DOI:10.3969/j.issn.1009-6868.2017.01.014
网络出版地址:http://www.cnki.net/kcms/detail/34.1228.TN.20170105.0903.002.html

一种基于安全标记的多租户访问控制方法

A Multi-Tenant Access Control Method Based on Security Mark

中图分类号:TN929.5 文献标志码:A 文章编号:1009-6868 (2017) 01-0058-005

摘要: 设计了一种安全标记机制,提出了一种支持多租户的安全访问控制方法,满足租户对于多域安全访问控制的需求。实验结果证明,这种基于安全标记的多租户安全访问控制方法兼具基于角色的访问控制模型(RBAC)和强制访问控制方法的优点,在易于管理的基础上,也使租户的访问控制系统达到了更高的访问控制安全级别。

关键词: 云计算;数据中心;多租户;访问控制;安全标记

Abstract: In this paper, a security mark method and a multi-tenant secure access control model are proposed to meet the demand from tenants in multi-domain secure access control. The results show that the multi-tenant access control method based on security mark has advantages of both role-based policies access control (RBAC) and mandatory access control, and helps tenants access control system reach higher security level on the basis of easy management.

Key words: cloud computing; data center; multi-tenant; access control; security mark

彭勇/PENG Yong[1]
侯超平/HOU Chaoping[1]
童遥/TONG Yao[2]
申光/SHEN Guang[2]
(1. 广西科技大学,广西 柳州 545006;
2. 中兴通讯股份有限公司,江苏 南京 210012)
(1. Guangxi University of Science and Technology, Liuzhou 545006, China;
2. ZTE Corporation, Nanjing 210012, China)

在云计算领域,软件即服务(SaaS)是一种新的软件应用模式,极大地减少了企业在信息基础设施上的投入,其数据模型有3种[1]:独立数据库模型、共享数据库单独模型和共享数据库共享模型。独立数据库模型中,每个客户在物理上都有自己的一整套数据,单独存放,其最大问题在于部署和维护的成本非常高,硬件资源消耗明显高于其它两种方案,单台服务器只能支持有限数量的客户;共享数据库单独模型下,客户使用独立模式,在数据共享和隔离之间获得了一定的平衡,不足之处是当系统出现异常,需要将历史备份数据重新恢复时,流程将变得相对复杂;共享数据库共享模型具有最低的硬件成本和维护成本,且每台服务器可以支持最大数量的客户,但由于所有客户使用同一套数据表,为保证数据安全性,需要花费更多的开发成本,以确保不会因系统异常而产生错误的数据访问。

收稿时间:2016-11-25
网络出版时间:2017-01-05

1 SaaS安全访问研究现状

目前对于SaaS模式下安全访问方法的研究大体可以分为以下3个方面:

(1)对应用权限控制[2-6];

(2)对应用访问许可[7-11];

(3)对系统数据访问控制[11-15]。

传统的多租户访问控制方式一般采用共享数据库共享模型,将各租户的控制策略整合在全局访问控制策略下,实现租户间的安全性互操作,其安全问题一般包括网络安全访问、系统权限模型等。在网络安全访问方面,通常对交互信息进行加密,防止用户信息被窃取[16],而对于系统权限模型,大多是通过租户间角色转换达到安全访问控制的目的。

但是使用共享数据库共享模型时,租户数据的共享数据库特性使得租户间的数据隔离性很差。鉴于此,文章提出了基于安全标记的多租户访问控制方法,采用强访问控制特性,利用安全标记互相授权实现租户间的数据共享,提高租户间数据共享的效率。

2 基于安全标记的访问控制方法

基于安全标记的多租户访问控制方法制定和维护了相应的角色森林和安全标记森林,并根据角色的职责赋予其相应的安全标记。用户访问数据时,通过比对角色所具有的安全标记以及访问该数据所需的安全

标记，来决定该用户是否具有访问权限，从而达到访问控制的效果。

（1）客体安全标记

如图1所示，用层次化的标记模型对客体进行标识，在使用服务前，由租户内部的管理人员根据需求，按照一定准则对公司进行划分，根据这些信息构造由很多安全标记树（SMT）组成的安全标记森林，SMT上的每个节点即代表该公司内部一个可控的安全标记，客体标记定义为 O:(*tenant*,安全标记集(SMS)) 或 (*tenant*, *mark* 1,*mark* 2,...,*mark n*)。

