International Journal of Innovation and Applied Studies
ISSN 2028-9324 Vol. 14 No. 3 Feb. 2016, pp. 795-800
© 2016 Innovative Space of Scientific Research Journals
http://www.ijias.issr-journals.org/

Implementation a dynamic security in the Cloud computing environment

Yassine EL MAHOTI[1-2]***, Noura AKNIN***[1-2]***, and Kamal Eddine EL-KADIRI***[2]

[1]Information Technology and Modeling Systems Research Unit,
Faculty of sciences Abdelmalek Essaadi University,
93030 Tétouan, Morocco

[2]Computer Sciences, Operational Research and Applied Statistics Laboratory,
Faculty of sciences Abdelmalek Essaadi University,
93030 Tétouan, Morocco

ABSTRACT: This recent years, the security of cloud computing has become a major challenge for all organizations because any attack can cause serious problems such as stealing customer and government information, control of systems by others entities (hackers) to perform any operation for their needs, etc. The last decade, the cyber-attacks have become increasingly complex, sophisticated, multiple and the majority of traditional security systems are unable to detect them.
The goal of this article is present a secure layer installed in the cloud providers that allows a high security performance in the cloud environment. This is achieved by controlling all the services executed by customers on their virtual machines and block or quarantine the unknown of them until the provider decision is made.

KEYWORDS: Cloud Computing, Dynamic security, Cyber-attacks, Virtualization.

1 INTRODUCTION

With cloud computing, companies, users or public organizations can use many services they would not otherwise have because of the cost. In particular, small organizations or individuals can use very IT advanced services that the cloud permits them to develop and sell their own services. Therefore, the cloud computing offers tremendous potential for creativity and innovation in the services on the internet.

Despite the great success proved by the cloud during the last years in terms of diversity of applications given for costumers, it began to have a serious problem especially in data and access security. In fact, the cloud is based on virtual environments, it allows many customers to share the same resources like (storage, network, CPU, RAM). This sharing of hardware and data between many costumers by virtual machines must be secured, because any mishandling of a VM can overthrow the datacenter and therefore overthrow all the cloud providers' activities.

This paper propose an implementation of a software layer in the cloud servers that permit to move from a static security system which is based generally by implementing the traditional security policy like as installing firewalls, network filtering, access restriction to another dynamic that monitors in real time all activities executed by the client in the cloud platform (resources consumed, applications executed, localization services, etc.). Moreover, the moment when it detects a suspect behavior of the client such as a strange localization, executing applications which isn't in his profit, it blocks the virtual machine infected and contacts the admin for taking the necessary precautions.

The paper is organized as follows: Section (1) gives an overview of the Cloud computing: its types and its deployment methods, Section (2) describes the virtualization environment and the last section (3) describes the functioning of the software layer proposed.

2 CLOUD COMPUTING

Faced with the ever-increasing costs of implementation and maintenance of IT systems, companies outsource more often their systems management. [2]

Indeed, this outsourcing of resources and software is cloud computing. Cloud computing allows the use of multiple services on demand, and the company pays only what it consume. This new model of IT management has given a great flexibility for companies to manage their data, and a significant economization at material and human resources. Cloud computing has proven to be a very important contributor at the ecological and economical levels by:

- Reducing the energy consumption by resources polling (sharing the same resources with several customers).
- Reducing cost: the companies pays only what they consume.
- Reducing waste: infrastructure managed internally are often underutilized, while a cloud infrastructure is pooling all resources for a large number of companies, and,
- Making resources flexible: the company can increase the capacity of its infrastructure without major investment.

The services offered by the cloud can be positioned in three areas: There are three types of cloud as shows the figure 1:

- SaaS: Software as a Service
- PaaS: Platform as a Service
- IaaS: Infrastructure as a Service

2.1 SOFTWARE AS A SERVICE: SAAS

Software as a Service (SaaS) is a software installed on remote servers rather than on the user's machine. Customers do not pay for a license version, but generally use free online service or pay a recurring subscription.

2.2 PLATFORM AS A SERVICE: PAAS

PaaS allows a test environment with all the necessary prerequisites for any company or individual that want to test their applications.

2.3 INFRASTRUCTURE AS A SERVICE: IAAS

IaaS (Infrastructure as a Service) provides a virtual IT infrastructure such as the computing power, virtual machines, including an operating system, storage and backup services.

