第47卷第4期 中国科学技术大学学报 Vol.47,No.4
2017年4月 JOURNAL OF UNIVERSITY OF SCIENCE AND TECHNOLOGY OF CHINA Apr. 2017

文章编号:0253-2778(2017)4-0304-07

一种基于节点映射关系的云数据安全代理访问机制

李华康[1,2],刘 盼[1],杨一涛[1],孙国梓[1]

(1.南京邮电大学计算机学院、软件学院,江苏南京 210023;2.江苏省大数据安全与智能处理重点实验室,江苏南京 210023)

摘要:随着移动终端多媒体技术的发展,用户逐渐将本地数据通过各种网络备份到云存储服务器上.云平台在提供廉价便捷的数据存储服务的同时也存在数据安全防护问题,尤其是密文数据访问控制完全依赖于云服务商.为了防止数据被非授权用户和半可信云存储提供商的非法访问,提出一种基于节点映射关系的CP-ABE属性加密算法,即通过属性管理降低权限管理的复杂度.在密文访问控制机制中引入密钥授权中心和安全代理实现存储服务与安全服务异地存储,保证在开放环境下云存储系统中数据的安全性.实验结果表明,这种属性管理机制在少量的系统开销下实现了数据存储与密钥存储的分离,具有较高的应用价值.

关键词:云存储;安全代理;属性加密;CP-ABE;节点映射

中图分类号:TP393 **文献标识码**:A doi:10.3969/j.issn.0253-2778.2017.04.004

引用格式:李华康,刘盼,杨一涛,等. 一种基于节点映射关系的云数据安全代理访问机制[J]. 中国科学技术大学学报,2017,47(4):304-310.

LI Huakang, LIU Pan, YANG Yitao, et al. A cloud storage access scheme with security proxy based on attribute mapping node[J]. Journal of University of Science and Technology of China, 2017,47(4):304-310.

A cloud storage access scheme with security proxy based on attribute mapping node

LI Huakang[1,2], LIU Pan[1], YANG Yitao[1], SUN Guozi[1]

(1. *School of Computer Science & School of Software, Nanjing University of Posts and Telecommunications, Nanjing* 210023, *China*; 2. *Jiangsu Province Key Lab of Big Data Security and Intelligent Processing, Nanjing* 210023, *China*)

Abstract: With the development of mobile technology, more and more people use cloud storage to back up their local data. The cloud platforms provide cheap and convenient data storage services while there are serious data security problems, especially the ciphertext data access control being totally dependent on the cloud provider. An advanced CP-ABE scheme based on mapping nodes was presented to prevent illegal access from unauthorized users or partially trusted cloud storage providers. In order to guarantee the security of cloud data in open environment, Key Generation Center and Security Proxy are introduced to separate the data service and security service in the access scheme. Experimental results show that the proposed attribute management scheme is capable of separating the secret key from data service at a low computational cost, showing great potential for applications.

Key words: cloud storage; security proxy; attribute encryption; CP-ABE; node mapping

收稿日期:2016-08-28;**修回日期**:2016-12-08

基金项目:国家自然科学基金(61502247, 11501302, 61502243, 91646116),国家博士后科学基金(2016M600434),江苏省自然科学基金(BK20140895, BK20150862),江苏省博士后科研资助计划(1601128B)资助.

作者简介:李华康,男,1982年生,博士/讲师,研究方向:智慧城市、大数据应用、互联网安全. E-mail: huakanglee@163.com

通讯作者:孙国梓,博士/教授. E-mail: sun@njupt.edu.cn

0 引言

随着移动终端技术的发展,用户可以便捷地编辑文本、采集多媒体信息,而移动设备有限的存储能力以及更换的短周期特性导致越来越多的用户将数据备份到云服务器.云存储系统虽然廉价便捷,但也存在诸多问题,如传统的安全域划分在云存储上的失效问题、数据传输的安全性问题、数据的可用性和可靠性问题以及数据的安全防护问题.

