Future Generation Computer Systems 63 (2016) 37–55

Contents lists available at ScienceDirect

Future Generation Computer Systems

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

Usage Control on Cloud systems

Enrico Carniani, Davide D'Arenzo, Aliaksandr Lazouski, Fabio Martinelli, Paolo Mori *

Istituto di Informatica e Telematica, Consiglio Nazionale delle Ricerche via Moruzzi, 1 - 56124 Pisa, Italy

HIGHLIGHTS

- Design of a framework regulating Cloud resource usage based on Usage Control model.
- Continuous enforcement of policies and revocation of running accesses.
- Integration of the proposed framework within OpenNebula.
- A working implementation of the proposed framework has been developed.
- A set of experiments has been performed to evaluate the performance of our framework.

ARTICLE INFO

Article history:
Received 30 July 2015
Received in revised form
4 March 2016
Accepted 18 April 2016
Available online 28 April 2016

Keywords:
Usage Control
Cloud Security
Authorization
OpenNebula
XACML

ABSTRACT

Cloud Computing is becoming increasingly popular because of its peculiarities, such as the availability on demand of (a large amount of) resources, even for a long time. For this reason, Cloud Computing represents a good solution for those companies that want to outsource part of their software processes. However, Cloud Computing introduces new security and management challenges with respect to traditional systems exposed on the Internet. This paper presents an advanced authorization service based on the Usage Control model to regulate the usage of Cloud resources, focussing on IaaS services.

Our framework addresses the issue of long lasting usage of resources, because it allows to define Usage Control policies which are continuously enforced while the access is in progress. In particular, our framework is able to interrupt the usage of such resources when the corresponding policy is not satisfied any more. In this paper, we present the architecture of the proposed framework describing the integration of a Usage Control based authorization service within one of the most popular software for running Cloud services: OpenNebula. Moreover, we describe the implementation of a prototype of the whole framework, along with some performance figures.

1. Introduction

The increasing popularity of Cloud systems is due to the on demand availability of big computational power for the execution of heavy parts of business and research processes [1–3]. As a matter of fact, Cloud providers allow their users to exploit a proper set of resources for their computation only when they actually need them. Cloud users, in turn, pay a fee depending on the resources they requested. Distinct Cloud service models have been defined by NIST [4], depending on the kind of resources that are provided. This paper is focused on the Infrastructure as a Service (IaaS) model, where the resources provided to users are computational infrastructures consisting of Virtual Machines (VMs) connected by virtual networks. When requesting VMs, users can choose the most proper network configuration, VM features (e.g., virtual CPU type and number, RAM memory and storage space), VM images (i.e., the operating system they need for their application). Moreover, users can install and run on the VMs allocated to them the applications they need. Once requested, the virtual computational infrastructure is available in a short time and the number of machines and/or their features can be updated by users (increased or decreased) on demand during the computation according to their needs. The other two Cloud service models defined by NIST are: Platform as a Service (PaaS), which provides an API for developing new services and a platform where these services can be deployed and executed, and Software as a Service (SaaS), where the provided resources are applications running on an existing Cloud infrastructure. The rest of the paper is focused on the IaaS model, although the approach proposed could be applicable to other Cloud service models. Usually,

* Corresponding author.
E-mail addresses: enrico.carniani@iit.cnr.it (E. Carniani), davide.darenzo@iit.cnr.it (D. D'Arenzo), aliaksandr.lazouski@iit.cnr.it (A. Lazouski), fabio.martinelli@iit.cnr.it (F. Martinelli), paolo.mori@iit.cnr.it (P. Mori).

http://dx.doi.org/10.1016/j.future.2016.04.010
0167-739X/

the instances of Cloud resources exploited by users are long-standing, and they are exposed to users through a proper interface. The VMs provided by an IaaS Cloud services are our reference example of long standing virtualized resources. In general, the Cloud user exploits them through a remote access using their IP addresses. IaaS Cloud facilities are currently provided by many big companies (Public Clouds), such as Amazon,[1] Google,[2] IBM,[3] and Microsoft.[4] Alternatively, a number of Cloud frameworks, such as OpenNebula,[5] Eucalyptus[6] or OpenStack,[7] are currently available to deploy Cloud systems in users' data centres, to use their physical machines to host virtual ones (Private Clouds).