（2）主体安全标记

主体安全标记是指主体通过其具有的角色获取的安全标记，定义为 R:(*tenant*,*SMS*) 或 (*tenant*,*mark* 1,*mark* 2, ...,*mark n*)。如图2所示，租户企业均以角色森林的方式表示，为满足安全需求，每个公司在使用服务前都需要各自建立角色森林，主体标记定义为 S:(*tenant*,*RS*) 或 (*tenant*,*role*1,*role*2,..., *role*n)，其中 $RS(RoleSet)$ 表示该用户所具有的角色集。每个角色都会有相应的安全标记进行标注，表示其在系统中的职责。

（3）SMS

以 $SMS(x)$ 表示对象所具有的安全标记集合，当 x 为客体关系或属性时，表示该客体所具有的安全标记集合；当 x 为主体时，表示该主体所具有的安全标记；当 x 为租户时，表示该租户授予当前租户的安全标记及其子标记的集合。此外，为区分租户授权的传递标记与非传递标记，将租户授予的非传递安全标记表示为 $SMS(t)$。

（4）属性安全标记集（ASMS）

用 $ASMS(x)$ 表示对属性进行标注的标记集合。

（5）扩展安全标记集（ESMS）

用户所具有的所有安全标记集合，包括本租户的，以及其它租户授权绑定的，用 $ESMS(U)=SMS(U)\cup(\bigcup_{i}^{m}SMS(t_i)\cup\overline{SMS}(t_i))$ 来表示，其中，m 表示授权租户的个数。$ESMS(U)$ 由3个并集组成，$SMS(u)$ 表示用户 U 所属租户分配给他的安全标记及其子标记，$SMS(t)$ 表示其它租户授权给他的传递安全标记及其子标记，$\overline{SMS}(t)$ 表示其他租户授权给他的非传递安全标记。

3 多域之间的安全访问控制方法

在SaaS应用中，当同一应用实例的两个租户需要实现相互之间的数据访问时，访问可以绕过角色转换过程，租户管理员通过给租户分配另一租户具有的安全标记，使该租户获得对另一租户资源的访问权限。

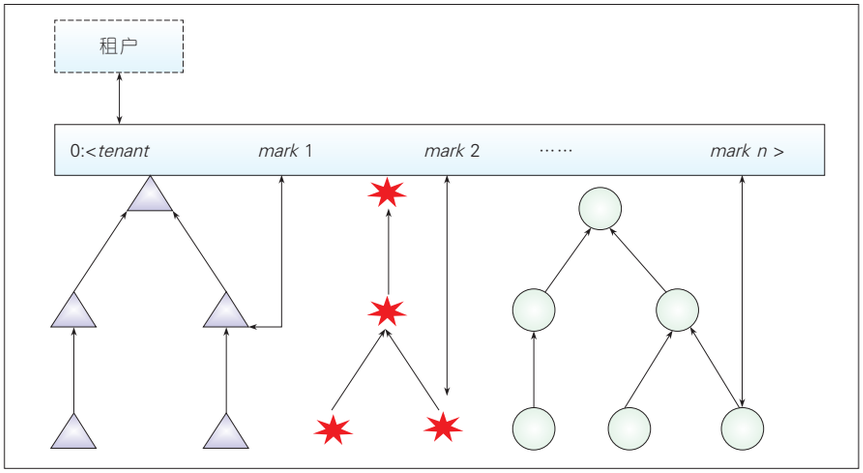
如图3所示，假设SaaS系统中有 A，B 两个租户，租户 A 和 B 的安全标记层次都只有一个，当租户 A 的 G 标记与租户 B 的 G 标记进行绑定时，租户 B 中具有标记 G 的用户同样可以访问 A 中具有 G 标记标注的数据。