其中一般用户主要涉及云存储数据的安全防护问题,即加密存储和检索、密文访问控制这两个技术要点.加密存储的主要技术是数据加密,包括用户自己加密和委托 CSP 加密两种方式.由于属性基加密技术[1]简化了用户的密钥管理操作,用户自主加密已成为云存储数据机密性保护的主要方法.同时许多云存储平台也开始提供加密服务,如 Amazon 在 S3 系列为用户提供 AES-256 加密数据服务[2].国内外专家在加密检索方面也提出了许多技术解决方案,如 Song 等提出的加密数据搜索的实用算法[3];Swaminathan 等通过对大量文档进行分析;提出了一种面向保护隐私的预排序搜索算法[4];黄永峰等将加密检索与云存储安全相结合提出的一种基于全同态加密的检索方法[5];Liang 等[6]提出了一种能够不断更新搜索关键字的加密云存储机制.

密文访问控制机制是数据所有者先将数据加密后托管到云端,然后通过线下或者分离的安全信道将解密钥分发给需要解密的授权用户,数据使用者获得密文数据及密钥后解密文件.如早期 Alk 等提出的基于公钥密码算法实现的分级访问控制系统(HAC)[7-8],后来出现了基于非对称加密、单向 Hash、身份基加密、属性基加密等算法实现密文访问控制机制.随着属性基加密技术的发展,研究者提出了一种新的基于"密文策略属性基加密"(CP-ABE)技术[9],该技术能够有效地提高访问策略的灵活性和密钥分发效率,进一步推动了密文访问控制的发展和应用.刘占斌等[10]利用切比雪夫映射的半群体特性实现对密文策略属性基加密,实现了轻量级属性加密的用户授权数据访问.

近年来,随着云存储服务商的增多,频频出现个人隐私数据被泄露事件.一种简单的运营策略是在用户与云存储服务商之间引入安全第三方,然而 CP-ABE 密文访问控制机制因只支持若干个单属性规则属性集,从技术上暂时无法解决.针对这个问题,本文提出一种用户属性集的节点映射机制对 CP-ABE 算法进行改进,并引入密钥授权中心和安全代理两个第三方,实现将用户的安全服务从云服务商分离的云存储密文访问.密钥授权中心负责数据加密的公共参数和私密参数,并授予不同用户不同的访问权限,同时管理密钥有效期属性、密钥属性升级和回收.安全代理负责存储用户数据加密的指纹库,并将秘密属性发给密钥授权中心和云服务器.加密过程中使用对称加密对用户数据进行加密,然后利用密钥分割的方法,优化云存储数据的访问结构树的构造,最后在用户相关属性为主的基本属性基加密的基础上添加一条用户秘密属性,实现密钥的三方管理.该方法在与 CP-ABE 的比较试验中以很小的系统开销导入了第三方可信代理机制,具有很好的技术价值和应用前景.

1 相关研究

基于属性的加密(attribute-based encryption, ABE)最早是由 Sahai 等[11]提出,属于公钥加密体制的加密方法,该方法是由模糊的身份加密(fuzzy IBE)发展而来,很好地实现了细粒度的访问控制问题.ABE 利用用户属性集合访问策略将用户与要访问的数据关联起来,只有当用户的访问属性结构满足访问控制策略时,才能够顺利访问数据.通过这种方法可以使得拥有相同属性集的用户共享一份密文数据,非常适合云存储环境中的数据共享场景.在云计算领域,很多学者已经将基于属性的加密方法应用到访问控制方案中,实现了更细粒度的访问控制和数据共享的目标[12-14].

为了加强分布式、共享存储加密访问,Bethencourt 等在 ABE 基础上提出了基于属性的密文策略加密(ciphertext-polity attribute-based encryption, CP-ABE)方案[15].在 CP-ABE 中方案中,属性集合是与用户私钥直接相关的,访问结构是与数据密文相联系的,如果用户的属性集合满足密文的访问结构树,则该用户可以解密密文,发送方可以通过对访问结构的设置决定哪些用户可以访问相应的数据密文,数据加密者无需了解解密者是谁.近年来,国内外研究者提出一系列属性加密方案,Waters[16]和 Daza 等[17]分别采用基于门限的访问控制策略,实现了基于属性加密,但其密文长度分别为 $n+O(1)$ 和 $2(n-t)+O(1)$,加密解密效率较低.文献[18]提出一种定长密文的 ABE 加密方案,

但存在用户私钥中的属性必须与制定的密文策略属性完全一致的局限性.程思嘉等[19]提出一种基于CP-ABE的密钥改进算法,降低了多属性密钥计算开销,提高了运算效率.

