文章编号:1671-4598(2015)01-0297-03　　中图分类号:TP393　　文献标识码:A

基于CP-ABE的云计算改进属性加密安全访问控制策略设计

周明快[1,2]

(1. 浙江大学 软件学院，杭州 310058；2. 浙江商业职业技术学院，杭州 310053)

摘要：针对云计算存储中心由于数据和访问控制的安全性无法得到有效保障，从而可能造成用户存储的敏感数据被盗取的问题，在对CP-ABE (eiphertext-policy attribute-based encryption) 进行深入分析的基础上提出了一种基于改进属性加密访问控制模型，对CP-ABE进行了改进，并对公钥和主密钥的生成、数据所有者加密文件、访问用户解密文件以及用户权限的全面管理过程均进行了详尽的定义和描述，从而设计了一种通用的安全访问机制；在仿真工具Ubuntu中进行实验，结果表明文中方法能有效地实现云计算环境下的安全访问控制，与其它方法相比，具有计算和存储开销低优点，具有较大的优越性。

关键词：云计算；属性加密；访问控制；密钥

Design for Strategy of Safety Access Control Cloud Computing Based on CP-ABE and Improved Attribute Encryption

Zhou Mingkuai[1,2]

(1. School of Software Technology, Zhejiang University, Hangzhou 310058, China;
2. Zhejiang Vocational College of Commerce, Hangzhou 310053, China)

Abstract: Aiming at safety of the data and access control in the cloud computing storage center not guaranteed comprehensively, mainly leading to losing the sensitive data of user, the CP-ABE is analyzed and a improved attribute encryption model is proposed. Then the CP-ABE is improved, the generation of public key and main key, the encryption of file of data owner, access of the encryption of file and the comprehensive manage process of user right are all described and defined, so a universal safety access control mechanism is designed. The experiment is operated in Ubuntu, the result shows the method in this paper can effectively realize access control with safety, and compared with the other methods, it has the properties of lower computing and storage expense, so it has some priority.

Keywords: cloud computing; attribute encryption; access control; key

0 引言

云计算[1] (cloud computing) 作为一种新型的高效计算模式应运而生，它是在分布式计算、网格计算和无线通信技术的基础上发展而来，目前已经成为信息技术领域的研究热点之一[2-3]。

云计算通过出租服务的方式，将各类应用云计算服务提供商 (cloud service providers, CSP) 并不是完全可信的，他们有可能在为用户提供存储服务的同时在挖掘用户隐私信息作为商业用途。如根据Gartner 2009年的调查显示，70%以上的企业认为对云计算数据安全性和隐私存有忧虑。同时发生在2009年的Google发生的用户文件外泄事件和亚马逊的简单存储服务中断导致的单一存储服务网站的瘫痪，使得人们对云计算的安全性有了更多的疑虑。目前，安全问题已经成为制约云A计算发展的重要因素[4-5]。

现有的加强云计算存储中心数据安全性的方法主要是通过单纯的加密技术来解决问题：如文献 [6] 设计了一种基于密钥策略的属性加密方法KP-ABE，但其缺少对请求加密数据的访问者进行直接控制的能力。文献 [7] 提出了一种基于CP-ABE算法密文访问机制。文献 [8] 通过公钥加密机制实现对访问控制机制建立访问能力，但该方法没有对用户权限退出的情况进行考虑。文献 [9] 在素数阶群上设计了一种支持单调的访问结构以及自适应的多授权安全密文策略。文献 [10] 设计了一个基于密文策略的属性加密实现方式，当属性满足密文对应的访问策略才能实现密文的解密。

上述工作都研究云环境下的安全存储问题，但没有对整个安全控制的过程进行全面的定义和描述。因此，本文提出了一种通用的基于属性加密的访问控制机制。

1 云计算安全访问机制和系统模型

1.1 云计算安全访问机制

云计算的安全访问控制机制通过对合法用户授权来访问指定资源。授权方法通常分为两类即密文机制和访问控制机制。

访问控制机制则是为用户建立访问控制列表来控制其访问特权，根据特定访问策略建立若干角色，并通过检查访问者的角色，实现对数据或系统的访问。

密文机制是采用文件加密密钥对信息进行加密，然后将加密密钥采用对称密钥进行加密，最后，将该对称密钥发送给授权用户。密文机制具有简单易于实现的优点，但仍然存在下列问题：数据所有者需要提供密钥管理机制，并对授权用户分发密钥，因此，当授权用户的数量很多时，该机制缺乏灵活性且

