

混合云下面向隐私保护的访问控制方法

屠袁飞^{1,2,3}, 夏 峰¹, 杨 庚^{2,3}

(1 南京工业大学 计算机科学与技术学院, 江苏 南京 211816; 2 南京邮电大学 计算机学院, 江苏 南京 210003; 3 江苏省无线传感网高技术研究重点实验室, 江苏 南京 210003)

摘 要: 基于属性的加密(Attribute-based encryption, ABE)已被广泛研究,其支持细粒度的访问控制可用来共享数据,然而存储容量大以及计算开销大使其难以得到广泛运用.将现有的支持属性匿名的 ABE 算法的密文数据进行分割并分别存储在不同的云环境中,用于匹配且计算量与存储量小的部分存储在私有云中,利用先匹配后解密思路提高系统的整体运行效率.从正确性、安全性以及复杂性等方面做出证明,通过与以往的部分 ABE 算法进行对比以及给出的具体实验说明方案的可行性.

关键词: 云计算;基于属性的访问控制;混合云;隐私保护

中图分类号: TP393

文献标识码: A

文章编号: 1000—7180(2016)10—0053—06

Privacy-preserving Ciphertext-Policy Attribute-Based Encryption in Hybrid Cloud

TU Yuan-fei^{1,2,3}, XIA Feng¹, YANG Geng^{2,3}

(1 School of Computer Science and Technology, Nanjing Tech University, Nanjing 211816, China;
2 College of Computer Science & Technology, Nanjing University of Post & Telecommunication, Nanjing 210003, China; 3 Jiangsu High Technology Research Key Laboratory for Wireless Sensor Networks, Nanjing 210003, China)

Abstract: Attribute-based encryption(ABE) has been widely studied recently to support fine-grained access control of shared data, but the file size and cost of computing make it hard to be widely used. This paper aims to solve the problem using hybrid cloud. This paper modify the existing privacy-preserving method to store some message with small size and low computing cost in the private cloud for matching, users could decrypt the file in the public cloud only after the matching phase under the “match-then-decrypt” method. The proposed construction is proven to be secure and the experiment result shows the solution is efficient and practical.

Key words: cloud computing; attribute-based access control; hybrid cloud; privacy-preserving

1 引言

随着云计算的流行,云存储技术的研究也受到越来越多的关注,作为云计算概念上衍生出来的一种技术,云存储可以有效利用网络中的存储资源,从而达到资源复用与节约成本的目的,但如何在云环境中提供高效安全的访问控制却备受关注.

作为一种一对多的公钥密码学原语,密文政策的基于属性的加密(Ciphertext-Policy Attribute-Based Encryption, CP-ABE)^[1]可用于实现云计算环境下的细粒度的数据共享.文献[2]提出第一个 CP-ABE 方案,但在方案中加密者把访问策略与密文一起发送给用户,因此将导致用户隐私的泄露.Yu 等人^[3]用了混合加密这种方式,解决 ABE 本身

收稿日期: 2016—03—17; 修回日期: 2016—05—08

基金项目: 国家自然科学基金资助项目(61572263, 61272084);江苏省高校自然科学研究重大项目(11KJA520002);高等学校博士学科点专项科研基金资助课题(20113223110003)

难以加密大型文件的缺陷. 文献[4]提出在密文中加入猜测访问结构的方式, 实现了访问结构的隐藏的 CP-ABE 方案, 此外还提出了一种基于属性的广播加密方案, 并证明了此方案具有更好的灵活性. Zhang 等人^[5]提出带有高效解密的 ABE 方案, 将解密分块, 以降低整个解密的负担. Zhu 等人^[6]提出一种新的基于属性层级的 ABE 方案, 方案采用一种紧凑的表示方法, 可降低密文与密钥的大小. 文献[7]对以往的多权威授权方式进行改进, 提出隐私保护分散的 CP-ABE 方案.

然而在目前复杂的云环境中, 云服务器并非完全可信, 为实现访问策略的隐私保护, 除了修改、完善已有的 CP-ABE 方案, 还有学者从云结构等方面做出研究. Zhang 等人^[8]的方案中安全的混合云是一种新型的云计算框架, 将公共数据和敏感数据分开存储. Zhou 等人^[9]则根据数据分割的基本思想, 将带有语义信息的属性集分成许多子集, 消除彼此间的相关性, 从而保护了数据隐私. 文献[10]采用一个混合云的架构, 达到数据使用过程中保护数据隐私的作用. Qin 等人^[11]采用李雅普诺夫优化技术, 设计了一个动态的控制算法, 控制混合云的整体运营成本随时间的推移而不断增大的问题.

