一、课题来源、目的、意义；国内外概况和预测

1.1 课题的来源

973 计划子项目“云存储服务和保障机制研究”

1.2 课题的目的

围绕当前主流云存储系统提供的多种不同的数据共享方式，结合云环境下用户的多态性、复杂性、动态性和易变性四大特点，针对不同数据共享方式对访问控制策略的需求不同，研究一种多模式协作的安全访问控制模型，根据用户访问数据的访问控制策略，动态调整该用户对于某资源的访问权限；再次基础之上，研究一种灵活的访问控制策略描述方法，让数据共享者能够方便简洁地表达数据的访问策略，而不需要遵守太多太复杂的形式化描述规则；研究一种高效的访问权限撤销方法，以尽可能低的开销及时回收访问权限。

1.3 课题的意义

云环境下用户呈现出多态性、复杂性、动态性和易变性等特点，多态性主要体现在云端用户的知识背景、文化层次、对云资源的需求和贡献、来自的群体等等都不相同；复杂性主要体现在云用户使用云资源的意图不同，不同用户在云存储中可访问的数据域是不同的；动态性主要体现在三个方面：一是用户访问云资源的类型会随着自己某段时间的喜好，或是研究方向等变化而改变；二是资源共享者可能会不定期地变更该资源的访问控制策略；三是根据用户共享资源的热度及用户访问行为制定的贡献度会随时间发生不规则的变动。易变性主要体现在不同场景用户具有不同的身份，同时用户身份的切换具有随机不可预料性。因此，随着云存储服务的多元化，复杂易变的用户群体给云存储系统的安全访问控制带来了巨大的挑战。一般来说，从功能需求来看，目前大部分云存储系统为用户主要提供了三种可访问的资源空间：个人空间、组空间和公共空间，不同的访问空间对于用户的授权和访问控制策略是不同。在个人空间中，用户的资源仅限于个人访问，数据的所有权和使用权仅局限于创建者本人；在组空间中，像 360 云盘、qq 微云，并没有对组内成员的访问权限进行区分，组内成员对组内资源享有相

同的访问权限，即同一组内所有成员都可以访问本组的所有资源，这样的共享方式可能会违背数据共享者的初衷；对于公共空间的资源，现有云存储系统均采用面向用户的无限制访问，即只要合法登录了系统的用户都可以自由访问公共空间的资源。这显然是不合理的，无法满足面向特定群体的数据共享需求，更不利于激励云用户相互分享更多有价值的资源。基于属性的访问控制虽然能够灵活地设置访问策略和访问粒度，但云端用户在上传数据时可能无法知晓云存储系统里定义了哪些基本属性，也不知道用户的身份信息，因此无论采用当前的基于身份的或是基于属性的方法制定访问控制策略，都无法较好地解决云环境下公共空间资源的访问控制问题。因此，必须围绕云存储系统提供的三种不同的数据共享方式，研究一种动态灵活的多模式协作的安全访问控制机制，在面对不同群体的用户访问共享资源时，能够快速地判断其访问权限，并能根据用户的访问行为可能对用户某些属性的影响，来动态的更新用户的动态属性；同时，为了确保某些机密数据的私密性，对于用户权限发生变更时，急需设计一种高校动态的用户权限回收方案，并解决由此带来的机密数据重加密的性能开销。

1.4 国内外概况和预测

云环境下的安全访问控制是云存储系统需要解决的首要问题之一，围绕这一问题，近年来研究者们主要从访问控制机制和访问控制策略的描述方法两方面展开了相应的研究。适合于分布式大规模环境下的访问控制机制主要有基于身份的访问控制和基于属性的访问控制，基于身份的访问控制一般采用传统的 ACL 管理文件/块的访问控制策略，当数据量和用户数量剧增时，ACL 会变得非常庞大，不仅给存储系统带来巨大的额外开销，而且维护和检索 ACL 表也变得非常复杂。基于属性的访问控制以用户属性为单位构造文件的访问策略，具有足够的灵活性和可扩展性，也使得安全的匿名访问成为可能，因此成为云环境下访问控制策略的首选，但目前仅处于学术研究阶段，尚未见将其应用到云存储系统的报道。

