基于 CP-ABE 算法的云存储数据访问控制

孙国梓[1,2,3]，董宇[1,2,3]，李云[1,2,3]

(1. 南京邮电大学 计算机学院，江苏 南京 210003；2. 江苏省无线传感网高技术研究重点实验室，江苏 南京 210003；
3. 南京邮电大学 宽带无线通信与传感网技术教育部重点实验室，江苏 南京 210003)

摘 要：针对云存储服务网络特性和数据共享特性安全问题，提出一种基于 CP-ABE 算法的密文访问控制机制。从访问权限控制及访问控制体系结构 2 个方面对上述访问控制机制进行研究。给出相应的安全算法数据结构，并对其进行了仿真和性能分析。该安全机制在服务提供商不可信的前提下，保证在开放环境下云存储系统中数据的安全性，并通过属性管理降低权限管理的复杂度。

关键词：云存储；存储安全；访问控制；CP-ABE 算法

中图分类号：TP393 **文献标识码**：A **文章编号**：1000-436X(2011)07-0146-07

CP-ABE based data access control for cloud storage

SUN Guo-zi[1,2,3], DONG Yu[1,2,3], LI Yun[1,2,3]

(1. College of Computer, Nanjing University of Posts & Telecommunications, Nanjing 210003, China;
2. Jiangsu High Technology Research Key Laboratory for Wireless Sensor Networks, Nanjing 210003, China;
3. Key Lab of Broadband Wireless Communication and Sensor Network Technology, Ministry of Education,
Nanjing University of Posts & Telecommunications, Nanjing 210003, China)

Abstract: To solve the safety issues in cloud storage services for network characteristics and data sharing characteristics, and based on the CP-ABE (cipertext policy–attribute based encryption) algorithm, a cipher text access control mechanism was proposed. According to access control and related architecture, the corresponding secure data structure algorithms were given. After this, the simulations and the performance analysis were given to evaluate our algorithm. Under the premise of untrusted service provider, the proposed mechanism can ensure the data security of the cloud storage system in an open environment, and can reduce right management complexity through property management.

Key words: cloud storage; storage security; access control; CP-ABE algorithms

1 引言

云存储是在云计算基础上延伸、发展出来的。与云计算系统相比，云存储可以认为是配置了大容量存储空间的一个云计算系统[1]，但从架构模型来看，云存储系统比云计算系统多了一个存储层，并且在基础管理中也增加了与数据管理和数据安全有关的功能。

从云计算诞生，安全性一直是企业实施云计算首要考虑的问题之一。同样在云存储方面，安全仍

收稿日期：2011-03-01；修回日期：2011-06-21

基金项目：国家自然科学基金资助项目（61073114）；国家“十一五”科技支撑计划基金资助项目（2007BAK34B06）；江苏省高校自然科学基金资助项目（09KJD520007）；江苏省高校优势学科建设工程基金资助项目

Foundation Items: The National Natural Science Foundation of China (61073114); The 11th Five Years Plans of the National Key Technology R&D Program (2007BAK34B06); The Universities Natural Science Foundation of Jiangsu Province (09KJD520007); Project Funded by the Priority Academic Program Development of Jiangsu Higher Education Institutions

是首要考虑的问题[2]。访问控制是实现用户数据机密性和进行隐私保护的重要手段。在云存储系统中的服务器应假设为是不可信的，服务提供商可能会因为经济利益或者权利等关系在不经用户允许的情况下违反既定访问控制策略，将用户数据交予第三方，从而造成数据信息泄露。因此，用户不愿意将核心机密信息放到云存储系统中，即使是明文数据，用户也会担心被非授权用户读取或引用，这使得云存储服务应用的发展受到了限制。

云存储的安全可以从以下方面进行考虑：通过加密机制增强存储系统的安全性，主要保证数据的机密性和完整性；使用防篡改技术，主要针对数据的完整性；使用备份和冗余技术，二者分别从时间和空间维度上保证系统的可用性；使用访问授权与认证服务技术，保证非授权用户没有资格访问特定的数据。

