基于 CP-ABE 的可撤销属性加密访问控制算法

屠袁飞[1,2,3] 高振宇[3] 李荣雨[3]
(南京邮电大学通信与信息工程学院 南京 210003)[1]
(江苏省无线传感网高技术研究重点实验室 南京 210003)[2]
(南京工业大学计算机科学与技术学院 南京 211800)[3]

摘 要 为了增强计算机网络的安全性,保证网络中的信息资源不被非法使用,需要进行访问控制。当前基于网格虚拟组织的访问控制算法通过在网格中建立不同的信任域、在主机之间建立基于身份和行为的访问控制策略,实现以任务发起者为中心的网格虚拟组织的跨域访问控制,建立互信的核心算法并进行逻辑推理,从而实现访问控制算法。但是,这类算法可能会使非法使用的网络被判定为安全网络,因此访问控制的准确度不高。为此,提出一种基于 CP-ABE 的可撤销属性加密访问控制算法,为实现访问控制,首先构建基于 CP-ABE 的可撤销属性加密访问控制的访问树,并通过 CP-ABE 完成访问控制的初始构建和密钥生成。在此基础上,为提高可撤销属性加密访问控制算法的访问控制效果,在加密算法以及解密算法中写入新文件创建、新用户授权、吊销用户、文件访问等方面过程的设计,实现基于 CP-ABE 的可撤销属性加密访问控制算法。实验结果表明,采用所提算法进行访问控制时耗时缩短,控制效果较好,且实现过程有所简化,对该领域的研究发展起到了积极作用。

关键词 CP-ABE,可撤销属性加密,访问控制
中图法分类号 TP393 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2018.11.027

Removable Attribute Encryption Access Control Algorithm Based on CP-ABE

TU Yuan-fei[1,2,3] GAO Zhen-yu[3] LI Rong-yu[3]
(College of Communications & Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)[1]
(Jiangsu High Technology Research Key Laboratory for Wireless Sensor Networks, Nanjing 210003, China)[2]
(College of Computer Science & Technology, Nanjing Tech University, Nanjing 211800, China)[3]

Abstract In order to enhance the security of the computer network and ensure that the information resources in the network will not be used illegally, access control is needed. Based on the access control algorithm of grid virtual organization, the existing algorithms established a different trust domain in the grid, achieved the identity and behavior based access control strategy between the hosts, realized the cross-domain access control of grid virtual organization and the establishment of mutual trust in the core algorithm and logical reasoning, so as to achieve access control algorithm. But these algorithms may make the illegal network as a secure network, so the accuracy of access control is not high. In order to achieve the access control, a removable attribute encryption access control algorithm based on CP-ABE was proposed. First, the access tree based on CP-ABE which can be used to encrypt the access control is constructed. Initial building and key generation of access control are completed through CP-ABE. On the basis of this, writing new file creation, new user authorization, revocation of users, file access and other aspects of the process are designed in the encryption algorithm and decryption algorithm, so as to improve the access control effect of revocable attribute encryption access control algorithm. The experimental results show that the proposed algorithm is easy to control, the consuming time of access control is reduced and the control effect is better. In addition, the implementation process of proposed method is simplified, and this study plays a positive role in the development of research in this field.

Keywords CP-ABE, Revocable attribute encryption, Access control

---

到稿日期:2017-07-21 返修日期:2017-10-05 本文受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:无线传感器网络数据融合安全关键技术研究(11KJA520002),高等学校博士学科点专项科研基金资助课题(20113223110003),中国博士后科学基金(2015M581794),江苏省博士后科研资助计划(1501023C),南京邮电大学校级科研基金(NY214127)资助。

屠袁飞(1984—),男,博士,助理工程师,主要研究领域为云计算安全与访问控制,E-mail:tuyuanfei01@163.com;**高振宇**(1992—),男,硕士生,主要研究领域为计算机应用技术、信息安全与密码学,E-mail:gaozhenyu_071027@163.com(通信作者);**李荣雨**(1977—),男,博士,副教授,主要研究领域为先进控制、机器学习、模拟优化。

