# Chapter 64
# Cloud Standards:
## Security and Interoperability Issues

**Fabio Bracci**
*University of Bologna, Italy*

**Antonio Corradi**
*University of Bologna, Italy*

**Luca Foschini**
*University of Bologna, Italy*

## ABSTRACT

*Starting from the core assumption that only a deep and broad knowledge of existing efforts can pave the way to the publication of widely-accepted future Cloud standards, this chapter aims at putting together current trends and open issues in Cloud standardization to derive an original and holistic view of the existing proposals and specifications. In particular, among the several Cloud technical areas, the analysis focuses on two main aspects, namely, security and interoperability, because they are the ones mostly covered by ongoing standardization efforts and currently represent two of the main limiting factors for the diffusion and large adoption of Cloud. After an in-depth presentation of security and interoperability requirements and standardization issues, the authors overview general frameworks and initiatives in these two areas, and then they introduce and survey the main related standards; finally, the authors compare the surveyed standards and give future standardization directions for Cloud.*

## 1. INTRODUCTION

Cloud computing has recently emerged as a new paradigm that offers a new concept and a completely innovative experience of use of various services through the network to final users. Cloud proposals build upon well-established technologies, such as Service Oriented Architectures (SOA), distributed and grid computing, and virtualization, but it also presents several new original aspects that contributed to establish it as a disruptive technology. In fact, after the first big explosion between the years 2008 and 2009, Cloud computing is spreading more and more with the result of establishing many new Cloud providers at the different layers of the Cloud provisioning stack, Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service

DOI: 10.4018/978-1-4666-6539-2.ch064

(SaaS), with different diffusion and differentiated penetration at the different levels. One of the main reasons behind the rapid expansion of Cloud technologies was the surge of IT companies to make substantial spending cuts in their activities; in fact, Cloud computing can significantly reduce both hardware and software infrastructure costs, by resulting also in a reduction of infrastructure private management, maintaining, and upgrading costs and thus, it may contribute to free precious personnel resources to employ in other, more productive, tasks.

Notwithstanding all potential advantages, Cloud adoption raises also big issues still unsolved, mainly due to the fact that Cloud providers, either IaaS (Amazon Web Services – AWS, Rackspace, IBM Cloud, Microsoft Azure, etc.), PaaS (Microsoft Azure), Google App Engine – GAE, AWS Elastic Beanstalk, CloudBees, CloudFoundry, OpenShift, etc., or SaaS (Google Apps), SalesForce, etc. use proprietary Cloud solutions and middleware platforms, thus resulting in isolated environments. This isolation risks to obstacle further advancements of Cloud computing because, although Cloud computing is very promising, the lack of proper Cloud standardization and certification processes, especially for security- and interoperability-related aspects, hinders the outsourcing of enterprise IT assets to third-party Cloud computing platforms. In fact, organizations are afraid of the loss of control over their Cloud-hosted assets, and also due to the fact that they find it difficult to migrate from one solution to another one because interoperability between different Clouds is still hard to face and solve.

Those problems call for new Cloud standardization efforts to overcome and deal more efficiently with those issues. In fact, the need for more Cloud standards is motivated not only by the fact that customers would like to buy from any vendor, even many at the same time, without changing the way they write, deploy, and run their applications for a specific vendor (and for non-commercial users, a better integration can lead to more effective collaboration too), but also because the guarantee of solid certifications, such as Organization for Standardization (ISO) 27000 and NIST Federal Information Security Management Act (FISMA) security certificates, would greatly help Cloud providers to improve costumer trust and willingness in using their Cloud platforms. At the same time, even if the lack of accepted and widely adopted Cloud computing standards is a potential roadblock to the adoption of Cloud, some seminal standardization efforts are currently becoming available in the Cloud arena today. For instance, since to overcome the vendor lock-in and interoperability problem in IaaS requires the freedom of moving virtual machines and data from Cloud to Cloud, the Distributed Management Task Force (DMTF) developed the Open Virtualization Format (OVF) to facilitate the mobility of virtual machines.

Hence, a large number of standardization organizations, proposals, and practical Cloud benchmark solutions and systems have recently emerged, each with its specific goals, advantages, and limitations. However, to the best of our knowledge, apart from a few very seminal efforts, an in-depth analysis of current Cloud standardization activities at different Cloud software stack levels (IaaS, PaaS, and SaaS), and especially focused on different management issues and functions, still misses. This chapter aims to fill that gap by putting together current Cloud standardization efforts so to present an original survey, classification, and analysis of existing proposals and specifications, and to derive from that comparison a clear picture of the current standardization status and of important ongoing and future standardization trends in this live research area.

The first part of the chapter will be more tutorial-oriented. First, in Section 2 we will introduce organizations that specify general development guidelines in Cloud computing by discussing the main key benefits and the main weaknesses, to be respectively included and overcome, that Cloud standards with a large agreement could produce. This first general analysis of main stan-