2　云存储的访问控制机制

访问控制机制可授权合法用户访问特定资源，同时拒绝非法用户的访问。授权方法一般分为 2 类：访问控制模型和密文机制。访问控制模型就是按照特定的访问策略建立若干角色，通过检查访问者的角色，控制对数据或系统的访问。密码机制通过加密数据使得只有具备相应密钥的授权人员才能解密密文。密文访问控制技术可在服务器端不可信的环境中保证数据的机密性。数据所有者在数据进行存储之前预先对其进行加密，通过控制用户对密钥的获取来实现访问控制目标，这要求加密密钥必须由数据所有者自己生成并管理。目前已提出了大量层次访问控制的密码解决方案。其中，文献[3]在详细分析了文献[4]等的基础上提出了一种简单有效的利用混合密码体制来实现层次访问控制的方案 CBHAC。CBHAC 利用对称加密体制实现数据的加密，利用非对称加密体制实现数据加密密钥的保护，其实现方案如下。

假设每一个用户的密钥对为（SK_i，PK_i），并且有 l 个祖先节点：$U_{i_1},U_{i_2},\cdots,U_{i_l}$。

加密：U_i 选择 K 作为对称密钥，用于数据加密。加密数据项 m 为 $C_m=\{m\}_K$。然后 U_i 利用 $E_{PK_{i_1}}(K)$, $E_{PK_{i_2}}(K),\cdots,E_{PK_{i_l}}(K)$ 分别加密 K，结果为 $c_k=E_{PK_{i_1}}\|E_{PK_{i_2}}\|\cdots\|E_{PK_{i_l}}$，$c_k$ 和 C_m 一起存档。

解密：对于 U_i 的任一祖先节点 U_{i_j}，为访问 U_i 的数据，U_{i_j} 首先要得到 c_k 以及分配给它的部分 $E_{PK_{i_j}}(K)$，然后利用其私钥 SK_{i_j} 计算 $D_{PK_{i_j}}(E_{PK_{i_j}}(K))$，得到 K，最后 U_{i_j} 使用 K 解密 C_m 得到 m。

如果一个用户不希望它的某些祖先节点访问它的数据或者希望其他一些不是其祖先节点的用户访问其数据，用户可以从 c_k 中删除不希望的 $E_{PK_i}(K)$ 或者将希望的 $E_{PK_i}(K)$ 包括在 c_k 之中。

虽然 CBHAC 访问控制具有足够的安全性，并且实现了密文访问控制功能，但是对于每个有权限访问文件的其他用户，文件所有者都必须利用访问者的公钥对文件的对称加密密钥加密，当更改用户权限时，为保证文件机密性，对称加密密钥将更新，从而加密计算将重新执行，在云存储的多用户应用环境下，共享机密文件将给文件所有者带来的密钥存储、更新及维护代价都是难以接受的。

基于属性的密码体制自 2005 年开始研究，其发展了传统的基于身份密码体制关于身份的概念，将身份看作是一系列属性的集合。Sahai 与 Waters 第一次提出基于模糊身份加密[5]，将生物学特性直接作为身份信息应用于基于身份的加密方案中，Sahai 在论文中引入了属性的概念，2006 年，Goyal 等人在基于模糊身份加密方案的基础上提出了基于属性的加密方案(ABE, attribute-based encryption)[6]。2007 年，Bethencourt 等人提出了密文策略的基于属性的加密方案(CP-ABE, cipertext-policy ABE)[7]，将用户的身份表示为一个属性集合，而加密数据则与访问控制结构相关联，一个用户能否解密密文，取决于密文所关联的属性集合与用户身份对应的访问控制结构是否匹配。

本文在基于密文属性的加密算法 CP-ABE 的基础上，提出了云存储数据安全访问控制方案。相比数据所有者直接进行分布式分发密钥的方法，基于 CP-ABE 的方法与服务器集中管理密钥分发的方式相似，更容易管理密钥，同时也对用户更透明，即少让用户涉及密钥生成、密钥发布等事务。