3.1 基本定义

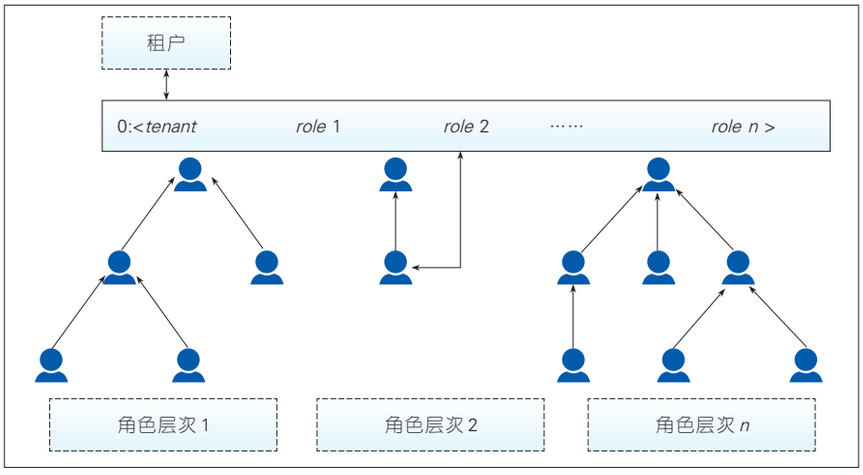
（1）$X>Y$，表示 X 在安全标记树中层次比 Y 高，或者 X 是 Y 的祖先，X_A 表示安全标记 X 来自租户 A。

（2）$X_a\rightarrow Y_b$，也可写成 $(Xa,Yb)\in T_{ab}$，表示安全标记关联，$T_{ab}\subseteq T_a*T_b$。如附图3中，有从 G_A 到 G_B 的关联，表示来自租户 A 将自己的 G 标记授予租户 B 中具有标记 G 的用户，可用 $(G_A,G_B)\in T_{ab}$ 表示这种关联。

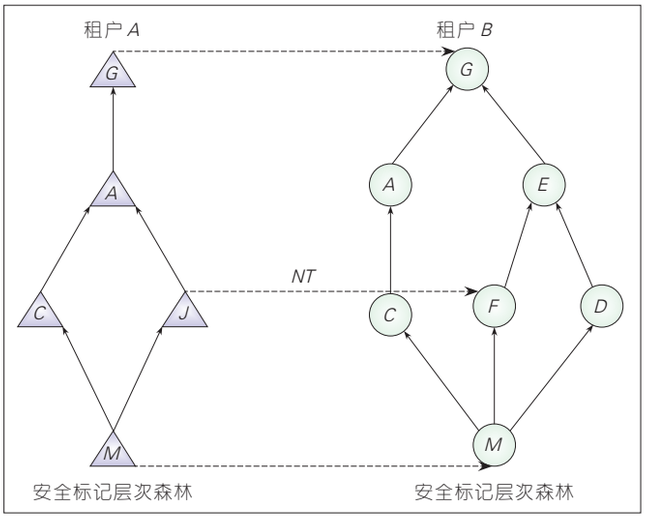
（3）传递关联：假设存在关联



▲图1 安全标记森林示意



▲图2 角色森林示意



◀图 3
多租户间标记绑定授予示意

$X_A \rightarrow a_B$ ，$\forall Y \in B$ ，如果 $Y_B > a_B$ ，则 $Y_B > X_A$ ，因为 Y_B 包含了对 a_B 的映射，所以 Y_B 也是 X_A 的祖先。从图 3 中可以看出 $M_A \rightarrow M_B$ 的关联，因此租户 B 中具有 M 标记的用户将可以访问 A 中具有 M 标记的资源，这也意味着所有 M_B 的祖先都可以访问租户 A 中具有 M 标记的资源。

（4）非传递关联：安全管理员可能想把本租户的安全标记与其它租户的安全标记相关联，而不想另一租户的标记的祖先继承这种传递关联，为此引入了非传递关联的概念，用 $X_A \xrightarrow{NT} Y_B$ 来表示。例如，图 3 中租户 A 的安全管理员想把 J_A 标记与租户 B 的 F_B 标记进行绑定，并否定 E_B 和 F_B 关联的继承，因此该映射为 $J_A \xrightarrow{NT} F_B$ 。

