

引用格式:张艺帆,庄富,林果园. 基于联盟链的云访问控制技术研究[J]. 微电子学与计算机, 2021, 38(7): 79-84. [ZHANG Y F, ZHUANG F, LIN G Y. Research on cloud access control technology based on consortium blockchains[J]. Microelectronics & Computer, 2021, 38(7): 79-84.]

基于联盟链的云访问控制技术研究

张 艺 帆^{1,2}, 庄 富^{1,2}, 林果园^{1,2,3}

(1 中国矿业大学 计算机科学与技术学院, 江苏 徐州 221116;

2 矿山数字化教育部工程研究中心, 江苏 徐州 221116;

3 南京大学 软件新技术国家重点实验室, 江苏 南京 210093)

摘 要: 针对云存储环境中单授权中心的安全性问题, 提出一种以 CP-ABE 模型为基础, 同时基于联盟区块链的可撤销多授权机构访问控制模型 (Revocable Multi-Authority Access Control Based on Consortium Blockchain, RMACB). 该模型以树形结构描述属性授权中心 (Attribute Authority, AA), 同时利用可信证书链 (Trusted Certificate Chain, TCC) 和成员服务提供商 (Membership Service Provider, MSP) 对联盟链上的节点进行身份管理和权限控制. 将用户密钥嵌入到密文中去, 实现可撤销的云访问控制技术, 由云服务提供商来执行重加密过程, 减轻了数据所有者的加密负担. 实验验证了提出方案具有更低的计算成本和较高的安全性.

关键词: 云访问控制; 联盟区块链; 属性撤销; 属性加密

中图分类号: TP309.7

文献标识码: A

文章编号: 1000-7180(2021)07-0079-06

Research on cloud access control technology based on consortium blockchains

ZHANG Yifan^{1,2}, ZHUANG Fu^{1,2}, LIN Guoyuan^{1,2,3}

(1 School of Computer Science and Technology, China University of Mining and Technology, Xuzhou 221116, China;

2 Engineering Research Center of Digital Mine, Ministry of Education, Xuzhou 221116, China;

3. State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing 210093, China)

Abstract: Aiming at the security problem of single authorization center in cloud storage environment, a revocable multi-authority access control based on CP-ABE model and federated block chain is proposed. Attribute Authority (AA) is described in a tree structure. At the same time, the Trusted Certificate Chain (TCC) and Membership Service Provider (MSP) are used to manage the identity and control the permissions of the nodes in the Chain. By embedding the user key into the ciphertext, the retractable cloud access control technology is realized, and the re-encryption process is performed by the cloud service provider, which reduces the encryption burden of the data owner. Experimental verification and analysis show that the proposed scheme has lower computational cost and higher security.

Key words: cloud access control; consortium blockchains; attribute revocation; attribute encryption

1 引言

随着云计算技术的发展,云存储为用户提供方便的数据存储和管理服务,越来越多的敏感数据被外包到云中.因此建立有效的访问控制机制是保障云数据安全的重要举措之一^[1].Sahai 和 Water^[2]提出了基于属性的加密机制,它提供了一种具有细粒度访问控制的加密方案.基于属性的加密可分为密钥属性加密 KP-ABE 和密文属性加密 CP-ABE.在 KP-ABE 中,密文通过属性集合加密而密钥根据访问策略生成.在 CP-ABE 中,密文通过访问策略加密而密钥根据属性集合生成.由于 CP-ABE 契合云环境下的访问机制,受到了国内外学者的广泛研究.王悦等人^[3]分析了云访问控制中的安全隐患并提出了一种高效的隐藏访问策略的 CP-ABE 方案,可以有效保护访问策略中的敏感信息,但其不支持属性撤销功能.文献^[4]讨论了基于属性的云访问控制中用户属性撤销的问题,采用安全外包机制,在系统中实现了密文和密钥的恒定大小,同时不需要定期更换密钥.但其使用的第三方服务器需要一直保持服务,对稳定性有较高的要求.郑良汉等人^[5]提出了一种基于区块链的多授权访问控制方案,但其并没有给出具体的实现方式.联盟链是一种新兴的区块链技术,仅限于联盟成员参加,成员参与联盟链运行需要按照规则获取读写记账的权限.利用联盟链实现属性验证和密钥颁发,可以对访问控制中的属性策略和属性集进行细粒度的管理,增加系统的可信性和可追溯性^[6].同时,将密钥颁发机制融入智能合约,并在合约中加入身份管理和权限控制,以增强系统的可靠性和公正性.