本文的主要工作是对以往的算法进行修改, 设计出一种在混合云环境下使用的 CP-ABE 方案, 将密文数据进行分离, 然后再存储在混合云中, 以此达到隐私保护的需求. 本文最后分析了本方案的效率与安全, 并给出实验结果.

2 系统方案

2.1 系统模型

本文采用混合云的解决方案, 图 1 展示了本系统方案中的几个主要实体.

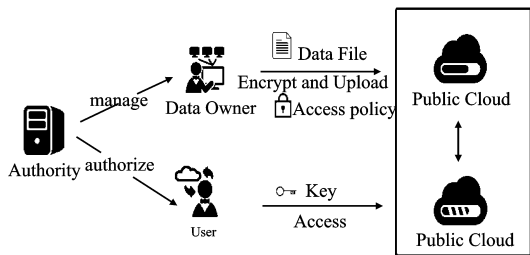


图 1 系统模型

本方案包含五个组成部分: 授权中心 (Authority Center)、数据属主 (Data Owner)、用户 (User)、公有云 (Public Cloud) 与私有云 (Private Cloud). 授

权中心主要负责生成系统参数并对方案中所有的用户进行授权管理, 数据属主将随机的选取一个访问策略, 并将隐私数据进行加密, 密文分开存储在公有云与私有云中, 用户为访问云中的数据, 首先需要与私有云中的信息进行匹配, 成功之后方可从公有云处下载密文进行解密.

2.2 安全模型

方案基于以下两个假设.

定义 1 (The Decisional Bilinear Diffie-Hellman Assumption, DBDH 假设) 令 $a, b, c, z \in_R Z_p$, 且 $g \in_K G$. 若在多项式时间内不可能以明显的优势区分出 $[g, g^a, g^b, g^c, g^z]$ 和 $[g, g^a, g^b, g^c, e(g, g)^{abc}]$, 假设成立.

定义 2 (The Decision Linear Assumption, D-Linear 假设) 令 $z_1, z_2, z_3, z_4, z \in_R Z_p$, 且 $g \in_K G$. 若在多项式时间内不可能以明显的优势区分出 $[g, g^{z_1}, g^{z_2}, g^{z_1 z_3}, g^{z_2 z_4}, g^z]$ 和 $[g, g^{z_1}, g^{z_2}, g^{z_1 z_3}, g^{z_2 z_4}, g^{z_3 + z_4}]$, 假设成立.

另外, 假设方案中个主体之间的通信信道完全安全. 此方案的安全模型可以定义为包含一个敌手 A 和一个挑战者 S 的游戏, 其中 A 可以看做是一个用户, S 即为我们系统中的混合云, 以下是该游戏的具体方案.

① 启动: A 首先提交两个密文政策 W_0^*, W_1^* .

② 建立: S 选择一个充分大的安全参数 λ , 然后运行 Setup 算法算出主密钥 MK 和公钥 PK , S 保留 MK , 并把 PK 传给 A .

③ 查询阶段 1: 除了散列查询, A 还发出一个如下的多项式时间界限内的查询来产生密钥:

A 提交一个属性集 L , 若 (L 满足 W_0^* 且 L 满足 W_1^*) 或者 (L 不满足 W_0^* 且 L 不满足 W_1^*), S 把密钥 SK_L 给 A , 否则将输出任意参数.

④ 挑战: 一旦 A 认定查询阶段 1 已经结束, A 将从文件空间中输出两个等长的文件 M_0, M_1 , 以这两个文件来挑战密文政策 W_0^*, W_1^* . 若能够查询到 L 中存在一个密钥使得 L 满足 W_0^* 且 L 满足 W_1^* 同时成立, 则可以得到 $M_0 = M_1$. S 选择 $v \in_R \{0, 1\}$, 并计算 $CT_{W_v^*} = \text{Encrypt}(PK, M_v, W_v^*)$, 把 $CT_{W_v^*}$ 传送给 A .

⑤ 查询阶段 2: 和查询阶段 1 一样.

⑥ 猜测: A 输出一个猜测的 $v' \in \{0, 1\}$, 如果 $v' = v$, 则 A 赢得该游戏.

