

**本科毕业设计(论文)英文翻译**

**题目：web云存储硬盘系统的设计与实现**

|  |  |
| --- | --- |
| **学生姓名：** | **李政** |
| **学 号：** | **1606031127** |
| **班 级：** | **16级软件工程1班** |
| **专 业：** | **软件工程** |
| **院 （系）：** | **计算机工程学院** |
| **指导教师：** | **刘明纲** |

二零二零年一月三十日

**一、英文原文**

**起止页码：**1-3

**出版日期：**2019年4月15日（1556-6021）

**出版单位：**IEEE Xplore Digital Library

An Attribute-based Controlled Collaborative Access Control Scheme for Public Cloud Storage

Abstract—In public cloud storage services, data are outsourced to semi-trusted cloud servers which are outside of data owners’ trusted domain. To prevent untrustworthy service providers from accessing data owners’ sensitive data, outsourced data are often encrypted. In this scenario, how to conduct access control over these data becomes a challenging issue. Attribute Based Encryp- tion (ABE) has been proven to be a powerful cryptographic tool to express access policies over attributes, which can provide a fine-grained, flexible, and secure access control over outsourced data. However, existing ABE-based access control schemes do not support users to gain the access permission by collaboration. In this paper, we explore a special attribute-based access control scenario where multiple users having different attribute sets can collaborate to gain access permission if the data owner allows their collaboration in the access policy. Meanwhile, the collaboration that is not designated in the access policy should be regarded as a collusion and the access request will be denied. We propose an attribute-based controlled collaborative access control scheme through designating translation nodes in the access structure. Security analysis shows that our proposed scheme can guarantee data confidentiality and has many other critical security properties. Extensive performance analysis shows that our proposed scheme is efficient in terms of storage and computation overhead.

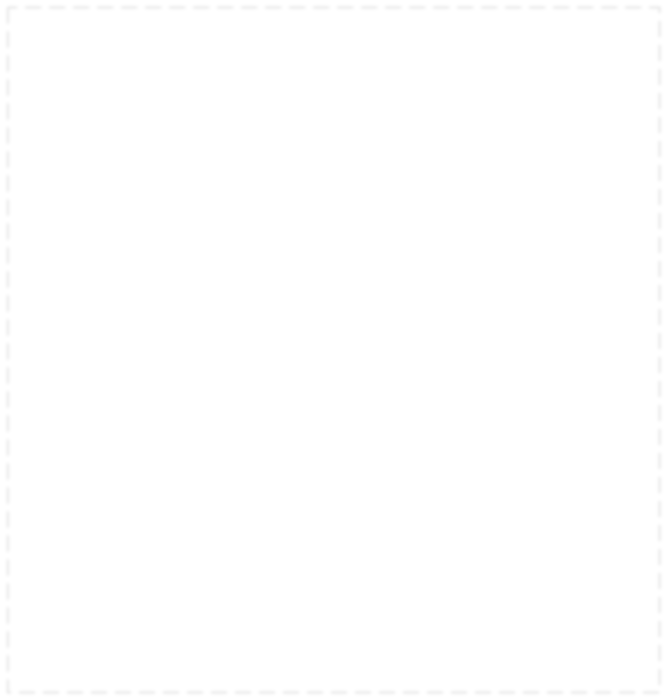
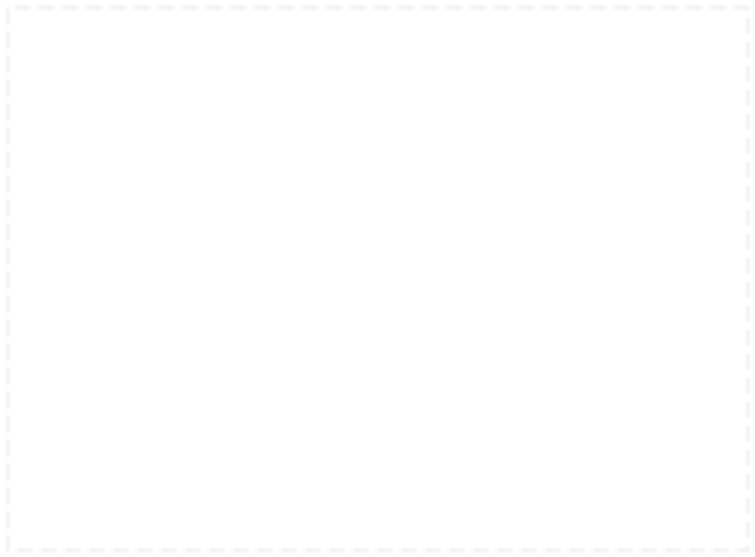
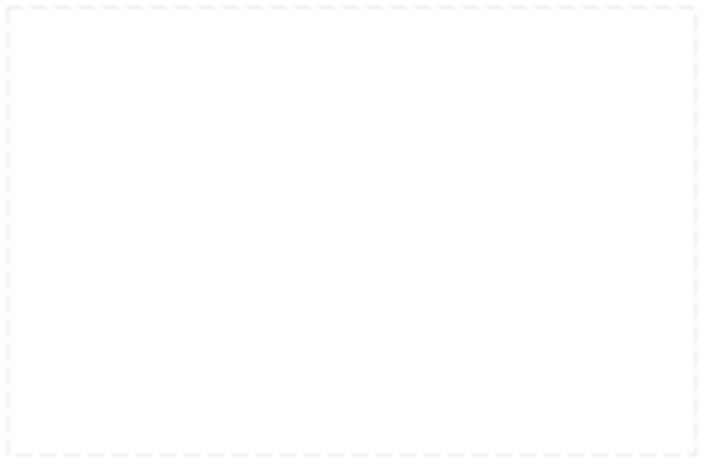
1. INTRODUCTION