收稿日期:2014-08-27；　**修回日期**:2014-09-28。

基金项目:浙江省教育厅科研项目(Y201432304)。

作者简介:周明快(1981-)，男，浙江温州人，硕士研究生，高级工程师，主要从事云计算与信息安全方向的研究。

较为低效。此外，当合法用户的权限被撤销时，其权限所访问的信息需要重新被加密，最后，数据所有者需要实时在线实现授权用户的密钥重新分配和数据的重加密。

基于属性加密[11]（attribute-based encryption）的密文安全访问机制由 Sahai 和 Waters 在身份加密时首次提出，其门限访问策略阈值在加密过程始终不能改变。Goyal 等在其基础上将其划分为 KP-ABE 和 CP-ABE。由于 ABE 安全访问控制机制具有灵活和弹性粒度访问控制特性，因此，文中设计一种基于 CP-ABE 的属性加密安全访问控制模型。

1.2 系统模型描述

文中提出的安全访问机制的主要参与者主要包括：数据所有者（数据提供者）、云存储服务器和用户和可信数据中心，其相互之间的关系可以描述为图 1 所示。

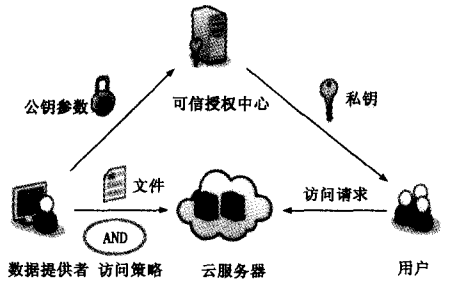

图 1 系统模型

文中描述的系统模型可以描述为：数据所有者将数据加密后存储在云服务器上，并将系统公钥和主密钥存储在可信授权中心；当用户对数据所有者上传的数据感兴趣时，向可信授权中心提交属性集合，可信授权中心判断其属性是否满足条件，当满足条件时，可信授权中心根据用户提供的属性生成私钥；用户在获得私钥后，当其属性集合满足密文数据的访问结构就可以实现对密文的解密。

2 CP-ABE 算法

CP-ABE（CP-ABE，cipertext-policy ABE）加密方案是基于密文策略和属性的加密方案，用户身份可以通过属性集合表示，加密数据与访问结构直接关联，用户解密密文的能力取决于密文所关联的属性集合与用户身份对应的访问结构是否完全匹配。

下面对 CP-ABE 算法中用到的属性、访问结构和访问树进行定义。

假设 $A=\{A_1,A_2,\cdots,A_n\}$ 为所有属性集合，则用户属性 UA 是 A 的非空子集，属性总个数为 n 的属性集一共可以定义 2^n 个属性子集，因此，最多可以鉴别 2^n 个用户。

访问结构 AS 是属性集 $A=\{A_1,A_2,\cdots,A_n\}$ 的一个非空子集，$AS\subseteq 2^{\{A_1,A_2,\cdots,A_n\}}$。当用户属性在访问结构 AS 中出现时，则为授权用户，否则为非授权用户。

访问树描述一个访问结构，树的每个叶节点表示表示属性项，访问树中除叶子节点外的每个节点都可以定义为一个多项式，多项式通常是关系运算符即与、或和门限等。

CP-ABE 算法主要包含 4 个组成部分：

1）Setup。数据拥有者生成主密钥 MK 和公钥 PK。

2）数据加密 Encrypt。数据拥有者采用 PK、访问结构 T 对明文数据进行加密，生成对应的密文。

3）生成私钥 KeyGen。用户采用主密钥和用户属性集 UA 生成私钥 SK。

4）解密密文 Decrypt。用户根据生成的私钥对密文进行解密得到明文数据。

3 改进的 CP-ABE 算法

3.1 公钥和主密钥计算

假设系统属性集 $A=\{A_1,A_2,\cdots,A_n\}$ 中的元素个数为 n，G 和 G_T 为素数阶 p 的乘法循环群，g 可以作为 G 的生成元，定义 G 上的双线形映射，且具有双线性、可计算性和非退化的特点。