3　CPE-ABE 算法

定义 1　属性。

设 $P=\{P_1,P_2,\cdots,P_n\}$ 为所有属性的集合，则每个用户的属性 A 是 P 的一个非空子集，$A\subseteq\{P_1,P_2,\cdots,P_n\}$，那么 N 个属性可用于鉴别 2^N 个用户。

定义 2　访问结构。

访问结构 T 是全集$\{P_1,P_2,\cdots,P_n\}$的一个非空子集，$T \subseteq 2^{\{P_1,P_2,\cdots,P_n\}} \setminus \{\phi\}$。$T$ 代表一个属性判断条件：在 T 中的属性集合称为授权集，不在 T 中的属性集合称为非授权集。

定义 3 访问树。

访问树用于描述一个访问结构，树的每个叶节点代表一个属性项，每个内部节点代表一个关系函数，关系函数可以是 AND(n of n)、OR(1of n)以及 n of m(m>n)门限等。实现过程中，访问树中的每一个节点（包括叶节点）都可定义一个多项式，节点的遍历方式为由根节点开始从上向下，从左向右的先序遍历方法。

CP-ABE 算法主要包含 4 个步骤。

1) Setup。生成主密钥 MK 和公开参数 PK。

2) $CT = Encrypt(PK, M, T)$。使用 PK、访问结构 T 和加密数据明文 M，加密后的密文为 CT。

3) $SK = KeyGen(MK, A)$。使用 MK 和用户属性集 A 生成用户的私钥 SK。

4) $M = Decrypt(CT, SK)$。使用私钥 SK 解密密文 CT 得到明文 M。

4 基于 CP-ABE 云存储数据访问控制

4.1 访问权限控制

用户对云存储系统中数据的最基本操作为读或写操作，一般具有写权限的用户也具有读权限，但由于应用的对象不同，也会出现其他的访问权限，比如说备份、拷贝、引用等，所以在设计访问控制策略的同时也要考虑其扩展性问题。首先，为了区分读写权限，可选用一对公私钥对（考虑到用户私钥的颁发过程中可能存在安全性问题，一般选用一次性会话密钥作加密[8]）来控制读写权限，在非对称密码体制中，私钥用来签名，公钥用来进行验证。假设签名/验证密钥为 $K_{\text{sign}}/K_{\text{verify}}$，那么 K_{sign} 对应读写权限，将其授予可写用户，在用户执行写操作后对数据进行签名；K_{verify} 对应读权限，将其授予只读用户，用于对签名结果验证。假设存在扩展权限 $Au_1, Au_2, \cdots, Au_n$，数据所有者可设置其权限特征值为 $X_1, X_2, \cdots, X_n$，即用 $X_1, X_2, \cdots, X_n$ 代表访问权限 $Au_1, Au_2, \cdots, Au_n$。

4.2 访问控制体系结构

云存储系统中每个用户拥有一个公私钥对 K_{pub}、K_{priv}，其中，K_{pub} 存储在用户证书中，对外公开；K_{priv} 由用户私有，存储在客户端。K_{priv} 用于信息签名，以保证信息来源的真实性，K_{pub} 则由其他用户验证信息来源的真实性。

下面主要对加密存储数据的访问控制体系结构进行描述。

4.2.1 读写权限控制

存储系统中每个需要保密的文件 F 都具有一个 AES 对称密钥 K_d，K_d 在文件创建时由数据所有者或者文件服务器生成，加密存储在服务器上，一个 RSA 公私钥对 $K_{\text{sign}}/K_{\text{verify}}$ 用于对加密后的数据进行签名/验证，读写用户要访问数据就应该持有 K_d、K_{verify} 和 K_{sign}，只写用户需持有 K_d 和 K_{verify}。数据密文 $E(F)$和签名 $SIG(F)$分别保存在存储端和元数据服务器上。

