ARTICLE IN PRESS

Future Generation Computer Systems ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Contents lists available at SciVerse ScienceDirect

Future Generation Computer Systems

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

Semantic-aware multi-tenancy authorization system for cloud architectures

Jorge Bernal Bernabe [a,b], Juan M. Marin Perez [a,b], Jose M. Alcaraz Calero [b,*], Felix J. Garcia Clemente [c], Gregorio Martinez Perez [a], Antonio F. Gomez Skarmeta [a]

[a] Departamento de Ingenieria de la Informacion y las Comunicaciones, University of Murcia, Murcia 30100, Spain

[b] Cloud and Security Lab, Hewlett-Packard Laboratories, Bristol, BS34 8QZ, UK

[c] Departamento de Ingenieria y Tecnologia de Computadores, University of Murcia, Murcia 30100, Spain

ARTICLE INFO

Article history:
Received 13 November 2011
Received in revised form
6 April 2012
Accepted 17 May 2012
Available online xxxx

Keywords:
Authorization system
Cloud computing
Multi-tenancy
Trust model
Semantic web

ABSTRACT

Cloud computing is an emerging paradigm to offer on-demand IT services to customers. The access control to resources located in the cloud is one of the critical aspects to enable business to shift into the cloud. Some recent works provide access control models suitable for the cloud; however there are important shortages that need to be addressed in this field. This work presents a step forward in the state-of-the-art of access control for cloud computing. We describe a high expressive authorization model that enables the management of advanced features such as role-based access control (RBAC), hierarchical RBAC (hRBAC), conditional RBAC (cRBAC) and hierarchical objects (HO). The access control model takes advantage of the logic formalism provided by the Semantic Web technologies to describe both the underlying infrastructure and the authorization model, as well as the rules employed to protect the access to resources in the cloud. The access control model has been specially designed taking into account the multi-tenancy nature of this kind of environment. Moreover, a trust model that allows a fine-grained definition of what information is available for each particular tenant has been described. This enables the establishment of business alliances among cloud tenants resulting in federation and coalition agreements. The proposed model has been validated by means of a proof of concept implementation of the access control system for OpenStack with promising performance results.

1. Introduction

Businesses are adapting their IT systems towards the cloud computing paradigm where flexible and dynamic services and infrastructures are able to scale and be delivered on demand. This new paradigm enables an efficient provisioning of virtual IT architectures to third-parties, where resources are dynamically created and dismantled according to customer needs.

Cloud computing describes a logical stack divided into three different layers: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). In summary, the IaaS layer is in charge of providing the virtual infrastructure (virtual machines, volumes, networks, routing capabilities, etc.). The PaaS layer is in charge of providing middleware services which may be seen as added-value services. In turn, the SaaS layer exposes software features to be used by end-users, making use of the underlying added-value services provided by PaaS.

However, many potential businesses which would be interested in cloud computing are still a bit reluctant to adopt it due to security and privacy concerns. In particular, cloud computing entails the usage of a common IT infrastructure and services which are shared between different tenants. This implies the design of strong security boundaries in order to isolate tenants when using these shared resources. Thus, the system to control the access to the available resources becomes a critical aspect in order to provide an efficient control over the usage of the cloud architecture.

Current cloud providers such as Rackspace[1] or Amazon EC2[2] only rely on simple authentication schemes which do not provide enhanced access control capabilities beyond full access as administrator to the whole system. These authorization solutions for cloud computing (lately described in Section 2) usually lack of enough expressiveness to describe advanced authorization and federation rules. The availability of advanced authorization capabilities can be a differentiating feature for cloud providers, which demand the design of suitable authorization models to enhance the access control to the cloud resources.

* Correspondence to: Stoke Gifford, Bristol BS34 8QZ, UK. Tel.: +34 616412041.
E-mail addresses: jorgebernal@um.es (J. Bernal-Bernabe), juanmanuel@um.es (J.M. Marin-Perez), jose.alcaraz-calero@hp.com, jose-maria.alcaraz-calero@hp.com (J.M. Alcaraz-Calero), fgarcia@um.es (F.J. Garcia-Clemente), gregorio@um.es (G. Martinez-Perez), skarmeta@um.es (A.F. Gomez-Skarmeta).

[1] Rackspace available at http://www.rackspace.com/index.php.

[2] Amazon EC2 available at http://aws.amazon.com/es/ec2/.

0167-739X/$ – see front matter © 2012 Elsevier B.V. All rights reserved.
doi:10.1016/j.future.2012.05.011

Please cite this article in press as: J. Bernal-Bernabe, et al., Semantic-aware multi-tenancy authorization system for cloud architectures, Future Generation Computer Systems (2012), doi:10.1016/j.future.2012.05.011

This paper presents an access control system suitable for cloud computing which manages grants providing high expressiveness. This enables the adoption of an advanced authorization model in which the following authorization features are supported: role-based access control (RBAC), hierarchical RBAC (hRBAC), conditional RBAC (cRBAC) and hierarchical objects (HO). The system provides multi-tenancy support and federation capabilities allowing a fine-grained definition of what resources are available for each particular tenant. The federation capabilities are defined by means of a trust model. The trust model determines the business alliances (coalitions and federation) among cloud tenants. Although the proposed access control system is potentially suitable for all layers of the cloud computing stack, its adaptation needs to consider some specifics of each layer, such as: (i) relationships with other layers, (ii) multi-vendor support, (iii) information model, etc. Thus, we have decided to validate this research work over the IaaS layer. This layer constitutes the first logical step of the cloud stack and there is also a clear lack of advanced access control systems for this layer.

