◎网络、通信、安全◎

一种多租户授权管理访问控制模型

边根庆[1],李 荣[1],邵必林[2]
BIAN Genqing[1], LI Rong[1], SHAO Bilin[2]

1.西安建筑科技大学 信息与控制工程学院,西安 710055
2.西安建筑科技大学 管理学院,西安 710055
1.School of Information and Control Engineering, Xi'an University of Architecture and Technology, Xi'an 710055, China
2.School of Management, Xi'an University of Architecture and Technology, Xi'an 710055, China

BIAN Genqing, LI Rong, SHAO Bilin. Access control model on multi-tenant authorization management. Computer Engineering and Applications, 2015, 51(19):80-83.

Abstract: Considering the problem of unauthorized access and malicious attacks in multi-tenant application in the cloud services, this paper presents a Multi-Tenant Access Control Model(MTACM) which combines clustering and Ciphertext-Policy Attribute-Based Encryption strategy(CP-ABE). The model separates persona task into different task group according to multi-tenant service feature, and utilizes matching factor to mark task group, then manages persona attribute that is authorized by task group, which not only achieves persona's fine-grained authorization access control management but also reduces the computational cost of the system and complexity of the system. The algorithm is realized in the virtual environment, and the model security and system access effectively is proof of logical deductions.
Key words: multi-tenant; cloud services; CP-ABE; authorization management

摘 要: 针对云服务中多租户应用面临越权访问和联合恶意攻击问题,综合聚类思想和基于密文策略的属性加密(CP-ABE)提出一种多租户授权管理访问控制模型(MTACM)。该模型根据多租户的业务特点将角色任务聚类为任务组,并采用匹配因子标记任务组,进而通过任务组授权管理角色属性,以实现角色的细粒度授权访问控制管理,减少系统计算量开销,降低系统的复杂度。在虚拟环境下实现了该模型算法,且通过逻辑推理证明了模型的安全性和系统访问的高效性。
关键词: 多租户;云服务;CP-ABE;授权管理
文献标志码: A **中图分类号:** TP309.2 doi:10.3778/j.issn.1002-8331.1309-0450

1 引言

云计算是指以互联网为基础将规模化资源池的处理、存储、基础设施和软件服务提供给用户,实现低成本、自动化、快速提供和灵活伸缩的IT服务[1]。企业可以通过网络租赁云计算提供的软硬件服务,即云服务,从而减少运营成本。云服务提供商将同一个实例租赁给不同租户,即多租户应用,租户通过非完全可信的云服务商存储和处理数据[2-3]。为此,多租户应用通过按需定制和共享存储的交互方式获得云服务的同时也面临新的挑战:(1)未授权租户为了获取商业秘密窃取信息;(2)具有部分权限的租户越权访问未授权资源;(3)云服务提供商可能对外泄露租户业务信息。因此云服务中的租户信息面临的主要问题是访问控制问题,需要通过有效控制租户的访问权限来保护其信息的安全。

基金项目: 国家自然科学基金(No.61272458);西安市2013技术转移促进工程项目(No.CXY1348-1)。
作者简介: 边根庆(1968—),男,副教授,主要研究领域为海量信息处理,云计算技术,信息安全等;李荣(1987—),女,硕士研究生,主要研究领域为云计算技术;邵必林(1965—),男,教授,主要研究领域为信息管控技术,云计算技术以及动态存储安全技术等。E-mail:huanglongzhijiao@126.com
收稿日期: 2013-09-30 **修回日期:** 2013-12-13 **文章编号:** 1002-8331(2015)19-0080-04
CNKI网络优先出版:2014-02-24, http://www.cnki.net/kcms/doi/10.3778/j.issn.1002-8331.1309-0450.html

云服务通过管理在线共享资源池的访问权限，以按需分配方式分配系统资源给租户[4-5]。为确保租户信息的完整性和机密性，本文提出一种多租户授权管理访问控制模型(Multi-Tenant Access Control Model，MTACM)，该模型根据任务聚类的思想分层授权管理角色属性，综合利用基于角色访问控制(Role-Based Access Control，RBAC)[6]和密文的属性加密策略(CP-ABE)[7]。首先将云服务授权给租户，再结合任务聚类思想组成任务组，采用以CP-ABE算法为基础的访问控制模型分组管理租户角色属性，将权限细粒度分配给租户角色，从而统一管理租户访问请求，提高云服务的安全性和系统访问的有效性。