1　引言

随着计算机网络的发展和普及，互联网技术被广泛应用于生活的各个领域，其为人们生活带来便利的同时，网络安全也成为了人们关注的重点[1-2]。在这种背景下，访问控制技术应运而生且快速发展，尤其是私有云技术被广泛应用，访问控制算法的研究也越来越深入，并成为研究的热点课题[3]。可撤销属性加密访问控制算法是访问控制算法的重要组成部分，为计算机网络安全带来了重要变革[4-5]。当前基于 ACAHSP 的访问控制算法[6]，在分析访问控制需求的基础上，分析服务聚合中访问的情景构成要素，并对构成情景的不同要素进行定义；在动态情景状态的状态演算和规则演算机制下，建立服务聚众模型，根据 CP-ABE 算法提出了服务聚众模型的安全验证算法，从而实现访问控制算法。这种算法由于访问控制的准确度高、访问控制效果好而成为当前研究的主要算法，引起了相关专家学者的广泛关注[7]。随着对计算机网络安全重视程度的增加，该课题逐渐成为相关专家学者研究的重点课题，随着研究内容的深入，产生了大量的研究成果。

文献[8]提出了一种基于异构服务聚合的协同访问控制算法。首先，分析访问服务的性能，确定访问控制需求，从多维角度完成情景要素的构成，对访问的动态情景构成要素进行分析；然后，以动态情景状态为依据，建立状态演算和规则演算的机制，构建动态情景约束下的服务聚众模型。在此基础上，利用 CP-ABE 给出访问控制模型的安全验证算法，从而完成访问控制。但是，该算法存在访问控制效率低的问题。文献[9]提出了一种支持更新操作的数据空间访问控制算法。首先，根据数据空间的数据更新，提出支持更新操作的映射算法；将动态数据映射到关系数据库中，定义支持更新操作权限的访问控制规则；建立与关系数据库访问控制规则之间的转换规则，以访问请求动态重写算法为依据，建立用户访问请求来检索相关访问控制规则，从而实现支持动态更新的访问控制算法。但是，这种算法存在访问控制精确度不高的问题。文献[10]提出了一种面向云计算环境的属性访问控制模型。首先，以属性访问控制算法为依据，确定本地域和跨域访问决策；然后，对属性访问控制模型进行形式化描述，并给出决策的核心算法；通过一种信号量和 P/V 操作机制实现属性表的调用和更新的互斥问题，从而实现域间属性的同步。但是，这种模型的应用范围较窄，不利于推广使用。

针对上述问题，文中提出一种基于 CP-ABE 的可撤销属性加密访问控制算法。首先，构建可撤销属性加密访问树，并利用 CP-ABE 算法实现访问控制的初始构建、密钥生成、加密算法以及解密算法过程，实现基于 CP-ABE 的可撤销属性加密的初始访问控制；在此基础上，通过对可撤销属性加密访问控制中新文件创建、新用户授权、吊销用户、文件访问等方面过程的设计，实现基于 CP-ABE 的可撤销属性加密访问控制算法。实验结果表明，所提算法进行访问控制的速度快、精确度高，进行访问控制花费的时间较短，对该课题的研究发展起到了积极作用，能推动该课题向应用领域迈进。

2　基于 CP-ABE 的可撤销属性加密访问控制算法

2.1　CP-ABE 属性加密过程

CP-ABE 属性加密过程为：访问控制方法由加密方制定，通过相互之间的秘密共享，密文与访问控制方法相关联，而用来解密的密钥则与属性集合密切相关。为实现以 CP-ABE 为基础的可撤销属性加密访问控制算法，需要对访问树进行构建。

访问树 T 表示访问结构的树。利用访问控制的属性对树中每一个节点属性加以解释，访问树中每个由子节点和阈值描述的阈门由非叶子节点表示[11]。假设叶子节点上的子节点的数量为 num_x，节点的阈值为 k_x，则有 $0<k_x\leqslant num_x$。当 T 表示一个根节点为 R 的访问树，T_x 表示树根为 x 的访问树 T 的子树时，可将 T 写为 T_r。当属性集合 γ 是访问树 T_x 的属性时，存在：

$$T_x(\gamma)=1 \tag{1}$$

若 x 表示非叶子节点，求非叶子节点 x 的子节点 x' 的 $T_{x'}(\gamma)$ 值，当且仅当不少于 k_x 个子节点返回 1 时，$T_x(\gamma)$ 返回 1。假设 x 是叶子节点，仅当 $att(x)\in\gamma$（其中 $att(x)$ 表示与叶子节点相关的属性）时，$T_x(\gamma)$ 返回 1。

