Haojin Zhu, Zhenfu Cao, Xiaolei Dong, WeiweiJia, Yunlu Chen, Athanasios V. Vasolakos. *Security and privacy for storage and computation in cloud computing*, Information Sciences, 2014, 258: 371-386.

DOI: 10.21279/1454-864X-16-I2-075