A 在该游戏中的优势定义为 $\text{Adv}(A) =$

$$\left| \Pr[v' = v] - \frac{1}{2} \right|.$$

定义 3 在没有明显优势下,敌手能够在多项式时间内破解该游戏的概率是非常小的,则文中采用的匿名的 CP-ABE 算法将被认为是安全的。

2.3 方案详述

本文采用“先匹配后解密”的思想,在混合云架构上进行数据的分割存储,使之能够更好地应用于云环境中。方案主要包含系统建立、为用户授权、创建新文件、访问文件。图 2 反映了方案的基本流程, Data Owner 为数据属主, User 为用户, AC 为授权中心, Public Cloud 为公有云, Private Cloud 为私有云。AC 开始生成公钥和主密钥,并为用户授权,将两把密钥发送给用户,数据属主加密文件并分别存储于公有云和私有云中,用户向混合云发出访问请求时,需要分别通过私有云和公有云,然后才可以得到密文进行解密。

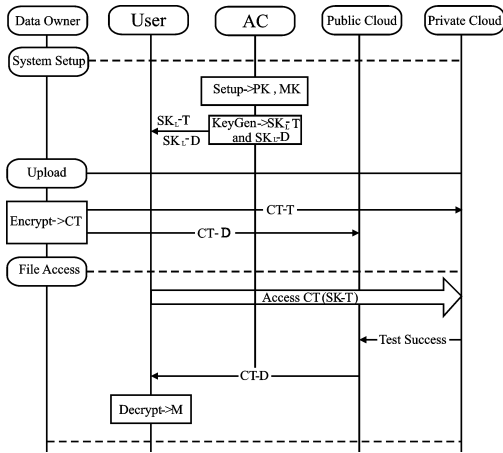


图 2 方案流程

2.3.1 系统建立

算法: Setup(1^λ)

输入: 系统安全参数 λ

输出: 公钥 PK, 主密钥 MK

令 G, G_T 是阶数为 p 的两个乘法循环群 (p 为大素数), 定义 $e: G \times G \rightarrow G_T$ 是双线性映射, 并定义 hash 功能函数 $H: \{0, 1\}^* \rightarrow G$. 假定全集中有 n 个属性, 一般的属性集定义为 $U = \{\omega_1, \omega_2, \dots, \omega_n\}$, 每一个属性具有多个值, 其中 $S_i = \{v_{i,1}, v_{i,2}, \dots, v_{i,n_i}\}$ 是属性 ω_i 的多属性值的集合, 且 $|S_i| = n_i$. y, g_1, g_2 满足 $y \in_R Z_p, g_1, g_2 \in_R G$, 计算 $Y = e(g_1, g_2)^y$. 得到系统公钥 $PK = \langle g, g_1, g_2, Y \rangle$, 主密钥 $MK = \langle y \rangle$.

2.3.2 为用户授权

授权中心 CA 根据用户的属性集 L 对用户进行授

权, 将产生的私钥按照功能分成用于匹配和用于解密的两个部分, 加密完成之后两把密钥同时传输给用户。此步骤调用 KeyGen 算法, 得到用户的私钥 SK_L .

算法: KeyGen(PK, MK, L)

输入: 公钥 PK, 主密钥 MK, 用户的属性集 L

输出: 私钥 SK_L

令 $L = [L_1, L_2, \dots, L_n]$ 为用户属性集. CA 选择

$r_1, r_2, \dots, r_{n-1} \in_R Z_p$, 计算 $r_n = y - \sum_{i=1}^{n-1} r_i \bmod p$. 另 CA 选择 $r \in_R Z_p$, 且 $\{\hat{r}_i, \lambda_i, \hat{\lambda}_i \in_R Z_p\}_{1 \leq i \leq n}$, 令 $\hat{r} = \sum_{i=1}^n r_i$, 计算 $[\hat{D}_0, D_{\Delta,0}] = [g_2^{y-\hat{r}}, g_1^r]$. 当 $1 \leq i \leq n$ 时, 做如下计算:

$$[D_{\Delta,i}, D_{i,0}, D_{i,1}, \hat{D}_{i,0}, \hat{D}_{i,1}] = [g_2^{\hat{r}_i} H(i \parallel v_{i,k_i})^r, g_2^{\lambda_i}, [g_1^{r_i} H(0 \parallel i \parallel v_{i,k_i})^{\lambda_i}, g_1^{\hat{\lambda}_i}, g_2^{r_i} H(1 \parallel i \parallel v_{i,k_i})^{\hat{\lambda}_i}]]$$