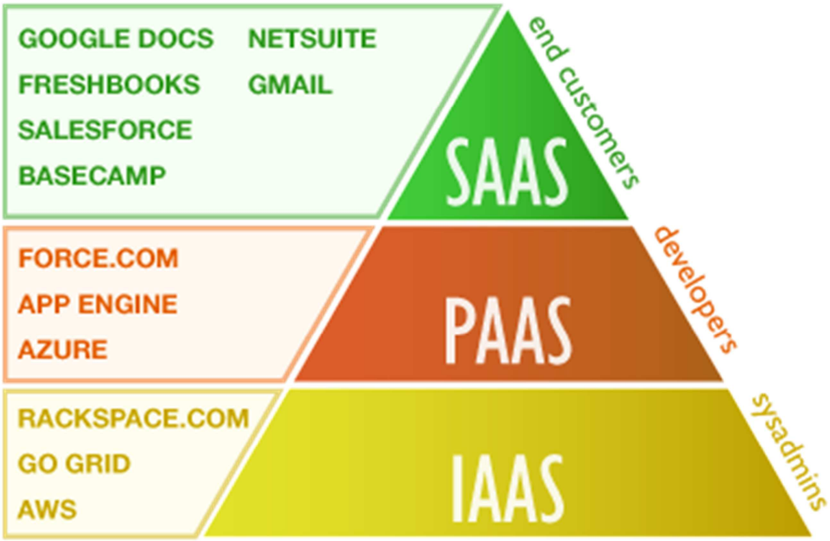


Fig. 1. Cloud computing types

2.4 DEPLOYMENT MODELS

There are three main deployment models in the IT world: public cloud, private and hybrid. Each model is used according to the need of the company or individual.

- Public cloud

Public clouds are managed by a specialized company that rents its services to many companies or individuals. This mode is open for everyone no matter how they are connected to the internet.

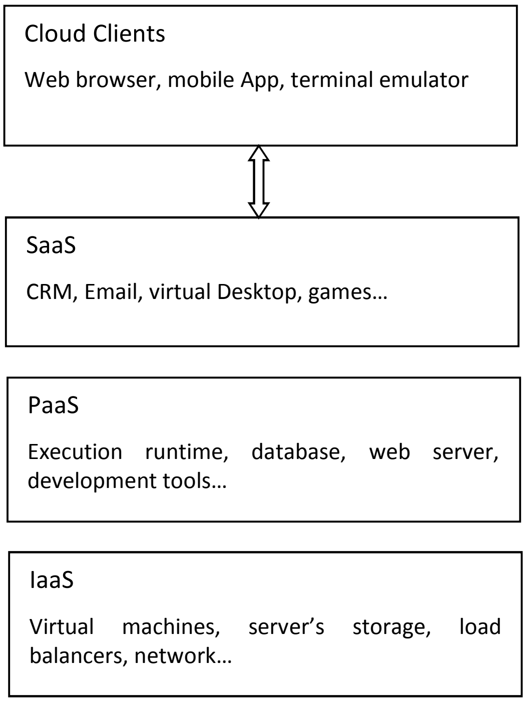
- Private cloud

Private clouds are dedicated to the needs of a single company or group of companies but hosted by a service provider.

- Hybrid cloud

Hybrid cloud is a combination of both public and private cloud models.

The Cloud is a topical environment that knows huge changes; diversity of services enables customers to have a fairly comprehensive list, we show the different services that can be benefited by the customer. [4]- [8]



Cloud Clients

Web browser, mobile App, terminal emulator

SaaS

CRM, Email, virtual Desktop, games…

PaaS

Execution runtime, database, web server, development tools…

IaaS

Virtual machines, server's storage, load balancers, network…

3 THE TRADITIONAL SECURITY POLICY

The majority of the Information Systems managers invest fully to mount a secure IT platforms, they know very well that a single attack can cause serious damage to their company's business, the security policy used by the most of them is based on the implementation of several security layer:

- Firewalls (Firewall): a component that protects a network from intrusions from Internet generally the third-party networks.
- Data encryption: a technique that reformulate a source information in order to be not interpreted by unauthorized entities. Encryption is an essential mechanism to make the highly secure information especially for governments, military and banks.
- Access management: a mechanism to clearly specify the entities that have the right of access to computers and IT platforms. The types of access can be physical like making access restrictions (access badges, biometrics), or logical as well make specified user profiles (administrator profile, user profile).
- IPS (Intrusion Protection System): The IPS is a prevention system / intrusion protection against malware and hackers. IPS is an extended an IDS (Intrusion Detection System) which aims to intercept intruders packets in the network.

