Journal of Computer and System Sciences 80 (2014) 1518–1533

Contents lists available at ScienceDirect

Journal of Computer and System Sciences

www.elsevier.com/locate/jcss

Secure administration of cryptographic role-based access control for large-scale cloud storage systems

Lan Zhou, Vijay Varadharajan*, Michael Hitchens

Information and Networked Systems Security Research, Department of Computing, Macquarie University, Australia

ARTICLE INFO

Article history:
Received 20 January 2013
Received in revised form 31 August 2013
Accepted 10 April 2014
Available online 14 May 2014

Keywords:
Role-based access control
Administration
Cryptographic RBAC
Role-based encryption
Cloud computing
Data storage

ABSTRACT

Cloud systems provide significant benefits by allowing users to store massive amount of data on demand in a cost-effective manner. Role-based access control (RBAC) is a well-known access control model which can be used to protect the security of cloud data storage. Although cryptographic RBAC schemes have been developed recently to secure data outsourcing, these schemes assume the existence of a trusted administrator managing all the users and roles, which is not realistic in large-scale systems. In this paper, we introduce a cryptographic administrative model AdC-RBAC for managing and enforcing access policies for cryptographic RBAC schemes. The AdC-RBAC model uses cryptographic techniques to ensure that the administrative tasks are performed only by authorised administrative roles. Then we propose a role-based encryption (RBE) scheme and show how the AdC-RBAC model decentralises the administrative tasks in the RBE scheme thereby making it practical for security policy management in large-scale cloud systems.

1. Introduction

With the rapid increase in the amount of digital information that needs to be stored, cloud storage has attracted much attention in recent times because of its ability to deliver resources for storage to users on demand in a cost effective manner. The cloud can provide a scalable high-performance storage architecture, and can help to significantly reduce the cost of maintenance of individual services. There are different types of infrastructures associated with a cloud [1]. A public cloud is a cloud which is made available to the general public, and resources are allocated in a pay-as-you-go manner. A private cloud is an internal cloud that is built and operated by a single organisation. Potentially there could be several benefits to storing data in the public cloud.[1] The storage capacity of a cloud is almost unlimited, and users only need to pay for the storage space for their actual needs. Outsourcing data to cloud can also help to save the costs and efforts in storage maintenance tasks, such as data backup and replication, disaster recovery, and hardware maintenance. Furthermore, cloud storage can provide a flexible and convenient way for users to access their data from anywhere on any device.

While the cloud storage has many benefits, it also brings important security issues. Since data in the cloud is stored in one or more data centres which are often distributed geographically in different locations, users do not know where their data is stored and there is a strong perception that users have lost control over their data after it is uploaded to the cloud. In order to allow users to control the access to their data stored in a public cloud, suitable access control policies and mechanisms are required. The access policies must restrict data access to only those intended by the data owners (users

* Corresponding author.
E-mail address: vijay@science.mq.edu.au (V. Varadharajan).

[1] In this paper, when we use the word cloud, we are referring to a public cloud.

http://dx.doi.org/10.1016/j.jcss.2014.04.019

who own the data). These policies need to be enforced by the cloud. In many existing cloud storage systems, data owners have to assume that the cloud providers are trusted to prevent unauthorised users from accessing their data. However, the data owner may not wish the cloud provider itself to view and access the data that is being stored in the cloud. Typically the cloud provider can include the employees of the cloud provider organisation. The greater the sensitivity of the data stored in the cloud, the more stringent are the security requirements on the access to data. For example, storage of electronic patient records in a healthcare system would warrant such stringent security needs.

Defining, on a piece by piece basis, which users have what access to data is a potentially time-consuming and error-prone approach. More sophisticated methods of handling access control structures have long been known. One of the most widely known approaches is the Role-Based Access Control (RBAC). The central notion of RBAC is that permissions are associated with roles, and users are assigned to appropriate roles. Roles are created for the various subsets of users based on users' responsibilities and qualifications, and roles can inherit permissions from other roles. If role A inherits all the permissions associated with role B, then users who belong to role A will have all the permissions of role B. In this paper, we will refer to this as role A being an ancestor role of role B, and role B being a descendent role of role A. This approach has a number of immediate benefits. Roles can be given permissions which match policies in real-world situations. Users can be easily switched between roles, automatically changing the permissions available to them. This is much simpler than other access control systems, such as Mandatory Access Control (MAC) and Discretionary Access Control (DAC), where the individual permissions for a given user would each have to be updated to reflect the abilities of the new position. This multi-level structure simplifies the task of organising and managing access.