式中, $L_i = v_{i,k_i}$. 私钥为 $SK_L = \langle \hat{D}_0, D_{\Delta,0}, \{D_{\Delta,i}, D_{i,0}, D_{i,1}, \hat{D}_{i,0}, \hat{D}_{i,1}\}_{1 \leq i \leq n} \rangle$, 发给用户时需将其分成两部分, 用于匹配的为 $SK_L - T = \langle \hat{D}_0, D_{\Delta,0}, \{D_{\Delta,i}\}_{1 \leq i \leq n} \rangle$, 用于解密的为 $SK_L - D = \langle \{D_{i,0}, D_{i,1}, \hat{D}_{i,0}, \hat{D}_{i,1}\}_{1 \leq i \leq n} \rangle$.

2.3.3 创建新文件

由于 ABE 算法自身复杂性问题, 导致其不适于加密大型数据文件, 因此本文采用与文献[3]一样的方式首先采用对称加密加密文件, 再采用本文中的公钥加密方法加密对称密钥, 得到密钥的密文, 步骤如下。

(1) 首先为密文选一个身份标识 ID.

(2) 随机从密钥空间中选取一个对称加密的密钥 DEK(Data Encryption key), 用此加密文件。

(3) 根据用户定义的访问结构, 调用文中的 Encrypt 算法加密对称密钥 DEK, 得到密钥密文 CT_w , 并将密文拆成两个部分上传。

算法: Encrypt(PK, M, W)

输入: 系统公钥 PK, 明文 M , 访问结构 W

输出: 对 DEK 加密的密文 CT_w

定义密文策略 $W = [W_1, W_2, \dots, W_n]$, 为了在该密文政策下加密文件 M , 选取 $s, s', s'' \in_R Z_p$, 并计算 $\tilde{C} = MY^s, C_{\Delta} = e(g, g)^s Y^{s'}, C_0 = g^s, \hat{C}_0 = g_1^{s'}, C_1 = g_2^{s''}, \hat{C}_1 = g_1^{s-s''}$. 当 $1 \leq i \leq n$ 与 $1 \leq t \leq n_i$ 时, 按如下方式计算 $[C_{i,t,\Delta}, C_{i,t,0}, \hat{C}_{i,t,0}]$.

1. 当 $v_{i,t} \in W_i$ 的时候, 可知 $[C_{i,t,\Delta}, C_{i,t,0}, \hat{C}_{i,t,0}] = [H(i \parallel v_{i,t})^{s'}, H(0 \parallel i \parallel v_{i,t})^{s''}, H(1 \parallel i \parallel v_{i,t})^{s-s''}]$.

2. 若 $v_{i,t} \notin W_i$, $[C_{i,t,\Delta}, C_{i,t,0}, \hat{C}_{i,t,0}]$ 输出 G 中的

任意元素.

因此密文为

$$CT_W = \langle C_\Delta, C_0, \hat{C}_0, \tilde{C}, C_1, \hat{C}_1, \{ \{ C_{i,t,\Delta}, C_{i,t,0}, \hat{C}_{i,t,0} \}_{1 \leq i \leq n_i} \}_{1 \leq i \leq n} \rangle$$

完成后上传至云服务器的文件存储格式如图 3 所示.

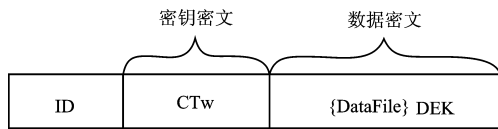


图 3 加密数据文件的格式

将密文按功能分为两部分,上传私有云中的为 $CT_W - T = \langle C_\Delta, C_0, \hat{C}_0, \{ \{ C_{i,t,\Delta} \}_{1 \leq i \leq n_i} \}_{1 \leq i \leq n} \rangle$, 用于用户访问文件时的身份匹配;另一部分 $CT_W - D = \langle C_1, \hat{C}_1, \tilde{C}, \{ \{ C_{i,t,0}, \hat{C}_{i,t,0} \}_{1 \leq i \leq n_i} \}_{1 \leq i \leq n} \rangle$, 用于解密, 其有别于匹配部分, 将单独存储在公有云里面.