As we can see, the majority of information systems managers were focused to build a very secure perimeter around their platforms while believing that the attacks came from outside their network. But in recent years, the attacks change target because the control and the supervision of users has become a very difficult task, he can connect through an insecure and an untrusted network with his mobile, so the hackers have taken advantage of this factor, they reprogrammed a user-oriented attacks to take the necessary information to seep invisibly in companies networks and make the desirable instructions and attacks.

Today, the type of attacks have become increasingly oriented and targeted, the hacking now has become a well-organized and defective crime and the hackers do not just target the single internet users, but rather they target big entities such as government, banks and multinational industries.

Faced with the implementation of these static security systems, the digital attacks have been redeveloped and reclaimed more maturity and became able to infiltrate invisibly in the network, the hackers know very well how this security systems are implemented and they are aware that attacking directly is a very difficult operation, so that the attacks were redirected towards users, they usually have no internet safety culture, and can install defective applications or navigate in malicious sites and share they sensitive business information that allows hackers to have the necessary information to build a very sophisticated and invisible attack.

4 PROPOSED WORK

4.1 DESCRIPTION

Since users have become the attractive targets for hackers, we implemented an additional architecture of the classical architecture (firewall, IPS), called the dynamic security for detecting the unknown user’s behavior. This software layer (as shows the figure 2) is dedicated to detect in real-time the unknown user’s behavior based on the previously reports consolidated on their various activities in the Cloud (location, interest profile, monitor running processes, resources consumed, etc.).

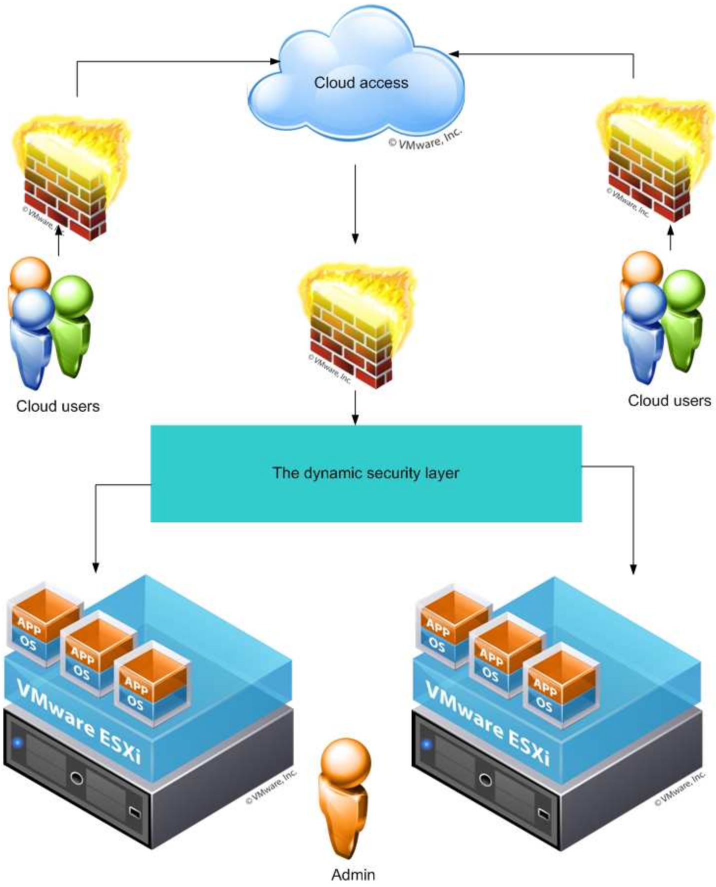


Fig. 2. The proposed architecture

This layer is a group of subsystems interconnected between them for having a real time monitoring for all activities executed by the customers:

- Localizer agent: return the localization of the client.
- Monitor Agent: this agent monitors the resources allocations and the executed applications in virtual machines.
- Reporter Agent: gets information from Localizer & Monitor agent and:
  - Contacts the firewall and VMM to block all unknown services or virtual machine when it founds an unknown service was in black list of service and notify the admin platform.
  - Notify the admin when it founds a new unknown service for staring investigation
- The virtual machine manager (VMM): the hypervisor of all virtual machine, It performs the migration of virtual machine (VM) between hosts, add resources to VM

This architecture proposed allows a very detailed report on all activities by the customers and also communicate with the major actors in the platform for providers (Virtual Machine monitor (VMM), firewall, etc.).