2 相关知识

乘法循环群 G 可用二元组 (g, p) 描述,其中 g 为 G 的生成元, p 为 G 中的元素个数,即群的阶数. G 中元素满足: $G = \{g^m \mid m \in \mathbb{Z}_p\}$, $\mathbb{Z}_p$ 为正整数.循环群哈希函数是一种可将数据映射到乘法循环群 G 中的特殊函数,即 $H(\{0, 1\}^*) \rightarrow G$.

2.1 双线性映射

双线性映射是验证审计聚合证据的重要数学工具.双线性映射可用四元组 (p, G_1, G_2, e) 描述,设 G_1 和 G_2 是两个质数阶乘法循环群,其阶数都为大质数 p ,定义映射关系 $e: G_1 \times G_1 \rightarrow G_2$,满足下列性质:

(1) 双线性:对于任意 $a, b \in \mathbb{Z}_p$ 和 $R, S \in G_1$,有 $e(R^a, S^b) = e(R, S)^{ab}$;

(2) 非退化性:存在 $R, S \in G_1$,使得 $e(R, S) \neq 1_{G_2}$ (1_{G_2} 代表 G_2 的单位元);

(3) 可计算性:存在有效的算法对任意的 $R, S \in G_1$,计算的 $e(R, S)$ 值.

2.2 访问树

本方案采用 CP-ABE 中的访问结构树来构建.访问结构树也称访问树,是访问策略的表现形式之一.如图 1 所示,访问树由叶子节点和非叶子节点组成.叶子节点由用户的属性组成,非叶子节点由若干个子节点的集合和阈值组成.每个节点处都存放有一个随机值,与密文解密相关的秘密存放在根节点处.不同的用户属性可以解密不同的叶子节点值,当叶节点达到阈值时,可以解密上层父节点.只有 $User_1$ 和 $User_4$ 可以得到根节点处的值,因为他们的属性集满足访问结构树.

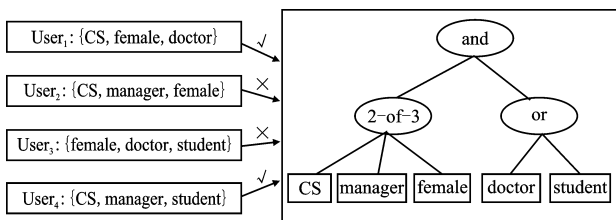


图 1 访问树结构

2.3 拉格朗日差值定理

假定存在 x 的 m 次多项式 $f(x)$,若给出它的 $m+1$ 个各不相同的点 $(x_i, f(x_i))$,则能够计算出 x 对应的唯一 $f(x)$ 值:

$$f(x) = \sum_{1 \leq k \leq n} f(x_k) \left(\prod_{1 \leq j \leq n, j \neq k} \frac{x - x_j}{x_k - x_j} \right)$$

令拉格朗日系数为 $\Delta_{i, S'_x}(x) = \prod_{i \in S, i \neq j}$

$\frac{x - x_j}{x_i - x_j}$,式中, $i, S \in \mathbb{Z}_p^*$.

3 RMACB 方案构造

3.1 方案概述

提出的基于联盟链的访问控制模型如图 2 所示,框架基于 CP-ABE 访问控制模型进行了改进, RMACB 模型包含 6 个实体:云服务提供商(CSP)、属性认证中心(ACA)、属性撤销中心(ARA)、密钥颁发中心(KIA)、数据拥有者(DO)、用户(User). ACA 中有 i 个节点,每个节点负责一个属性 Att_i ,与 KIA 共同生成密钥 SK 和重加密密钥;ARA 负责更新用户属性的撤销,并将撤销属性相关的用户和数

第 i 行组织在其通道内未拥有第 j 列的权限,反之则拥有该权限.

4 算法定义与实现

RMACB 模型包含个 6 个算法:即 Setup 算法、Encrypt 算法、UKeyGen 算法、AKeyGen 算法、REncrypt 算法、Decrypt 算法,具体描述如下:

(1) Setup 算法

建立算法需要选择一个素数 p 作为双线性群 G_0 的阶,其生成元为 g . Setup 算法由 KIA 执行,选择两个随机数 $\alpha, \beta \in Z_p$,生成系统公钥 P_K 和主密钥 M_K . 保持 P_K 公开, M_K 机密:

$$P_K = \{g, G_0, h = g^h, e(g, g)^\alpha\}, M_K = \{\beta, g^\alpha\}$$

(2) Encrypt 算法

Encrypt 算法由 DO 运行,通过系统公钥 P_K 以及访问策略 Γ 对数据 M 进行加密生成密文 C_T . 只有满足访问策略的用户才能对 C_T 进行解密. 首先该算法需要为访问策略 Γ 中的每个节点 x 设置一个次数为 $d_x = k_x - 1$ 的多项式 q_x , 然后该算法选择一个随机数 $s \in Z_p$ 使根节点处的多项式满足 $q_R(0) = s$. 对于其他节点, 其设置的多项式满足 $q_x(0) = q_{\text{parent}(x)}(\text{index}(x))$, 因此通过 d_x 个子节点的值即可完全定义父节点处的多项式 q_x .