文件所有者将具有相同访问属性的密钥集中存放到密钥体中，为了保证密钥信息的安全性，采用 CP-ABE 算法将其加密，即 $Encrypt(PK, \{K_d, K_{\text{sign}} / K_{\text{verify}}\}, T)$，假设具有读写权限的用户访问结构为 T_{rw}，对应的密文为 $CT_{rw} = Encrypt(PK, \{K_d, K_{\text{sign}}, K_{\text{verify}}\}, T_{rw})$，具有只读访问权限的用户访问结构为 T_{ro}，对应的密文为 $CT_{ro} = Encrypt(PK, \{K_d, K_{\text{verify}}\}, T_{ro})$。文件所有者为每个用户设定属性值 A_i，然后计算生成用户的私钥 $SK_i = KeyGen(MK, A_i)$，并用访问者的公钥安全发送给各个用户，其中，文件所有者维护主密钥 MK 和公开参数 PK，并且默认具有读写权限。此外，为了保证文件体的真实性，文件创建者还要对文件体用自己的私钥 K_{priv} 进行签名。

以下以用户 U 读写文件 F 为例，描述对数据进行读写的流程。

1) 读数据。

U 通过认证后从服务器读取文件体，在文件体中查询相应的数据项获取 CT_{ro} 信息；

U 使用 $Decrypt(CT_{ro}, SK_U)$ 得到 K_d 和 K_{verify}；

U 从云存储系统中获取加密文件 $E(F)$和签名 $SIG(F)$；

U 使用 K_{verify} 验证签名 $SIG(F)$的正确性；

U 使用 K_d 解密 $E(F)$得到数据明文。

2) 写数据。

U 在文件体中查询相应的数据项获取 CT_{rw}；

U 使用 $Decrypt(CT_{rw}, SK_U)$ 得到 K_d 和 K_{sign}；

U 使用 K_d 加密文件 F 得到 $E(F)$，并使用 K_{sign}

对 $E(F)$进行签名得到 $SIG(F)$；

U 将 $E(F)$和 $SIG(F)$发送到云存储系统中。

以下仅以数据所有者 Owner 授予/撤销用户 U'读写文件 F 的权限为例，描述用户对数据进行访问控制权限的更改。其中，$A_{U'}$ 表示为用户 U'的属性值。

1) 授予读写权限。

Owner 在密钥体中查询相应的数据项获取 CT_{rw}；

Owner 使用 $Decrypt(CT_{\mathrm{rw}}, SK_{U'})$ 得到 K_d、K_{sign}、K_{verify}；

Owner 生成新的访问结构 $T' = T \vee V_{U'}$；

Owner 生成新的数据项 $CT'_{\mathrm{rw}} = Encrypt(PK, \{K_d, K_{\mathrm{sign}}, K_{\mathrm{verify}}\}, T')$；

Owner 将 F 的密钥体中的原 CT_{rw} 替换为 CT'_{rw}。

2) 撤销读写权限。

定义 $\sim V_{U'}$ 为 U'的补集中所有属性的析取，$\sim V_{U'} = P_1 \vee P_2 \vee \cdots \vee P_N, P_i \in C(V_{U'})$；

Owner 生成新的数据密钥 K'_d，新的签名/验证密钥 K'_{sign}, K'_{verify}；

Owner 生成新的访问结构 $T' = T \vee \sim V_U$；

Owner 生成新的数据项 $CT'_{\mathrm{rw}} = Encrypt(PK, \{K_d, K'_{\mathrm{sign}}, K_{\mathrm{verify}}\}, T')$，$CT'_{\mathrm{ro}} = (PK, \{K'_d, K'_{\mathrm{verify}}\}, T')$；