CP-ABE 可撤销属性加密访问算法的具体相关变量及其定义如下。

若 G_0 是一个阶为素数 p、生成元为 g 的双线性群，则双线性映射 e 可以表示为：

$$e:G_0\times G_0\rightarrow G_1 \tag{2}$$

CP-ABE 算法中的拉格朗日系数为 $\Delta_{i,s}$。对 CP-ABE 算法初步构建 Setup，生成密钥 KeyGen，加密算法 Encrypt 以及解密算法 Decrypt 的过程如下。

算法 Setup$(g,G_0,\alpha,\beta)\rightarrow(PK,MK)$。其中，$\alpha,\beta\in Z_p$ 表示两个随机选择的指数；公钥 PK 由双线性群 G_0、生成元 g 等组成；主密钥 MK 由随机指数 β 和生成数据 g^{α} 组成。

为生成算法密钥，首先需要为访问控制的每个属性选择随机指数 $r\in Z_p$，并通过式(3)和式(4)计算 D_y 和 D_j。

$$D_y=g^r\cdot H(j)^{rj} \tag{3}$$

$$D_j'=g^{rj} \tag{4}$$

通过 $D=g^{(\alpha+\beta)/\beta}$，$\forall j\in S:D_y=g^r\cdot H(j)^{rj}$ 和 $D_j'=g^{rj}$ 组成算法的密钥。

在算法的加密过程中，针对决策树 T 中的节点 x，为其选择一个多项式 q_x，并且设定节点的阈值比该多项式的次数大 1。首先从决策树的根节点 R 开始，随机选择一个数 $s\in Z_p$，且设 $q_R(0)=s$；然后在多项式中选择其他点，完成完整定义。

密钥的生成是通过决策树的访问结构完成的。设定决策树 T 中叶子节点的集合为 Y，则叶子节点 $y\in Y$，通过式(5)和式(6)对叶子节点中的密钥组成要素进行计算。

$$C_y=g^{q_y(0)} \tag{5}$$

$$C_y'=H(att(y))^{q_y(0)} \tag{6}$$

可以看出：CP-ABE 算法的密钥是由 $T,C'=Me(g,g)^{\alpha s},C=h^s,\forall y\in Y:C_y=g^{q_y(0)}$ 以及 $C_y'=H(att(y))^{q_y(0)}$ 组成的。

CP-ABE 算法的解密过程可以转化为递归算法 DecryptNode(CT,SK,x) 的执行过程，因此该递归算法的执行过程可以描述如下。

对于叶子节点 x，令 $i=att(x)$，当 $i\in S$ 时，定义 DecryptNode(CT,SK,x) 为：

$$\text{DecryptNode}(CT,SK,x)=\frac{e(D_i,C_x)}{e(D_i',C_x')}=e(g,g)^{rq_x(0)} \tag{7}$$

若 $i \notin S$，则递归算法的执行过程可以定义为：

$$\text{DecryptNode}(CT, SK, x) = \perp \tag{8}$$

当 x 表示非叶子节点时，可以通过递归算法 DecryptNode(CT，SK，z)将其存储为 F_z。若 S_x 表示任意 k_x 大小的子节点 z 的集合，且存在 $F_z \neq \perp$，则可以计算：

$$F_x = \prod_{z \in S_x} F_z^{\Delta i, S_x'(0)} = e(g,g)^{r \times q_x(0)} \tag{9}$$