设 Y 为访问策略 Γ 中叶子节点的集合, 该算法生成的密文 C_T 为:

$$C_T = \{\Gamma, C = M \cdot e(g, g)^\alpha, C' = h^s, \forall y \in Y: C_y = g^{q_y(0)}, C'_y = H(\text{att}(y))^{q_y(0)}\}$$

(3) UKeyGen 算法

UKeyGen 算法由 ACA 运行, 当新用户加入系统时, 需要向 ACA 请求属性认证时. 首先, 用户将唯一身份凭证 uid 发送给 ACA, 然后 ACA 对用户进行属性检查并生成用户密钥 k_u , 最后 ACA 随机生成用户密钥 $k_u \in Z_p$ 并将用户 uid、用户属性集 A_u 和 k_u 通过共识机制写入到通道 AC-KI 的超级账本中. 此外, ACA 需要将 k_u 发送给用户, 由用户进行保存.

(4) AKeyGen 算法

AkeyGen 算法由 KIA 运行, 输入主密钥 MK 和用户属性集合 A_u , 输出属性相关的密钥 S_K . 该算法选择一个随机数 $r \in Z_p$, 并为属性集合 A_u 中的每个属性 Att_i 选择一个随机 $r_i \in Z_p$. 则计算得到密钥 S_K 为:

$$S_K =$$

$$\{D = g^{(\alpha+r)\beta},$$

$$\forall \text{Att}_i \in A_u, D_j = g^r \cdot H(j)^{r_j}, D'_j = g^{r_j}\}$$

(5) REncrypt 算法

REncrypt 算法需要 KIA、CSP 共同运行, 输入密文 CT 以及对应的用户访问列表从而输出重加密密文 RT. 用户访问列表包含用户 uid 以及对应的用户密钥 k_u . 选择一个随机数 $k \in Z_p$, 该算法将构造一个访问多项式:

$$P_{\text{acc}}(x) = (x - k_{u_1})(x - k_{u_2}) \cdots (x - k_{u_n}) + k$$

则重新加密的密文 R_T 是:

$$R_T = \{\Gamma, P_{\text{acc}}(x), \tilde{C} = (M \cdot e(g, g)^\alpha)^k, C' = h^s, \forall y \in Y: C_y = g^{q_y(0)}, C'_y = H(\text{att}(y))^{q_y(0)}\}$$

(6) Decrypt 算法

Decrypt 算法由用户运行, 输入重加密密文 R_T 、用户密钥 k_u 和密钥 S_K , 即可得到数据 M . 首先, 用户需要从访问多项式中恢复 k , 则只需将用户密钥 k_u 代入访问多项式 $P_{\text{acc}}(x)$ 中:

$$\begin{aligned} P_{\text{acc}}(x) &= (x - k_{u_1})(x - k_{u_2}) \cdots (x - k_u) \cdots (x - k_{u_n}) + k \\ &= (x - k_{u_1})(x - k_{u_2}) \cdots 0 \cdots (x - k_{u_n}) + k \\ &= k \end{aligned}$$

如果用户不在访问列表当中, 则无法从 $P_{\text{acc}}(x)$ 获得 k , 只能取得一个随机值. 当用户成功获得 k 之后, 则可恢复原始密文 C_T :

$$C_T = \{\Gamma, C = (\tilde{C})^{\frac{1}{k}}, C' = h^s, \forall y \in Y: C_y = g^{q_y(0)}, C'_y = H(\text{att}(y))^{q_y(0)}\}$$

然后用户使用 S_K 对 C_T 进行解密. 根据访问策略中节点位置的不同, 将其分为两种情况.

① 节点 x 为叶子节点. 如果节点 x 处的属性 $i = \text{Att}_x$ 属于用户属性集合 A_u , 即 $i \in A_u$, 则可通过 DecryptNode 计算:

$$\begin{aligned} \text{DecryptNode}(x) &= \frac{e(D_i, C_x)}{e(D'_i, C'_x)} \\ &= \frac{e(g^r \cdot H(i)^{r_i}, h^{q_x(0)})}{e(g^{r_i}, H(i)^{q_x(0)})} \\ &= e(g, g)^{q_x(0)} \end{aligned}$$

如果 $i \notin A_u$, 则 DecryptNode 的值为 NULL.

