Chapter 7
Cloud Access Control Mechanisms

Ciro Formisano
Engineering Ingegneria Informatica SPA, Italy

Lucia Bonelli
Engineering Ingegneria Informatica SPA, Italy

Kanchanna Ramasamy Balraj
Engineering Ingegneria Informatica SPA, Italy

Alexandra Shulman-Peleg
IBM Haifa Research Lab, Israel

ABSTRACT

Cloud storage systems provide highly scalable and continuously available storage services to millions of geographically distributed clients. In order for users to trust their data to these systems, they need to be confident that their data is secure. Thus, cloud services should implement an access control mechanism preventing unauthorized access and manipulation of their data. This chapter presents the existing access control mechanisms and describes their advantages and limitations in the Cloud set-up. The authors address the main access control aspects that include managing the identities and defining access policies. Furthermore, they describe more complex scenarios of identity federation and integration of separate identity silos which is required in various scenarios, like collaboration, merge on acquisition, or migration. For each topic, the authors present the existing solutions and describe the motivation for the architecture developed by the VISION Cloud project.

INTRODUCTION

The cloud architecture, and storage cloud in particular, opens up new security related issues and intensifies other known vulnerabilities and threats. For example, most cloud storage services are offered by external providers on infrastructures also used for storing other customer's data. Thus, many customers are rightfully worried about moving their data to a storage cloud and data security risks are a key barrier to the wide adoption of cloud storage (Wilson, 2009; Mitchel, 2009; Messmer, 2009). Storage cloud providers must, therefore, implement a secure access control system in order to reduce the risk of unauthorized access to a reasonably low level.

DOI: 10.4018/978-1-4666-3934-8.ch007

Security has its costs and the structure of very large scale storage systems incurs a trade-off between performance, availability and security (Leung, Miller, & Jones, 2007). Balancing this trade-off is particularly challenging in the cloud environment due to the scalability and high availability requirements. Moreover, even though the consistency of the data itself can be reduced to improve availability (Trusted Computer System Evaluation Criteria, 1985), the access control configurations and their enforcement should be always consistent across all access points. Furthermore, since data in the storage cloud resides on a shared infrastructure, it may be repeatedly migrated, hosted and managed by parties which may be untrusted and can be exposed to unauthorized access. The early cloud storage offerings mostly neglected security or provided minimal security guarantees. However, recently security is gaining more and more attention. This issue becomes central both to the existing vendors, that improve their offerings, as well as new companies and services that aim to add an additional level of security or access control over the existing solutions.

In addition to the scale and availability requirements, today's new Web applications introduce new characteristics to data access. For example, data is not necessarily accessed directly by its owner but rather through various applications, in flexible sharing scenarios and with various billing methods. These applications put forth new functional requirements that include, for example, the requirement for the federated identity and Single Sign On (SSO) as well as the ability of a client to delegate a subset of his access rights, supporting the related notion of Discretionary Access Control (DAC) (Messmer, 2009). Another requirement is a support for hierarchical management of rights, assigning administrators' privileges to domains and allowing them to delegate partial access to other principals under their control.

An access control system is considered to be safe if no permission can be leaked to an unauthorized or uninvited principal. Thus, it is essential to ensure that the access control architecture cannot lead to leakage of permissions to an unauthorized principal. When considering the highly distributed architecture of cloud storage systems, this is an extremely challenging task. Each architectural component can introduce new threats. Furthermore, there is a requirement to support multi-tenancy while isolating the configuration parameters and the data of the different tenancy. This is a very ambitious goal, especially since even a well-known functionality, such as deduplication, in a cloud setting can lead to privacy violations (Harnik, Pinkas, & Shulman-Peleg, 2010). Unfortunately, when addressing the required rich functionality together with the next generation cloud scale, most of the existing solutions require high performance overhead or lead to new security threats and bottlenecks.

This chapter is structured as follows. First, we present the background section, which describes the requirements of the cloud access control mechanisms as recognized by the VISION Cloud project. The section titled "Access Control Models and Components" describes the access control fundamentals, presenting the existing access control models. It compares the various schemes describing the challenges that occur in the Cloud Storage set up. The section titled "Access Policy Modelling and Management" focuses on existing solutions in the field of policy based management and the section on "Federated Identity" addresses the important issue of identity federation, which gives clients a unified access control system. Finally, the section on "Future Research Directions" presents the VISION Cloud approach, justifying its design decisions and describing its advantages.

BACKGROUND

The challenge of access control is to control the access and allow only users with the proper privilege to carry out operations. There are two basic access control components: (1) Authentication,