Owner 对文件 F 使用 K'_{sign} 重新进行签名；

Owner 将文件 F 对应的密钥体中的 CT_{rw} 和 CT_{ro} 替换为 CT'_{rw} 和 CT'_{ro}。

4.2.2 扩展权限控制

假设数据所有者 Owner 设定特征值 X 代表访问权限 Au_x。

1) 权限设置。

Owner 维护主密钥 MK_{Au_x} 与公开参数 PK_{Au_x}；

为每个用户生成私钥 $SK_i = KeyGen(MK_{Au_x}, A_i)$；

Owner 选取特征值 X 代表访问权限 Au_x，将 X 安全发送到元数据服务器，并存入文件的元数据信息中；

Owner 生成访问结构 T_{Au_x}；

Owner 生成权限数据项：$CT_{Au_x} = Encrypt(PK, X, T_{Au_x})$；

将 CT_{Au_x} 写入密钥体。

2) 权限获取。

以用户 U 申请授权为例，对权限获取描述如下。

U 通过认证后从服务器读取密钥体，在密钥体中查询相应的数据项获取 CT_{Au_x}；

U 使用 $Decrypt(CT_{Au_x}, SK_U)$ 得到 X；

U 向认证服务器发送认证请求，其中包含有 X；

认证服务器将 U 认证请求中的 X 与从元数据服务器获得的属性特征值进行匹配，匹配成功 U 将获得数据的访问权限 Au_x。

用户撤销情况与读写访问权限撤销类似，只是特征值在密钥体与文件元数据信息中需同步更新。

假如用户数据选择明文存储，那么只需将密文存储中读写权限数据项中的密钥信息去除，即只包含读写权限信息，明文读写权限撤销过程与密文存储类似，只是缺少加密及加密密钥更新过程，对于扩展权限的控制过程，明文存储与密文存储相同，故不再重复。

该安全访问控制策略具有以下特点。

1) 提供数据加密机制，允许用户对其所存信息进行加密/解密，并且将对称和非对称密钥系统有效结合，在保护数据机密性的前提下，降低了加密密钥管理的复杂度。

2) 实现了在服务器不可信的情况下，保证存储系统中数据的机密性、完整性及用户不可抵赖性，并且简化了数据访问控制中的权限变更过程，减轻了密钥管理复杂度。

3) 提供一个像 AFS 一样的访问控制清单(ACL, access control list)。云存储系统通过 ACL 提供给一个用户组中的多用户共享一个文件的信息，多用户可按照属性组成一个组，共享一个对该目录中的文件加密的密钥。

4) 基于 CP-ABE 的方法将生成访问控制的权利交给数据所有者，这样让数据所有者拥有更多的选择权限，即对用户更友好，数据所有者可以自主方便地选择用户访问文件。

在基于密文的访问控制中，用户权限撤销操作发生后，数据所有者将更改文件体中相关的密钥信息，并用新的文件密钥重新加密文件，这在云存储环境中会导致严重的系统性能问题，对此可效仿 Plutus[9]系统，在撤销行为发生后，文件所有者将该数据的密钥 K 更换为 K'（此时具有写权限的用户会有 2 个数据密钥：K 和 K'），但是并不立即使用 K' 对数据进行重新加密，而是将 K'发布给所有有写权限的用户，当用户执行写操作时才使用 K'加密数据，然后丢弃 K，以后读取数据均使用 K'。文件重加密之前被撤销用户仍然可以用缓存的文件对称

密钥读取文件，但不能修改文件，考虑到被撤销用户原来就具有读权限，因此可以认为懒惰重加密所带来的旧数据泄露造成的损失是可以接受的。

5 安全算法数据结构

本文中涉及的安全算法有证书体、访问权限体、密钥体和文件体 4 种数据结构，其中证书体和访问权限体位于认证服务器上，文件体是由文件的属性元数据及组成该文件的一个或多个数据块（密文或明文）组成，分别位于元数据服务器和相应的存储节点中，密钥体也位于认证服务器上。

在云存储系统中，对用户身份的认证是经过专门的认证服务器完成，认证过程基于多个信任证书文件。证书文件格式如图 1 所示。一个证书体包括多个清单，每个清单由用户 ID、用户公钥、用户口令和时间戳组成。用户 ID 标明清单后各项所属的用户或组；用户公钥存储在认证服务器上，方便用户查询；口令是认证服务器用来认证用户身份的。用户的口令是被加密存放在认证服务器的非易失存储器中。当启动认证服务时，证书文件被装载到内存中，用户口令被解密和缓存在内存中。时间戳记录用户修改其口令的时间。