本文针对上述文献中的不足,在现有CP-ABE方案的基础上,针对带有重复数据删除功能的云存储系统,提出映射节点概念以及改进原始的基于属性加密的方法,使得CP-ABE方案中的访问控制树具有更强的表达力,解决原始CP-ABE方案中密钥结构的属性子集中的属性必须来源于用户属性集合的缺陷.

2 基于节点映射的属性加密

与原始的属性基加密方案相比,CP-ABE方案在访问结构树上有不错的改进,可以构造出更具表达力的访问控制策略,但是由于CP-ABE方案的密钥结构只支持若干单个属性的规则属性子集且不支持来源于用户集以外的属性,导致CP-ABE方案在云存储加密访问中存在不支持多属性赋值操作的表达性缺陷.与此同时传统的非对称属性加密方式存在并发效率过低的问题,为此本文提出一种对基于映射关系的基本属性基加密方案.利用对称加密算法具有较高的运算速度的优点对用户数据进行加密,同时利用密钥分割的方法优化访问结构树的构造.

2.1 云数据访问结构树

假设在云存储服务器上一个超大文件 F 被分割成 N 个数据块,服务器为了减少冗余存储并提高访问效率,采用访问结构树(access structure tree,AST)(如图1所示)的方法对海量存储文件进行去重排序.其访问结构树可以如下定义:

定义 2.1 共享度(sharing degree,SD)

如果一个数据块被多个文件共享访问,定义某个数据块被共享的文件数量为该数据块的共享度,则可将共享度少的作为底层节点,共享度高的作为上层节点的方式来构造访问结构树.如定义AST叶子节点的SD在区间[1 10]之间,则根节点数的SD为(1000 ∞)(如图1所示).

定义 2.2 子树关系(children relationship,CR)

子树关系表示子节点数据块与父节点数据块之间的关系.如果构成某文件需要访问当前数据块的所有子块,则CR为And;如果构成文件需要部分子数据块,则CR为Or或者 n/m ,其中 n 为子块序列数,且 $1<n<m$.叶子节点的CR为Null.

定义 2.3 阈值(threshold value)

阈值主要描述某个文件的AST在当前数据块需要访问子数据块的量,因此叶子节点的阈值为1,其他节点的阈值为 $1<kx<m$.

当某用户需要访问文件 F 时,客户端向服务器递交访问结构树 λ ,当且仅当 $T(\lambda)=1$ 时,云存储服务器根据其AST将允许访问的文件F反馈给用户.其中 $T(\lambda)=\{Tx(\lambda),x=\{1,\cdots,m\}\}$,即 T 的所有子树为1时, $T(\lambda)$ 为1.

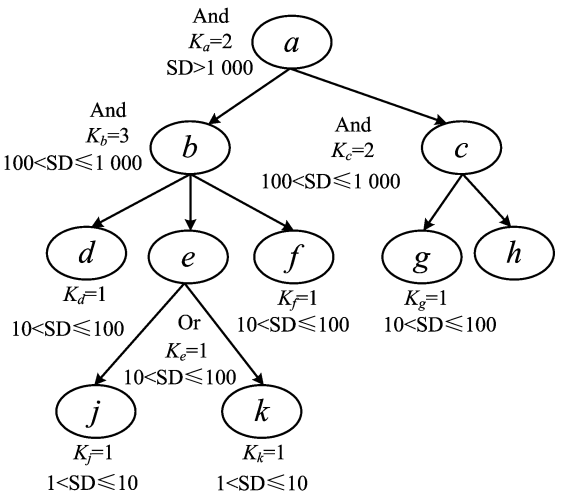

图1 云存储文件访问树示意图

Fig.1 Access structure tree of cloud storage

2.2 节点映射机制

本文在访问结构树中引入节点映射机制(node mapping scheme),利用映射节点(mapping node)以非常小的计算代价对访问结构树进行扩展.该映射 $e:\{SA,expiration\}\rightarrow\{\rho\lambda\}$ 关系用来转化属性集 U 以外的其他属性,并产生新的密钥结构 $S^{new}\{\rho\lambda,\rho i,\rho j,\rho k,\cdots\}$,其中 $\rho\lambda\in U-S$.其新的访问结构树 $T_x(S^{new})$ 的调用机制如下:

