

一种高效属性撤销的云存储访问控制方案

刘伯红, 史慧丽

(重庆邮电大学 计算机科学与技术学院, 重庆 400065)

摘 要: 提出了一种高效细粒度属性撤销的云存储访问控制方案, 用析取范式代替一般的 AND/OR 结构, 对 CP-ABE 算法中的访问树进行优化, 大大减少了加解密过程中的递归运算及开销. 在进行属性撤销时, 代理重加密和属性版本号的使用不仅降低了数据属主的计算开销, 还提高了属性撤销效率. 对方案进行的相关分析和仿真实验表明, 新方案是高效且安全的.

关键词: 属性基加密; 云存储; 访问控制; 属性撤销

中图分类号: TP309

文献标识码: A

文章编号: 1000-7180(2016)04-0041-05

Attribute-based Access Control with Efficient Revocation in Cloud Storage Systems

LIU Bo-hong, SHI Hui-li

(College of Computer Science and Technology, Chongqing University of Posts and
Telecommunications, Chongqing 400065, China)

Abstract: An efficient fine-grained access control scheme is presented. The use of disjunctive normal form(DNF) instead of traditional AND/OR structure can optimize the access tree of CP-ABE algorithm and greatly reduce the recursive computation and cost in the process of encryption and decryption. The use of proxy re-encryption and attribute version numbers not only reduces the computational overhead of the data owner but also improves the efficiency of attribute revocation. Finally, the related analysis and simulation experiment results show that the new scheme is efficient.

Key words: attribute-based encryption; cloud storage; access control; attribute revocation

1 引言

伴随着云计算的发展及大数据的到来, 人们对云存储越来越关注. 作为一种云计算新服务技术, 云存储主要通过网络集合不同的存储设备进行协作, 向用户提供在线存储服务. 但由于云存储服务器和用户属主不在相同的可信域, 造成人们对其相关安全问题^[1]的担忧. 为了确保敏感数据的安全, 以及用户的高效细粒度访问, 在云存储环境中引入以属性基加密(Attribute based Encryption, ABE)^[2]的方法. 随着深入研究, Vipul Goyal 等^[3]以访问决策者为主, 把其分为密文策略的属性基加密方案^[4](Ciphertext Policy Attribute based Encryption, CP-

ABE)和密钥策略的属性基加密方案(Key Policy Attribute based Encryption, KP-ABE). CP-ABE 可以给数据属主更多直接控制访问策略的权力, 使其更适应于云存储访问控制中. 在 CP-ABE 中, 属性撤销是一个需要解决的问题, 为此, Liang Xiaohui^[5]等人提出代理重加密方案(attribute-based proxy re-encryption, ABPRE), 此方案可实现一类属性集的撤销. 吕志泉^[6]等通过在重加密时利用密钥分割技术和代理重加密技术, 将部分重加密工作转移给云服务提供商实现属性撤销, 大大降低了数据属主的计算代价, 但复杂的访问树结构, 加重了解密算法的计算量. 刘帆^[7]通过引入用户 ID, 构造复合访问结构以实现属性撤销, 但这样的设计造成数据属主

的负担增加,密钥的分发效率降低. Lai Junzuo 等^[8]部分地隐藏访问结构实现访问控制,但对于属性撤销没有提高. Yang 等^[9]提出了基于 CP-ABE 的细粒度数据访问控制,但采用线性秘密共享机制的矩阵实现.

为了减少加解密计算量,实现高效的属性撤销,本文提出了一种高效、细粒度数据访问控制方案.

2 云存储访问控制模型及安全定义

2.1 云存储访问控制模型

为了降低数据属主的负担,确保数据的安全高效访问,本方案设计的云存储访问控制系统模型如图 1 所示. 系统中共有四个实体:授权中心(Authority)、数据属主(Data owners, DO)、云存储服务器(Cloud Storage Provider, CSP)、用户(users).