随机定义 M 个群元素 $s_1,s_2\cdots s_M\in G$ 与系统属性 $A=\{A_1,A_2,\cdots,A_n\}$ 进行关联，随机选择两个指数 $a,b\in \mathbf{Z}_p$，则数据拥有者的系统公钥可以通过下式获得：

$$PK=\{g,e(g,g)^a,g^b,h_1,\cdots,h_M\} \tag{1}$$

主密钥可以通过下式计算：

$$MK=g^a \tag{2}$$

3.2 文件的加密

数据所有者对需要加密存储在云存储中心的文件设定唯一的一个 ID，随机选择一个对称密钥 SYK，采用对称密钥 SYK 对数据文件进行加密，并设置该文件的访问结构 μ，则加密后的密文可以表示为：

$$CT(t)=Encypt(PK,\{SYK,K_{si},K_{ve}\},u,t) \tag{3}$$

其中：t 表示加密过程时间戳，K_{si} 为签名密钥对应写权限，主要针对可写用户，当用户执行写操作后对数据进行签名，K_{ve} 为验证密钥对应读权限，主要针对只读用户，用于对签名结果进行验证。

然后，数据所有者将用户权限列表中的每个用户指定属性集 A_u，然后计算用户私钥：

$$K_{pru}=keyGen(MK,A_u) \tag{4}$$

在计算了用户的私钥 K_{pru} 后，并根据访问用户的公钥 K_{veu} 对其进行加密，并将其发送给访问用户。

数据拥有者将数据文件上传到云端进行存储，并将该文件共享的用户权限列表存储在云端，其中，包含了该文件可以访问的用户 ID，文件的有效状态，该文件共享的用户列表 UL 和已删除权限的用户列表。

3.3 用户授权获取和对文件的读写

云存储系统中的每个用户都有一个公私钥对 K_{pu} 和 K_{pr}，用户的公钥 K_{pu} 存储在用户证书中并对外公开用于验证信息来源的真实性；K_{pr} 由用户私有存储在客户端，由数据所有者在创建文件时发送，主要是对消息签名以保证数据来源的真实性。

当用户要读取加密文件 CT 时，用户通过在密钥体数据项中首先查询相应的访问结构 u、加密文件 EF 和签名 $Sign(F)$。

采用通过 $Decrypt(CT,K_{pr})$ 得到对称密钥 SYK 和验证密钥 K_{veu}，此时用户向可信授权中心发送认证请求，认证请求中包含对称密钥 SYK 和验证密钥 K_{veu} 的信息，可信授权中心将从云存储服务器上获得的用户权限列表中与 SYK 和 K_{veu} 进行比较，当匹配成功，则获得数据的访问权限。

此时，用户可以通过采用验证密钥来验证签名 $Sign(F)$ 的正确性，当签名正确时，通过 SYK 解密加密文件 EF 得到

数据明文。

3.4 用户权限控制

3.4.1 权限授予

用户权限的授予就是将用户的属性集加入到访问结构中，具体过程可以描述为：

数据所有者在文件 F 的密钥体中获得相应的密文 CT，采用自己的私钥和访问结构，即通过 $Decrypt(CT,K_{pr})$ 得到对称密钥 SYK、签名密钥 K_{si} 和验证密钥 K_{ver}，然后将用户的属性 A_u 访问集加入到访问结构中，即：

$$u' = u \vee A_u \tag{5}$$

此时，根据新的访问结构生成新的密文数据项：

$$CT'(t) = Encypt(PK,\{SYK,K_{si},K_{ve}\},u',t) \tag{6}$$

文件所有者将文件 F 的密钥体中的密文由 CT 更新为 CT'。

3.4.2 权限扩展

用户权限的授予就是将用户的属性集加入到访问结构中，具体过程可以描述为：

当数据所有者根据用户属性集根据式（4）生成私钥，然后根据该用户需要新增加的权限 pri，将对应的权限属性加入到元数据信息中，根据式（5）和式（6）生成访问结构 u 和新的数据项 CT'，并将 CT' 写入密钥体。

