Chapter 15
Access Control Framework for Cloud Computing

Kashif Munir
King Fahd University of Petroleum and Minerals, Saudi Arabia

Lawan A. Mohammed
King Fahd University of Petroleum and Minerals, Saudi Arabia

ABSTRACT

Access control is generally a rule or procedure that allows, denies, restricts or limit access to system's resources. It may, as well, monitor and record all attempts made to access a system. Access Control may also identify users attempting to access unauthorized resources. It is a mechanism which is very much important for protection in computer security. Various access control models are in use, including the most common Mandatory Access Control (MAC), Discretionary Access Control (DAC) and Role Based Access Control (RBAC). All these models are known as identity based access control models. In all these access control models, user (subjects) and resources (objects) are identified by unique names. Identification may be done directly or through roles assigned to the subjects. These access control methods are effective in unchangeable distributed system, where there are only a set of Users with a known set of services. For this reason, we propose a framework which is well suited to many situations in cloud computing where users or applications can be clearly separated according to their job functions. In this chapter, we proposes a role based access control framework with various features including security of sensitive data, authorization policy and secure data from hackers. Our proposed role based access control algorithm provides tailored and fine level of user access control services without adding complexity, and supports access privileges updates dynamically when a user's role is added or updated.

INTRODUCTION

Cloud computing describes a new delivery model for IT services based on the Internet, and it typically involves over-the-Internet provision of dynamically scalable and often virtualized resources. It is a byproduct and consequence of the ease-of-access to remote computing sites provided by the Internet. This frequently takes the form of web-based tools or applications that users can access and use through a web browser as if it is a program installed locally on their own computer (Armbrust et. al, 2009).

DOI: 10.4018/978-1-4666-8387-7.ch015

In the "cloud", all data processing tasks are handled by a large number of distributed computers, end-users get access to the computer and storage systems through network on their demand. Enterprise Data Center is responsible for handling customer' task which is from customer' computer, so that it can provide data services for all kinds of users who use variety of different devices through just one data center and allow anyone who has the right Internet links to get access to the cloud applications (Arnold, 2008).

Aside from the huge marketing efforts, cloud security has been criticized for its unknown privacy and security protection. There could be benefits from a security perspective since most customers utilizing cloud may not have the expertise to safeguarding their information assets using traditional IT approaches, and using cloud services could mitigate this problem. On the other side, companies hosting the cloud services have in general full control over the services they provide. They could control and monitor data essentially at will. It has been noted by the research community that confidentiality and auditability are one of the top 10 obstacles to the growth of cloud computing (Armbrust et. al, 2009(b)).

As the goal of Cloud Computing is to share resources among the cloud service consumers, cloud partners, and cloud vendors in the cloud value chain. There has been a growing trend to use the cloud for large-scale data storage. However, the multi-tenant nature of the cloud is vulnerable to data leaks, threats, and malicious attacks. Therefore, it is important for enterprises to have strong access control policies in place to maintain the privacy and confidentiality of data in the cloud. The cloud computing platform is highly dynamic and diverse. Current access control techniques, like firewalls and VLAN, are not exactly well-suited to meet the challenges of cloud computing environment. They were originally designed to support IT systems in an enterprise environment. In addition, any weak access control mechanisms in the cloud can lead to major data breaches.

For instance, a few years back a massive data breach took place on the server of Utah Department Technology Services (DTS) as reported in *InformationWeek* (http://www.darkreading.com/risk-management/utahs-medicaid-data-breach-worse-than-expected/d/d-id/1103823). A hacker group from Eastern Europe succeeded in accessing the servers of DTS, compromising 181,604 Medicaid recipients and the Social Security numbers of 25,096 individual clients. The reason behind this massive breach is believed to be a configuration issue at the authentication level when DTS moved its claims to a new server. The hacker took advantage of this busy situation and managed to infiltrate the system, which contained sensitive user information like client names, addresses, birth dates, SSNs, physicians' names, national provider identifiers, addresses, tax identification numbers, and procedure codes designed for billing purposes. The Utah Department of Technology Services had proper access controls, policies, and procedures in place to secure sensitive data. However, in this particular case, a configuration error occurred while entering the password into the system. The hacker got access to the password of the system administrator, and as a result accessed the personal information of thousands of users. The biggest lesson from this incident is that even if the data is encrypted, a flaw in authentication system could render a system vulnerable. Enterprises should be sure to limit access to control policies, enforcing privileges and permissions for secure management of sensitive user data in the cloud. In another cloud computing survey conducted by *PC Connection* (PCConnection, 2013), it was mentioned that in 2011, 174 million records were compromised, costing organizations an average of $5.5 million—or $194 per compromised record.

According to the *Ponemon Institute* (Ponemon, 2013) Research Report of 2013 findings, organizations have improved their security practices around cloud use when compared to 2010 responses. However, only about half of respondents had positive perceptions about how their organiza-