4.2 ALGORITHM

The architecture proposed runs scripts on the network for returning on real time all services executed in providers network and communicates in a dynamic and interactive way with the VMM and the admin to block or permit an execution of an application. The functioning process of this software layer Middleware is defined as shows the figure 3.

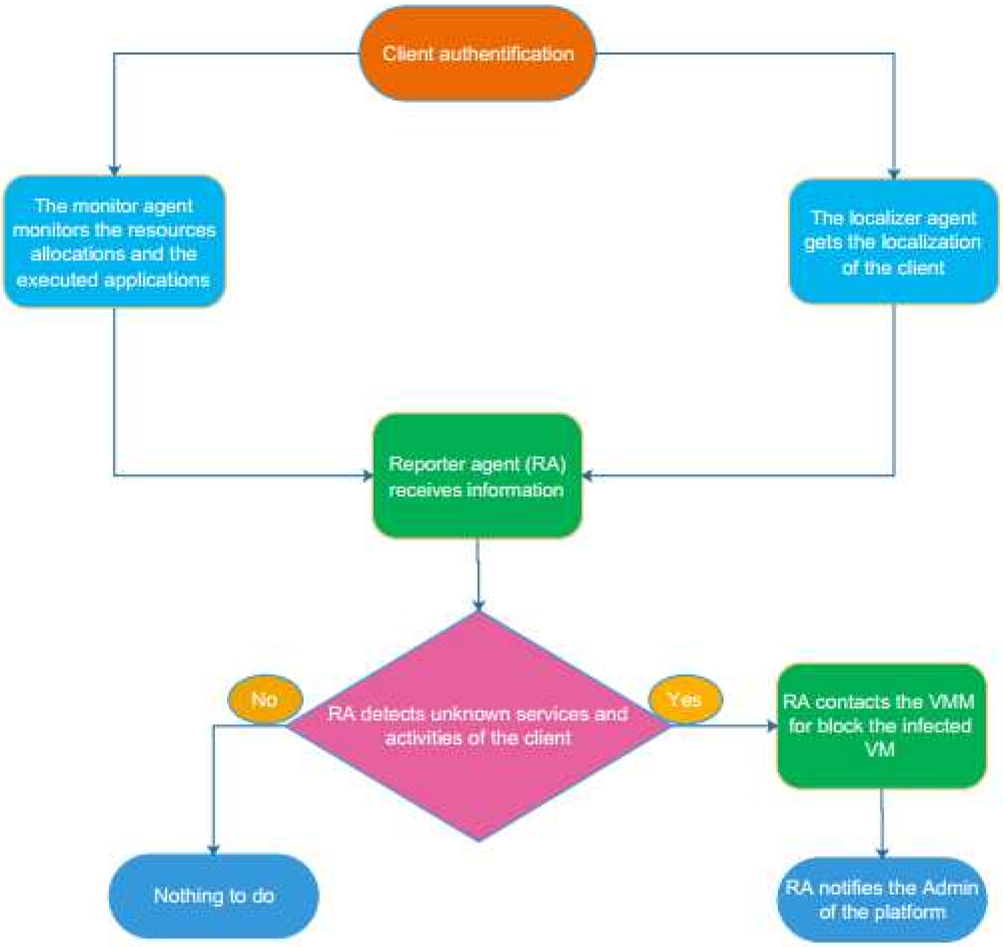

Client authentification
The monitor agent monitors the resources allocations and the executed applications
The localizer agent gets the localization of the client
Reporter agent (RA) receives information
RA detects unknown services and activities of the client
No
Yes
RA contacts the VMM for block the infected VM
Nothing to do
RA notifies the Admin of the platform

Fig. 3. The proposed algorithm for detecting the unknown services

When user authenticates in the cloud, the localizer and the monitor agent come back in real time information to the reporter agent like as resources allocations, executed services, its location, etc. This information will be compared with already consolidated reports of the customer, and the moment of the RA detects a suspicious behavior such as a different location of the client or a mysterious applications are running witch are not in its profits, it contacts the VMM to quarantine the infected virtual machine and notifies the cloud administrator to take the necessary precautions.