2　理论基础

2.1　基于角色的访问控制模型

基于角色访问控制模型(RBAC)是指在实现访问控制管理时，通过引入中间元素角色，根据不同租户的任务授予租户不同的资源操作权限。RBAC的主要思想就是先由角色聚合权限，再把权限赋予租户，将租户、权限和角色通过映射关系联系在一起，而租户被分配到合适的角色，大大简化了授权的管理。RBAC的特点是将不同类别和级别的权限赋予不同的角色，即角色对应业务系统中的任务，然后再将角色分配到租户，在租户和权限访问控制之间搭建一座桥梁[8]。

RBAC支持3个安全原则：最小特权、责任分开和数据抽象。最小特权原则要求不能赋予租户多于他进行工作的特权；责任分开要求确保一项任务可以调用各个互斥的角色[9-10]；数据抽象的支持指的是允许抽象的许可，例如一个目标账号的贷款和借款，而不只是经典的读、写和执行许可。

RBAC的关系模型如图1所示，RBAC0置于最底层表明它是任何支持RBAC系统的最小要求，RBAC1和RBAC2都包括了RBAC0，但是有其自身独立的特性，这个相当于角色层次的概念。统一的模型RBAC3包括RBAC1和RBAC2，同时根据传递性拥有了RBAC0模型。

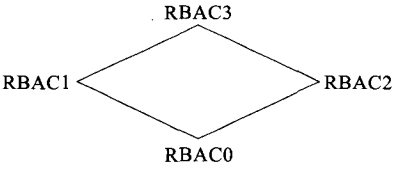

图1　RBAC模型关系图

2.2　基于密文策略的属性加密

CP-ABE是基于属性加密的密文策略，密文隐藏在访问控制树中，密钥与可描述的属性相关[11]，只有当访问者的属性符合密文访问策略时，才能解密密文，获取资源的访问权限，即访问结构区分密文，属性相当于私钥。访问控制基于属性而不是基于整个系统，则可以实现细粒度权限访问控制管理[12-13]。

CP-ABE算法的基本步骤如下。

(1)初始化：服务器端输入参数 λ，通过循环群 G 计算输出公钥 PK 和主密钥 MK。

(2)生成私钥：根据主密钥 MK 和访问者属性集 A 生成私钥 SK。

(3)加密：对服务资源 M 加密，生成密文 CT 和访问控制树 T，访问控制树 T 由属性集组成，CT 中暗含 T。

(4)解密：结合访问者的私钥 SK，通过解密算法判断是否授权给访问者。

3　多租户授权管理访问控制模型

多租户应用是云计算技术架构中面向服务的最为典型的应用模式，它要求服务器计算环境，存储资源及其网络资源的设计和部署必须满足自动化、快速性、动态性以及移动性、安全性和面向商业服务等需求。云服务中服务器虚拟化将传统的物理服务器虚拟化成若干个虚拟服务器，每个虚拟服务器运行独立的操作系统。每个租户拥有虚拟服务器资源池中的一台虚拟服务器或一组虚拟服务器。不同租户在共享数据中心基础设施的同时，会按照各自的需求定义他们的虚拟化资源。而这些虚拟化资源，对于不同的租户相互独立和隔离。云服务提供商必须按照协定动态地进行部署，满足租户的需求。

为了满足多组户环境的安全性，降低系统复杂度，本文提出一种多租户授权管理访问控制模型(MTACM)：租户租赁到云服务，采用 K-modes 算法[14]将各个租户根据属性特点聚类为任务组，即通过聚类实现租户中角色的划分，并将租户中相同项目组的角色分配在同一任务组。任务组用来管理角色，是租户和角色的桥梁，通过聚类后的任务组管理简化访问控制模型的管理策略；进而结合CP-ABE算法，针对任务组设置解密密文需要的属性，租户中角色通过任务组解密密文，无需单独完成解密密文的属性匹配。与传统访问控制模型对比，针对多租户应用，MTACM采用聚类构建基于任务组管理的模型，在保证租户安全的前提下，减少了属性匹配次数，进一步降低了系统复杂度。具体框架如图2所示，通过任务聚类授权管理访问控制，实现角色的细粒度管理。