The remainder of this paper is organized as follows. Section 2 overviews related work about access control systems for cloud computing, indicating what are the differentiating points of our proposal. After that, Section 3 describes the languages and models that are used to define the underlying system infrastructure. Then, Section 4 describes the capabilities provided by our proposed authorization model. Afterwards, Section 5 delves into the authorization architecture. The proposed trust model is presented in Section 6. The workflow carried out during the authorization process is presented in Section 7. Moreover, a proof of concept implementation and some performance results are shown in Section 8. Finally, Section 9 provides some concluding remarks.

2. Related work

There is an important number of contributions in the field of access control for distributed systems. Rather than providing a complete historical review, this section is focused only on those which provide multi-tenancy support, which is a required feature in order to fit cloud computing. In essence, multi-tenancy is the ability to efficiently deal with multiple administrative domains (tenants) that are using the same service which, in turn, has isolated resources belonging to particular tenants. Many distributed systems like Grid and cloud computing demand multi-tenancy support. Cloud computing is usually related to a single provider and homogeneous information models whereas Grid computing is designed on the assumption of multiple providers with heterogeneous information models [1]. Thus, although there are several access control systems provided for grid computing, they do not directly fit in cloud computing.

We proposed a semantic-aware access control system for grid computing that enables basic coalitions and federation capabilities [2]. This work assumes heterogeneous tenants and enables basic federation capabilities between them. This is achieved by means of the virtual organization concept, which is articulated by the alignment of information available for tenants as a homogenization tool. In case the reader is interested, Perez et al. [2] provide a comprehensible overview on grid-related authorization systems. However, they do not fit cloud computing for the same reason, i.e. they are based on design principles different from cloud computing characteristics.

Perez et al. [2] is, in turn, the application to Grid computing of a previous contribution in which we designed an authorization framework for distributed environments providing a multi-tenancy authorization model with support for RBAC, hRBAC, cRBAC and HO [3]. This access control model is the basis of the work available in both Perez et al. [2] and this contribution. Although there are some similarities, there is significant work done in order to achieve an access control model which really fits cloud computing. In SECRYPT 2011 [4], we presented a short paper in which we focus on describing an overview of an access control system based on the design assumptions of cloud computing. It is mainly focused on providing the description of a new information model to cope with cloud-related concepts like *Virtual Machine* or *Hosted Operating System*. Now, we are significantly extending that contribution, mainly by providing the following features: Firstly, a real implementation of the access control system which has been integrated in the well-known Open Stack cloud platform. Secondly, a completely new trust management model in order to provide fine-grained cloud federation capabilities. Finally, a complete performance evaluation of the proposed prototype is also provided.

Regarding access control models for cloud computing, Li et al. [5] provide a basic multi-tenancy access control model with discretional access control (DAC) support. Li et al. [6] extends this model providing support for role management (RBAC) for cloud computing. Shirisha and Kumari [7] provide the next step supporting role hierarchies (hRBAC) in an access model designed to control the invocation of methods available in cloud computing APIs. Tsai and Shao [8] provide a semantic-aware multi-tenancy access control model with hRBAC and cRBAC support. The authors use an ontology for building up the role hierarchy for a specific domain. Ontology transformation operation algorithms are provided to compare the similarity of different ontologies.

Pereira [9] and Xu et al. [10] provide access control systems for the cloud with analogous functionality. The main difference is that Pereira is focused on the IaaS layer whereas Xu et al. are focused on the SaaS layer. They provide not only a multi-tenancy access control model with hRBAC and cRBAC support, but also a dynamic activation of roles in order to control a proper separation of duties in the cloud. Danwei et al. [11] delves into an access control system based on the *Usage CONtrol* access model (UCON) [12] which includes negotiation techniques in order to provide federation capabilities in cloud computing. The UCON model encompasses hRBAC, cRBAC, and attribute-based access control (ABAC) support. Fall et al. [13] provide a similar access control system for cloud computing with the differentiating feature that federations between tenants are dynamically established, according to a risk management model in charge of deciding if two tenants can collaborate according to their previous interactions. Alcaraz-Calero et al. [14] have provided an advanced multi-tenancy authorization model with RBAC, hRBAC and HO support for cloud computing based on authorization statements defined by means of paths. This approach provides efficiency and performance making the system scalable. However, a path-based representation could suffer from expressiveness limitations when authorization information needs to be expressed over information models that cannot be expressed using paths.

All the previously described models represent good attempts to provide access control models adapted to cloud computing. However, there is still an important effort in the way of providing efficient and highly expressive models. These models have been compared with respect to our contribution presented in this paper in order to provide a clear overview about what is our main contribution to the field.

The aspects to be compared are described in Table 1 and the comparison is shown in Table 2. Note that the columns of Table 2 match with the IDs specified in Table 1. Note that Perez et al. [2] provide a fine-grained federation model. However it is labelled as partial because it does not fit cloud computing requirements at all.

As can be seen in Table 2, the proposed access control model combines the previous proposals in order to go a step forward by describing a multi-tenancy authorization model suitable for

Please cite this article in press as: J. Bernal-Bernabe, et al., Semantic-aware multi-tenancy authorization system for cloud architectures, Future Generation Computer Systems (2012), doi:10.1016/j.future.2012.05.011