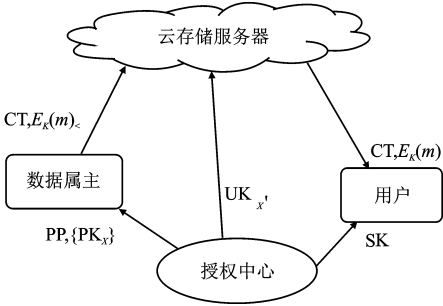


图 1 云存储访问控制系统模型

方案中,可信的授权中心主要负责所有属性的授权、撤销及发布公开密钥和信息的更新,给指定属性的用户发布密钥并维护所有属性的版本. 当有属性撤销时,授权中心更新撤销属性的版本,并重新加密未撤销的用户. 上传加密文件并为文件设访问结构等任务由数据属主负责(即用户的属性满足访问结构时能进行解密). 云存储服务器存储用户数据并向用户提供访问服务. 但是,用户在进行访问数据时云存储服务器并不参与. 根据用户的角色,用户被授予一些属性,用户满足访问策略时可以访问相应的数据.

2.2 CP-ABE 相关介绍

定义 1 属性: 设 $P = \{P_1, P_2, \dots, P_n\}$ 为所有的属性, 每个用户私钥关联的属性集 A 是 P 的一个非空子集, $A \subseteq \{P_1, P_2, \dots, P_n\}$.

定义 2 访问结构树: 用来描述访问控制策略. 树的叶节点代表属性, 内部节点代表关系函数, 访问控制策略如图 2 所示. 加密时, 自顶向下为每个节点赋值, 解密时则自底往上恢复秘密. 为了减少运算

量, 优化结构成为关键, 传统的 AND/OR 访问结构树被析取范式^[10]访问结构取代, 如图 3 所示.

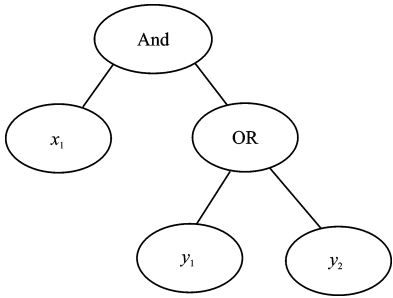


图 2 访问树

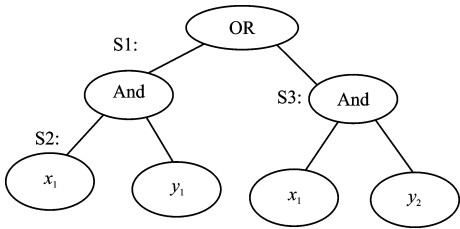


图 3 析取范式访问结构

根节点以 OR 操作为准, 剩下的结点用 AND 操作, 属性用孩子节点代表, 用 AS(Access Structure)表示访问结构, Attr 表示属性, S_i 表示属性集合, x, y, z 表示节点的属性, 如图 3 所示. 与传统相比, 改进的访问树描述简单, 易理解, 而且减少了递归运算, 效率的提高得以实现, 还能阻止非法用户的共谋攻击. 一般的访问树通过下面的步骤转化为析取范式访问树:

(1) 用若干的 $\vee$ (OR), $\wedge$ (And) 操作来表示一般访问树的逻辑表达式;

(2) 利用分配率和结合律进行转化.

这样可以使原来的访问树变成一颗析取范式, 而属性的同层表示, 进一步使树的层次简化, 访问结构表达更加清晰、简洁.

2.3 安全假设

在 CSP 的不完全可信情况下, DO 的计算量和分发密钥的代价是巨大的. 根据以往的相关研究介绍, 假定本方案中的 CSP 会忠诚地执行运行程序及相关访问策略, 但不会通过输入获取秘密信息. 还假定其获取的秘密没有其他的秘密信息, 与数据属主 DO、用户 users 之间的通信信道都是安全的.