2.3.4 访问文件

用户向混合云发出访问文件的有关请求,私有云首先进行私钥匹配,若匹配成功,私有云对共有云发出确认信息,反之用户将得不到密文,用户收到公有云中的密文之后进行解密. 此阶段调用 Decrypt 算法.

算法: Decrypt(PK, CT_W, SK_L)

输入: 公钥 PK, 密文 CT_W, 私钥 SK_L

输出: 明文 M(即对称密钥 DEK)

1. 匹配阶段: 用户首先向私有云发出访问请求, 并进行等式(1)中的匹配, 检查 L 是否满足 W:

$$\begin{aligned} & \frac{e(\hat{C}_0, \hat{D}_0 \prod_{i=1}^n D_{\Delta,i})}{e(\prod_{i=1}^n C_{i,t,\Delta}, D_{\Delta,0})} \\ &= \frac{e(g_1^{s'}, g_2^{y^{-r}} \prod_{i=1}^n (g_2^{\hat{r}_i} H(i \| v_{i,t})^r))}{e(\prod_{i=1}^n H(i \| v_{i,t})^{s'}, g_1^r)} \\ &= e(g_1^{s'}, g_2^{y^{-r}} \prod_{i=1}^n g_2^{\hat{r}_i}) \\ &= e(g_1^{s'}, g_2^{y^{-r}} g_2^{\hat{r}}) \\ &= e(g_1^{s'}, g_2^y) \\ &= e(g_1, g_2)^{s'} \\ &= \frac{C_\Delta}{e(g, C_0)} \end{aligned}$$

式中, $L_i = v_{i,t}$. 若 L 满足 W, 则用户通过匹配, 私有云将发送确认信息给公有云, 否则用户将得到一个随机值.

2. 解密阶段: 若满足匹配则公有云返回密文进行解密, 用户对密文的操作如下:

$$\begin{aligned} & M' \\ &= \frac{\tilde{C} \prod_{i=1}^n e(C_{i,t,0}, D_{i,0}) e(\hat{C}_{i,t,0}, D_{i,0})}{\prod_{i=1}^n e(C_1, D_{1,1}) e(\hat{C}_1, D_{1,1})} \\ &= \frac{M \cdot e(g_1, g_2)^{s''} \prod_{i=1}^n e(H(0 \| i \| v_{i,t})^{s''}, g_2^{\hat{k}}) e(H(1 \| i \| v_{i,t})^{s''}, g_1^{\hat{k}})}{\prod_{i=1}^n e(g_2^{s''}, g_1^r) H(0 \| i \| v_{i,t})^{\hat{k}} e(g_1^{r-s'}, g_2^r) H(1 \| i \| v_{i,t})^{\hat{k}}} \\ &= \frac{M \cdot e(g_1, g_2)^{s''}}{\prod_{i=1}^n e(g_2^{s''}, g_1^r) e(g_1^{r-s'}, g_2^r)} \\ &= \frac{M \cdot e(g_1, g_2)^{s''}}{\prod_{i=1}^n e(g_1, g_2)^{s''}} \\ &= M \end{aligned}$$

式中, $L_i = v_{i,t}$, 由上述等式用户可解密出明文 M(即对称密钥 DEK).

3 方案分析

3.1 安全性分析

若存在一个敌手(带有优势 σ) 不能够在多项式时间内在安全模型中攻击本文结构, 可认为 σ 是可以忽略的, 且 $\sigma \leq \sigma_{\text{DBDH}} + n\sigma_{\text{DL}}$, 其中 σ_{DBDH} 和 σ_{DL} 代表 DBDH 挑战和 D-Linear 挑战的优势要素, n 表示全集中属性元素的个数.

敌手 A 提交的访问策略为 $W_0^* = [W_{0,1}^*, W_{0,2}^*, \dots, W_{0,n}^*]$ 和 $W_1^* = [W_{1,1}^*, W_{1,2}^*, \dots, W_{1,n}^*]$. 根据安全模型, 我们使用一个序列的混合游戏来证明 A 不能在 G 中定义有不可忽略的概率下赢得原始的安全游戏. 首先把游戏 G 修改成游戏 G_0 , G 和 G_0 的定义除了产生挑战密文的方式不同, 其他一样. 在 G_0 中, 若敌手没有密钥 SK_L (其中 L 既能满足 W_0^* 又能满足 W_1^*), 则挑战密文中的 $\tilde{C} \in_R G_T$, 其他正常. 若敌手拥有上述 SK_L, 则挑战密文将会完全正确地产生, 这种情况下, $G = G_0$. 在任意情况下, 以下两个引理都成立:

引理 1 在 DBDH 条件下, 拥有安全参数 λ 时, A 在 G 和 G_0 中的优势没有区别, 即 $|\Pr[\epsilon] - \Pr[\epsilon_0]| \leq \sigma_{\text{DBDH}}$.