加州大学洛杉矶分校的 Amit Sahai 等人提出一种采用密文策略的属性加密(CP-ABE，Ciphertext-Policy Attribute-Based Encryption)机制实现文件的访问控制。该机制中访问策略由消息发送方来制定，每个文件对应一个访问控制策略，描述能够访问该文件的用户所必须具备的属性，使用该策略来加密文件，只有满足访

问控制策略的用户，才能用其属性密钥解密密文。美国伍斯特理工学院的 Shucheng Yu 等人提出了一种采用密钥策略的属性加密(KP-ABE，Key-Policy Attribute-Based Encryption)机制实现云存储的细粒度访问控制。每个用户拥有一个访问控制树，描述该用户能够访问的文件集合，每个文件都带有一些属性，每个属性对应一个公钥，用这些公钥加密对称密钥，访问树就是对应的用户私钥的正则表达式，如果访问树能够匹配文件的属性，则它能够解密该文件，用户就能访问这个文件。CP-ABE 和 KP-ABE 都是基于属性的加密方式，不同的是，前者访问控制树是和密文绑定在一起，描述的是能够访问该文件的用户范围，适合于访问控制类应用，如信息存储系统和社交类网站等。后者访问控制树和用户绑定在一起，描述的是用户能够访问的文件范围，适用于查询类应用，如视频点播系统和付费电视系统。虽然基于属性的访问控制机制在制定访问策略时比较灵活，但在权限撤销时非常麻烦，而且存在安全隐患。在进行权限撤销时，它们首先需要确定一个最小的属性集，然后对这个属性集中任何一个属性对应的公钥进行更新，再对相应的文件重新加密并对使用了这些属性的用户重新分发密钥，不仅开销大，而且在文件重加密之前该文件可能会被拥有旧密钥的用户再次访问，从而带来极大的安全隐患。

针对基于属性的访问控制（ABAC，Attribute-Based Access Control）存在的问题，国外内研究学者纷纷对其进行了扩充，如 ABAC 访问策略的策略描述与语义互操作研究，借用了 XACML 的思路对访问策略进行了形式化的约束，然而却没有考虑属性的动态变化问题；文献[6]在私有云中采用角色访问控制和属性访问控制相结合的方案，实现强制访问控制和自主访问控制的可选，但无法避免角色访问控制无法适应多环境多系统的短板，同时与角色访问控制的结合，失去了属性访问控制的灵活性；文献[7]从属性分层出发，一定程度上缓解了云环境中属性集庞大的问题，却没能从根本解决云环境中属性集的多元化、多样性问题；文献[9]则针对单授权中心造成性能瓶颈问题，提出多授权中心的属性访问控制模型，但存在属性回收引起多授权中心属性冲突以及无法解决用户权限回收的问题；文献[10]针对用户权限回收问题，结合属性加密算法，从密钥更新方面提出一种懒惰权限回收机制，同样存在重加密引起的密钥更新及懒惰回收机制中重加密时间不确定性引起的安全隐患问题，而且无法解决只读数据的重加密问题。

此外，目前国内外尚无学者针对公有云提出数据共享的访问控制策略，现有的云存储系统都是默认公有云中数据对所有用户是可以无限制访问的，针对云用户向特定群体进行数据共享的需求尚未见解决方案。