Besides the benefits previously described, the adoption of Cloud Computing to perform critical part of the business and research processes introduces also some problems, security being one of them. These security issues are described by the "European Network and Information Security Agency" (ENISA) in the report: "Cloud Computing. Benefits, Risks and Recommendations for Information Security" [5]. The "Cloud Security Alliance" (CSA) published two reports [6,7] as well: "The Notorius Nine. Cloud Computing Top Threats in 2013" and "Security Guidance for Critical Areas of Focus in Cloud Computing" which, again, are focused on identifying the security problems peculiar of Cloud Computing. Some other research papers describe the main security issues in Cloud Computing such as [8,9]. These documents point out that, besides the well-known threats of systems exposed on the Internet, the Cloud introduces further security challenges due to its specific peculiarities. These peculiarities include virtualization, multi-tenancy environment and long lasting accesses.

In this paper we propose an enhanced authorization service for Cloud IaaS services, which is able to continuously enforce security policies in order to interrupt accesses that are in progress when the corresponding access rights do not hold any more. This paper is an extension of our previous work, presented in [10], and our approach is based on the Usage Control (UCON) model, defined by Sandhu and Park in [11,12]. In recent years, UCON has drawn a significant interest from the research community on formalization and enforcement of policies. There were several attempts to implement Usage Control, while the realization based on existing security standards is still an open issue. The design of an efficient and flexible framework (i.e., a policy schema, an architecture and an implementation) for Usage Control based on the OASIS XACML [13] standard is a challenge we address in our work.

1.1. Motivation and contribution

The Usage Control model can be successfully adopted in the Cloud environment to regulate the usage of Cloud IaaS services because the accesses to those services could last for a long time, such as hours, days, or even more. Hence, some of the factors that have been evaluated by the security support to grant the initial access to the service could change while the access is in progress. As a consequence, it is possible that the right to access the service does not hold any more. For example, a computer science researcher *R* could request to a IaaS service provider the creation of a VM to host the Subversion server of his new three-years project. This VM will be used by all the project participants to manage the development of the project code, and it will be dismissed at the end of the project. Once created and deployed, the VM will be accessed by *R* using directly the public IP address (i.e., without any intervention of the Cloud service provider). *R* will configure the VM to allow the project participants to access the subversion service using directly the public IP address as well. Hence, after the creation request, no further request is sent to the Cloud service provider to use the VM. Let us suppose that the IaaS service provider allows users to run VMs only if their reputation is excellent. Adopting the traditional access control models, the value of the reputation of the user is controlled at request time only. Once the access has been granted and the VM has been started, this machine keeps on running until the user terminates it, even when the value of the user's reputation is not excellent any more. As a matter of fact, the VM creation and deployment requests are the only interactions among the Cloud service provider and the user, and no further controls on the reputation of the user are initiated by the security support during the VM life time. To address this issue, the Usage Control model enables the policy to state that some predicates that evaluate some mutable decision factors must be satisfied for the whole access time. This means that the access must be interrupted (or suspended) when these factors change in a way such that the policy is not satisfied any more. In the previous example, a predicate of the Usage Control policy could state that the user reputation must be excellent for all the VM life time. As soon as the reputation of the user decreases, his VM is suspended. Hence, the Usage Control approach prevents Cloud users from continuing the use of resources that have been previously assigned to them as soon as the rights of using these have resources expired. This enhances the Cloud service security, avoiding that accesses are carried on when they become potentially dangerous. With reference to the previous example, if the reputation of the user *R* has decreased, it means that *R* has tried to perform a number of unauthorized operations, and most probably he will try to perform further malicious operations.

The main contributions of this paper are the following:

- The design of a complete framework for regulating the usage of Cloud IaaS services based on the Usage Control model. The paper provides a detailed description of the architecture of the proposed Usage Control service, focusing on the aspects concerning the implementation of the Usage Control model peculiarities, such as the continuous policy enforcement and the revocation of ongoing accesses;
- The integration of the Usage Control service within one of the most used tools for the provision of Cloud services, i.e., OpenNebula;
- A working implementation of the proposed framework;
- A set of experiments to evaluate the performance of our prototype.

Some attempt to adopt the UCON model in the Cloud have been proposed in the past (see Section 6). However, this paper represents a step forward because, to the best of our knowledge, none of the previous works presented the design and implementation of the overall authorization system architecture, and the integration within an existing Cloud framework.

1.2. Paper structure

The paper is structured as follows. Section 2 gives a brief overview of the security support provided by two widespread Cloud frameworks, OpenNebula and OpenStack, and of the Usage Control model. Section 3 proposes our approach to regulate the usage of Cloud resources, presenting the detailed architecture of the proposed framework, describing the integration with OpenNebula, and also giving some examples of Usage Control

[1] http://aws.amazon.com/.
[2] https://cloud.google.com/.
[3] http://www.ibm.com/cloud-computing/us/en/.
[4] https://azure.microsoft.com/en-us/.
[5] http://opennebula.org/.
[6] http://eucalyptus.com/.
[7] http://openstack.org/.