② 节点 x 为非叶子节点. 那么对于节点 x 的子节点 z , 均需要计算 DecryptNode(z) 并记为 F_z . 设 S_x 为节点 x 的 k_x 个子节点的集合, 如果存在 $z \in S_x$ 且 F_z 为 NULL, 则 F_x 也为 NULL, 否则 F_x 的计算如下:

$$\begin{aligned} F_x &= \prod_{z \in S_x} F_{z, S_x}^{\Delta_{i, S_x}^{(0)}} \\ &= \prod_{z \in S_x} (e(g, g)^{r \cdot q_z^{(0)}})^{\Delta_{i, S_x}^{(0)}} \\ &= \prod_{z \in S_x} (e(g, g)^{r \cdot q_{\text{parent}(z)}^{(0)} (\text{index}(z))})^{\Delta_{i, S_x}^{(0)}} \\ &= \prod_{z \in S_x} e(g, g)^{r \cdot q_z^{(i)} \cdot \Delta_{i, S_x}^{(0)}} = e(g, g)^{r \cdot q_x^{(0)}} \end{aligned}$$

式中, $i = \text{index}(z)$, $S'_x = \{\text{index}(z); z \in S_x\}$

如果访问策略 Γ 中节点的属性均在用户属性集合中 A_u , 则可计算得到根节点处的 F_r 值:

$$F_r = \text{DecryptNode}(r) = e(g, g)^{rs}$$

则 M 可以通过下式计算:

$$\begin{aligned} &C / (e(C', D) / F_r) \\ &= C / (e(h^s, g^{(a+r)\beta}) / e(g, g)^{rs}) \\ &= M \end{aligned}$$

5 安全性与性能分析

5.1 安全性分析

在 Water 提出的 CP-ABE 算法中已经对其安全性进行了证明, RMACB 模型中的访问控制方法在 CP-ABE 的基础上增加了重加密阶段, 因此将从数据安全性、抗合谋攻击和属性撤销安全等方面进行分析。

(1) 数据安全性

在该算法中, 攻击者为了解密, 则必须恢复访问策略中的 $e(g, g)^s$ 和密文对应的用户密钥 k_u . 只有攻击者拥有足够多的属性密钥, $e(g, g)^s$ 才可以被计算得出. 而用户密钥 k_u 是一个随机值, 非预期用户的用户密钥从 $P_{\text{acc}}(x)$ 中只能获得一个错误值, 因此该算法可以有效保护数据的安全性。

(2) 抗合谋攻击

如果多个用户串通, 那么这些用户必须拥有解密密文所需要的属性密钥, 由于合谋用户所拥有的属性是随机的, 因此难以恢复通过组合密钥的方式恢复密文. 同时 k_u 无法通过拉格朗日插值法来获取, 除了满足访问策略的用户拥有之外, 只有 KIA 保存有该值. 任何数量的用户合谋都无法获得正确的用户密钥, 因此 RMACB 的访问控制方案是抗共谋的。

(3) 属性撤销安全

在本方案中, 当 ARA 对一个或多个属性进行撤销时, 只需要高性能 CSP 完成重加密工作. 新的重加密密文与更新后的可访问用户有关, 属性密钥和用户密钥并没有改变. 因此本方案的属性撤销有

很高的即时性和安全性.

5.2 性能分析

RMACB 以联盟链为核心, 将云访问控制过程中所涉及的各方有机地组织起来, 以 CP-ABE 为算法基础, 相较于其他云访问控制方案, RMACB 具备特征如表 1 所示.

表 1 模型特征比对

名称	访问控制	属性撤销	可追溯性	授权中心
Zhao ^[4] 等方案	支持	支持	支持	单个
郑 ^[5] 等方案	支持	不支持	不支持	多个
RMACB	支持	支持	支持	多个

相较于其他审计方案, RMACB 在联盟链的支持下, 为云存储完整性审计提供了安全保障. 虽然无法保证本方案有最短的密文长度, 但本方案采用 CSP 重加密的方式, 保障了系统的效率. 且本文方案在密文中嵌入了用户密钥, 减少了属性撤销时的运算消耗。