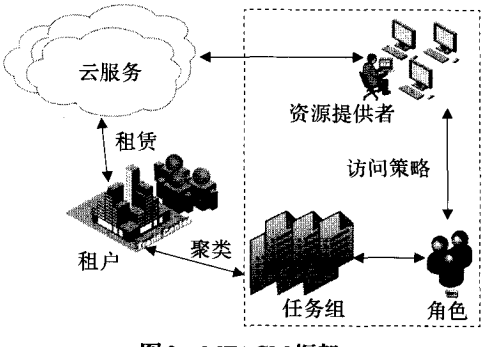

图2　MTACM框架

3.1 多租户授权管理访问控制流程

租户按需定制云服务，获得云服务的使用权后，各个租户根据任务和自身组织结构聚类，形成任务组，将不同资源访问权分配到任务组，角色通过任务组获得解密密文，即图2虚框所示，访问控制流程见图3。

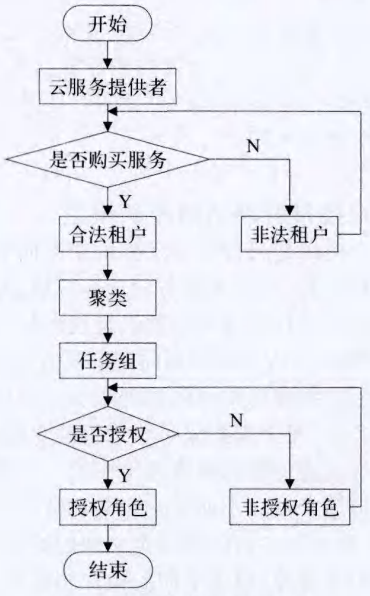

图3 多租户访问控制流程

3.2 多租户访问控制模型算法

合法租户购买云服务后得到授权，此时租户根据业务需求，可分配到某一任务组的角色，相同项目组的角色分配到同一任务组 $U_i \in U$，U_i 的角色 $e \in E$ 具有相同属性 $U_i(A)$，角色根据自己的属性通过任务组获取资源访问权限。

多租户授权管理访问控制模型的构建算法如下所示。

(1) Setup(λ)：云服务端输入安全参数 λ（λ 决定循环群 G 的阶数），由素数为 p、生成元为 g 的循环群 G 随机选择两个指数 $\alpha,\beta \in Z_p$，输出公钥 PK 和主密钥 MK。

$$PK=G,g,g_1=g^{\beta},\mathrm{g}_2=e(g,g)^{\alpha}$$

$$MK=\{\beta,g^{\alpha}\}$$

(2) KeyGen(MK,A,U)：输入主密钥 MK，角色属性集 A 和任务组集合 $U,\gamma \in Z_p,\gamma_i \in Z_p,\forall a_i \in A$，输出 U 中每个角色的私钥 SK。

$$SK=(D=g^{\frac{\alpha+r}{\beta}},\{D_i=g^{\gamma}H(a_i)^{\gamma_i},D_i'=g^{\gamma_i}\}\forall a_i \in A)$$

其中，租户根据任务给角色 e 增加任务组集合 U 的属性列 $U_i(A)$，给相同任务组的角色属性列 $U_i(A)$ 赋予相同的属性值。

(3) δ KeyGen (U)：输入任务组集合 U，输出 U 中每个任务组中角色的匹配因子 δ。

(4) Encrypt(PK,M,T)：云服务端数据提供者对服务资源 M 加密生成密文 CT 和访问控制树 T。

步骤1 访问树 T 中每个节点 N_j 对应多项式 f_j，节点 N_j 的度为 $d_j(d_j=n_j-1,n_j$ 为节点 j 的阈值)。

步骤2 根节点 N_1 选取随机数 $s \in Z_p$，且多项式 $f_1(0)=s$。

步骤3 使用加密公式 CT 加密：

$$CT=(B=Mg_2^s=Me(g,g)^{\alpha s},C=g_2^s=(g^{\beta})^s=g^{\beta s},$$

$$\{E_j=g^{f_j(0)}E_j'=(H_i(a_i))^{f_j(0)}\})$$

其中，a_i 属于所有角色属性集，j 是叶节点。

(5) Decrypt(CT,T,SK,A,δ)：私钥为 SK，属性为 A，匹配因子为 δ 的角色通过解密算法解密密文 CT，当角色属于某个任务组时，通过该任务组的匹配因子实现资源共享。