Cloud computing has emerged as the natural evolution and integration of advances in several fields, including utility computing, distributed computing, grid computing, and service oriented architecture [1]. It promotes the concept of leasing remote resources rather than buying hardwares, which frees cloud customers (such as enterprises and individuals) from maintenance expenses. Cloud customers are able to utilize cloud services on a pay-as-you-use basis, where the price is relatively low. What’s more, since services are provided via the Internet, customers can access applications and data anywhere and anytime. To benefit from the above advantages, but not limited to, an increasing number of enterprises and individuals are willing to outsource their data and applications to cloud platforms.

Despite many advantages of cloud computing, there still re- main various challenging issues that impede cloud computing from being widely adopted, among which, privacy and security of users’ data have been the major issues. Traditionally, a data owner stores his/her data in trusted servers which are generally controlled by a fully trusted administrator. However, in public cloud storage, which is a popular service model in cloud computing, data are usually stored and managed on remote cloud servers which are administrated by a semi-trusted third party, i.e. the cloud service provider. Data are no longer in data owners’ trusted domains and they cannot trust cloud servers to conduct secure data access control. Therefore, the secure access control has become a challenging issue in public cloud storage, in which traditional security technologies cannot be directly applied.

In recent years, many researches have been devoted on data access control in public cloud storage, such as the work in [2– 7]. Among those literatures, Ciphertext-policy Attribute-based Encryption (CP-ABE) is regarded as one of the most suitable schemes due to the fact that it can guarantee data owners’ direct control over their data and provide a fine-grained access control service. In CP-ABE schemes, each user is associated with a set of attributes and every ciphertext is embedded with an access structure over some chosen attributes. The access structure is used to express the specific access policy that should be satisfied to access data contents. Only if a user’s attribute set satisfies the access structure embedded in the ciphertext can he/she decrypt the ciphertext. Therefore, by using access structures over attributes to express access policies, CP-ABE is a promising tool to provide fine-grained, flexible, and secure data access control in public cloud storage.

Nevertheless, the existing CP-ABE schemes can merely assign access permission to individuals who own attribute sets satisfying the access policy. However, in many scenarios, the secret information cannot be obtained individually by a single user alone. For example, in enterprises and organizations, some important files/documents are shared among multiple users who have distinct responsibilities according to their positions, but have the same goal to protect data confidentiality. A data access request may be permitted only when multiple users with different responsibilities collaborate. Such requirement of collaboration to access secret data has been widely studied in secret sharing schemes [8, 9], where data can only be accessed by a number of participants together and the number is no less than a given threshold. Unfortunately, the existing secret sharing schemes cannot express access policies in a fine- grained and flexible way. For a fine-grained access control, we can label each user by an attribute set where his/her responsibility/role can be expressed as a single attribute or a set of attributes. To design a general access control system, we let data be accessed on one of the following two conditions: 1) (Non-collaboration scenario) As the existing CP-ABE schemes do, an individual who has a sufficiently powerful attribute set satisfying the access structure can access data individually; 2) (Collaboration scenario) For a user whose attribute set doesn’t have sufficient authority to gain access individually, he/she can collaborate with other users who have some different attributes such that their integrated attribute set has sufficient authority to access data. Here, we take an example to illustrate the scenario. In a company, the data owner requires a financial document to be accessed on the following circumstances, as shown in Fig. 1: The left side with two boxes shows that two policies can be utilized to access data. The word “OR” between the two boxes means that the data users can access the data if they can satisfy either sub-policy A or sub-policy B. Sub-policy A denotes the case that the policy tree must be satisfied by an independent user, and sub-policy B denotes the case that the ciphertext can be accessed by collaboration on the condition that one user has an attribute set that can satisfy the tree on the left side (in the box denoting sub-policy B) and the other user has the attribute ‘Auditor’. The word “AND” means the mentioned two users can collaborate to satisfy sub-policy B. We observe that it is usually impossible for a user to have both attribute sets ‘Manager’/‘Accountant’ and ‘Auditor’ . Thus, sub-policy A and sub-policy B can be expressed in a more efficient way by a compound policy tree as shown on the right side in Fig.1. The node denoted ‘Auditor’ has two circular edges to indicate that it is a special node that allows collaboration to be performed on it.