之后, 改变 $\{ \{ C_{i,t,\Delta}, C_{i,t,0}, \hat{C}_{i,t,0} \}_{1 \leq i \leq n_i} \}_{1 \leq i \leq n}$ 和做如下的一些定义来改变游戏 G_0 . 对于满足 $(v_{i,t} \in W_{0,i}^* \wedge v_{i,t} \in W_{1,i}^*)$ 或者 $(v_{i,t} \notin W_{0,i}^* \wedge v_{i,t} \notin W_{1,i}^*)$ 的 $v_{i,t}$, $\{ C_{i,t,\Delta}, C_{i,t,0}, \hat{C}_{i,t,0} \}$ 将会正常产生. 另一种情况, 对于满足 $(v_{i,t} \in W_{0,i}^* \wedge v_{i,t} \notin W_{1,i}^*)$ 或者 $(v_{i,t} \notin W_{0,i}^* \wedge v_{i,t} \in W_{1,i}^*)$ 的 $v_{i,t}$, 则原本应由游戏 G_{l-1} 正常产生的 $\{ C_{i,t,\Delta}, C_{i,t,0}, \hat{C}_{i,t,0} \}$ 将会在新游戏 G_l 中被来自群 G 中的随机元素所取代. 过程重复至没有满足 $(v_{i,t} \in W_{0,i}^* \wedge v_{i,t} \notin W_{1,i}^*)$ 或 $(v_{i,t} \notin W_{0,i}^* \wedge v_{i,t} \in W_{1,i}^*)$ 的 $v_{i,t}$. 最后, 即使 A 得到密文, 其优势也会是 0. 通过使用 G_l 中群 G 的随机元素来代替

G_{l-1} 中正常的密文成分的方法,可嵌入一个 D-Linear 挑战到密文中,即有如下引理 2:

引理 2 在 D-Linear 条件中,拥有安全参数 λ 时, A 在 G 和 G_0 中的优势没有区别. 即 $1 \leq l \leq l_{\max}$ 时, $|\Pr[\epsilon_{l-1}] - \Pr[\epsilon_l]| \leq \sigma_{DL}$.

假定以上的游戏为 $\{G, G_0, G_1, \dots, G_{l_{\max}}\}$, G 是原始攻击游戏, $G_{l_{\max}}$ 是最终没有给 A 任何优势的攻 击游戏. ϵ 是 G 里 $v' = v$ 情况, ϵ_l 是 G_l 里 $v' = v$ 的情 况 ($0 \leq l \leq l_{\max}$), 可得 $\sigma = \left| \Pr[\epsilon] - \frac{1}{2} \right| = |\Pr[\epsilon] - \Pr[\epsilon_{l_{\max}}]|$, 据三角形公理, 可知 $\sigma \leq |\Pr[\epsilon] - \Pr[\epsilon_0]| + \sum_{l=1}^{l_{\max}} |\Pr[\epsilon_{l-1}] - \Pr[\epsilon_l]| \leq \sigma_{DBDH} + n\sigma_{DL}$.

由此说明 σ 是微不足道的, 因而本方案在 DBDH 假设和 D-Linear 假设下是安全的.

3.2 效率分析

本小节将从安全性以及密文密钥长度来将本文 算法与部分已有算法进行对比.

表 1 中给出了各方案的访问结构、安全性假设 以及是否匿名方面的比较, 为了简化对比方式, 将定 义如下几个符号: $|G|$ 为群 G 中元素长度 ($|G_T|$ 类 似), $|Z_p|$ 为 Z_p 的长度, $|W|$ 为访问结构中所有 元素的总长度, n 为所有属性的个数, $n' = \sum_{i=1}^n n_i$ 为所有属性的所有取值情况. 表 2 用 PK、MK、SK、 CT 代表系统公钥、主密钥、私钥及密文.