（5）标记关联策略

● 缺省策略

当租户 B 的用户需要对租户 A 进行访问时，租户 A 可以提供默认的安全访问标记，如标记所标定的数据都是不敏感的，任何人都可以访问的，使得域间访问很安全且管理方便。

● 直接策略

与缺省策略比，直接策略就是对租户 B 可能要访问该系统而需要使用的标记都一一绑定，充分满足了用户的安全访问需求，但这种指派不能满足不同用户的不同访问需求，标记的指派及管理将是棘手问题，并且在某些情况下，安全标记并不希望与其绑定标记的父标记拥有相同的权限，在这种情况下，租户管理员就需要建立非传递安全标记绑定，此时可以将标记绑定有序对表示为 $(X_A, Y_B)NT$ 。

● 部分策略

为了安全，租户间的安全标记绑定需要系统管理员一一指派，使用非传递关联。但在某些情况下，既有继承关系的标记可以指派到同样的标记集，此时可使用传递关联来减少系统中指派关系的复杂程度，使标记绑定更加容易管理。例如，租户 T_B 具有安全标记 a_B，a_B 是安全标记 b_B 的父标记，且租户 T_A 已有相应的标记绑定 (c_A, b_B)，则租户 T_B 中拥有标记 a_B 的用户可以直接得到 A 租户中具有安全标记 c_A 的数据，而无需 A 租户再次指定标记绑定 (c_A, b_B) 。

（6）安全标记分类

● 行级安全标记

通过给关系 R 绑定安全标记集，来控制用户对 R 的访问，由于是对 R 的整体标注，则用户只有可以访问或不可以访问两种情况，可以用 $((A_1, A_2, ..., A_n), (SM_1, SM_2, ..., SM_m))$ 来标注，其中 SM_1，SM_2，……，SM_m 各属不同的安全标记树。则行级安全标记的控制规则可以表示如下：(T, SMS, R, Q) ，T 表示该规则所属的租户，SMS 表示标记集合，R 表示 SMS 作用的关系对象，而 Q 则表示先期访问控制的约束条件。

● 列级安全标记

为达到更细粒度的访问控制，可以对关系属性进行安全标记，即关系 R 的每个属性都通过安全标记标注的方式实现安全访问，用 $((A_1, SM_{a_1}), ..., (A_n, SM_{a_n}), (SM_1, ..., SM_m))$ 表示。列级安全标记的控制规则可以表示为 (T, AMS, SMS, R, Q) ，其中 T 表示该规则所属的租户，AMS 表示 (A, SM) 二元组的集合，SMS 是行级安全标记集合，用来对没有被 AMS 中所包含的属性做出标记标注，R 表示 AMS、SMS 作用的关系对象，Q 代表先期访问控制约束条件。

3.2 安全访问控制方法

租户对客体进行安全标记并制定数据访问控制规则后，用户访问数据库时，访问控制模块对用户的请求进行检查，根据已经存于系统中的规则信息确定用户的访问结果。文章提出的安全访问控制方法根据规则信息对访问语句进行转换。请求处理过程可以分为以下两个步骤：

（1）检查用户安全标记以及系统安全规则数据；

（2）根据已有的信息产生用户访问语句，并提交数据库进行访问。

假设此时租户 T 有用户 U，其提交的访问语句为：$Select\ a_{q_1}, a_{q_2}, ..., a_{q_n}\ from\ R_{q_1}, R_{q_2}, ..., R_{q_m}\ where\ Q_q$ 。当 T 对 R_{q_i} 所进行的安全标记为行级，即 R_{q_i} 客体安全标记为 $(T, AMS_{q_i}, SMS_{q_i}, R_{q_i}, Q_{q_i})$ ，则当 $SMS(R_{qi}) \subseteq SMS(U)$ 时，只要条件 Q_i 为真，则该用户可以对 a_{q_i} 进行此次访问。当 T 对 R_{q_i} 所进行的安全标记为列级，即 R_{q_i} 的客体安全标记为 $(T, AMS_{q_i}, SMS_{q_i}, R_{q_i}, Q_{q_i})$ ，则当 $AMS(a_{q_i}) \subseteq SMS(U)$ 时，该用户可以对 a_{q_i} 进行此次访问。