利用递归算法定义 CP-ABE 算法的解密过程，从决策树的根节点开始利用递归函数。设定属性集合 S 满足访问决策树 T，则：

$$A = \text{DecryptNode}(CT, SK, r) = e(g,g)^{rs} \tag{10}$$

由此完成 CP-ABE 算法的解密过程。基于上文描述，首先构建访问决策树，对 CP-ABE 算法实现访问控制的初始构建和密钥生成，并对加密算法以及解密算法的过程进行描述，从而实现 CP-ABE 属性加密。

2.2 基于 CP-ABE 的可撤销属性加密访问控制算法

为实现基于 CP-ABE 的可撤销属性加密访问控制算法，在 2.1 节的基础上，对新文件创建、新用户授权、吊销用户、文件访问等方面进行过程设计。

在进行访问控制时，数据拥有者 DO 确定通用属性集 U 和最大属性规模数 $n_{\max}$，完成密钥更新节点 $KUN(rl,t)$ 和吊销节点在访问路径 $Path(u_{id})$ 时的计算，从而产生公钥参数 P_K 和主密钥 M_K。

若有新的用户要访问，数据拥有者 DO 首先要完成对新申请用户的验证，然后完成如下步骤：

1)为该访问用户分配标识符和属性集 $S \subset U$，该标识符具有唯一性。

2)产生具有安全性的密钥，用于确定该访问地址曾经是否被使用过，需要对访问地址 u_{id} 进行不同的运算。假设被使用过，则确定属性是否与之前相同；假设没有被使用过，则为该用户选择一个叶节点(要求该叶节点未在吊销树上被使用过)并将其与 u_{id} 绑定，从而产生密钥。

3)使用 E_{PUUSR} 表示用户的公钥加密数据元组(P_K，S_K，S，$\delta_{o,(P_K,S_K,S)}$)。

4)利用公钥加密数据元组，从而实现访问用户的授权。

数据的拥有者根据用户的管理规则变更用户权限，具体过程如下。

1)在访问树中计算密钥更新节点 $KUN(rl,t)$ 和吊销节点的路径 $Path(u_{id})$，数据拥有者更新用户吊销列表 RL。

2)将用户管理规则作为数据拥有者变更用户权限的依据，数据拥有者输入时间戳 t 和吊销列表 RL，然后运用 CP-ABE 的密钥更新算法计算出更新信息 UI。

3)用新的时间戳 t，以(M，ρ)的格式对 CP-ABE 的 DEK 方法进行重新加密步骤，用 $CT(t)$ 表示密文。

在进行基于 CP-ABE 的可撤销属性加密访问控制过程中，首先对访问者的有效性进行验证，并将通过验证的访问者的访问请求文件发送到计算机中，从而实现访问控制。

3 实验结果与分析

以 Intel P4 2GB 处理器为硬件环境，MATLAB 2008a 为平台，来证明本文所提基于 CP-ABE 的可撤销属性加密访问控制算法的有效性和可行性，实验环境如图 1 所示。通过模拟算法的实际运行情况，比较本文提出的属性加密访问控制算法和文献[8]、文献[9]所提属性加密访问控制算法的实际运行情况。

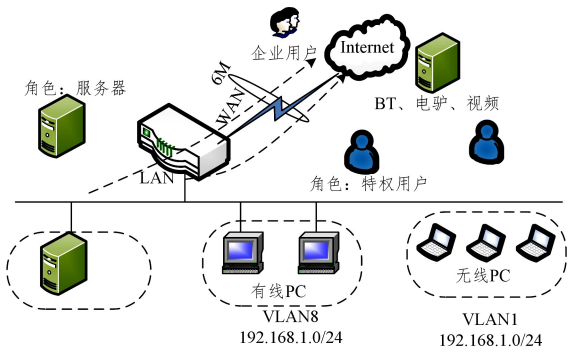

图 1 实验环境

Fig. 1 Experimental environment

首先比较 3 种算法进行访问控制时对网络拥堵程度的影响。假设以网络访问速度表示网络拥堵程度，通过实验得到 3 种算法对网络堵塞率的影响，对比结果如图 2 所示。

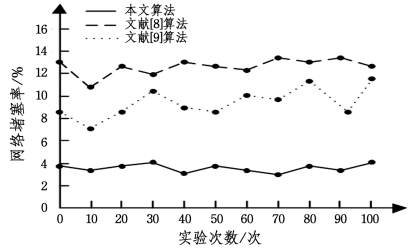

图 2 3 种算法的网络堵塞率对比

Fig. 2 Comparison of network congestion rate of three algorithms

通过图 2 可以看出，本文所提算法进行访问控制后的网络堵塞率低于文献[8]算法和文献[9]算法访问控制后的网络堵塞率，说明采用本文所提算法进行访问控制的速度较快，这是因为本文所提算法访问控制的过程较为简单。