(Ⅰ)如果 x 是叶子节点,当且仅当 $attribute(x)\in S^{new}$ 时,即属性 $attribute(x)$ 属于密钥属性集合, $T(x)$ 返回1;

(Ⅱ)如果 x 是非叶子节点,设 x' 是 x 的子节点,存在大于等于 kx 个子节点的 x' 调用 $T(x')$ 并且返回值为1时, $T(x)$ 的返回值才为1;

(Ⅲ)如果 x 是映射节点并且 x 节点的属性集 $Sx\neq\varnothing$,首先利用映射 e 转化 Sx 为 $\rho\lambda$,然后映射节点变为叶子节点,执行叶子节点的匹配操作.

2.3 节点映射属性加密

为了引入可信代理进行管理,本文在用户相关

属性为主的基本属性基加密方案的基础上，添加一个秘密属性(secret attribute，SA).如图 2 所示，该秘密属性节点同时也称为映射节点，包括用户账号的有效期属性、秘密属性等，并且与源 ADT 根节点以“And”门限生成一棵新的访问结构树.对于属性集合的操作(包括属性添加、撤销)均不包含该秘密属性，所以不管对密钥的更新操作是在云服务器还是在第三方安全代理上进行，都无法获得用户的全部私钥，从而保证了用户数据的机密性，进一步防止了云服务器的恶意攻击.

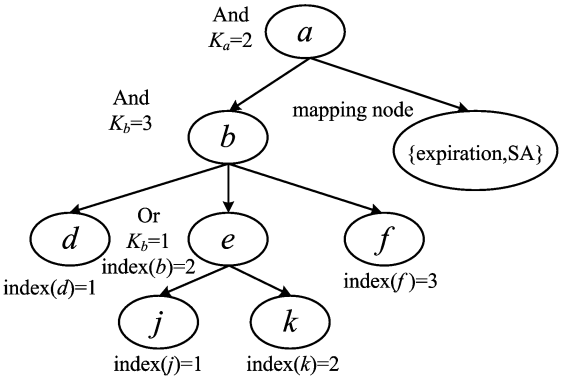

图 2　基于节点映射的访问结构树

Fig.2　Access structure tree based on mapping node

3　访问控制策略设计

3.1　安全代理访问控制模型

传统的云存储加密访问机制主要基于密钥授权管理中心，但是密钥授权中心也存在一定的风险，为此本文引入安全代理，其访问控制系统结构如图 3 所示，以下是每个功能模块的任务描述.

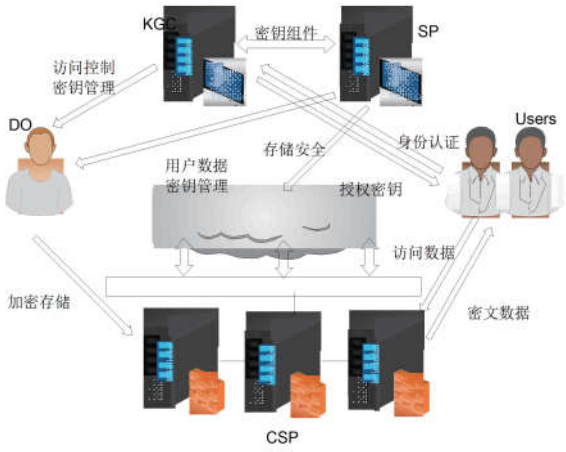

图 3　云存储访问控制系统模型图

Fig.3　System structure of cloud storage access

(Ⅰ)密钥授权中心(key generation center，KGC).主要负责系统公共参数和私密参数的产生，给用户分配对应的属性组件，从而授予用户不同的访问权限，并负责验证密钥有效期属性以及用户私钥属性组的升级和回收等工作.在本文中，KGC 被假设为半可信的，这就意味着 KGC 会按照系统设计的功能执行，但是它们会尽可能地挖掘更多的用户隐私信息.