3.4.3 权限删除

用户权限的删除主要是将用户属性集从文件 F 密钥体的访问结构中去除，具体过程可以描述为：

当数据所有者根据用户属性集根据式（4）生成私钥，在密钥体数据项中首先查询相应的访问结构 u，将用户属性集从原有的访问结构中移除即 $u'=u-A_u$，然后数据所有者生成新的对称密钥 SYK'、签名密钥 K_{si}' 和验证密钥 K_{ve}'，此时生成新的数据密文即密钥体数据项：

$$CT'(t) = Encypt(PK,\{SYK',K_{si}',K_{ve}'\},u',t) \tag{6}$$

在此基础上，用户对文件 F 采用 K_{si}' 进行重新签名并采用 $CT'(t)$ 替换原来有的密钥体数据项 CT。

4 仿真实验

4.1 实验环境和参数

为了对文中方法进行验证，对文中方法进行实验，实验环境为：处理器为 Inter Core 2.2 GHz CPU，内存为 8 G，操作系统为 Windows 2012，虚拟机为 VMware Workstation 6.5.2，性能仿真软件为 Ubuntu 10.10，对文中算法从用户私钥产生的时间和存储空间两个角度进行计算，并与文献［9］和文献［10］进行比较，在试验中忽略数据在分布式网络中存在的传输延迟。

4.2 私钥产生时间比较

图 2 描述了随着属性个数变化数据所有者生成用户私钥的时间比较：

从图 2 中可以看出，3 种方法对应私钥产生时间随着属性个数由 0 变化到 100 的过程中呈现增加的趋势，文献［9］方法、文献［10］方法和文中方法的私钥产生时间平均约为 298 ms、262 ms 和 205 ms，文献［9］和文献［10］方法在属性个数小于 60 时，性能差别不大，但当属性个数大于 60 时，文献［9］方法增加的更快，而文中方法在整个仿真期间对应的私钥产生时间均少于另外两种方法。

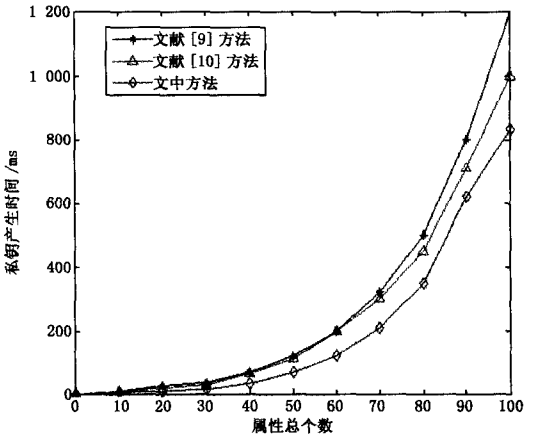

图 2　私钥产生时间随属性个数变化比较

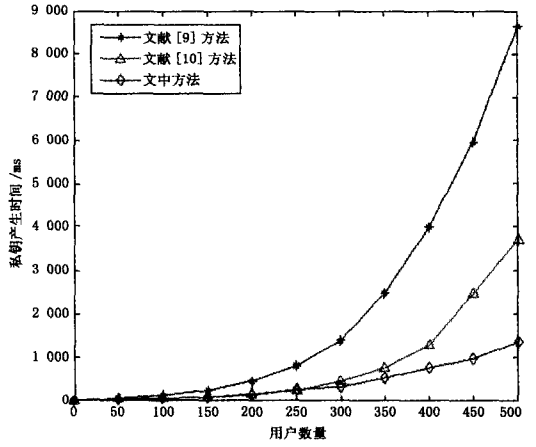

图 3　私钥产生时间随用户个数变化比较

从图 3 可以看出，随着用户个数从 0 到 500 的变化，三种方法对应的私钥产生时间呈现增长的趋势，但文献［9］方法增长的最快，文献［10］次之，文中方法增长的最为缓慢，文献［9］方法、文献［10］方法和文中方法的私钥产生时间平均约为 2 184 ms、829 ms 和 401 ms，显然文中方法的私钥产生时间远远低于另外两种方法。