证书文件 ID			
用户 ID	用户口令	用户公钥	时间戳
用户 ID	用户口令	用户公钥	时间戳
⋮			
用户 ID	用户口令	用户公钥	时间戳

图 1 证书体格式

在认证服务器中，除存放用户证书文件外，还存放有用户区分用户访问权限的数据库。每个用户在使用云存储系统服务注册时，认证服务器都会为该用户生成一条用户的访问权限记录，并存在认证服务器相应的数据库中。当用户登录云存储系统时，认证服务器将该用户的访问权限信息发给元数据服务器，元数据服务器根据该信息对用户提供存储服务。访问权限记录如图 2 所示。

用户或组 ID 是用户或组在系统注册时的 ID；文件清单是该用户或组可以访问的文件清单。权限记录中包含文件安全级别及共享方式，基于 CP-ABE 算法的级别应为自加密，允许多用户共享，在访问权限记录中也可设置时间戳选项来记录权限记录发生改变的情况。

用户或组 ID	文件清单	安全级别	共享方式	时间戳
用户或组 ID	文件清单	安全级别	共享方式	时间戳
⋮				
用户或组 ID	文件清单	安全级别	共享方式	时间戳

图 2 访问权限记录

文件体的结构如图 3 所示，其数据块为明文或者使用 AES 对称密钥加密的密文，数据块是系统中能读/写的最小单元。文件 ID 是在存储系统中文件对象的唯一标识，ACV 是访问控制版本号，创建者为创建文件的用户，授权特征值包括读写权限及其他扩展权限，块校验和（block check sum）与其对应的数据块指针存放在一起。

文件 ID	ACV
创建者	
授权特征值 X_1，X_2，…，X_n	
长度、建立时间、修改时间	
Hash（File）	
块校验和	数据块指针
0x1334	指向 Block（明文或密文）
⋮	⋮
0xBA41	指向 Block（明文或密文）

图 3 文件体结构

密钥体的结构如图 4 所示，其中文件 ID 唯一标识该密钥体，文件 ID 以下每一行都包含一个用户 ID 和加密的密钥及时间戳。密钥体中包含了利用 CP-ABE 算法加密的文件加密密钥信息，即 CT_{rw}、CT_{ro} 以及其他扩展权限信息等。

文件 ID	
创建者	
时间戳	
$E_{K_{\mathrm{priv}}}$(Hashkey file)	
CT_{rw}	CT_{ro}
CT_{Au_1}	
⋮	
CT_{Au_n}	

图 4 共享文件的密钥体结构

当用户访问云存储中的文件时，首先必须通过口令认证自己的身份。如果通过认证，认证服务器返回确认信息的同时也会发给该用户一个资格证，用户持有资格证才能访问云存储系统中的加密文件。该资格证书中主要包括从密钥体中读取的加密密钥信息 *CT*，即文件加密密钥 K_d 和签名/验证密钥。当用户读取 *CT* 后，在客户端用文件所有者分发的私钥对其解密获得加密文件的密钥，可用该密钥在客户端将从云存储系统中读取的密文进行解密得到明文。当用户向存储系统中相应的目录写文件时，在客户端利用该密钥对文件加密并用 K_{sign} 签名。

证书体、访问权限体、密钥体和文件体之间的关系如图 5 所示。

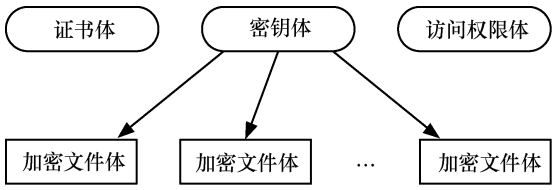

图 5　证书体、访问权限体、密钥体和文件体之间关系

6　安全性分析

在基于 CP-ABE 算法的访问控制策略中，数据访问者需根据所掌握的密钥信息对云存储中加密存储数据进行相应的访问操作。下面对该访问控制策略的安全性进行如下分析。

1) 数据访问权限的安全管理。在服务提供商不可信的云存储环境中，不让服务提供商参与数据加密密钥的产生与管理，完全由数据所有者对其他用户进行访问授权增加了访问权限管理的安全。

