Chapter 71
Authentication and Identity Management for Secure Cloud Businesses and Services

Bing He
Cisco Systems, Inc., USA

Tuan T. Tran
InfoBeyond Technology LLC, USA

Bin Xie
InfoBeyond Technology LLC, USA

ABSTRACT

Today, cloud-based services and applications are ubiquitous in many systems. The cloud provides undeniable potential benefits to the users by offering lower costs and simpler deployment. The users significantly reduce their system management responsibilities by outsourcing services to the cloud service providers. However, the management shift has posed significant security challenges to the cloud service providers. Security concerns are the main reasons that delay organizations from moving to the cloud. The security and efficiency of user identity management and access control in the cloud needs to be well addressed to realize the power of the cloud. In this chapter, the authors identify the key challenges and provide solutions to the authentication and identity management for secure cloud business and services. The authors first identify and discuss the challenges and requirements of the authentication and identity management system in the cloud. Several prevailing industry standards and protocols for authentication and access control in cloud environments are provided and discussed. The authors then present and discuss the latest advances in authentication and identity management in cloud, especially for mobile cloud computing and identity as a service. They further discuss how proximity-based access control can be applied for an effective and fine-grained data access control in the cloud.

DOI: 10.4018/978-1-5225-0159-6.ch071

1. INTRODUCTION

Cloud computing offers us the state of the art technique to accomplish businesses or services over the networked cloud platforms while we don't need to own or manage the corresponding infrastructure. It provides our business many benefits, such as allowing us to set up a virtual office and thus connecting to our business anywhere and anytime. Such a capability is more flexible with the even growing popularity of web-enabled devices in today's business environment (e.g., smartphones, tablets), ubiquitously accessing the business data and performing various business operations in the cloud, which again is named as cloud business. The directly benefit of cloud business is the reduced IT costs as purchasing IT system can be avoided for running our business, consequently resulting in no cost on system upgrades, system maintenance, and IT staff. The other benefit is that our business can scale up or scale down easily with less cost. In addition, the business on the cloud promotes collaboration efficiency and flexibility of business practices.

New technology brings new risks and challenges. In the cloud, security is a critical issue for cloud users and the question is that if our business data and operations are well protected. For example, the business data should be protected from various cyber attackers as well as the insiders. For any requests of accessing the cloud data, the users have to be reliably and effectively authenticated to provide a secure and seamless user experience in cloud-based services. Identity Management (IDM) refers to the policies, processes, and technologies that establish user identities and enforce rules about access to certain resources and services. In cloud environment, service providers need to identify different users for bill purpose, to grant different access to resources and information, or to analyze user's behavior to optimize the customer experience with customized service and highly relevant content. All these rely on the IDM mechanism. An IDM mechanism can authenticate users and services based on credentials and characteristics, and protect private and sensitive information related to users and processes. Authentication is the process of verify the identity of an individual, an entity or an organization through verifying the credentials. Typically there are three type of credentials a user could provide, i.e., what you know, e.g., passwords; what you have, e.g., ID card, wrist band, etc.; and what you are, e.g., biometric identifiers including fingerprints, palmprints, retinal pattern, signature, etc. Each of them has advantages and disadvantages in different application scenarios.

In a cloud environment, service are delivered through servers that are dynamically launched or terminated, IP address are dynamically allocated and assigned, and services are dynamically started or stopped. Traditional IDM may not be sufficient in this dynamic-changing and distributed cloud computing environment. The unique security and privacy implications in cloud computing imposes special requirements to IDM in cloud computing (Rhoton, 2011; Gopalakrishnan, 2009; Takabi, 2010):

- **Multi-Tenant Cloud Environments:** The multi-tenant cloud environments can affect the privacy of identity information. In multi-tenant cloud environments, providers must separate customer identity and authentication information. While users interact with a front-end service, their identity should be protected from other services which are running in back-end.
- **Volatility of Cloud Relations:** In traditional model, IDM is based on the long-term relations of users to an organization, company or trust domain. While in could, the relationships between tenant and venders change dynamically and quickly, imposing additional challenges for cloud IDM.
- **On-Demand Provisioning and Real-Time De-Provisioning:** An appropriate authentication and IDM solution in could need to make sure current user gain access to requested resource imme-