然后对 3 种访问控制算法的丢包率进行对比。丢包率(%)的计算式如式(11)所示，图 3 给出了 3 种算法的丢包率对比。

$$\text{丢包率} = 1 - \frac{\text{进行访问控制的次数}}{\text{访问的总次数}} \tag{11}$$

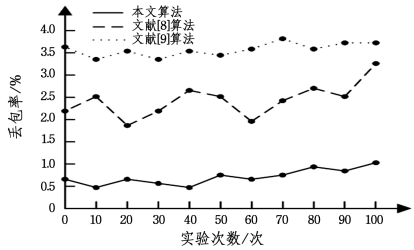

图 3 3 种算法的丢包率对比

Fig. 3 Comparison of packet loss rate of three algorithms

由图 3 可以看出，本文所提算法进行访问控制的丢包率低于文献[8]算法和文献[9]算法进行访问控制的丢包率，这说明本文算法进行访问控制的内容较为全面，访问控制效果较好。

图 4 对比了 3 种算法的网络延迟时间。

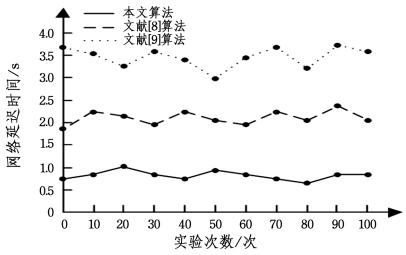

图 4　3 种算法的网络延迟时间对比

Fig. 4　Comparison of network delay time of three algorithms

通过图 4 可以看出，本文所提算法进行访问控制的网络延迟时间小于文献[8]算法和文献[9]算法的网络延迟时间，说明所提算法的访问控制速度较快。

最后对比了 CP-ABE 属性数为 15、用户数目小于 1000 时，3 种算法进行权限变更所需时间的结果如图 5 所示。

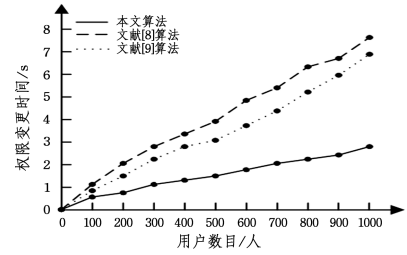

图 5　3 种算法进行权限变更所需时间的对比

Fig. 5　Comparison of required time for changing permissions of three algorithms

由图 5 可知，本文所提算法进行权限变更的速度快于文献[8]算法和文献[9]算法的速度，这是因为本文所提算法进行访问控制时权限变更的过程较简单，缩短了权限变更所需的时间。

综上所述，采用本文所提算法进行访问控制，访问控制后网络的堵塞率较低，因此本文所提算法进行访问控制的速度较快；采用本文所提算法进行访问控制的丢包率较低，因此访问控制的效果较好；另外，采用本文所提算法进行访问控制的计算过程也较为简单。因此，本文所提算法的使用效果较好，推动了该课题在研究领域的发展。

结束语　访问控制算法一直是计算机安全领域研究的重点问题，随着对计算机安全重视程度的加深，对访问控制的研究不断深入。针对当前访问控制算法存在的访问控制效率低、操作过程复杂等问题，文中提出了一种基于 CP-ABE 的可撤销属性加密访问控制算法。实验结果表明，本文所提算法能够有效提高访问控制的速度及效果，推动了该领域的研究发展。

参 考 文 献

[1] MA J. Design and implementation access control system based on the AWS[J]. Electronic Design Engineering, 2016, 24(6): 182-184. (in Chinese)
马洁. 基于 AWS 的访问控制系统设计与实现[J]. 电子设计工程，2016，24(6)：182-184.