3.3 多租户访问控制模型实现

实验环境：在操作系统为 Windows Server 2003 的 VMware Workstation 虚拟机上安装 Ubuntu 13.04，内存 4 GB。具体实现过程如下所示。

(1) 在 Ubuntu 安装需要的库[15]：M4，gmp，pbc，glit，openssl，libbswabe，cpabe，它们的依赖关系如图4所示。

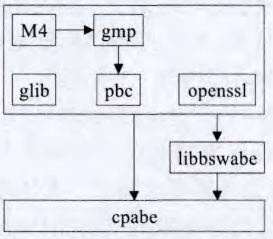

图4 实现访问控制需要安装的库

(2) 运行初始化函数 Setup(λ)，生成租户租赁云服务的公钥 pub_key 和主密钥 master_key，如图5所示。

(3) 角色根据自己的属性集和访问策略运行 KeyGen(MK,A,U) 函数，将任务组中角色的属性列赋值 $U_i(A)$，相同任务组的角色标记相同的匹配因子 δ，生成角色 ea 和 eb 的私钥 ea_priv_key、eb_priv_key，如图5所示。

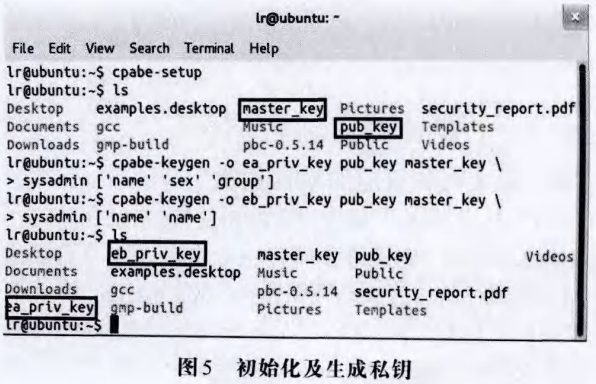

图5 初始化及生成私钥

(4)运行 Encrypt(PK, M, T)加密信息security_report.pdf，生成密文security_report.pdf.cpabe，如图6所示。

(5)角色利用解密算法 Decrypt(CT, T, SK, A, δ)解密密文security_report.pdf.cpabe，角色属性不符合访问策略则提示无法成功解密密文，如图6所示。

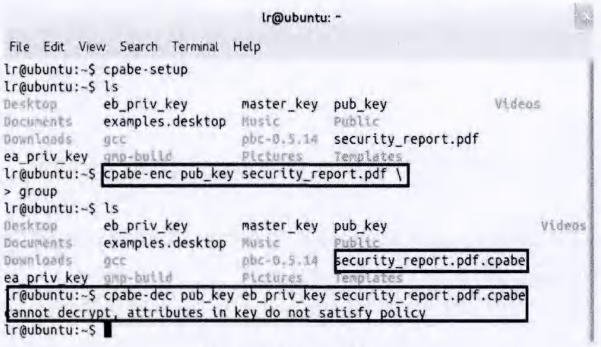

图6　加密、解密过程

4　认证与分析

4.1　安全性认证

MTACM在CP-ABE的基础上引入聚类和任务组，聚类针对租户划分人员，并将相同任务的人员分配在同一任务组，用匹配因子 δ 标记，故要证明MTACM的安全性，必须证明基于CP-ABE通过聚类和任务组管理后构建的模型的安全性。

因为CP-ABE的映射函数 $H_i(a_i)$ 将属性 a_i 映射为循环群 G 上的一个随机元素，加密密文为：

$$CT=(B=Mg_2^s=Me(g,g)^{\alpha s},\ C=g_2^s=(g^{\beta})^s=g^{\beta s},$$
$$\{E_j=g^{f_{j(0)}},\ E_j'=(H_i(a_i))^{f_{j(0)}}\})$$

由于聚类和任务组管理是对租户中人员分任务组管理，即根据任务组实现CP-ABE中的属性匹配，依然按照CP-ABE算法实现交互，故MTACM实质上只是减少了加密密文中属性 a_i 的个数，因此MTACM模型与CP-ABE具有相同的安全性，文献[7]已经证明了CP-ABE算法的安全性，故本文提出的MTACM模型也是安全的。此模型可以避免非授权租户角色访问云中存储的数据和恶意访问者的联合攻击，进而可以保证多租户应用环境下的安全。