表 1 安全性对比表

scheme	Access Structure	Complexity assumption	Anonymous
BSW ^[2]	Tree	Generic group model	No
ZHW ^[4]	AND gates ¹	DBDH	Yes
HSMZM ^[7]	AND gates ²	Q-PBDHE, q-SDH	Yes
Ours	AND gates ²	DBDH, D-Linear	Yes

注: AND gates¹ 表示支持正负值的与门, AND gates² 表示支持多种值的与门.

表 2 密文密钥长度对比

scheme	PK	MK	SK	CT
BSW ^[2]	$3 G + G_T $	$ G + 2 Z_p $	$(2n+1) G $	$(2n+1) G + G_T + W $
ZHW ^[4]	$(6n+2) G $	$2 Z_p $	$(2n+1) G $	$2 G + G_T + W $
HSMZM ^[7]	$6n G + n G_T $	$5n Z_p $	$2n G $	$(2n+3n') G + G_T $
Ours	$3 G + G_T $	$ Z_p $	$(5n+2) G $	$(3n+4) G + 2 G_T $

由于本文的密文分别存储于公有云与私有云 中, 因此实际的密文与密钥的长度如图 3 所示.

从表 3 中可知, 当 n 增大时, 存储在私有云中的 数据量将比存储在公有云中的要小很多, 因此可以 有效节省私有云的存储开销, 提高系统整体的效率.

表 3 方案实际存储部件

SK		CT	
SK _L -T	SK _L -D	CT-T	CT-D
$(n+1) G $	$4n G $	$(n'+2) G + G_T $	$(2n'+2) G + G_T $

4 实验仿真

实验环境: Inter(R) Core(TM) i5-3470 3.20 GHz CPU, 4.00 GB 内存, Windows 7 操作系统. 实 验中对称加密使用 128 bit AES (Advanced Encryp- tion Standard), 不计应用中的传输延时.

由于在方案开始、密钥生成以及加密的阶段没 有采取过多的改进方法, 其算法的运行时间还是随 着属性的个数增长而线性增加的, 因此本节并未列 出其仿真图. 图 4 中给出了方案的匹配时间, 图 5 中 给出了方案的解密时间.

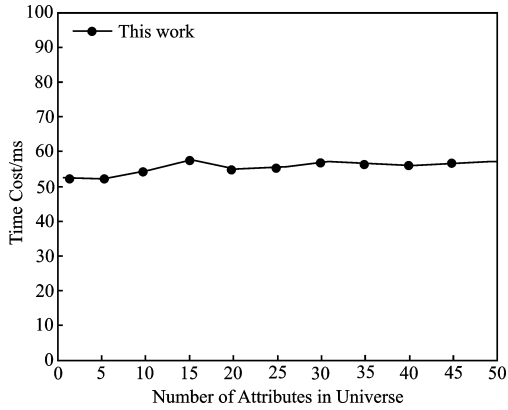


图 4 匹配时间

方案通过将原本的解密算法分拆成两个部分 (匹配、解密) 存储, 匹配部分单独存储在私有云中用 于匹配, 只有通过私有云中的匹配部分才会进行公 有云的解密操作, 而图 4 中匹配算法的运行时间是 基本固定而且计算量相对于图 5 中解密来说非常 小, 这个差距随着属性个数的增加, 会变得更加明 显. 因此若用户没有通过私有云中的匹配, 则没有必 要进行下一个步骤, 系统将直接返回一个随机值给 用户, 省去了方案中的解密操作, 由此降低了整体的 解密运行负担, 提高了方案效率.

5 结束语

云计算环境中用户的隐私保护一直是人们关注

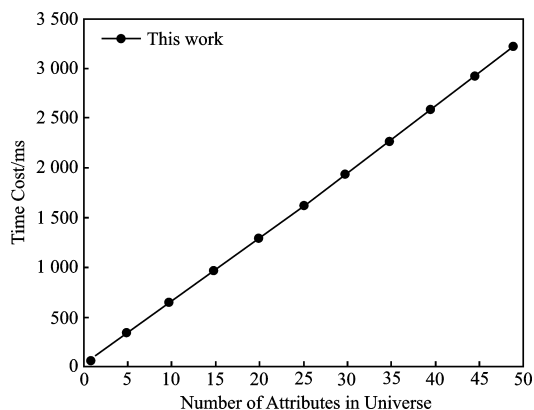


图5 解密时间

的焦点,在使用基于属性的加密算法保护用户隐私的同时也不能对用户或系统造成过重的负担。本文采用混合云的架构,使用数据分割的思想将 CP-ABE 算法的密文分别存储在公有云与私有云中,减轻云存储的负担,提升整体的运行效率,实验结果表明,本方案是可行且有效的。进一步的工作将会扩展本文中提出的算法,以适应除与门外更加普遍的访问结构,使其更适合实现现实的云计算中复杂的访问控制。