[2] HU X Y. Cloud Storage Data Dynamic Access Control Method Research and Simulation[J]. Computer Simulation, 2017, 34(3): 365-368. (in Chinese)
胡晓燕. 云计算存储数据动态访问控制方法研究与仿真[J]. 计算机仿真，2017，34(3)：365-368.

[3] ZHOU M K. Design for Strategy of Safety Access Control Cloud Computing Based on CP-ABE and Improved Attribute Encryption[J]. Computer Measurement & Control, 2015, 23(1): 297-299. (in Chinese)
周明快. 基于 CP-ABE 的云计算改进属性加密安全访问控制策略设计[J]. 计算机测量与控制，2015，23(1)：297-299.

[4] HUANG Z P. Efficient Concurrent Access Control Algorithm Based on Distributed B Tree Encoding[J]. Bulletin of Science and Technology, 2015, 31(8): 81-83. (in Chinese)
黄正鹏. 基于分布式 B 树编译的高效并发访问控制算法[J]. 科技通报，2015，31(8)：81-83.

[5] WANG T, YU J P, HUANG M Q. A Fast ABE Scheme in Access Control of Cloud Storage[J]. Science Technology and Engineering, 2017, 17(1): 54-60. (in Chinese)
王廷，喻建平，黄敏强. 云存储访问控制中的快速属性基加密方案[J]. 科学技术与工程，2017，17(1)：54-60.

[6] LIU Y, CHEN C K, CUI Z R. Optimization Research on Adaptive Back off Tuning Medium Access Control Algorithm[J]. Computer Engineering, 2017, 43(1): 162-167. (in Chinese)
刘云，陈昌凯，崔自如. 自适应退避调整介质访问控制算法的优化研究[J]. 计算机工程，2017，43(1)：162-167.

[7] TU Y F, XIA F, YANG G. Privacy-preserving Ciphertext-Policy Attribute-Based Encryption in Hybrid Cloud[J]. Microelectronics & Computer, 2016, 33(10): 53-58. (in Chinese)
屠袁飞，夏峰，杨庚. 混合云下面向隐私保护的访问控制方法[J]. 微电子学与计算机，2016，33(10)：53-58.

[8] ZHANG X Y. Research on access control algorithm of heterogeneous services polymerizatio[J]. Journal of Sichuan University (Natural Science Edition), 2015, 52(6): 1277-1284. (in Chinese)
张秀玉. 异构服务聚合的协同访问控制算法研究[J]. 四川大学学报(自然科学版)，2015，52(6)：1277-1284.

[9] PAN Y, YUAN C A, LI W J, et al. Access Control Method for Supporting Update Operations in Dataspace[J]. Journal of Electronics & Information Technology, 2016, 38(8): 1935-1941. (in Chinese)
潘颖，元昌安，李文敬，等. 一种支持更新操作的数据空间访问控制方法[J]. 电子与信息学报，2016，38(8)：1935-1941.

[10] WANG J Y, FENG L X, ZHENG X F. Attribute-based access control model for cloud computing[J]. Journal of Central South University (Science and Technology), 2015, 46(6): 2090-2097. (in Chinese)
王静宇，冯黎晓，郑雪峰. 一种面向云计算环境的属性访问控制模型[J]. 中南大学学报(自然科学版)，2015，46(6)：2090-2097.

[11] HUANG Z P. Efficient Concurrent Access Control Algorithm Based on Distributed B Tree Encoding[J]. Bulletin of Science and Technology, 2015, 31(8): 81-83. (in Chinese)
黄正鹏. 基于分布式 B 树编译的高效并发访问控制算法[J]. 科技通报，2015，31(8)：81-83.

[12] LIU C Y, YU W S. Access Control Model of Learning Flow Based on Task and Role[J]. Journal of Chongqing University of Technology (Natural Science), 2013, 27(12): 72-76. (in Chinese)
刘长勇，余文森. 基于任务和角色的学习流访问控制模型[J]. 重庆理工大学学报(自然科学)，2013，27(12)：72-76.