Chapter 37
Policy Management in Cloud: Challenges and Approaches

Hassan Takabi
University of Pittsburgh, USA

James B. D. Joshi
University of Pittsburgh, USA

ABSTRACT

Cloud computing paradigm is still an evolving paradigm but has recently gained tremendous momentum due to its potential for significant cost reduction and increased operating efficiencies in computing. However, its unique aspects exacerbate security and privacy challenges that pose as the key roadblock to its fast adoption. Cloud computing has already become very popular, and practitioners need to provide security mechanisms to ensure its secure adoption. In this chapter, the authors discuss access control systems and policy management in cloud computing environments. The cloud computing environments may not allow use of a single access control system, single policy language, or single management tool for the various cloud services that it offers. Currently, users must use diverse access control solutions available for each cloud service provider to secure data. Access control policies may be composed in incompatible ways because of diverse policy languages that are maintained separately at every cloud provider. Heterogeneity and distribution of these policies pose problems in managing access policy rules for a cloud environment. In this chapter, the authors discuss challenges of policy management and introduce a cloud based policy management framework that is designed to give users a unified control point for managing access policies to control access to their resources no matter where they are stored.

INTRODUCTION

Cloud computing has recently generated intensive interest within computing research communities. It essentially tries to consolidate the economic utility model with the evolutionary development of many existing computing approaches and technologies such as distributed services, applications, information and infrastructure consisting of pools of computers, networks, information and storage resources (Cloud Security Alliance, 2011), Catteddu & Hogben, 2009). Cloud computing has shown tremendous potential to enhance collaboration, agility, scale, and availability (Takabi, Joshi, &

DOI: 10.4018/978-1-4666-2919-6.ch037

Ahn, 2010). Its definitions, attributes, characteristics, issues, underlying technologies, risks, and values have been evolving and change over time. Confusion still exists about how a cloud is different from existing models and how these differences might affect its adoption. Some see a cloud as a novel technical revolution while others consider it a natural evolution of technology, economy and culture (Takabi, Joshi, & Ahn, 2010).

So far, no single, agreed upon definition of cloud computing exists. The US National Institute of Standards and Technology (NIST) defines cloud as follows: "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models." (Mell & Grance, 2011). The five key characteristics of cloud computing include on demand self-service, ubiquitous network access, location independent resource pooling, rapid elasticity, and measured service, all of which are geared toward using clouds seamlessly and transparently (Mell & Grance, 2011). The three key cloud delivery models are software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS) (Mell & Grance, 2011).

In IaaS, the cloud provider provides a set of virtualized infrastructural components such as virtual machines and storage on which the customers can build and run applications. The most basic component is a virtual machine (VM) and the virtual operating system (OS) where the application will eventually reside. Issues such as trusting the virtual machine image, hardening hosts, and securing inter-host communication are critical areas in IaaS. PaaS enables the programming environments to access and utilize the additional application building blocks. Such programming environments have a visible impact on the application architecture. One such impact would be that of the constraints on what services the application can request from an OS. For example, a PaaS environment may limit access to well-defined parts of the file system, thus requiring a fine-grained authorization service. In SaaS, the cloud providers enable and provide application software enabled as on-demand-services. As clients acquire and use software components from different providers, securely composing them and ensuring that information handled by these composed services are well protected become crucial issues.

Various cloud deployment models include public cloud, private cloud, community cloud, and hybrid cloud composed of multiple clouds (Mell & Grance, 2011). A public cloud refers to an external or publicly available cloud environment that is accessible to multiple tenants, while a private cloud is typically a tailored environment with dedicated virtualized resources for a particular organization. Similarly, community cloud is tailored for a particular group of customers.

As more and more consumers start using cloud services, Service Level Agreement (SLA) is becoming a key aspect of immigrating to the cloud. The SLA is used to describe the relationship between cloud providers and consumers and is fundamental of consumers' trust in cloud service providers. An SLA should clearly address several factors like a list of services the provider delivers along with a specific definition of these services, the responsibilities of both parties, a set of metrics to ensure the provider is delivering the services as stated, an auditing mechanism to monitor the quality of services, business continuity and disaster recovery plan, location of data, seizure of data, how to address failures of the provider and disputes between the provider and consumer, the available options when the terms of the SLA are not met, system redundancy and maintenance, jurisdiction, and how the SLA term can be modified over time. Some of the other requirements that need to be taken in account in SLAs are