Chapter 10
Security Issues in Cloud Federations

Massimiliano Rak  
*Second University of Naples, Italy*

Massimo Ficco  
*Second University of Naples, Italy*

Jesus Luna  
*TU Darmstadt, Germany*

Hamza Ghani  
*TU Darmstadt, Germany*

Neeraj Suri  
*TU Darmstadt, Germany*

Silviu Panica  
*Institute e-Austria Timisoara, Romania*

Dana Petcu  
*Institute e-Austria Timisoara, Romania*

**ABSTRACT**

The cloud paradigm, based on the idea of delegating to the network any kind of computational resources, is showing a considerable success. The estimated trend is that the number of different cloud-based solutions, approaches, and service providers (CSP) will continue growing. Despite the big number of different cloud solutions that currently exist, most of them are “walled gardens” unable to interoperate. On the other side, a large effort is taking place in the cloud community to develop and identify open solutions and standards. In such a context the concept of cloud federation, an architecture that combines the functionalities of different CSP, is a hot topic. This chapter presents an overview of the cloud federation topic, with special focus on its most important security challenges. Furthermore, it proposes a taxonomy of possible approaches to federation. Then it proposes a comparison of security problems in cloud and grid environment, and a detailed analysis of two relevant security problems, identity management and Cyber Attacks analysis, trying to outline how they can be applied in a federated context.

DOI: 10.4018/978-1-4666-1631-8.ch010
INTRODUCTION

The cloud just as defined in (Mell, 2009), has increasingly become a computing/communication paradigm that seems to have the potential to change the way we consider systems and services. At the state of the art Microsoft (with Azure), Google (Google App Engine), IBM (IBM Cloud Reference Architecture), Oracle (Oracle on Demand) are just some of the “big players” offering their services for both Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) solutions, which have adopted completely proprietary approaches. Because of the latter, a typical cloud user (e.g., a developer) might find herself completely “locked” into a specific CSP, once she has chosen it from the available technological stack. On the other hand and in order to promote interoperability, a large effort is being spent in the cloud computing community to identify open solutions and standards through open consortiums (e.g. the Open Cloud Manifesto (OpenCloud Manifesto, 2009) and the Cloud Security Alliance (Cloud Security Alliance, 2009), open source-based solutions (e.g., OpenNebula (J.Fontan, 2008)) and, standards like OCCI (Open Cloud Computing Interface (Edmonds, 2010)), and the Cloud Data Management Interface (CDMI (SNIA, 2010)).

Considerable pressure is being put by the CSP to ensure the means for using cloud services (compatible or not) from different providers. This kind of approach is desired from two different perspectives:

1. That of the application developers, who are interested to combine different cloud services from different providers or even to ensure the availability of their cloud services by replicating them to different providers;
2. That of the cloud service providers (CSP), who are interested to extend their infrastructure capabilities or to build on top of others CSP’s offers.

When a cloud compliant application is distributed across two or more CSP and administrative domains simultaneously, there are two possible approaches:

- **Federated clouds**: when the providers agree how to mutually enforce policy and governance, establishing a common trust boundary.
- **Hybrid cloud**: when the application crosses a private-public trust boundary or spans multiple clouds (simultaneous use of multiple CSP where both, administrative domains and trust boundaries are crossed).

The main subject of this chapter is related to federation of clouds, where two use cases are already well recognized: scale-out, and mutual backup/recovery- from a disaster. In the case of scale-out scenario, if an event occurs unexpectedly or in a peak, a stable operation is possible by distributing dynamically the workloads between the resources of the local –private- cloud and the public cloud. In the case of a mutual backup and recovery from a disaster, if an event damages one provider’s cloud or causes a power outage, then cloud resources in other providers are used to restore the damaged services.

A federation of clouds can be organized in different ways:

- **Horizontal federation**: when two or more cloud providers join together to build a facility for capacity on-demand. Participants having an excess capacity share their resources (for a price agreed beforehand), with those other participants needing additional resources to deal with their workload’s spikes.
- **Intercloud**: when a federation of clouds is built with a common set of features like, e.g., addressing, naming, identity, trust, presence, messaging, multicast, time domain, and application messaging (the re-