4.2　复杂度分析

本节从理论上分析多租户授权管理访问控制模型比基于密文策略的属性加密的计算量开销小。如果访问树中的属性总数为 m，那么将角色属性集 A 转换成访问矩阵 $\boldsymbol{R}$ 的时间复杂度为 $O(m)$，故 $\sum_{x\in X'} c_x R_x=(1,0,\cdots,0)$ 的时间复杂度为 $O(mh)$。

本文提出的模型中花费时间最长的是解密函数中用到的配对运算。假定 T_p 代表一次配对运算时间，T_m 代表纯量乘法时间。在Encrypt算法中，每一位角色 e 计算 $e(g,g)$ 只需要 $1T_p$ 时间，但是对于每一个属性相关的行 x，角色总共需要 $4mT_m$ 时间，其中 $2T_m$ 的时间计算 $C_1,x,1T_m$ 时间计算 $C_2,x,1T_m$ 时间计算 C_3,x。在Decrypt过程中，每个 x 都必须运行两次配对算法，分别计算 $e(H(u),C_3,x)$ 和 $e(ski,u,C_2,x)$，总共需要 $2mT_p$ 时间。角色还需要计算 $(e(g,g)^{\lambda_x}e(H(u),g)^{\omega_x})^{c_x}$，最多需要 mT_m。因此，Encrypt和Decrypt总共需要 $(2m+1)T_p+5mT_m$ 时间。租户以任务组的形式把任务分配给角色，假设某一任务组有 $n(n<m)$ 个角色具有相同属性，通过其中某一个角色属性即可解密，则Encrypt和Decrypt总共需要的时间为 $(2m-2n+1)T_p+5(m-n+1)T_m<(2m+1)T_p+5mT_m$，设 $n=5$，为一个任务组，当 m 值变化时MTACM和CP-ABE解密时间如图7所示，随着角色属性不断增加，MTACM明显比CP-ABE花费的解密时间少，故本文提出的模型比CP-ABE计算量开销小。

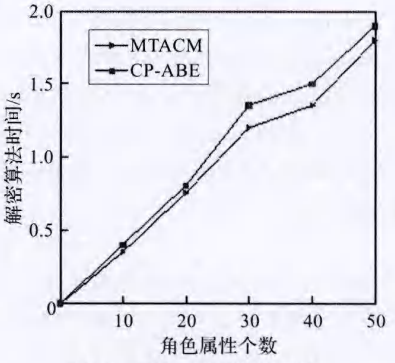

图7　解密算法所需时间

从图7分析：采用任务组授权管理访问控制模型时，在任务组个数确定的情况下，随着属性数量增加，该模型解密所需时间比CP-ABE算法少，因为两种算法加密时间相同，故该模型比CP-ABE算法复杂度小。

5　结论

针对多租户应用在云服务中存在访问控制方面的安全隐患和匹配运算复杂度较高的问题，提出了多租户授权管理访问控制模型。本文模型利用聚类思想将任务分组，引入匹配因子标记同任务组的角色，实现角色的细粒度授权访问控制管理，减少了属性匹配运算次数，防止了越权管理，避免了非法访问者联合恶意攻击问题。因此，通过访问控制提高了云服务下多租户的安全性，通过角色属性的任务组管理减少了系统计算量开销，降低了系统的复杂度。

参考文献：

[1] 冯登国，张敏，张妍，等.云计算安全研究[J].软件学报，2011，22(1)：71-83.

(下转215页)

关参数设置简单,计算量较小。实验证实了本文方法可有效提高识别精度。

参考文献:

[1] Wang Zhan, Ruan Qiuqi, An Gaoyun.Facial expression recognition based on tensor local linear discriminant analysis[C]//2012 IEEE 11th International Conference on Signal Processing,2012:1226-1229.

[2] Asharaf A B, Lucey S, Chen T.Reinterpreting the application of Gabor filters as a manipulation of the margin in linear support vector machines[J].IEEE Transactions on Pattern Analysis and Machine Intelligence, 2010, 32(7): 2510-2521.

[3] Liu Weifeng, Wang Zengfu.Facial expression recognition based on fusion of multiple Gabor features[C]//The 18th International Conference on Pattern Recognition, 2006:536-539.