3 云存储访问控制方案的设计

3.1 方案概述

直接用 CP-ABE 加密大型数据文件, 会降低效

率,所以数据属主 DO 需要先把上传数据文件用对称密钥进行加密处理.然后,设置访问策略,利用 CP-ABE 算法对对称密钥进行处理.不同身份的用户,授权中心会分配不同的属性.根据用户的属性产生相应的密钥,用户可通过解密密文和数据密文对相应的文件进行访问.

传统的 CP-ABE 在进行属性撤销时会严重降低访问效率,为此本方案为每个属性指定一个版本号用来处理属性撤销.当用户的某个属性被撤销时,授权中心为此属性生成一个新的版本号并更新撤销属性的密钥.未撤销的用户用新的密钥更新自己的密钥,密文中与撤销属性相关的部分进行更新,从而保证了向后安全(拥有足够多属性的新用户可以解密原密文).为了降低数据属主 DO 的代价,提高效率,CSP 通过用代理重加密实现密文的更新.这样可以保证新加入的用户可以解密之前已经加密的数据文件,达到了向前安全(已撤销权限的用户不能解密更新后的密文).

3.2 方案的具体构造

3.2.1 系统初始化

$\text{Setup}() \rightarrow (\text{MK}, \text{PP}, \{\text{PK}_x\}, \{\text{VK}_x\})$: 首先构造阶为素数 p , 生成元为 g 的双线性群 G_0 , 双线性映射为 $e: G_0 \times G_0 \rightarrow G_T$. $H: \{0, 1\}^* \rightarrow G_0$, 其可以将 H 中的元素映射为 G_0 中的一个元素. 授权中心管理的属性集用 Y 来表示. 从 Z_p 里选择三个随机值 a, α, β . 对于每个 x , 随机选取 $v_x \in Z_p$.

$$\text{MK} = (a, \alpha, \beta) \quad (1)$$

$$\text{PP} = (g, g^a, g^\beta, g^{1/\beta}, e(g, g)^a) \quad (2)$$

$$\text{PK}_x = H(x)^{v_x} \quad (3)$$

$$\text{VK}_x = v_x \quad (4)$$

授权中心发布所有的 PP, PK_x , 确保系统中的数据属主可以容易得到.

3.2.2 用户私钥的生成

$\text{KeyGen}(\text{MK}, S, \{\text{VK}_x\}_{x \in S}) \rightarrow \text{SK}$: 授权中心根据加入用户的身份给用户分一些属性 S , 运行 KeyGen , 生成 SK . 随机选择 $r \in Z_p$, 生成的用户私钥为

$$\begin{aligned} \text{SK} &= (D = g^{(\alpha+r)/\beta}, \forall x \in S: \\ D_x &= g^r \cdot H(x)^{v_x}, D'_x = g^{v_x}) \end{aligned} \quad (5)$$

3.2.3 数据属主加密数据

$\text{Encrypt}(\text{PP}, \text{PK}_x, m, \Gamma) \rightarrow \text{CT}$. 把数据传送到 CSP 之前要进行加密. 算法中定义的 $H(i)$ 函数是将属性 i 映射为双线性群上随机的某个元素. 访问结构树的思想是: 为改进的结构树上的每个节点

x 选取一随机多项式 q_x , 则 $q_x(0)$ 表示节点的秘密, 设置多项式的度 $d_x = k_x - 1$ (k_x 为非根父节点 S_i 中所有的属性个数. 设访问树中有 n 个节点, 构造 n 个多项式, 且令 $q_R(0) = s$, 令 $q_x(0) = q_{\text{parent}(x)}(\text{index}(x))$. Y 表示树中节点的集合. 则

$$\begin{aligned} \text{CT} &= (\Gamma, C = me(g, g)^\alpha, C' = g^{\beta s}, \\ \forall y \in Y, C_y &= g^{q_y(0)}, \\ C'_y &= H(\text{attr}(y))^{q_y(0)}) \end{aligned} \quad (6)$$

之后, 数据属主上传加密的数据到 CSP.