***OR***

***Manager***

***Accountant***

***Senior***

***OR***

***Auditor***

***AND***

***AND***

**Sub-policy B**

***Compound Policy Tree***

***Manager Auditor***

***Accountant***

***Senior***

***(2,3)***

***AND***

***Senior***

***Manager***

***Accountant***

***AND***

**Sub-policy A**

Fig. 1: An Example of An Access Policy

It is not straightforward to design a suitable mechanism to allow collaboration embedded in the access policy. To tackle the above problem, Li et al. [10] firstly addressed the collaboration problem among users with different attribute sets, and they proposed a Group-Oriented Attribute-Based Encryption (GO-ABE) scheme. Constructed on CP-ABE, GO- ABE further divides users into groups and allows users from the same group to collaborate to access data. Allowing users within the same group to collaborate is reasonable, since users responsible for one project may have more motivations to pro- tect their data. However, their scheme allows all attributes to be collaborated within the same group, even if the data owner disallows such data access. That is to say, in the example of Fig. 1, a user with the attribute set ‘Junior’, ‘Accountant’, ‘Manager’ can also collaborate with a user with the attribute set ‘Senior’, ‘Programmer’ to gain the permission to access data, by collaborating on the attribute ‘Senior’. However, this should be considered as a malicious behavior from the view- point of data owners. Thus, it is a challenging issue to design such mechanism that allows expected collaboration among honest users and also simultaneously resist unwanted collusion among curious users. As the access policy specified in Fig 1, only a user with the attribute set ‘Senior’, ‘Accountant’ or ‘Senior’, ‘Manager’ collaborating with a user with the attribute ‘Auditor’ is regarded as valid collaboration to access data. Any other kind of collaboration should be considered as malicious and the access is not permitted.

In this paper, we address the collaboration issue in practical scenarios and propose an attribute-based controlled collabora- tive access control scheme for public cloud storage. Specifi- cally, like GO-ABE [10], we restrict user collaboration in the same group that corresponds to the same project for which the involved people are responsible. Thus, in our work, in order to provide both data confidentiality and collaborative access control, only people who are in charge of the same project are allowed to collaborate. Technically, data owners allow expected collaboration by designating translation nodes in the access structure. In this way, unwanted collusion can be resisted if the attribute sets by which users are collaborating are not corresponded to translation nodes. For each translation node, an additional translation value is generated. Using this translation value and special translation keys embedded in users’ secret keys, users within the same group can collaborate to satisfy the access structure and gain the data access per- mission. For colluding users across groups, their access is not permitted as their secret keys do not correspond to the same group. The main contributions of this work can be summarized as follows.

1) We address the problem of data access control in collabo- ration scenarios and propose an attribute-based controlled collaborative access control scheme. Data owners can specify expected collaboration among users when they define access policies. Meanwhile, unwanted collusion can be denied to access the data.

2) We design a mechanism to achieve our goal by designat- ing translation nodes in policy trees and modifying secret keys and ciphertexts. More specifically, our approach embeds a translation key inside the secret key of BSW scheme [11] and adds a translation value in the ciphertext for each translation node. The combination of translation keys and translation values enables users to collaborate to satisfy a policy tree.

3) Users are divided into groups in a way such that the collaboration is restricted and secure. That is to say, only users responsible for the same project are allowed to collaborate in case that malicious users who are not responsible for the project collude. Extensive security analysis is given to show the security properties of our proposed scheme.