在访问控制策略的描述方法方面，国内外学者也进行了很多的研究，并有一些已经进入到实用阶段，结构化信息标准促进组织（OASIS）还制定了 XACML 策略描述语言标准。英国伦敦大学的 Royal Holloway 等人在研究过程中发现，诸如 XACML 这样的策略描述语言都没有一个良好定义的丰富的语言特征集，即使是开放环境中的基于属性的访问控制也没有满足这一点。基于此，他们在策略目标语言（PTL）和策略生成语言（PCL）的基础上提出了 PTaCL 语言，该语言具有丰富的语言特征集，能够支持更广的策略域，但同时也增加了访问控制策略的不确定性。加拿大魁北克大学的 Nadera Slimani 等人认为现有的访问控制模型语言都是建立在一定的访问控制模型上，因此仅为设计的模型服务，他们提出了一种基于 XML 的元数据访问控制技术，该方案适用于多种访问控制模型，从而增强了访问控制策略描述语言的灵活性和泛用性。但其缺点也较为明显，不同的访问控制模型针对的对象特征不同，例如基于属性的访问控制使用的是请求者所具有的属性特征，基于角色的访问控制使用的是用户的身份，两者使用授权的实体依据具有较大的差别，决策器的授权过程也不同，单纯的统一描述并不能让访问控制策略起到良好的作用。沃特福德理工学院 Steven Davy 等人提出一种语言驱动的方法来描述访问控制策略，该方案能够确保访问控制高效执行，底层访问控制策略能够良好地反应制定者的目的和意图，使得访问策略更加明确且结构化。不过，访问控制策略能否准确灵活地执行、语意是否明确是该设计的一个重要问题。美国匹兹堡大学的 Yann Le Gall 提出一种名为 PlexC 的策略描述语言，该语言能够控制社交网络中信息的传播，降低了人为干预访问控制授权的影响；另一方面，该方案也解决了隐私相关的一些风险，能更好地适应动态环境。但该方案缺乏授权的精确性，尤其是在社交网络中人际网络比较复杂的情况下，该方案不能准确地反应策略制定者的意图。

由上可知，关于访问控制策略描述语言的研究，国内外学者主要集中在策略描述语言与访问控制模型之间的契合，针对云环境下的特定场景和公有云中的访问控制策略描述的研究目前还很缺乏，随着云存储数据共享服务的推广，数据创

建者会越来越期望访问策略的制定能够方便、简洁，最好能以自然语言的方式来表达。这样一来，针对基于不同访问策略的数据的访问请求，策略决策器的设计会变得更加复杂，因此迫切需要研究针对云环境下访问策略的统一描述方法，灵活地表达不同数据共享空间的访问策略，且易于解析其中的语义

二、预计需达到的要求，预计的技术关键、技术方案和主要实验研究情况

2.1 预计需达到的要求

本论文将围绕当前主流云存储系统提供的三种不同的数据共享方式，结合云用户的特点，以及不同数据空间对访问控制策略的需求不同，研究一种动态灵活的多模式协作的安全访问控制机制，和灵活有效的云环境下访问控制策略描述方法，在面对复杂、易变的庞大用户群体访问时，能够快速地解析出访问策略语义，及时地判断用户在当前时域的访问权限；同时，为解决机密数据的安全性，设计并实现一种高效的用户权限回收方案。

2.2 研究内容

1) 高效、灵活的多模式访问控制

云存储系统中，如何才能最大限度的满足用户个性化需求成为当前国内学术界、工业界的一个新的研究热点。在现有作为数据备份的云存储系统上，结合基于身份访问控制与基于属性访问控制的优点，针对用户个人空间及组空间，构建一种适用于满足用户个性化需求的数据共享的多模式访问控制机制，以此实现安全的数据共享。

针对小范围群体，用户数可控，且分布相对集中、人员相对稳定、互信任度较高，此时可采用计算复杂度较低的基于身份的访问控制模式，采用访问控制列表（ACL）组织和管理云资源的访问控制策略，以此实现高效细粒度的数据共享;组空间内用户互熟悉度较低,且分布散、基量大、变动频繁，采用基于属性的访问控制一方面能制定灵活的数据共享方式，通过用户属性