(Ⅱ)安全代理(security proxy，SP).设计用户将数据的安全服务从云存储中分离出来，在访问控制机制中主要负责存储用户数据加密的指纹库以及分发用户数据的秘密属性(SA).SP 也可能是半可信的.

(Ⅲ)云存储提供商(cloud storage provider，CSP).为用户提供数据的存储服务，根据访问用户的私钥属性结构与访问控制树的匹配结果来控制其对数据的访问.CSP 最有可能根据用户的数据以及行为进行深层挖掘，暴露用户隐私信息.

(Ⅳ)数据属主(data owner，DO).数据的拥有者，为了降低存储成本，将自己的数据上传至云存储服务器，并可以向其他用户共享数据资源.DO 负责定义访问控制策略，并在上传数据前进行加密操作防止 CSP 对用户隐私的非法利用.

(Ⅴ)用户(users).从 DO 获取数据访问权限并访问存储在云服务上的数据文件.如果该用户拥有的属性结构能够满足访问控制策略，并且该用户的操作没有超出他的权限，则可以访问共享数据资源.

3.2　算法设计

为了适应重复数据删除技术在云存储中的应用以及降低安全代理进行重加密承受的计算压力，对于用户原始文件，我们首先进行利用定长分块将文件切割成若干数据块，并计算得到每个数据块的 Hash 值 h，并运用收敛加密方法对数据块进行加密，算法描述过程中的符号见表 1.

假设密钥授权中心(KGC)可分配的属性个数最多为 n，安全代理(SP)负责分配秘密属性(SA)和有效期属性(expiration).

(Ⅰ)系统初始化

对于任何的 $i \in Z_p$ 集合 S 的中的任意 $a \in Z_p$，定义拉格朗日参数 $\Delta_{i,s}$ 如下：

$$\Delta_{i,s}=\prod_{j\in S,j\neq i}\frac{x-j}{i-j},$$

表 1 符号描述

Tab.1 Symbol descriptions

符号	描述
KGC	密钥授权中心
SP	安全代理
SA	秘密属性
expiration	有效期属性
PK	系统公共参数
MK	主密钥
SK	用户私钥
U	属性集合
M	用户数据
CT	密文

由安全参数产生双线性群 G_1 和 G_2，且皆为素数 p，g 为 G_1 的一个生成元，定义双线性映射 $e: G_1 * G_1 \rightarrow G_2$，同时定义伪随机函数：

$$T(x)=g_2^{x^n}\prod_{i=1}^{n+1} t\Delta_{i,s}(x)_i.$$

式中，T 可以看作函数 $g_2^{x^n}g^{h(x)}$，$h(x)$ 是一个 n 阶的多项式.

定义属性全集 $U=\{u_1, u_2, u_3, \cdots, u_n, sa^*, \text{expiration}\}$，其中 sa^* 是与具体数据块相关的秘密属性，expiration 则是由安全代理产生的密钥有效期属性.对于任意属性 $u_i \in U$，$T(u_i)$ 与其相关联，随机选取一个 $y \in Z_p$，生成如下的系统公共参数 PK.

$$T_1=g^{t_1}, \cdots, T_{|u|}=g^{t_{|u|}}, Y=e(g,g)^y$$

系统主密钥 MK 为：$t_1, \cdots, t_{|u|}, y$.

（Ⅱ）加密算法

算法输入为：数据 M、公共参数 PK 以及访问结构树 Γ.从访问结构树 Γ 的根节点 r 开始，从上往下为访问树中的每个节点 x 选取一个多项式 P_x，其中多项式的次数 $d_x=k_x-1$.随机选取 $s \in Z_p$，且根节点 r 的多项式值为 s，即 $P_r(0)=s$，随机选取其他的 d_r 个节点.对于非叶子节点 x，有 $P_x(0)=P_{\text{parent}}(x)(\text{index}(x))$，随机选取其他 d_x 个节点.最后生成如下形式的密文：

$$\text{CT}=\{\Gamma, C^*=M\cdot e(g,g)^{\alpha_s}, C=h^s, \forall y \in L, Cy=H(|y|)^{P_y(0)}\}.$$

其中，L 是访问结构树中所有的叶子节点的集合.

