Computers and Electrical Engineering 000 (2016) 1–15

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

Cloud security: Emerging threats and current solutions

Luigi Coppolino*, Salvatore D'Antonio, Giovanni Mazzeo, Luigi Romano

Dipt. Ingegneria, Univ. of Naples Parthenope (DI), Naples, Italy

ARTICLE INFO

Article history:
Received 12 August 2015
Revised 4 March 2016
Accepted 7 March 2016
Available online xxx

Keywords:
Cloud computing security
Security techniques
Intel SGX
Homomorphic cryptography
Cloud platforms

ABSTRACT

Many organizations are stuck in the cloudify or not to cloudify limbo, mainly due to concerns related to the security of enterprise sensitive data. Removing this barrier is a key pre-condition to fully unleash the tremendous potential of cloud computing. In this paper, we provide a comprehensive analysis of the main threats that hamper cloud computing adoption on a wide scale, and a right to the point review of the solutions that are currently being provided by the major vendors. The paper also presents the (near) future directions of cloud security research, by taking a snapshot of the main research trends and most accredited approaches. The study is done on a best of breed selection of proprietary and Open Source cloud offerings. The paper is thus a useful navigation tool, that can be used by the IT personnel to gain more insight into the security risks related to the use of cloud computing, as well as to quickly weigh the pros and cons of state of the art solutions.

1. Introduction

Cloud computing is gaining more and more momentum, due to a mix of market and technology related factors. Rapidly changing business conditions are driving a change in the computing infrastructure of many companies. The number of enterprise services and applications is constantly increasing, with new ones being continuously added and old ones being removed. Over three quarters of North American and European companies outsource parts of their business. This implies that relevant business-related information is not only spread across the different computing systems within one enterprise, but it is also distributed across multiple IT infrastructures of the company business network. On the technology axe, the availability of ever cheaper processors and lower latency networks, combined with the astonishing progress in virtualization, enable to move the computation from local IT platforms to distributed cloud infrastructures.

However, evidence is demonstrating that despite cloud computing being seen as a major business avenue for the next years, migration to the cloud paradigm is hampered by concerns on security. For example, financial institutes are attracted by cloud computing but for security reasons they are still in the early stages of adoption. Recent attacks to the cloud, as the one in 2014 when 50 million user accounts of Dropbox were hacked,[1] prove that cloud data security has become a hot topic. Evidence of the risks to which the cloud is exposed have been demonstrated by Al Awadhi et al. [16]. They used honey-pots to confirm that the cloud environment is insecure, and that it is the target of many attacks from different countries.

In order for cloud computing to be seen as a viable alternative, it must provide (at least) the same level of security as traditional IT systems. To achieve this goal, greater awareness is needed about measures and tools that are currently

* Corresponding author. Tel.: +390815476702.
E-mail addresses: luigi.copppolino@uniparthenope.it, luigi.coppolino@gmail.com (L. Coppolino), salvatore.dantonio@uniparthenope.it (S. D'Antonio), giovanni.mazzeo@uniparthenope.it (G. Mazzeo), luigi.romano@uniparthenope.it (L. Romano).

[1] https://blogs.dropbox.com/dropbox/2011/06/yesterdays-authentication-bug/

http://dx.doi.org/10.1016/j.compeleceng.2016.03.004
0045-7906/© 2016 Elsevier Ltd. All rights reserved.

