Chapter 8
Access Control in Federated Clouds:
The Cloudgrid Case Study

Valentina Casola
University of Naples "Federico II", Italy

Umberto Villano
University of Sannio, Italy

Antonio Cuomo
University of Sannio, Italy

Massimiliano Rak
Second University of Naples, Italy

ABSTRACT

Resource sharing problem is one of the most important aspects of Cloud architectures whose primary goal is to fully enable the concept of accessing computing resources on-demand. Access control and resource federation are hot research topics and a lot of open issues should be addressed on functionalities, technological interoperability, quality of services and security of the federated infrastructures. This chapter aims at offering a view on the problems of access control on federated Clouds; since they strongly depend on chosen architectures and platforms, the chapter will discuss some solutions applied on a real case study: the PerfCloud framework, which is based on the integration of Grid and Cloud platforms. The proposed architecture is based on the adoption of an interoperability system to cope with identity federation and access control, it is strictly related to the adopted framework nevertheless it helps the reader to have an idea of the involved open issues and available solutions in commercial or experimental clouds.

INTRODUCTION

Cloud Computing is undoubtedly an innovation that is going to change every business area. As a matter of fact, the possibility to access computing resources on-demand creates many opportunities and economic efficiencies. On the minus side, Cloud services may be vulnerable to malicious attacks; attackers can potentially locate where data are physically stored within the Cloud, and use clever strategies to obtain access to them.

The Cloud Security Alliance points out a set of 15 different security domains related to the Cloud paradigm that are primary related to the "security management and governance" (to be able to manage the risk associated with a particular

DOI: 10.4018/978-1-4666-2919-6.ch008

provider) and to the security "operational aspects" (as access control privacy, confidentiality and data integrity, business continuity, disaster recovery,...). Each of these domains involves a great number of open issues, which strongly depend on the Cloud architecture and the delivery and deployment model (IaaS, …) adopted. According to these considerations and despite of many Cloud providers policies, to cope with security issues, we need to characterize any Cloud architecture as a complex layered system; in fact, any architectural choices and service provision activities imply the adoption of proper security policies and mechanisms to guarantee data integrity, privacy and user confidentiality.

In this chapter we will illustrate and discuss two primary security problems, actively investigated by the scientific community today: (i) *identity federation* to enable authentication and security cooperation among the untrusted domains that build up the Cloud environment and (ii) *access control* to properly protect physical and virtual resources.

As for identity federation, it is crucial for Cloud providers to support the overall lifecycle management of users in a completely automated way; this includes user identity management, provisioning/ de-provisioning and, in general, access control policies. It is not uncommon for a Cloud provider to delegate authentication to external trusted identity providers using federation standard such as SAML. This model offers the flexibility to enforce the appropriate authentication strength according to the customer's information protection and data classification policies and standards. Unfortunately, many providers are not ready to be compliant with these new standards and *ad hoc* solutions are enforced, not enabling security monitoring and auditing capabilities.

As for access control, Cloud customers should be aware that fine-grain authorization models are also immature. Where they do exist, they are usually implemented in a proprietary fashion, specific to the Cloud provider. Nevertheless, in many distributed environments role-based access control models and their standard implementation (as XACML) are now commonly adopted and they can be used even in the Cloud environment.

The above described security problems can be found in a very large number of situations and when solutions are implemented, they strongly depend on the technological choices done on specific requirements. In this chapter we will classify cloud architectures from a security point of view, showing that for some of them, it is possible to generalize security solutions to access control and federation.

The first assumption we will do is that cloud users can access services that are offered "on the top" of many different independent providers, each provider having its own security domain (i.e. each of them has its own set of users, being able to authenticate, profile and authorize them to access specific resource).

To enable access to all providers, a federation approach is needed; providers face this problem by federating the security domains. The federation implies the possibility to authenticate users even if they where identified in different domains, to associate them a specific role and finally to grant fine-grain access to their resources. This activity can be performed with the adoption of Trusted Third parties whose primary goal is to extent the validity of user credentials and their permissions, it is accomplished with the adoption of common standard for interoperability purposes but also with explicit agreements among the involved parties. Such agreements should be accomplished in a completely transparent way respect to cloud users. As a practical example, we will consider a digital certificate based authentication mechanism where different users are authenticated by different Certification Authorities and the interoperability among their security domains is accomplished with automatic cross certification processes.

In the reminder of the chapter, we will illustrate how the adoption of an Interoperability System can be useful to federate untrusted domains in