The rest of this paper is organized as follows. In Section II, we introduce some related works about access control schemes in public cloud storage, along with the researches on the topic of collaborative access control. In Section III, technical prelim- inaries are presented, and the definition of the system model and security assumptions are presented in Section IV. We introduce our proposed attribute-based controlled collaborative access control scheme for public cloud storage in Section V. In Sections VI and VII, we analyze our proposed scheme in terms of security and performance, respectively. Finally, the conclusion is given in Section VIII.

**二、中文译文**

**一种基于属性的公共云存储受控协同访问控制方案**

摘要：在公共云存储服务中，数据被传送给半信任的云服务器，这些服务器位于用户的可信域之外。为了阻止不值得信赖的服务提供商获取用户的敏感数据，这些数据通常被加密。在这种情况下，如何执行这些数据的访问控制变成一个十分具有挑战性的问题。基于属性的加密（简称ABE）已经变成一项十分强大的加密工具，可以表达对属性的访问策略，能够数据提供一种精密、灵活和安全的访问控制。然而，现存的基于ABE的访问控制模式并不支持用户通过协作获取访问许可。在这篇论文中，我们探索了一种特殊的基于属性的访问控制方式，在这种场景中，如果数据所有者允许用户在访问策略中进行协作，则具有不同属性集的多个用户可以协作以获得访问权限。同时，在访问策略中没有指定的协作应该被看作为一种共谋，而且访问请求应该被拒绝。我们通过在访问结构中指定翻译节点提出了一种基于属性的受控协作访问控制模式。安全分析表明我们提出的模式能够保证数据的机密性，并且还有许多其他的严格的安全属性。广泛的性能分析表明我们提出的模式在存储和计算开销方面是有效的。

I. INTRODUCTION

云计算是几个领域自然进化和集成的产物，这些领域包括效用计算、分布式计算、网格计算和面向服务的架构。它提出了租用远程资源的概念，而不是购买硬件，这减轻了云消费者（比如说企业和个人）的维护开销。云消费者能够利用云服务基于根据用多少付多少原则，价格就相对较低。而且，由于服务是通过网络提供，消费者能够在任何时间任何地点获取应用和数据。受益于上述但不限于上述的优势，越来越多的企业和个人愿意将他们的应用和数据外包给云平台。

尽管云计算拥有许多计算优势，但仍然存在很多问题，阻碍着云计算被广泛接受，特别是因为用户数据的隐私和安全问题。通常，数据拥有者将他们的数据存储在可信服务器那里，这些服务器通常由完全可信的管理员控制着。然而，在公共云存储领域，云计算中的流行的服务模型中，数据通常存储在远程服务器，由第三方的半可信云服务提供商所管理。数据不再是数据拥有着的可信域并且他们不能信任服务商能够提供安全的数据访问控制。因此安全访问控制在公共存储领域已经变成一个富有挑战性的问题，传统的安全技术不能直接应用。

最近几年，许多研究者致力于公共云存储的访问控制。在众多这些文献中，基于属性的加密文本策略（简称 CP-ABE）被认为是最适合的方案之一，因为它能保证数据拥有者直接控制他们的数据并且提供严格的访问控制服务。在这种方案中，每个用户和一套属性关联，而且每个加密文本内嵌了一个针对部分这些属性的访问结构。访问结构用于表示访问数据内容时应该满足的特定访问策略。只有一套用户属性集满足了内嵌于密文中的访问结构，才能够对密文解密。因此，通过使用基于属性的访问控制结构来表示访问策略，CP-ABE是一个有希望在公共云存储领域提供细粒度、灵活和安全的数据访问控制的工具。

然而，现有的CP-ABE方案只对拥有能够满足访问控制策略的属性集的用户提供访问许可。但是，在许多情况下，保密信息不能只由一人持有。例如，在企业或组织中，一些重要的文件资料被分享给多个用户，这些用户根据他们的职位有不同的职责，但是都有保护数据保密性的目标。数据访问请求只有当多个承担着不同责任的人协作，数据访问请求才能够被许可。这种协同访问保密数据的要求已经被大量保密数据分享方案广为研究，数据只有由大量参与者一起才能够被获取，而且人数不能低于一个给定值。不幸的是，现有的方案不能通过一种细粒度且灵活的方式实现。对于一种细粒度的访问控制，我们能够通过一套属性标记每个用户，他的责任或角色能够被解释为单个或一套属性。设计一个通用的访问控制系统，我们让数据通过下列两项条件中的任意一项来获取：