available to counter malicious actions. In the literature, there are many works proposing surveys of defence mechanisms implemented in cloud infrastructures [1–7]. However, to the best of our knowledge, they all provide a partial view of the problem: some only describe the countermeasures taken by a specific provider and/or on a specific platform (i.e., [4]), others focus on security techniques that can be used in specific domains (i.e., [3]), yet others limit their analysis to Open Source cloud solutions (i.e., [5]). Our work here is a response to this gap in the literature, in that: i) it provides a study focusing on main challenges and issues at the various levels of a cloud stack, ii) it takes into account both general security approaches and specific solutions currently used in real cloud platforms, and iii) it covers both Open Source and proprietary cloud solutions. In this paper, we provide a comprehensive analysis of techniques and tools that are currently being used by cloud providers to secure their platforms. We perform such an analysis by cross-correlating methods that are applicable in different technical domains to multiple attack vectors, and in particular: network, hypervisor, and computing hardware. For each attack vector, we discuss the type of attacks that can be launched, and the type of countermeasures that are currently implemented/enforced by leading Cloud Providers (CP) and/or platform vendors. The platforms that are analyzed were chosen based on Gartner's magic quadrant[2] report. We selected: Amazon and Microsoft because they are leaders among IaaS providers, VMWare because it is one of the visionary providers, and OpenStack because it is one of the most widespread software stacks (since RackSpace, for example, offers private cloud solutions based on VMWare vCloud or OpenStack). Also importantly, our work provides pointers to emerging research trends and technologies for the (near) future.

The remainder of this paper is organized as follows. Section 2 discusses open issues and current threats in a cloud environment. Section 3 surveys the main attack vectors. Section 4 reviews related research.Sections 5–7 describe, for each attack vector, the mechanisms that are currently available to secure the cloud. Section 8 provides an overview of current trends for addressing open issues. Finally, Section 9 concludes the paper by summarizing the main results of the study and making some final remarks.

2. Security open issues and threats

Cloud computing suffers from a number of security issues which cannot be overlooked. ENISA in its recent report has identified thirteen technical risks. According to NIST, cloud computing presents certain unique security challenges resulting from the cloud's very high degree of outsourcing, dependence on networks, sharing (multi-tenancy), and scale [10]. Fernandes et al. [11] provide a thorough review of the research literature to clearly define cloud security open issues and challenges.

In light of [10,11], it can be claimed that nowadays main security challenges are:

- IS1: Shared technologies vulnerabilities: What makes the cloud so fascinating is also a point of criticality in terms of security. As Navati et al. [12] demonstrate that attackers could exploit vulnerabilities in the hypervisor and gain access to the physical host where other neighboring virtual machines (VM) reside.
- IS2: Data breach: Users' data can suffer both from accidental data loss and from malicious intrusive actions. Data loss is out of the scope of this work, since we only consider here data breaches, that is the action of stealing sensitive data (such as personal or credit card information).
- IS3: Account or service traffic hijacking: A user can lose control over its own account. Many attacks that will be described in Section 3 can lead to account or service hijacking. This enables the intruder to get into critical areas of a deployed service and possibly compromise the confidentiality, integrity, and availability of those services.
- IS4: Denial of Service (DoS): One of the most alarming scenarios is when the cloud infrastructure is made unavailable (just think that an outage costs Amazon 66 K dollars per minute). DoS in a cloud context is even more dangerous than in a traditional one, since when the workload increases with respect to a specific service, the cloud environment provides additional computational power to that service. This means that on the one hand the cloud system counters the effects of the attack, but on the other hand it supports the attacker in his evil activity, by providing him with more resources [13].
- IS5: Malicious insiders: This is climbing the list of cloud top threats. The possibility that a malicious insider – e.g. an employee – might try to take advantage of his privileged position to access sensitive information is becoming more and more concrete and worrisome [14].

3. Attack vectors

The aforementioned open issues can be caused by three main vectors of attack (Fig. 1): Network, Hypervisor, and Computing Hardware. Three types of attackers map on these vectors: external users, internal users, and the cloud provider itself (embodied in a malicious employee).

- External users can launch many attacks against the cloud infrastructure through the network. They can affect data confidentiality and integrity by tampering with the communication channels or by landing on the system to subsequently launch an attack. In addition, they can affect the availability of the CP's data centers.

[2] Magic Quadrant for Cloud Infrastructure as a Service Worldwide: http://www.gartner.com/technology/reprints.do?id=1-2G2O5FC&ct=150519&st=sb