[4] Ojala T, Pietikainan M.Multiresolution gray-scale and rotation invariant texture classification with local binary patterns[J].IEEE Transactions on Pattern Analysis and Machine Intelligence, 2002, 24(7):971-987.

[5] Marko H, Matti P, Cordelia S.Description of interest region with center-symmetric local binary pattern[C]//Proc of Conf on Computer Vision Graphic and Image Processing, 2006:58-69.

[6] 卢建云,何中市,余磊.基于多级CS-LBP特征融合的人脸识别方法[J].计算机工程与科学,2010,32(6).

[7] Wang Yan, He Guoqing.Expression recognition algorithm based on local directional binary pattern[J].Journal of Computational Information Systems, 2014, 10(8):3221-3228.

[8] 龚劬,叶剑英,华桃桃.结合改进的LBP和LDP的人脸表情识别[J].计算机工程与应用,2013,49(22):197-200.

[9] Zhang Wenchao, Shan Shiguang, Gao Wen, et al.Local Gabor Binary Pattern Histogram Sequence (LGBPS): a novel non-statistical model for face representation and recognition[C]//Proceedings of the 10th International Conference on Computer Vision, Beijing, China, 2005:150-155.

[10] Bafandehkar A, Rahat M, Nazari M.Pictorial structure based keyparts localization for facial expression recognition using Gabor filters and local binary patterns operator[C]//International Conference on Soft Computing and Pattern Recognition, 2011.

[11] 朱明旱,李树涛,叶华.基于子空间稀疏系数的表情识别方法[J].计算机工程与应用,2014,50(12):33-37.

[12] 邵诗强,施立欣,周龙沙.基于环形Gabor小波与CS-LBP算法在人脸识别中的应用[J].光电子技术,2012(3):180-184.

[13] 何中市,卢建云,余磊.基于多通道Gabor滤波与CS-LBP的人脸识别方法[J].计算机科学,2010,37(5).

[14] Zhang Yankun, Liu Chongqing.Efficient face recognition method based on DCT and LDA[J].Journal of Engineer and Electronics, 2004, 15(2):211-216.

[15] Jiang Bin, Yang Guosheng, Zhang Huanlong.Cpmparative study of dimension reduction and recognition algorithms of DCT and 2DPCA[C]//Proceedings of the 7th International Conference on Machine Learning and Cybernetics, Kunming, 2008:12-15.

(上接83页)

[2] 徐光侠,陈蜀宇.面向移动云计算弹性应用的安全模型[J].计算机应用,2011,31(4):952-955.

[3] 史玉良,栾帅,李庆忠,等.基于TLA的SaaS业务流程定制及验证机制研究[J].计算机学报,2010,33(11):2055-2067.

[4] Itani W, Kayssi A, Chehab A.Privacy as a service: Privacy aware data storage and processingin cloud computing architectures[C]//Proceedings of the 8th IEEE International Conference on Dependable, Autonomic and Secure Computing, 2009:711-716.

[5] 张逢結,陈进,陈海波,等.云计算中的数据隐私性保护与自我销毁[J].计算机研究与发展,2011,48(7):1155-1167.

[6] 刘伟,蔡嘉勇,贺也平.基于角色的管理模型隐式授权分析[J].软件学报,2000,20(4):1048-1057.

[7] Bethencourt J, Sahai A, Waters B.Ciphertext-policy attribute based encryption[C]//Proc of IEEE Symp Security Privacy, 2007:321-334.

[8] 杨庚,沈剑刚.基于角色的访问控制理论研究[J].南京邮电大学学报:自然科学版,2006,26(3):1-8.

[9] 王凤英.访问控制原理与实践[M].北京:北京邮电大学出版社,2010.

[10] Baden R, Bender A, Spring N, et al.Persona: An online social network with user defined privacy[C]//Proc of ACM SIGCOMM Conf Data Commun, 2009:135-146.

[11] 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.

[12] 王小明,付红,张立臣.基于属性的访问控制研究进展[J].电子学报,2010,38(7):1660-1667.

[13] 李晓峰,冯登国,陈朝武,等.基于属性的访问控制模型[J].通信学报,2008,29(4):90-98.

[14] 孙吉贵,刘杰,赵连宇,等.聚类算法研究[J].软件学报,2008,19(1):48-61.

[15] The GNU multiple precision arithmetic library[EB/OL].[2013-05-20].http://www.gmplib.org/.