（Ⅲ）身份验证

假设用户访问文件 $f=<a_1, a_2, \cdots, a_i, \cdots, a_n>$，其中 a_i 为文件 f 的数据块，安全代理根据随机抽取 m 个数据块，$m \leqslant n$，生成访问控制树 Π，并要求访问用户提供的属性集合能够完全匹配 Π.

（Ⅳ）私钥生成

算法输入为：属性集合 U、主密钥 MK、公共参数 PK；算法输出为：用户私钥 SK.随机选取 $\gamma \in Z_p$，$\forall x \in S$，随机选取 $\gamma_x \in Z_p$.那么将会产生如下形式的用户私钥：

$$\text{SK}=(D=g^{(\alpha+\gamma)/\beta}, \forall j \in S: D_j=g^{\gamma}\cdot H(j)^{\gamma_j}, D_j=g^{\gamma_j}).$$

（Ⅴ）解密密文数据：

算法输入为：密文 CT，私钥 SK，公共参数 MK.当且仅当用户的属性集合能够满足密文访问结构树时，才可以解密该密文.对于叶子节点 x，首先做如下计算，其中 $i=\text{attribute}(x)$，且 $i \in S$，

$$\text{Decrypt}(\text{CT},\text{SK},x)=\frac{e(D_i,C_x)}{e(D_i',C_x')}=\frac{e(g^{\gamma}\cdot H(i)^{\gamma_i}, g^{P_x(0)})}{e(g^{\gamma_i}, H(i)^{P_x(0)})}=e(g,g)^{\gamma\cdot p_x(0)}.$$

如果 $i \notin S$，$\text{Decrypt}(\text{CT},\text{SK},x)=\perp$；对于非叶子节点 x，可以通过它的子节点 λ 返回值 F_λ，然后通过多项式插值法自下而上递归，可以计算得到

$$F_x=\sum_{\lambda\in S_x} F_\lambda^{\Delta_{i,s_x}(0)}=e(g,g)^{S\cdot P_x(0)},$$

式中，S_x 是一个能够使 $F_\lambda \neq 0$ 成立的任意 k_x 个子节点构成的集合，$i=\text{index}(\lambda)$，$S_x'=\{\text{index}(\lambda): \lambda\in S\}$，$\Delta_{i,S}(x)=\prod_{j\in S, j\neq i}\frac{x-j}{i-j}$.按照这种方法由下往上递归到根节点时就可以恢复出盲因子 $A=e(g,g)^{\gamma q_\gamma(0)}=e(g,g)^{\gamma S}$.最后通过 $C^*/(e(C,D)/A)=C^*/(e(h^S, g^{(\alpha+\gamma)/\beta})/e(g,g)^{\gamma S})=M$，解密得到数据明文 M.

4 安全和性能分析

4.1 访问结构的保密性分析

本文假设 KGC 与 SP 是半可信的，让共享用户通过 KGC 和 SP 获得授权访问结构，因此数据所有者不需要知道用户的访问结构，另外 CSP 也不参与用户私钥的产生，所以也不能获取用户的访问结构，从而无法对共享数据进行非授权访问.

4.2 数据机密性

数据机密性包括数据密文的机密性和加密密钥密文的机密性.假设对称密钥加密算法（如 DES、

AES 等)是安全的,本方案的机密性问题则转换为密钥密文的安全性问题.密钥密文的安全性可以归结为 CP-ABE 算法的安全性问题.由于在 DBDH 假设下,本文所采用的 CP-ABE 算法是在基于属性的选择集模型下被证明是安全的.如果数据的属性集不满足用户访问结构,则不能成功解密数据,因为没有足够的私钥组件完成与密文组件的配对.系统中所需要的 MK 由安全代理 SP 生成和拥有,对于 CSP 来说是透明的,因此 CSP 也无法通过获取解密密钥来解密存储于其中的用户数据密文.基于 CP-ABE 算法本身就具有抗合谋攻击的性质,未授权的用户即使进行合谋也无法恢复出对称密钥.