与访问策略之间的契合度来确定用户的访问权限，另一方面存储及性能开销相对稳定，以此解决 ACL 随用户量直线上升的性能波动问题。

2) 用户权限回收解决机制

研究云存储系统中，如何高效、安全的实现用户权限回收，以及由此引入的密文重加密问题。传统的立即回收机制中，对于回收权限用户所有可访问的数据均需要实现重加密处理，即首先进行密文解密，然后采用生成新的加密密钥对原文重加密再上传云端，这将带来严重的性能开销，尤其是云存储系统中，庞大用户、海量资源的背景下，用户权限变更的高频性、可访问资源的庞大性，更加大了重加密的性能开销；学术界普遍采用的懒惰回收机制，在拥有特定权限用户执行写操作时，再进行重加密处理，由于执行写操作的不可控性，可能造成只读资源将无法执行重加密，因此回收权限用户密钥将一直有效，将造成严重的安全隐患。此外，即便该资源拥有写操作，由于懒惰回收机制中，允许撤销权限用户在资源未被重加密处理之前进行数据访问处理，因此，将无法干预撤销权限用户再次期间对数据进行写脏数据。

为此，研究一种高效的立即权限回收机制，设计一种基于密文掷乱处理算法，在云端进行代理密文掷乱算法处理，以此实现高效、安全、可靠的立即回收机制。

2.3 技术方案

1)多模式安全访问控制的协作模型

结合云用户的特点，以及不同数据空间对访问控制策略的需求不同，设计出一种灵活、简洁的访问策略统一描述语言，抽象用户行为特征，将用户行为属性和静态属性相结合，实现一种多模式访问控制模型，以解决用户多样化的数据共享需求。该模型的整体结构如图 1 所示。

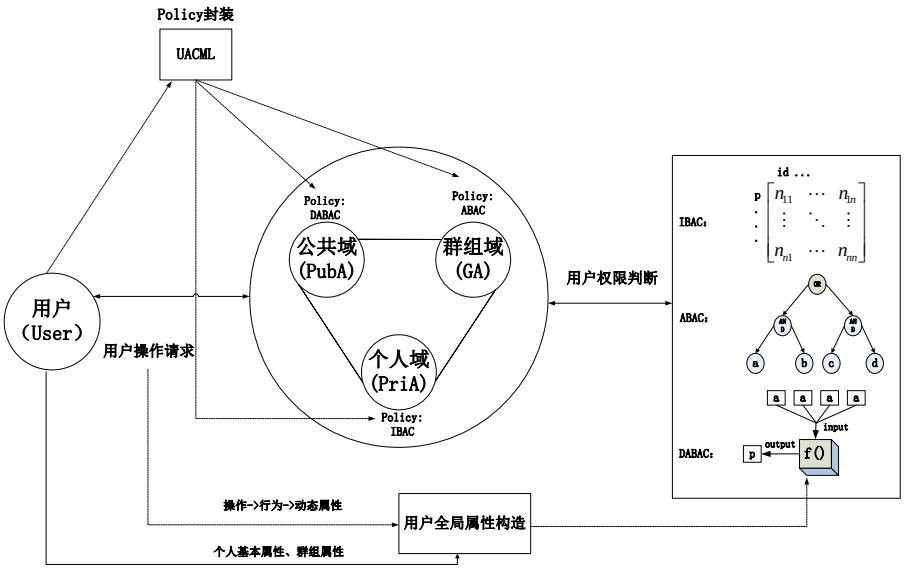

图 1 多模式访问控制模型

2) 多模式访问策略

在云存储系统中，用户对应可访问的数据主要位于个人空间、组空间、公共空间，如图 2 所示。在这三个空间中，用户可访问的资源不同，数据访问控制的需求不同。

个人空间主要存放用户私人数据，因此提供的数据共享主要是针对用户面向个人好友的特定数据共享，因此，在这个空间中我们将数据限定于所有者个人访问，采用基于身份的访问控制来实现

