Different Attacks On Cloud Computing

Conference Paper · December 2014

CITATIONS
0

READS
339

3 authors:

Omar Achbarou
Cadi Ayyad University
12 PUBLICATIONS **23** CITATIONS
SEE PROFILE

My Ahmed El Kiram
Cadi Ayyad University
19 PUBLICATIONS **27** CITATIONS
SEE PROFILE

Salim Elbouanani
Cadi Ayyad University
9 PUBLICATIONS **22** CITATIONS
SEE PROFILE

A survey of Cloud Computing Attacks

Omar ACHBAROU[1], My Ahmed EL KIRAM[2], Salim ELBOUANANI[3]
Computer Science Dept, Laboratory ISI
Cadi Ayyad University
Marrakech, Morocco
[1]Omar.achbarou@gmail.com
[2]Kiram@uca.ma
[3]elbouanani.salim@gmail.com

Abstract — ***Cloud computing is a new computing model is to provide a set of computer resources, services and consumable data available on demand, and accessible from anywhere, anytime and by anyone through Internet.***

This system have some similarities of distributed system, according to this similarities cloud computing also uses the features of networking. Therefore the security is the biggest problem of this system, because the services of cloud computing is based on the sharing.

The aim of this work is to present a classification of attacks threatening the availability, confidentiality and integrity of cloud resources and services. Furthermore, we provide literature review of attacks related to the identified categories.

Keywords: cloud computing, cloud security, threats, security categories, attacks on cloud.

I. INTRODUCTION

Cloud computing is internet based where shared resources; software and information are provided to computers and other devices on-demand.

The National Institute of Standards and Technology (NIST) defined five essential characteristics of cloud computing [1]: on-demand self-service, broad network access, resource pooling, rapid elasticity or expansion, and measured service. It also defined three "service models" (software, platform and infrastructure), and four "deployment models" (private, community, public and hybrid) that together categorize ways to deliver cloud services.

Figure 1 shows cloud deployment models together with their internal infrastructure (Infrastructure as a Service IaaS, Platform as a Service PaaS and Software as a Service SaaS), and the essential characteristics of this environment.

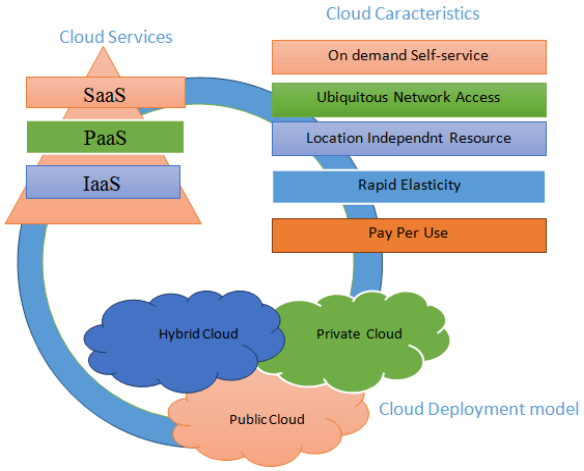

Figure 1. Cloud deployment models, Characteristics, and infrastructures

Despite the enormous technical and business benefits of cloud, concern for security and privacy has been one of the main obstacles that impede its widespread.

In this work, we classify security problems and attacks of cloud computing environments such as Flooding Attack, Denial of Service (DoS) attacks, Side Channel Attacks, phishing, malware Cloud Injection Attacks.

The reminder of this paper is structured as follows. In the next section two presents the main categories of cloud computing security. In Section 3, we present description of the well known attacks affecting cloud computing. And the last section summarizes the main contribution of this work and details our perspectives.

II. CATEGORIES OF CLOUD SECURITY

As part of this work, we started an investigation into the security issues and attacks on cloud computing. Cloud computing also suffers from various traditional attacks such as Flooding Attack, Side Channel Attack, port scanning, denial of service (DoS), Distributed Denial of Service (DDoS) etc. We classify these attacks and problems related to the security of cloud computing in the five categories, which are also summarized in Table 1 [2]:

TABLE I. CLOUD SECURITY CATEGORIES.

Category	Description
Security Standards	Describes the standards required to take precaution measures in cloud computing in order to prevent attacks.
Network	Included network attacks such as denial of service (DoS), DDoS, etc
Access Control	Included identification, authentication and authorization attacks.
Cloud Infrastructure	Includes attacks each layer of the cloud as SaaS, PaaS and IaaS, it is particularly associated with the virtualization environment.
Data	Covers data related security issues including data migration, integrity, confidentiality, and data warehousing.

III. ATTACKS RELATED TO THE CLOUD SECURITY CATEGORIES:

In what follows, we present a list of attacks cloud. We briefly explain each attack and accompanied by a brief discussion of the consequences of the attacks in the cloud environment. Table 2 presents a summary of attack names and attack category [2] [7] [9].

TABLE II. KNOWN ATTACKS ON CLOUDS.

Attack name	Category
Flooding attack	Cloud Infrastructure
Denial of service	Network, cloud Infrastructure
Port Scanning	Network
Attacks on Virtual Machine (VM) or hypervisor	Cloud Infrastructure
Cloud Malware Injection Attack	Cloud Infrastructure, Access
Cross VM side channels	cloud Infrastructure
Phishing	cloud Infrastructure, Network, Access

A. Flooding attack

Here, the attacker tries to flood the victim by sending large amounts of packets from exploited information resources, and they are called as zombie [3].