4.3　时间开销测试

为了检测本文提出的加密算法的性能,我们在同一服务器上对原始 CP-ABE 方案与本文方案的实际加密和解密的时间开销进行对比.测试环境如表 2 所示,系统硬件平台是 Intel Xeon 5420 2.5G CPU,4G 内存,操作系统为 Ubuntu12.04 64 bit,SDK 为 java-1.7 版本.在参数设置方面,随机生成 20 到 50 个节点,用户的属性集设置为 10 个,提前为每个属性组计算好 KEK 函数.算法使用 PCB 实验室的标准加密算法库 PBC-0.5.14,在 512 位有限域中,使用 160 bit 的椭圆曲线函数($y^2 = x^3 + x$)群.

表 2　测试环境

Tab.2　Experimental environment

系统环境		试验参数	
CPU	2.5GHz	Leaf Nodes	[20 50]
Memory	4G	Attribute Set	10
System	Ubuntu 12.04	$SK_{eq.5}$	KEK
SDK	JDK 1.7.0	$Z_p{}^*$	512
Lib	PBC-0.5.14	Decry F	$y^2 = x^3 + x$

加密时间测试结果如图 4 所示,两种方案的加密时间基本与叶子节点数成线性关系,本文方案平均时间比基本 CP-ABE 方案大约多 0.36 s,平均增幅约为 27.6%.在解密时间测试中(如图 5 所示),基本 CP-ABE 方案的平均耗时为 0.126 s,本文方案的平均耗时为 0.376 s,虽然本文的方案比基本 CP-ABE,不论在加密还是解密时间开销都有所提高,但是从增幅的绝对值来看,并不是很高,在提高安全性的同时,时间增幅在可接受范围内.

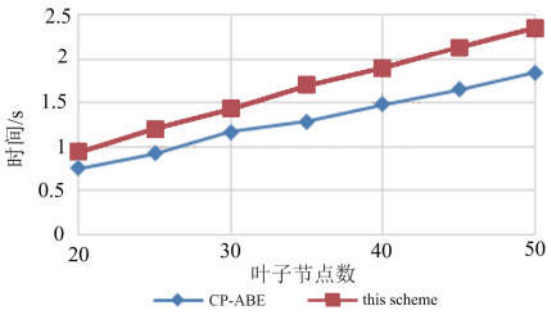

图 4　加密时间测试

Fig.4　Results of encryption

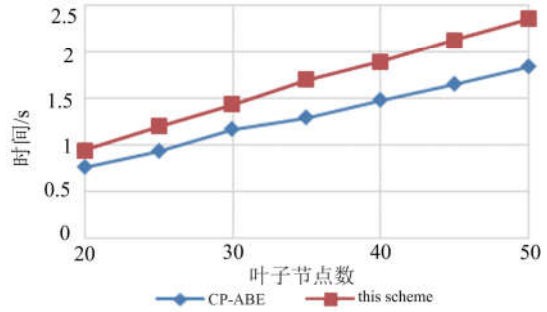

图 5　解密时间测试

Fig.5　Results of decryption

5　结论

本文针对 CP-ABE 云存储加密只支持若干单个单属性规则属性子集,无法引入三方安全代理提升云数据加密的安全性问题,提出一种用户属性集的节点映射机制对 CP-ABE 算法进行改进.该方法首先利用对称加密相对属性基加密具有较高的运算速度的优点对用户数据进行加密;然后利用密钥分割的方法,优化访问结构树的构造;最后在用户相关属性为主的基本属性基加密方案的基础上,添加一个秘密属性,实现可信代理对密钥的三方管理.在访问结构的保密性和数据机密性分析后,本文提出的方法与 CP-ABE 对比试验显示,该方法在很小的系统开销前提下实现了第三方可信代理机制导入,具有很好的技术价值和应用前景.

参考文献(References)

[1] 苏金树, 曹丹, 王小峰, 等. 属性基加密机制[J]. 软件学报, 2011, 22(6): 1299-1315.
SU Jinshu, CAO Dan, WANG Xiao, et al. Attribute-based encryption schemes[J]. Journal of Software, 2011, 22(6): 1299-1315.