组空间主要是在一些共同特征的基础上建立，即在本系统中主要是以拥有共同类型的属性集合为前提进行的划分，因此同一个组空间的用户数是在一定程度上可以预知的，用户互熟悉度较低，且分布散、基量大、变动频繁，在组内空间我们则采用基于静态属性的访问控制来实现

公共空间，这里我们主要是指一种侠义的公共空间，即用户的属性集不确定，用户特征无法明确，属性值动态变动，用户频繁加入退出的情况。因此，我们主要采用一种基于动态属性的访问控制方法来实现数据共享

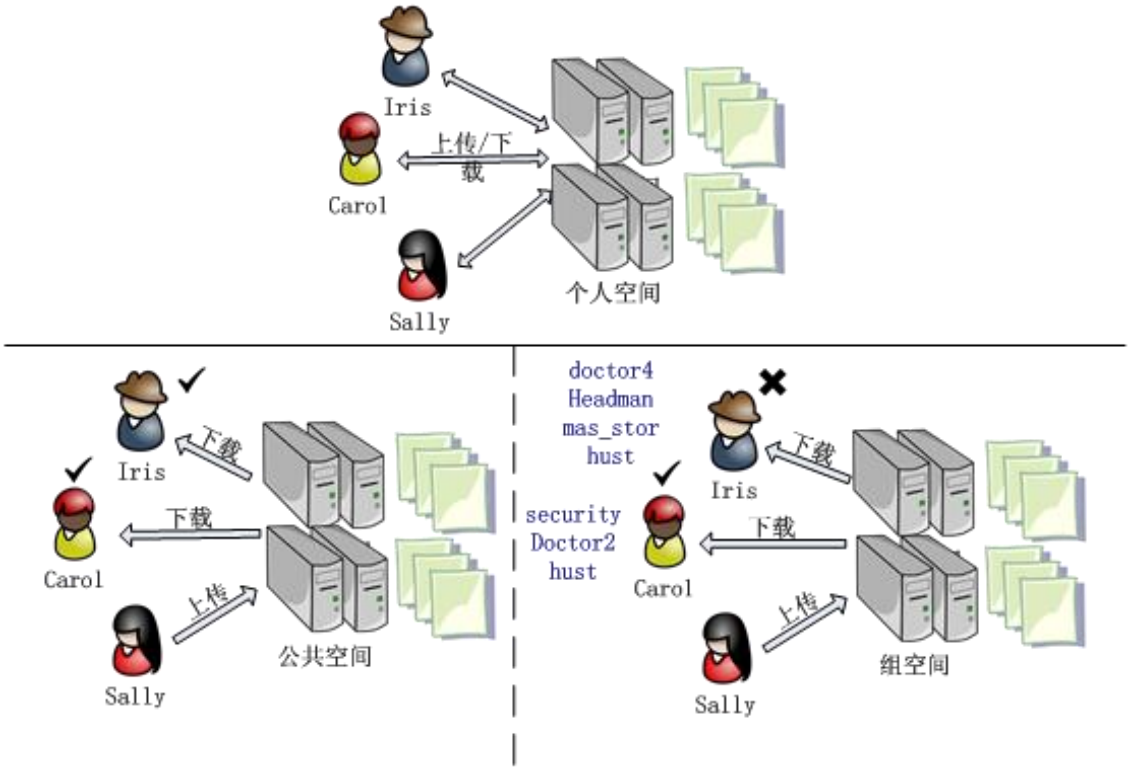

图 2 云存储空间

3) 用户权限回收机制

由于用户权限回收引起的重加密问题，我们拟设计一种采用基于密文的置乱算法，采用立即回收方案，对密文进行代理置乱算法处理，并利用令牌机制保存置乱规则，合法用户利用解密密钥及令牌以获得原始数据。