从图 2 和图 3 的仿真结果可以发现，由于文中方法根据用户属性集和主密钥产生，因此，其产生的时间复杂度与密文长度无关，而另外两种方法与密文长度具有线性关系。由此可以看出，文中方法的私钥产生机制具有简单有效的优点。

4.3 存储空间比较

3 种方法的存储空间随着用户数目的从 0 到 500 的增加而变化的趋势如图 4 示：

从图 4 可以看出，3 种方法随用户数量从 0 到 500 变化的过程中，存储空间均呈增长趋势，且在前期增加较为迅速，而在后期增长较为缓慢，文献［9］方法、文献［10］方法和文中方法的存储空间大小平均约为 5.17 MB、4.36 MB 和 3.18 MB，显然文中方法相对文献［9］和文献［10］分别提高了 38.5%和 27.0%，显然，文中方法的更具有优越性，这是因为文中方法产生能将文件对应的密钥体信息进行更为紧致地存储，因此，具有相对较小的存储空间开销。

（下转第 303 页）

示，改善后的噪声信号串扰峰值为 147.4 mV 和－96.9 mV。

通过上图得出参考层 10 mil，线宽 6 mil，线间距 10 mil 的走线可以较大程度抑制信号线串扰现象。

4　结论

通过对系统典型模块的建模分析以及仿真，给出了时序仿真系统信号完整性问题的抑制和解决方法。

系统顶层和参考层层叠距离为 10 mil，采用 0.5 盎司（T =0.709 mil）铜箔厚度走线，差分线宽度 18.4 mil，线间距 12 mil，可有效匹配 USB 3.0 差分线 90 Ω 阻抗；采用 Semtech 公司的 RCLAMP0524J 器件可有效抑制 USB 接口静电攻击；IC 器件供电放置去耦电容减少地弹；信号线通过串联端接电阻抑制反射，减小过冲、振铃；通过软件仿真调整信号线宽和线间距减小串扰。

综上所述，对时序仿真系统进行信号完整性分析可以有效改善信号质量，提高系统可靠性。

参考文献：

[1] 孔　繁，盛卫星，韩玉兵，等. 基于矢量拟合的过孔等效电路提取方法 [J]. 电波科学学报，2013，28 (5)：869－876

[2] 陈建华，周立鹏，李　瑛. 差分对非对称性对信号完整性及噪声的影响 [J]. 河南大学学报：自然科学版，2013，34 (4)：45－50

[3] 张景璐，胡　赤，于　京. 利用眼图解决 USB 在布线中的信号完整性问题 [J]. 制造业自动化，2014 (1)：98－100

[4] 韩　刚，耿　征. 基于 FPGA 的高速度密度 PCB 设计中的信号完整性分析 [J]. 计算机应用，2010，30 (10)：160－185

[5] 吴　健，孔德升. 高速数据采集卡的信号完整性分析 [J]. 仪表技术与传感器，2013 (12)：93－96

[6] 张志伟. 高速互连总线结构中多评先传输线间串扰分析与控制 [J]. 计算机应用研究，2013，30 (12)：3729－3734

[7] 赵鑫斌，李龙海，周　磊，等. AFM 中高精度信号采集模块设计 [J]. 计算机测量与控制，2013，21 (10)：2875－2877

[8] Bob Dunstan. USB 3.0 Architecture overview. USB 3.0 Technical Workgroup Chair [R]. 2009.

[9] 刘雷波，赵　岩译. 信号完整性与 PCB 设计 [M]. 北京：电子工业出版社，2012.

[10] IPC－D-317N. Design Guidelines for Electronic Packaging Utilizing High-Speed Techniques [Z].