需要利用系统中已制定好的规则，对访问语句进行转换，假设租户

T有规则$r_i=(T, ASMS, SMS, R, Q)$，那么当且仅当该规则满足如下条件时才会采用：

（1）关系R的属性集的子集$A=(a_1,a_2,...,a_m)$是$A_q=(a_{q1},a_{q2},...,a_{qm})$的子集；

（2）$\bigcup_{l}^{m} ASMS(a_i)\subseteq SMS(U)$。

处理该语句时，涉及租户T的相关规则为$r_i=(T, ASMS, SMS, R, Q)(1\leqslant i\leqslant k)$，其中$k$为该语句涉及到的$k$条规则，可用$Rule(T, query)$表示，其意义为$t$租户在查询语句中涉及到的规则集，此处有如下表示：

（1）记$R_q=(R_{q_1},R_{q_2},...,R_{q_m})$，$R_r=\bigcup_{l}^{k} R(r_i)$，其中$R(r_i)$表示规则$r_i$中涉及到的关系；

（2）记$Q_r=\bigcup_{l}^{k} Q(r_i)$，其中$Q(r_i)$表示规则$r_i$中涉及到的约束条件。

访问语句可变为$Query(t)$：$Select\ a_{q_1}, a_{q_2}\cdots a_{q_n}\ from\ R_q\cap R_r\ where\ Q_q\cap Q_r$。则对租户$T$，其访问语句转换就完成了，对于要访问的其他租户的数据的语句转换同理，对于某一查询语句，转换后的结果为语句集，可表示为：$Q(U)=Query(T)\cup\bigcup_{l}^{n} Query(t_i)$，其中，$Query(T)$表示该语句相对该用户所属租户的转换语句，$\bigcup_{l}^{n} Query(t_i)$表示该语句相对其它租户的语句转换集合，语句在转换完成后，就可以提交数据库处理。

4 基于安全标记的多域访问控制系统

4.1 系统架构

基于安全标记的多域访问控制系统中，有两个主要模块：安全信息定义模块和访问控制模块，系统架构如图4所示。

安全信息定义模块：该模块负责完成安全标记森林的定义及系统中访问主体与访问客体的安全标记标注，同时负责主客体安全标记的完整性与一致性检查。

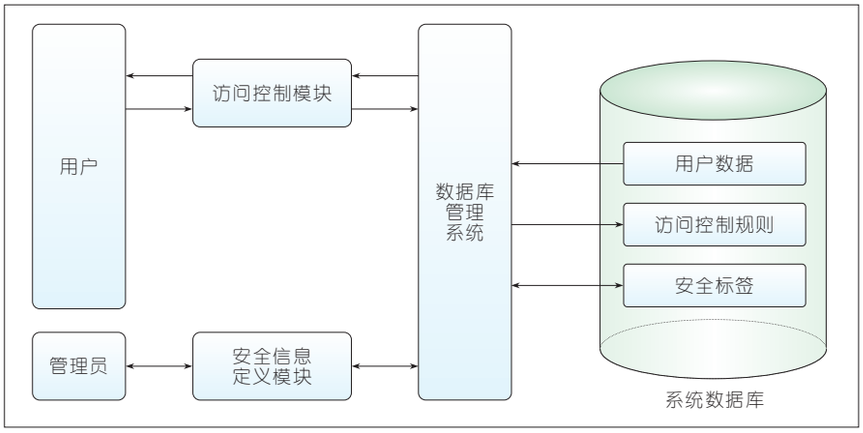
访问控制模块：该模块负责对用户的访问进行控制，其根据访问主客体所具有的安全标记，并结合已有的访问控制规则信息，做出最后的访问控制结果。