2) 端到端的加密。允许用户在客户端对数据进行加密/解密，保证在数据传输与存储中的机密性。

3) 加密密钥的安全管理。采用混合加密体制（用对称密钥加密数据以保证加密的高效性，用公钥密码体制对加密密钥进行加密）来保证加密密钥不被非法用户所获得。

4) 阻止非法用户破坏合法用户在存储系统中的信息。一方面通过身份认证，另一方面即使非法用户能够破解读取加密数据，在它向合法用户的文件中写数据时，由于不知该用户的签名密钥 K_{sign}，非法修改的数据在传到云存储系统中时也能被检验出来。

7　仿真及性能分析

实验环境：Inter(R) Core(TM) 1.73GHz 的 CPU、1GB 的 DDR2 内存，操作系统为 Windows Server 2003，实验环境构造为：在 VMware Workstation 6.5.2 上安装 Ubuntu 10.10，分配有 1GB 内存。实验中数据对称加密算法采用 128bit AES 密钥，且主要考虑该访问控制策略在云存储服务用户数目增长情况下对系统性能的影响，忽略了数据在分布式网络中的传输延迟。

图 6 显示 CP-ABE 算法中在不同属性个数的情况下，用户根据自身属性集合主密钥 SK 生成用户私钥的时间，可见，私钥生成的时间是随着属性集中属性个数的增长而增长的。

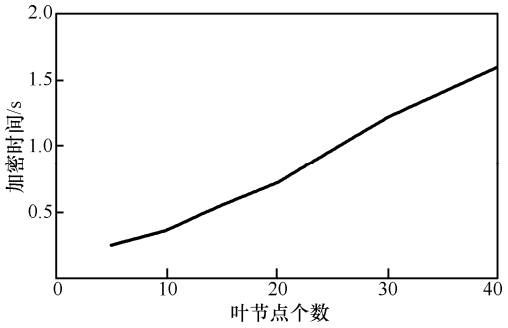

图 6　CP-ABE 算法私钥产生时间

图 7 给出了访问树中不同叶结点数用户对数据对称密钥等信息的加密时间，随着叶结点数的增加，加密时间也加长。

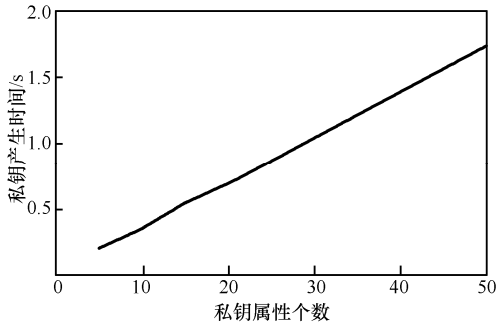

图 7　CP-ABE 算法加密时间

图 8 给出了 CP-ABE 算法属性数为 10，用户数目在 500 以内的情况下，分别采用 CP-ABE 与 CBHAC 访问控制策略进行权限变更时所需时间对比。