1. 非协作模式：正如现存的CP-ABE方案所做的那样，拥有足够强大的属性集的个人能够独自获取数据， 这个属性集能够满足访问结构。
2. 协作模式：对于一个没有足够授权的用户，他可以和其他拥有不同属性的人联合，最终他们的属性全集持有访问数据的授权。在这里，我们举一个例子来阐述这种情况。在一个公司中，数据持有者要求一份金融文件在以下情况下才能被获取，如图1中所示，左边那幅由两个箱子表示两种能够被用来访问数据的策略。在这两个箱子之间的单词“OR”表示数据持有者在他们满足两种策略之一的情况下就能够获取数据。子策略A表示策略树必须满足独立的单个用户，子策略B表示在其中一个用户持有的属性集能够满足图中左边所表示的策略树和其他用户持有属性“Auditor”的条件下，密文才能够本协作访问。单词“AND”表示上述两个用户协作满足子策略B。我们观察到一个用户既拥有属性集“{Manager|Accountant}”和属性集”{Auditor}”的情况通常是不可能的。因此，子策略A和子策略B能够通过一种复合策略树（图右边所示）来更有效地表示。“Auditor”节点有两个圆边，表明它是一个允许在其上执行协作的特殊节点。

在这种访问策略中涉及一种允许内嵌联合的机制并不简单。为了解决上述问题，Li et al首先解决了持有不同属性集的用户的联合问题，并且他们提出了一种面向小组、基于属性集（GO-ABE）的加密方案。建立在CP-ABE基础上，GO-ABE进一步把用户按小组区分，并且允许同一小组的用户能够联合访问数据。允许同一小组内部的人员联合是合理的。因为为同一个项目的负责人对于保护数据有更多的动机。然而，他们的方案允许同一希小组所有的属性都参与联合，即使数据持有者不允许这种数据访问。说起来很容器，在图1的例子中，一个持有属性集“{Junior, Accountant, Manager}”的人员能够和另一个拥有属性集“{Senior，Programmer}”的人员一起联合获取访问许可，通过在属性“Senior”上联合。然而，在数据持有者来看，这应该被看成一种蓄意的行文。因此，设计这样一种机制是有问题的，这种机制预期诚实的用户联合而且同时抵制其他动机奇怪的用户的共谋。正如图1中所示，只有一个用户持有“{Senior, Accountant}”属性集或者是“{Senior, Manager}”属性集联合其他持有属性“Auditor”的用户时，这样的联合才能被看作是有效的。任何其他类型的联合都应该被认为是蓄意的并且访问不能被许可。

在这篇论文中，我们解决了在实际情况中的联合问题，并且提出了一种在公共云存储中基于属性的控制联合访问控制的方案。特别是，类似GO-ABE，我们将用户协作限制在与相关人员负责的同一项目相对应的同一组中。因此，在我们的工作中，为了提供数据保密性和联合访问控制，只有为同一个项目负责的人员才能被允许联合。从技术上讲，数据所有者通过在访问结构中指定转换节点来实现预期的协作。在这种方式中，如果用户联合的属性集和转化节点并不对应的话，有害的共谋能够被抵制。对于每个转化节点，都会生成一个额外的转化值。使用该转化值和嵌入在用户密钥中的特殊转化密钥，同一组内的用户可以协作以满足访问结构并获得每个任务的数据访问。对于跨组共谋的用户，不允许访问他们的权限，因为他们的密钥与同一组不对应。这项工作的主要贡献可以概括如下：

1. 针对排序场景中的数据访问控制问题，提出了一种基于属性的受控协同访问控制方案。数据所有者在定义访问策略时可以指定用户之间的预期协作。与此同时，不受欢迎的串通可以被拒绝访问数据。
2. 我们设计了一种机制，通过设计策略树中的转化节点和修改密钥和密文来实现这一目标。更具体地说，我们的方法将一个翻译键嵌入到BSW方案[11]的秘钥中，并为每个转化节点在密文中添加一个转化值。转化键和转化值的组合使用户能够协作以满足策略树。
3. 用户以一种限制和安全协作的方式被分成组。也就是说，只有对同一项目负责的用户才允许进行协作，以防不负责该项目的恶意用户串通。通过大量的安全性分析，证明了该方案的安全性。

本文的其余部分组织如下：第二部分介绍了公共云存储中访问控制方案的相关工作，以及协同访问控制的相关研究。在第三部分,技术预备测试——inaries,和系统模型的定义和安全假设在第四节提出, 在第六部分和第七部分介绍我们的提议属性控制协作访问控制方案,我们分别分析方案的安全性和性能。最后，结论见第八部分。

指导教师（签字）：

年 月 日