In the case of Cloud, virtual machine applications are available to all through the Internet, which can cause attacks by floods that affect the availability of service to the authorized user. Attacking a single server providing a particular service, the attacker can cause a loss of availability on the service provided. Such an attack is called direct DoS attack. If physical server resources are completely exhausted by the treatment of flood claims, other service instances on the same machine equipment are no longer able to fulfill their tasks under. This type of attack is called a distributed indirect DDOS attack.

B. Denial of Service Attacks

A DoS attack is an attempt to make the affected services to authorized users unable to be used by them. In such an attack, the server providing the service is flooded with a large number of applications and therefore the service becomes unavailable for the authorized user. Sometimes when you try to access a website, we see that due to overload the server with the website access requests, we are unable to access the website and observe a mistake. This occurs when the number of requests that can be processed by a server exceeds its capacity [4].

Thus, the attacker does not have to flood all n servers that provide a certain service in target, but merely can flood a single, Cloud-based address in order to perform a full loss of availability on the intended service [5].

C. Port Scanning

An attack that identifies open, closed and iltered ports on a system [3]. In port scanning, intruders can seize information with the help of open ports like services that run on a system, IP and MAC addresses which belong to a connection, and router, gateway and firewall rules. In the scenario of Cloud, the attacker can attack the services available through the scanning of ports (discovering open ports on which these services are provided) [10].

D. Malware Injection Attacks

In the cloud, a lot of data is transferred between the cloud provider and the consumer; it is necessary user authentication and authorization [5]. When data is transferred between the cloud provider and the user, the attacker can introduce malicious code between the two actors.

This attack requires the adversary to create its own malicious service implementation module (SaaS or PaaS) or virtual machine instance (IaaS), and add it to the Cloud system. Then, the adversary has to trick the Cloud system so that it treats the new service implementation instance as one of the valid instances for the particular service attacked by the adversary. If this succeeds, the Cloud system automatically redirects valid user requests to the malicious service implementation, and the adversary's code is executed [7].

E. Attacks on Virtual Machine (VM) or hypervisor

The attacker can take control of virtual machines installed by compromising the lower layer hypervisor. With these attacks, hackers may be able to compromise the hypervisor installed to take control of virtual machines. New vulnerabilities, such as zero-day vulnerability found in virtual machines (VM) that attract an attacker access to the hypervisor or other VMs installed. The zero-day vulnerability has been exploited in the application virtualization HyperVM which

resulted in the destruction of many websites based on the virtual server [3].

F. Side Channel Attacks

VM side channel attack is an access-driven attack in which an attacker VM alternates execution with the victim VM and leverages the processor cashes to infer the behavior of the victim. It requires that the attacker resides on a different VM on the same physical hardware as that of the victim's VM [2]. In this attack, the attacker Enjoy a sharing of physical components (par example, the cache Processor) to steal information (eg, a cryptographic key) of the victim. Specifically, the attacker tries to recover the value one cryptographic key by observing the activity of the processor cache.

G. Phishing Attacks

In cloud computing, phishing attacks can be classified into two categories of threats: first, as an abusive behavior in which an attacker hosts a phishing attack site on cloud by using one of the cloud services and second hijack accounts and services in the cloud through traditional social engineering techniques [8].

IV. CONCLUSIONS AND FUTURE WORK

Cloud Computing is at the keen interest and numerous works has been published in this field.

This research is primarily done to study the problems and attacks of cloud computing such as DoS Attack, Flooding Attack, and Phishing Attacks on Virtual Machine. Moreover, we classified these attacks into five security categories, namely: security standards, network, access, cloud infrastructure, and data. And we have detailed each one of these attacks.

The perspectives of this works will be focused on technical solutions to detect this kind of attacks including intrusion detection systems, autonomous systems, and systems for federated identity management. We will also emphasize the shortcomings of these systems based on high communication and computation overhead and the detection efficiency and coverage.

REFERENCES

[1] Final Version of NIST Cloud Computing Definition Published. Available online : http://www.nist.gov/itl/csd/cloud-102511.cfm (accessed on 03 April 2014).

[2] Issa M. Khalil, Abdallah Khreishah and Muhammad Azeem. Cloud Computing Security: A Survey", 2014.

[3] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan, "A survey of intrusion detection techniques in Cloud", January 2013.

[4] Rohit Bhadauria, Rituparna Chaki, Nabendu Chaki, Sugata Sanyal "A Survey on Security Issues in Cloud Computing", 2013.

[5] Mohamed H. Sqalli, Fahd Al-Haidari and Khaled Salah3, "EDoS-Shield- A Two- Steps Mitigation Technique against EDoS Attacks in Cloud Computing", 2011.

[6] R. Balasubramanian, Dr.M.Aramuthan, "Security Problems and Possible Security Approaches In Cloud Computing", 2011.

[7] Nils Gruschka and Meiko Jensen "Attack Surfaces: A Taxonomy for Attacks on Cloud Computing", 3rd International Conference on Cloud Computing, 2010.

[8] J. Archer, A. Boehme, D. Cullinane, P. Kurtz, N. Puhlmann, J. Reavis, 2010, Top threats to cloud computing, version 1.0. Cloud security alliance retrieved 7 May 2011, from http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf.

[9] Ajey Singh, Dr. Maneesh Shrivastava. "Overview of Attacks on Cloud Computing", IJEIT, April 2012

[10] Damien Riquet, Gilles Grimaud and Michaël Hauspie. "Study of the impact of the attacks and distributed multi-path on network security solutions", MajecSTIC, 2012.