3.2.4 用户解密

$\text{Decrypt}(\text{CT}, \text{SK}) \rightarrow m$. 用户访问数据时首先要进行解密, 只有满足要求的用户才能访问数据. 根据改进后访问结构的特点, 用户的属性只要满足任意非根节点 S_j , 即 $S_j \subseteq S_{\text{user}}$. 解密时输入密文 CT , 访问结构 Γ , 用户私钥 SK . 输出解密密文消息 m . 若用户属性集 S_{user} 使得析取范式访问结构返回值为 1, 对于每个属性 $x \in S_j$, 调用函数

$$\text{DecryptNode}(\text{CT}, \text{SK}, x) = \frac{e(D_x, C_x)}{e(D'_x, C'_x)} = e^{m_x(0)} \quad (7)$$

改进的方案只需要对析取范式下的满足要求的子集进行计算, 与传统相比, 系统的计算开销大大减少. 根据 Lagrange 插值多项式门限密码理论, 计算结果如下:

$$\begin{aligned} F_x &= \prod_{z \in S_x} F_z^{\Delta_i \cdot S'_x(0)} \\ &= \prod_{z \in S_x} (e(g, g)^{r \cdot q_z(0)})^{\Delta_i \cdot S'_x(0)} \\ &= \prod_{z \in S_x} (e(g, g)^{r \cdot q_{\text{parent}(z)}(\text{index}(z))})^{\Delta_i \cdot S'_x(0)} \\ &= \prod_{z \in S_x} e(g, g)^{r \cdot q_x(i) \cdot \Delta_i \cdot S'_x(0)} \\ &= e(g, g)^{r \cdot q_x(0)} \end{aligned} \quad (8)$$

并令 $B = F_x$ 之后通过如下计算恢复出密文 m :

$$\begin{aligned} &= \bar{C} / (e(C, \text{SK}_u) / B) \\ &= \bar{C} / (e(g^{\beta s}, g^{(\alpha+r)/\beta}) / e(g, g)^{r \cdot s}) \\ &= m \end{aligned} \quad (9)$$

用户用解密出来的 m 进行对数据进行解密, 得到需要访问的数据.

4 云存储访问控制属性撤销研究

为了提高属性撤销, 减小计算开销, 本方案通过加入属性的版本号来实现. 当一个属性 x' 从用户 u 中撤销时, 撤销要进行如下操作: 授权中心更新密

钥,未撤销用户更新私钥及 CSP 更新相关密文.

4.1 授权中心更新密钥

$UKeyGen(MK, VK_{x'}) \rightarrow (\overline{VK_{x'}}, UK_{x'})$. 授权中心运行此算法. 随机选择 $\overline{v_{x'}} \in Z_p$, 并计算出 $UK_{x'} = \overline{v_{x'}}/v_{x'} UK_{x'}$ 主要用于更新未撤销用户的私钥及与此属性相关的密文. 授权中心把更新后的 $UK_{x'}$ 通过安全通道上传给 CSP. 另外, 与 x' 相关的 PK 也要进行更新, 得到 $PK_{x'} = H(x')^{\overline{v_{x'}}}$ 撤销属性更新后的公共属性秘钥所有的用户可以得到.

4.2 更新未撤销用户的密钥

$KUUpdate(SK, x') \rightarrow \overline{SK}$. 授权中心运行此算法更新与撤销属性 x' 相关的组成部分. $D'_{x'} = g^{v_{x'}}$, $D_x = g^r \cdot H(x')^{v_{x'}}$, 则更新后的私钥为

$$\overline{SK} = (D, D'_{x'}, \forall x \in S \setminus \{x'\}; D_x, D'_{x'}) \quad (10)$$

另外, 更新后的私钥与撤销属性 x' 无关的部分无需进行更新.