图 9 为采用 CP-ABE 和 CBHAC 方法的访问控制策略存储访问控制信息所需空间的比较，实验选取文件数目为 500，属性数 10。

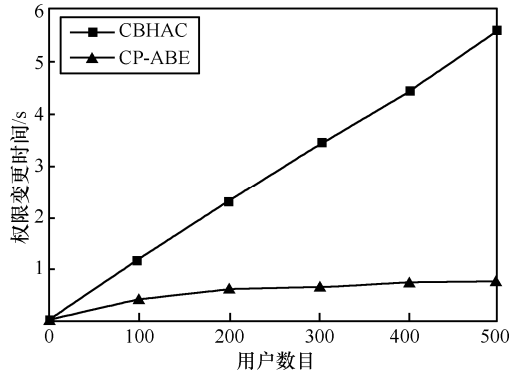

图 8　权限变更时间

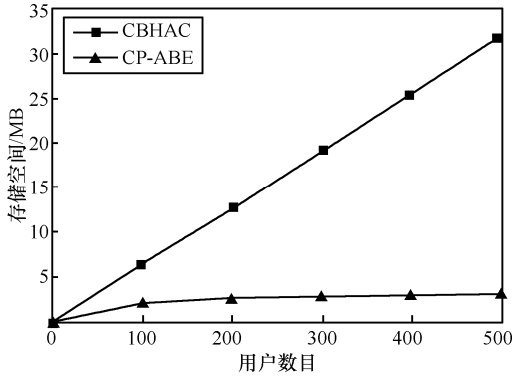

图 9　存储空间比较

实验结果表明，随着用户数目的提升，基于 CP-ABE 的访问控制策略在权限管理及控制文件所用存储空间方面表现出极大的优势。

8　结束语

云存储的安全问题影响着云存储应用的发展，合理有效的访问控制方法能够提高云存储服务用户对云存储服务的信任，同时也应考虑云存储系统的性能代价。引入了基于 CP-ABE 算法的访问控制技术，使得在服务器不可信前提下，利用密码访问控制方法保证用户数据机密性的同时，也实现了密文文件的共享，实验结果表明，该机制降低了权限管理的复杂度以及访问控制信息的存储空间。此外，CP-ABE 算法中对属性条件的设置会影响系统的性能，因此，应对用户属性及访问权限中属性条件的设置进一步研究，使其更好地应用到云存储系统中。

参考文献：

[1] ZHENG W M, XU P Z, HUANG X M, *et al*. Design a cloud storage platform for pervasive computing environments [J]. Cluster Computing, 2010, 13(2): 141-151.

[2] WANG Q, WANG C, REN K. Enabling public auditability and data dynamics for storage security in cloud computing[J]. IEEE Transactions on Parallel and Distributed Systems, 2011, 22(5): 847-859.

[3] 王连强，张剑，吕述望等. 一种基于密码的层次访问控制方案及其分析[J]. 计算机工程与应用, 2005, 33: 7-10.
WANG L Q, ZHANG J, LV S W, *et al*. An efficient cryptosystem based hierarchical access control scheme and its analysis[J]. Computer Engineering and Applications, 2005, 33: 7-10.

[4] RAY I, RAY I, NARASIMHAMURTHI N. A cryptographic solution to implement access control in a hierarchy and more[A]. Proceedings of the Seventh ACM Symposium on Access Control Models and Technologies[C]. Monterey, California, USA, 2002. 65-73.

[5] SAHAI A, WATERS B. Fuzzy identity-based encryption [A]. 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques[C]. Aarhus, Denmark, 2005. 457-473.

[6] GOYAL V, PANDEY O, SAHAI A, *et al*. Attribute based encryption for fine-grained access control of encrypted data[A]. ACM conference on Computer and Communications Security[C]. Alexandria, Virginia, USA, 2006. 89-98.

[7] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-policy attribute-based encryption[A]. 2007 IEEE Symposium on Security and Privacy(SP '07)[C]. Berkeley, California, USA. 2007. 321-334.

[8] 张淼, 徐国爱, 胡正名等. 可信计算环境下基于主机身份的一次性密钥交换协议[J]. 电子与信息学报, 2007, 29(6): 1348-1351.
ZHANG M X, XU G A, HU Z M, *et al*. A host identity based one-time key exchange protocol in trusted computing[J]. Journal of Electronics & Information Technology, 2007, 29(6): 1348-1351.

[9] KALLAHALLA M, RIEDEL E, SWAMINATHAN R, *et al*. Plutus: scalable secure file sharing on untrusted storage [A]. 2nd USENIX Conference on File and Storage Technologies (FAST '03)[C]. San Francisco, CA, 2003. 29-42.

作者简介：

孙国梓（1972-），男，安徽天长人，博士，南京邮电大学副教授，主要研究方向为云存储、电子数据取证、网络与通信安全。

董宇（1986-），女，辽宁朝阳人，南京邮电大学硕士生，主要研究方向为云存储。

李云（1974-），男，安徽望江人，博士，南京邮电大学副教授，主要研究方向为云计算、机器学习。