CONCLUSION

The cloud security requires a deep reflection on the establishment of security policies. In a cloud environment, the connection management and access profile were exceeded, we had to go to the next level and think of security in terms of use and type of hosted data. The amount and variety of information exchanged in the cloud need to have a security system that takes into account these factors. For this it is necessary have a dynamic system that analyzes each information separately and specifically.

The architecture proposed in this paper permits this dynamic treatment because it ensures a real time monitoring for all services executed in the cloud platform and block any unknown of them, to avoid any execution of any services by a virtual machine which can damage the shared resources of the cloud platform.

REFERENCES

[1] M. Hsieh, C.Chang, L. Ho, J. Wu and P. Lui. "SQLMR: A Scalable Database Management System for Cloud Computing

[2] Yassine ELMAHOTI , Noura AKNIN, Souad Amjad, Kamal Eddine El Kadiri Process optimization time for a service in 4G network by SNMP monitoring and IaaS cloud computing", International Journal of Computer Applications , august 2013.

[3] Sanjay P. Ahuja and Deepa Komathukattil, A Survey of the State of Cloud Security, Network and Communication Technologies; Vol. 1, No. 2; 2012, ISSN 1927-064X.

[4] Bashir Alam1, M.N. Doja1, Mansaf Alam, Shweta Mongia, 5-Layered Architecture of Cloud Database Management System, 2013 AASRI Conference on Parallel and Distributed Computing and Systems.

[5] Maricela-Georgiana Avram (Olaru), Advantages and challenges of adopting cloud computing from an enterprise perspective, The 7th International Conference Interdisciplinarity in Engineering (INTER-ENG 2013).

[6] Lee SY, Tang D, Chen T, Chu WC (2012) A QoS Assurance middleware model for enterprise cloud computing. In: IEEE 36th Annual Computer Software and Applications Conference Workshops (COMPSACW), 2012, pp 322–327

[7] Bahram S, Jiang X, Zi W, Grace M, Li J, Srinivasan D, Rhee J, Xu D (2010)"DKSM: subverting virtual machine introspection for fun and profit". 29thIEEE International Symposium on Reliable Distributed Systems, pp 82–91

[8] Yuki Ashino,Masayuki Nakae ,"Virtual Machine Migration Method between Different Hypervisor Implementations and its Evaluation, IEEE,2012 26th International Conference on Advanced Information

[9] Chen, J. Multilingual Information Access for Digital Libraries and the Machine Translation of Metadata Records. Public Library Journal, 2012; 36(3):51-58.

[10] Masudur Rahman and Wah Man Cheung," Analysis of Cloud Computing Vulnerabilities", International Journal of Innovation and Scientific Research ISSN 2351-8014 Vol. 2 No. 2 Jun. 2014, pp. 308-312

[11] A. Dharini, R.M. Saranya Devi, and I. Chandrasekar, "Data Security for Cloud Computing Using RSA with Magic Square Algorithm", International Journal of Innovation and Scientific Research Volume 11, Issue 2, November 2014, Pages 439–444.

[12] Ms. Punam U. Lambat, Prof. Mr. Parag Jawarkar, and Mr. G. Rajesh Babu, "SECURITY STORAGE SYSTEM FOR CLOUD USER USING OSD WITH A SELF-DESTRUCTING DATA", International Journal of Innovation and Scientific Research Volume 11, Issue 1, October 2014, Pages 19–26

[13] Divya Kapil ,Emmanual S. Pilli and Ramesh C. Joshi ," Live Virtual Machine Migration Techniques:Survey and research Challenges" .Third IEEE International Advance Computing Conference(IACC), 2013.

[14] Fernando Rodr´ıguez-Haroa, Felix Freitag, Leandro Navarro, Efra´ın

[15] Hernandez-S ´ anchez ´ , Nicandro Far´ıas-Mendozaa,, Juan Antonio Guerrero-Iba´nez ˜ , Apolinar Gonzalez-Potes, A summary of virtualization techniques, The 2012 Iberoamerican Conference on Electronics Engineering and Computer Science.

[16] K. Dutta, R. Guin, S. Banerjee, S. Chakrabarti, U. Biswas, A smart job schedulingsystem for cloud computing service providers and users: modeling and simulation, in: Proc. 2012 1st Int. Conf. Recent Advances in Information Technology, RAIT, 2012, pp. 346–351.