4.3 CSP 更新密文

$CTUpdate(CT, UK_{x'}) \rightarrow \overline{CT}$. 为了确保新加入的用户可以解密之前的用户, 与撤销属性相关的密文部分需要进行更新. 另外, 为了减轻数据属主的负担, 重加密由 CSP 完成. 通过利用代理重加密提高效率, 减轻数据属主计算负担. 接收授权中心更新的 $UK_{x'}$, CSP 以 CT, $UK_{x'}$ 为输入信息, 利用 $CTUpdate$ 算法更新密文, 与撤销属性 x' 相关的更新如下:

$$\begin{aligned} \overline{CT} &= (\Gamma, \overline{C} = C, \overline{C'} = C', \forall y \in Y \setminus \{x'\}; \\ \overline{C_y} &= C_y, \overline{C'_y} = C'_y, y = x': \\ \overline{C_y} &= C_y \cdot (C'_y)^{UK_{x'}}, \overline{C'_y} = (C'_y)^{UK_{x'}} \end{aligned} \quad (11)$$

从以上公式可以看出, 与撤销属性相关的密文部分需要进行更新, 而别的部分不用进行更新. 利用此方案可以提高属性撤销的效率, 存储负担, 也保证了其的向前安全.

5 方案分析

5.1 安全性分析

本方案在生成密文时, 使用了双线性计算, 且选择随机数. 所以攻击者要想解密消息, 需要恢复双线性对和获得私钥. 另外在解密时还要满足访问树的要求. 所以, 本文的方案是可以达到数据机密性的.

本方案的访问是以属性为单位, 只要满足访问结构的用户均可以访问对应的消息, 这样用户的身

份也不易暴露, 可防止匿名访问. 另外, 基于属性加密的本身可抵抗共谋攻击, 由于为每个属性都指定了版本号, 攻击者在进行解密时是无从得知的, 所以能确保多用户联合也不能解密. 属性撤销时, 授权中心为撤销属性选择新版本, 生成更新密钥, 然后上传 CSP, 并对与撤销属性相关的密文进行更新, 属性的不同版本确保已撤销属性的用户不能用之前的私钥解密密文.

5.2 性能分析

与 Yang^[9] 等提出的以 LSSS 为访问结构进行细粒度的属性撤销的云存储访问控制不同, 本文采用的是基于树的访问结构. 传统的 CP-ABE 算法在解密过程中使用的双线性对运算的效率影响很大, 尤其是在节点增加, 实现细粒度访问控制时, 而本文在一般访问树的基础上, 引用析取范式, 简化了解密中的递归, 只需对满足条件的 S_j 进行解密调用.

在进行比较时, 假设 $|p|$ 为 Z_p 的大小. $|g|$ 和 $|g_t|$ 分别为 G 和 G_T 的大小, n_a 为总属性的个数, n_u 为总用户的个数, 而 $n_{a,i}$ 表示第 i 个用户拥有的属性数, y 表示参与加密的属性个数.

通过表 1 分析可得, 使用改进的树型结构与文献^[9]中使用的 LSSS 访问结构相比, 在进行数据加密及上传到 CSP 中存储有一定的改进.

表 1 存储负担比较

实体	本方案	文献[9]
授权中心	$(4 + n_a) p $	$(4 + n_a) p $
数据属主	$(2 + n_a) g + g_t $	$(2 + n_a) g + g_t $
CSP	$ g_t + (2y + 1) g $	$ g_t + (3y + 1) g $
用户	$(1 + n_{a,i}) g $	$(2 + n_{a,i}) g $

与传统 CP-ABE 各算法的复杂度比较可得出, 在用户属性个数为 n , 访问树叶节点为 x 的情况下, 解密过程中的双线性对运算量大, 这样一定程度上会加重计算负担. 而析取访问树的结构简单, 执行方便, 解密也能减少递归运算等优势, 可以使整体计算量减少, 提高效率. 改进后的解密复杂度与相对应的结构有关, 这大大减少了双线性运算, 提高了计算效率. 为此对传统的 CP-ABE 和改进后的 CP-ABE 在访问树结点数与解密时间的关系做出如下对比, 如图 4 所示. 实验环境为 windows7 系统, 搭建 VMware Workstation, 并安装 Ubuntu 14. 04 进行实验测试.