In traditional systems, access control enforcement is carried out by trusted parties who have the control over all the resources of the systems. However, the enforcement of access policies is not guaranteed in cloud as cloud is usually considered to be untrusted due to its distributed nature. In order to enforce RBAC policies for data storage in the cloud, one approach is to use cryptographic techniques to encrypt the data before storing it in the cloud. This would allow only the users who have access to the key(s) to decrypt the data and to view the data in the plain form. Several schemes [2–4] have been proposed that integrate cryptographic techniques with RBAC models. In these cryptographic RBAC schemes, data is encrypted to specified roles before being outsourced to the cloud, and only the users who have been granted membership to these roles can decrypt the data using their secret keys. Other parties, including the cloud provider itself, cannot reveal the content of the data. Using these schemes ensures the security of the data stored in cloud, and retains the flexibility in controlling the access to the data in the mean time. However, the administration in cryptographic RBAC schemes relies on a central authority. Decentralising the administration privileges in cryptographic RBAC raises several significant security and design challenges, especially in large-scale systems. Hence in this paper, we focus on the administration of privileges in cryptographic role-based access systems in a cloud environment.

RBAC has been widely used for security administration in distributed systems since being first formalised in the 1990's. However, the administration of RBAC systems themselves has been less widely studied. In small RBAC systems, a central authority is usually sufficient to manage all the users and permissions. However, large-scale RBAC systems may have hundreds or even thousands of roles and hundreds of thousands of users and permissions. In such cases, it becomes impractical to centralise the task of managing these users and permissions, and their relationships with the roles to a small team of security administrators. Therefore, decentralising the administration tasks of RBAC systems is an important issue when developing such large-scale role-based systems. Several administrative RBAC (ARBAC) models have been developed to provide solutions to decentralise the administration privileges. The administrative model for RBAC was first considered in [5], and a comprehensive model ARBAC97 was proposed in this work. It was later extended and improved in [6–11]. A common feature of these works is managing a RBAC system using RBAC itself. The administration privileges are decentralised to a set of administrative roles in these models, and administrative policies are specified to limit the privileges of administrative roles. Each administrative role is assigned an administration domain, and the role is allowed to perform administration task only on the roles that are covered by the administration domain.

When using these ARBAC models to manage the RBAC systems which are using cryptographic RBAC schemes, the security issue of enforcement of the administrative polices of the administrative models becomes significant. In ARBAC models, the privileges of each administrator are restricted by the systems themselves, so that administrators cannot change the roles that they do not have permissions to change. However, existing ARBAC models cannot work with cryptographic RBAC in a distributed environment, as the administrative policies cannot be enforced and there is no authority that can restrict the privileges of the administrative roles.

This paper has two main contributions: (i) a new cryptographic administrative RBAC model AdC-RBAC that can manage and enforce administrative policies for cryptographic RBAC schemes in large-scale cloud systems and (ii) a new role-based encryption scheme that can work with the proposed AdC-RBAC model to secure data in a cloud storage system. In this paper, we first introduce the new RBE scheme and show how this scheme can be used to secure data storage in a cloud system in an effective manner. Then we propose the cryptographic administrative model AdC-RBAC and show how the proposed model can be used in an untrusted cloud while guaranteeing its security using cryptographic access control enforcement techniques for the proposed RBE scheme. The AdC-RBAC model uses cryptographic techniques to ensure that the administrative tasks such as user, permission and role management are performed only by authorised administrative roles; any party else, including the cloud providers themselves, cannot change RBAC systems and policies. We describe three components in this model: UAM for user membership management, PAM for permission management, and RAM for role management.