参考文献:

- [1] Goyal V, Pandey O, Sahai A, et al. Attribute-Based encryption for fine-grained access control of encrypted data[C] // Computer and Communications Security Conference. New York: ACM, 2006: 89-98.
- [2] Bethencourt J, Sahai A, Waters B. Ciphertext-Policy attribute-based encryption[C] // IEEE Symposium on Security and Privacy. Berkeley: IEEE, 2007: 321-334.
- [3] Yu S C, Wang C, Ren K, et al. Achieving secure, scalable, and fine-grained data access control in cloud computing [C] // INFOCOM. Piscataway: IEEE, 2010: 534-542.

- [4] Zhou Z B, Huang D J, Wang Z J. Efficient privacy preserving ciphertext-policy attribute based-encryption and broadcast encryption[J]. IEEE Transactions on Computers, 2015, 64(1):126-138.
- [5] Zhang Y H, Chen X F, Li J, et al. Anonymous attribute-based encryption supporting efficient decryption test[C] // ACM Conference on Computer and Communications Security. NY, USA: ACM, 2013: 511-516.
- [6] Zhu Y, Huang D J, Hu C J, et al. From RBAC to ABAC: Constructing flexible data access control for cloud storage services[J]. IEEE Transactions on Services Computing, 2014, 8(4): 601-616.
- [7] Han J G, Susilo W, Mu Y, et al. Improving privacy and security in decentralized ciphertext-policy attribute-based encryption[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(3):665-678.
- [8] Zhang K, Zhou X, Chen Y, et al. Sedic: Privacy-aware data intensive computing on hybrid clouds[C] // Acm Conference on Computer & Communications Security. New York: ACM, 2011: 515-525.
- [9] Zhou Z G, Zhang H L, Du X J, et al. Prometheus: Privacy-aware data retrieval on hybrid cloud[C] // INFOCOM. Turin: IEEE, 2013: 2643-2651.
- [10] Li J W, Li J, Chen X F, et al. Privacy-preserving data utilization in hybrid clouds [J]. Future Generation Computer System, 2014, 30(1):98-106.
- [11] Qin X J, Li H X, Wu C, et al. Cost-minimizing dynamic migration of content distribution services into hybrid clouds[J]. Parallel and Distributed Systems, IEEE Transactions on, 2015, 26(12): 3330-3345.

作者简介:

屠袁飞 男, (1984-), 博士研究生, 助理工程师. 研究方向为数据隐私保护与访问控制. E-mail: 935127868@qq.com.

杨庚 男, (1961-), 博士, 教授, 博士生导师. 研究方向为网络安全、分布与并行计算、大规模科学与工程计算.

(上接第 52 页)

- [7] 罗钧旻, 李俊伟. Agent 自我意识的研究[J]. 微电子学与计算机, 2015, 32(12): 72-75.
- [8] 罗钧旻, 罗建龙. 基于互表性的个性化网页研究[J]. 微电子学与计算机, 2013, 30(3): 12-15.
- [9] 罗钧旻, 桑蓓蓓. 基于动态本体的语义 B/S 研究[J]. 微电子学与计算机, 2014, 31(8): 136-138.
- [10] Decker S, Melnik S, VanHarmelen F, et al. The semantic web: The roles of XML and RDF[J]. IEEE Internet Computing, 2000, 4(5): 63-74.

- [11] McGuinness D L, van Harmelen F. OWL Web ontology language overview[R]. W3C Recommendation, 2004.

作者简介:

罗钧旻 男, (1963-), 博士, 教授. 研究方向为人工智能.

赵丹(通讯作者) 女, (1992-), 硕士. 研究方向为人工智能. E-mail: zd754603233@126.com.

高武奇 男, (1975-), 博士, 副教授. 研究方向为人工智能.

黄姝娟 女, (1975-), 博士, 讲师. 研究方向为嵌入式与网络.