与文献^[9]相同, 利用更改属性的版本号实现属

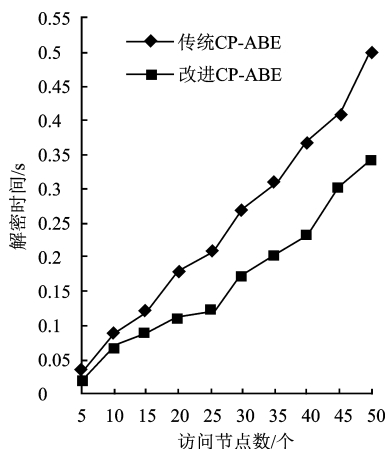


图4 解密消耗

性撤销. 在撤销过程中, 本方案只需要更新与撤销属性相关的密文部分, 所以重加密时消耗的时间与属性的个数是线性相关.

6 结束语

改进复杂的访问结构, 实现属性级的属性撤销一直是研究的热点和难点. 本方从改进访问结构, 实现属性级的属性撤销着手, 提出了一种高效属性级撤销的云存储访问控制方案. 对于属性的撤销, 属性版本号 的设置, 代理重加密的使用, 将部分重加密交给 CSP 执行, 大大降低 DO 的计算代价. 通过分析可知, 本方案是高效且安全的. 在接下来的工作中, 将对本方案继续改进, 使撤销效率更高、访问结构更简单, 从而满足更丰富的操作.

参考文献:

- [1] Cachin C, Keidar I, Shraer A. Trusting the cloud[J]. ACM SIGACT News, 2009, 40(2): 81-89.
- [2] Sahai A, Wates B. Fuzzy identity-based encryption[C]// Cryptology Encrypt. Berlin: Springer-Verlag, 2005: 457-473.
- [3] Vipul Goyal, Omkant Pandey, Amit Sahai, et al. Attribute-based encryption for fine-grained access control of encrypted data[C]// ACM Conference on Computer

and communications Security. New York: ACM, 2006: 89-98.

- [4] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption[C]// Proceedings of the 2007 IEEE Symposium on Security and Privacy, Oakland, California, USA, 2007. Washington, DC: IEEE Computer Society, 2007: 321-334.
- [5] Liang Xiaohui, Cao Zhenfu, Lin Huang, et al. Attribute based proxy re-encryption with delegating capabilities [C]// Proceedings of the 4th International Symposium on Information, Computer and Communications Security (ASIACCS 2009). New York: ACM, 2009: 276-286.
- [6] 吕志泉, 张敏, 冯登国. 云存储密文访问控制方案[J]. Journal of frontiers of computer science and technology, 2011, 5(9): 836-844.
- [7] 刘帆, 杨明. 一种用于云存储的密文策略属性基加密方案[J]. 计算机应用研究, 2012, 29(4): 1452-1456.
- [8] Lai Junzuo, Deng Robert h, Li Yingjiu. Expressive CP-ABE with partially hidden access structures[C]// Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security. New York: ACM, 2012: 18-19.
- [9] Yang Kan, Jia Xiaohua, Ren Kui. Attribute-based fine-grained access control with efficient revocation in cloud storage systems[C]// Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security. New York: ACM, 2013: 523-528.
- [10] Miller S, Katzenbeisser S, Eekert C. Distributed attribute-based encryption[J]. Lecture Notes in Computer Science, 2008, 5461: 20-36.

作者简介:

刘伯红 男, (1973-), 副教授, 硕士生导师. 研究方向为云计算、时空数据挖掘.

史慧丽(通讯作者) 女, (1988-), 硕士研究生. 研究方向为云计算. E-mail: 1070502865@qq.com.