置乱算法原理如下：

1. 云端首先将上传的密文数据分为$(n\times n-m)$块，利用随机算法生成m块大小与密文数据块大小相同的二进制置乱块；
2. 将生成的n块置乱块随机插入密文，得到新的密文并保存，同时维护一张$n\times n$矩阵表 A，其中置乱块对应内容为 0，密文块对应内容为 1，如：

$$\begin{bmatrix} n_{11} & \cdots & n_{1n} \\ \vdots & \ddots & \vdots \\ n_{n1} & \cdots & n_{nn} \end{bmatrix} \text{其中} n_{ij} \text{取 1 或者 0}$$

3. 令牌保存一张 n 阶方阵 B，其满足公式:，其中 I 为单位阵，计算并将得

到的方阵作为密文元数据保存；

4. 用户获取原始数据，首先得利用授权中心赋予的令牌与获得密文元数据进行矩阵乘积运算，得到矩阵，然后利用得到的矩阵内容去除插入密文的置乱块；最后利用解密密钥获得原文；

   如理如下：

   $A \times B = C \qquad B \times B = nI$

   $C \times B = A \times B \times B = A \times (B \times B) = A \times (nI) = nA$

5. 用户权限回收时，由授权中心发给云端原始令牌及一个新的令牌，云端首先利用原始令牌剔除密文中的置乱块，然后利用新的令牌对密文数据进行如步骤 1、2 的代理置乱处理，并更新元数据中的矩阵表；合法权限用户则通过原始密钥及更新的令牌进行数据访问。

三 参考文献

【1】 Zhou T, Wang Q, Xu C. Concept Alignment in Attribute Based Access Control[C]//Multimedia Information Networking and Security (MINES), 2010 International Conference on. IEEE, 2010: 536-540.

【2】 洪澄, 张敏, 冯登国. 面向云存储的高效动态密文访问控制方法[J]. 通信学报, 2011, 32(7): 125-132.

【3】 冯登国, 张敏, 张妍, 等. 云计算安全研究[J]. 软件学报, 2011, 22(1).

【4】 Kandala S, Sandhu R, Bhamidipati V. An attribute based framework for risk-adaptive access control models[C]//Availability, Reliability and Security (ARES), 2011 Sixth International Conference on. IEEE, 2011: 236-241.

【5】 Hur J, Noh D K. Attribute-based access control with efficient revocation in data outsourcing systems[J]. Parallel and Distributed Systems, IEEE Transactions on, 2011, 22(7): 1214-1221.

【6】 Mon E E, Naing T T. The privacy-aware access control system using attribute-and role-based access control in private cloud[C]//Broadband Network and Multimedia Technology (IC-BNMT), 2011 4th IEEE International

Conference on. IEEE, 2011: 447-451.

【7】 Wan Z, Liu J, Deng R H. HASBE: A hierarchical attribute-based solution for flexible and scalable access control in cloud computing[J]. Information Forensics and Security, IEEE Transactions on, 2012, 7(2): 743-754.

【8】 林果园, 贺珊, 黄皓, 等. 基于行为的云计算访问控制安全模型[J]. 通信学报, 2012, 33(3): 59-66.

【9】 Yang K, Jia X. Attributed-based access control for multi-authority systems in cloud storage[C]//Distributed Computing Systems (ICDCS), 2012 IEEE 32nd International Conference on. IEEE, 2012: 536-545.

【10】 Xu Z, Martin K M. Dynamic User Revocation and Key Refreshing for Attribute-Based Encryption in Cloud Storage[C]//Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on. IEEE, 2012: 844-849.

【11】 熊金波, 姚志强, 马建峰, 等. 基于行为的结构化文档多级访问控制[J]. 计算机研究与发展, 2013, 50(7): 1399-1408.

研　究　生　签　字 _____

指　导　教　师　签　字 _____

院(系、所)领导签字 _____

年　　月　　日