为了测试 RMACB 的性能, 以 Hyperledger 构架为基础模型, 搭建实验联盟区块链系统, ACA 节点数量与系统属性数量一致, KIA 和 ARA 各 4 个节点, 各组织节点均部署在 Openstack 云平台上. 算法过程基于 cpabe-0.11 库进行编写. 用户由个人 PC 模拟, 采用属性数量逐渐增加的方式来测试各方案的算法性能, 每种结果取 20 次测量的平均值。

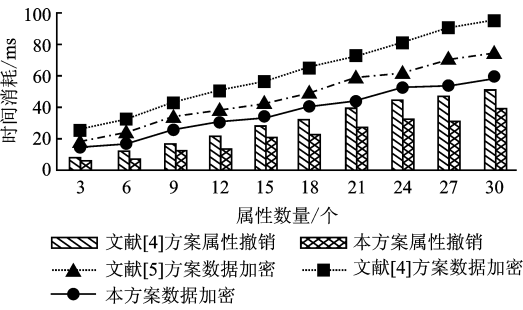


图 4 数据加密和属性撤销消耗

图 4 表示的是用户加密以及属性撤销的时间开销. 由图可知, 三个方案加密过程的开销都随着系统的属性数量线性增加, 这是由于加密开销与密文长度呈线性关系, 而属性数量的增加会导致密文长度的线性增加. 同时, 本方案将重加密过程交给高性能 CSP 来处理, 减少了加密开销与通信消耗. 因此, RMACB 的时间消耗均小于其他两个方案. 在属性撤销方面, 由于本方案不需要重新颁发密钥, 节省了大量的计算消耗, 相较文献[4]的方案, 时间缩短近 30%.

6 结束语

本文提出了一种基于联盟链的云访问控制模型,通过建立联盟成员身份管理机制实现了联盟节点组织和权限的控制,有效保障了系统的安全性和稳定性.除此之外,将数据加密分为两个阶段,实现了安全高效的属性撤销.最后通过理论和实验分析,证实了 RMACB 具有良好的性能.

参考文献:

[1] 王于丁,杨家海,徐聪,等. 云计算访问控制技术研究综述[J]. 软件学报, 2015, 26(5): 1129-1150. DOI: 10.13328/j.cnki.jos.004820.
WANG Y D, YANG J H, XU C, et al. Survey on access control technologies for cloud computing [J]. Journal of Software, 2015, 26(5): 1129-1150. DOI: 10.13328/j.cnki.jos.004820.

[2] SAHAI A, WATERS B. Fuzzy identity-based encryption[C]//Proceedings of the 24th International Conference on the Theory and Applications of Cryptographic Techniques. Aarhus, Denmark: Springer, 2005. DOI: 10.1007/11426639_27.

[3] 王悦,樊凯. 隐藏访问策略的高效 CP-ABE 方案[J]. 计算机研究与发展, 2019, 56(10): 2151-2159. DOI: 10.7544/issn1000-1239.2019.20190343.
WANG Y, FAN K. Effective CP-ABE with hidden access policy[J]. Journal of Computer Research and Development, 2019, 56(10): 2151-2159. DOI: 10.

7544/issn1000-1239.2019.20190343.

[4] ZHAO Y, REN M, JIANG S Q, et al. An efficient and revocable storage CP-ABE scheme in the cloud computing [J]. Computing, 2019, 101(8): 1041-1065. DOI: 10.1007/s00607-018-0637-2.

[5] 郑良汉,何亨,童潜,等. 云环境中的多授权机构访问控制方案[J]. 计算机科学与探索, 2020, 14(11): 1865-1878. DOI: 10.3778/j.issn.1673-9418.1911020.
ZHENG H L, HE H, TONG Q, et al. Multi-authority access control scheme in cloud environment [J]. Journal of Frontiers of Computer Science and Technology, 2020, 14(11): 1865-1878. DOI: 10.3778/j.issn.1673-9418.1911020.

[6] 刘敖迪,杜学绘,王娜,等. 基于区块链的大数据访问控制机制[J]. 软件学报, 2019, 30(9): 2636-2654. DOI: 10.13328/j.cnki.jos.005771.
LIU A D, DU X H, WANG N, et al. Blockchain-based access control mechanism for big data[J]. Journal of Software, 2019, 30(9): 2636-2654. DOI: 10.13328/j.cnki.jos.005771.

作者简介:

张艺帆 男,(1997-),硕士研究生.研究方向为云计算与安全. E-mail:zhangyf@cumt.edu.cn.

庄 富 男,(1996-),硕士研究生.研究方向为云计算与安全.

林果园 男,(1975-),博士,副教授.研究方向为云计算安全、信息系统安全.