[11] 邱燕军，申功勋. 基于 DSP＋FPGA 的高速信号采集与处理系统的信号完整性分析 [J]. 测控技术，2007，26 (12)：8－11

[12] 李玉山，蒋冬初. 数字信号完整性：互连、封装的建模与仿真 [M]. 北京：机械工业出版社，2008：

（上接第 299 页）

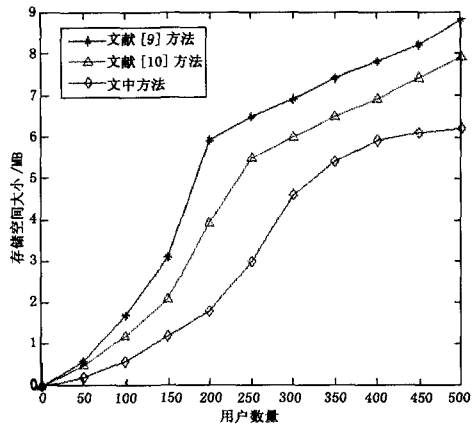

图 4　存储空间随用户个数变化比较

5　结论

为了实现云计算存储中心的有效和安全访问控制，并具有较小的计算和存储开销，文中设计了一种基于属性加密 CP-ABE 算法的安全访问控制策略。首先对 CP-ABE 算法进行了探讨，然后在 CP-ABE 算法的基础上，对公钥和主密钥计算、数据所有者对数据的加密、访问用户的认证和解密、用户权限的删除、扩展和新建都给出了具体的计算和操作流程。仿真实验表明了文中方法能较为全面和通用的实现云计算存储中心的整个访问控制过程，具有较强的实用性，且与其他方法相比，具有计算和存储开销小的优点。

参考文献：

[1] Vaquero L, Rodero Marino L, Cacerce J, et al. A break in the clouds: towards a cloud definition [J]. SIGCOMM Computer Communication Review, 2009, 39 (1): 50－55.

[2] 程芳权，彭智勇，宋　伟，等. 可信云存储环境下支持访问控制的密钥管理 [J]. 计算机研究与发展，2013，50 (8)：1613－1627.

[3] Wan Z G, Liu J, Deng R H. HASBE: A Hierarchical Attribute-Based Solution for Flexibleand Scalable Access Control in Cloud Computing [J]. IEEE Transactions on Information Forensics and Security, 2012, 7 (2): 743－754.

[4] 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.

[5] 孙国梓，董　宇，李　云. 基于 CP-ABE 算法的云存储数据访问控制 [J]. 通信学报，2011，32 (7)：146－152.

[6] Yu S, Wang C, Ren K, et al. Achieving secure, scalable, and fine-grained data access control in cloud computing [A]. INFOCOM, 2010 Proceeding IEEE. San Diego, CA: IEEE [C]. Conference Publications, 2010: 534－542.

[7] 邹佳顺，张永胜，高　艳. 基于改进 CP-ABE 算法的 ABAC 机制研究 [J]. 计算机应用研究，2014，6 (31)：1860－1862.

[8] Hota C, Sanka S, Rajaraja M N, et al. Capability-based cryptographic Data Access Control in cloud computing [J]. International Journal of Advanced Networking and Applications, 2011, 3 (3): 1152－1161.

[9] 李　琦，马建峰，熊金波，等. 一种素数阶群上构造的自适应安全的多授权机构 CP-ABE 方案 [J]. 电子学报，2014，4 (42)：696－702.

[10] Li X H, Lu R X, Lin X D, et al. Ciphertext policy attribute based encryption with efficient revocation [EB/OL]. 2012-09-25]. http://bbcr. uwaterloo. Ca/～ x27liang/papers/abe%20with%20revocati on. pdf.

[11] Sahai A, Waters B. Fuzzy identity-based Encryption [M]. Advances in Cryptology-EUROCRYPT 2005. Springer Berlin Heidelberg, 2005: 457－473.

[12] Cheung L, Newport C. Provably SecureCiphertext Policy ABE [A]. Proceedings of the 14thACM Conference on Computer and Communications Security [C]. ACM. 2007: 456－465.