[2] YAO J H, CHEN S P, NEPAL S, et al. TrustStore: Making Amazon s3 trustworthy with services

composition[C]// Proceedings of the 10th IEEE/ACM International Conference on Cluster, Cloud and Grid Computing. Melbourne, Australia: IEEE Computer Society, 2010: 600-605.

[3] SONG D X, WAGNER D, PERRIG A. Practical techniques for searches on encrypted data [C]// Proceedings of the IEEE Symposium on Security and Privacy. Berkeley, USA: IEEE Press, 2000: 44-55.

[4] SWAMINATHAN A, MAO Y N, SU G M, et al. Confidentiality-preserving rank-ordered search [C]// Proceedings of the ACM workshop on Storage Security and Survivability. Alexandria, USA: ACM Press, 2007: 7-12.

[5] 黄永峰，张久岭，李星. 云存储应用中的加密存储及其检索技术[J]. 中兴通讯技术，2010，16(4)：33-35.
HUANG Yongfeng, ZHANG Jiuling, LI Xing. Encrypted storage and its retrieval in cloud storage applications[J]. ZTE Communications, 2010, 16(4): 33-35.

[6] LIANG K T, SUSILO W. Searchable attribute-based mechanism with efficient data sharing for secure cloud storage [J]. IEEE Transactions on Information Forensics and Security, 2015, 10(9): 1981-1992.

[7] AKL S G, TAYLOR P D. Cryptographic solution to a multilevel security problem [C]// Proceedings of CRYPTO'82. Santa Barbara, USA: Springer, 1983: 237-249.

[8] AKL S G, TAYLOR P D. Cryptographic solution to a problem of access control in a hierarchy [J]. ACM Transactions on Computer Systems, 2012, 20(3): 251-261.

[9] YANG K, JIA X H. Attributed-based access control for multi-authority systems in cloud storage [C]// Proceedings of the 32nd International Conference on Distributed Computing Systems. Macau, China: IEEE Press, 2012: 536-545.

[10] 刘占斌，刘虹，火一莽. 云计算中基于密文策略属性基加密的数据访问控制协议[J]. 信息网络安全，2014，(7)：57-60.
LIU Zhanbin, LIU Hong, HUO Yi. Data access control protocol for the cloud computing based on ciphertext-policy attribute based encryption (CP-ABE) [J]. Netinfo Security, 2014, (7): 57-60.

[11] SAHAI A, WATERS B. Fuzzy identity-based encryption [A]// Advances in Cryptology - EUROCRYPT 2005[M]. Berlin Heidelberg: Springer, 2005: 457-473.

[12] YU S C, WANG C, REN K, et al. Achieving secure, scalable, and fine-grained data access control in cloud computing[C]// Proceedings of the 29th conference on Information communications. San Diego, USA: IEEE Press. 2010: 534-542.

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

[14] LIU C W, HSIEN W F, YANG C C, et al. A survey of attribute-based access control with user revocation in cloud data storage[J]. International Journal of Network Security, 2016, 18(5): 900-916.

[15] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-policy attribute-based encryption [C]// Proceedings of the IEEE Symposium on Security and Privacy. Berkeley, USA: IEEE Press, 2007: 321-334.

[16] Waters B. Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization[A]// Public Key Cryptography - PKC[M]. Berlin Heidelberg: Springer, 2011: 53-70.

[17] DAZA V, HERRANZ J, MORILLO P, et al. Extensions of access structures and their cryptographic applications[J]. Applicable Algebra in Engineering, Communication and Computing, 2010, 21(4): 257-284.

[18] Emura K, Miyaji A, Nomura A, et al. A ciphertext-policy attribute-based encryption scheme with constant ciphertext length[A]// Information Security Practice and Experience[M]. Berlin, Heidelberg: Springer, 2009: 13-23.

[19] 程思嘉，张昌宏，潘帅卿. 基于CP-ABE算法的云存储数据访问控制方案设计[J]. 信息网络安全，2016，(2)：1-6.
CHENG Sijia, ZHANG Changhong, PAN Shuaiqing. Design on data access control scheme for cloud storage based on CP-ABE algorithm [J]. Netinfo Security, 2016, (2): 1-6.