4.2 访问控制流程

在制定好系统角色森林、标记森林及相应的访问控制规则后，系统的访问控制模块才会根据已经制定好的规则来进行。图5是系统访问控制流程。

5 实验结果及分析

我们实现了一个基于安全标记的多租户访问控制方法的原型系统，并部署在模拟数据中心。从该数据中心选取2台安装、运行Redhat Linux RHEL6.3操作系统和Oracle数据库的虚拟机，分别部署基于安全标记的多租户访问控制方法的原型系统和基于角色的访问控制模型（RBAC）系统，两个系统使用同一组



▲图4 基于安全标记的多域访问控制系统架构

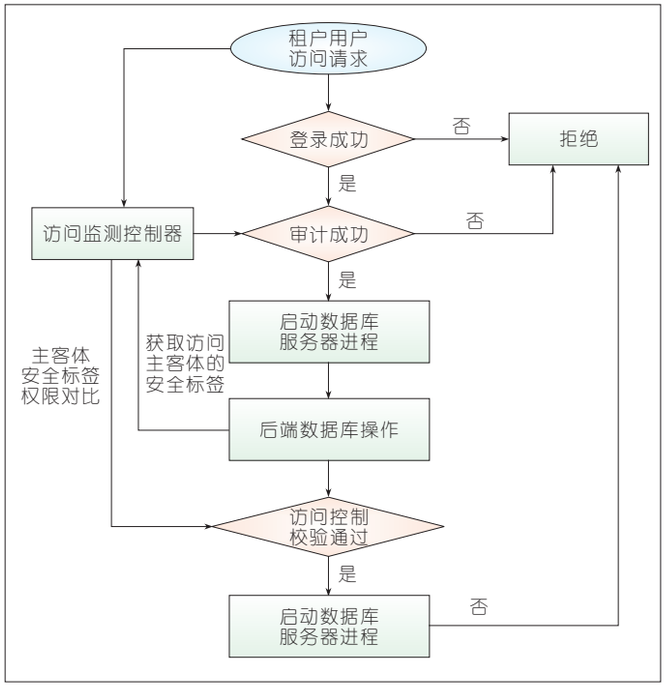


图5▶ 访问控制流程

结构化查询语言(SQL)语句进行对比测试。

通过对实验结果的分析可以发现,基于安全标记的多租户访问控制方法在访问效率上没有降低,甚至优于基于RBAC的系统,且从原型系统的设计上看,也优于基于RBAC的系统,主要体现在了如下几点。

(1)租户之间数据的强隔离性

由于每次访问都需要比较主客体的安全标签是否属于同一租户,杜绝了用户对其他租户数据非法访问的可能性。

(2)灵活的租户内部数据隔离

每个租户都可以自由定义层次化的主体角色和客体标签森林,对主客体进行自由的标签标注,满足租户不同的访问控制需求。

(3)租户之间数据的受控、高效共享

租户间通过安全标签的互相授予来达到共享的目的,使得有授权的租户可以方便、高效地访问共享的数据,同时屏蔽非法访问。

6 结束语

利用租户数据共享模式的特点,我们结合RBAC和强制访问控制模型的特性,创新性地提出基于安全标记的多域安全访问控制方法,并通过原型系统的实现,证明了该方法的有效性。然而,有关安全标记的使用规则还有待进一步研究,力求在保障数据安全的同时,进一步提高访问效率。

参考文献

[1] JU J, WANG Y, FU J, et al. Research on Key Technology in SaaS[C]//2010 International Conference on Intelligent Computing and Cognitive Informatics. USA:IEEE, 2010:384–387. DOI:10.1109/ICICCI.2010.120
[2] 马立林, 李红. 基于RBAC的SaaS系统的权限模型[J]. 计算机应用与软件, 2010, 27(4):42–44. DOI:10.3969/j.issn.1000–386X.2010.04.014
[3] 朱养鹏, 张璟. SaaS平台访问控制研究[J]. 计算机工程与应用, 2011, 47(24):12–16. DOI:10.3778/j.issn.1002–8331.2011.24.004
[4] 佟彤. RBAC扩展模型在SaaS系统中的研究与应用[D]. 郑州:郑州大学, 2011
[5] 王丰锦, 张群芳. SaaS工作流访问控制模型设计[J]. 计算机时代, 2012, 30(3):12–14. DOI:10.3969/j.issn.1006–8228.2012.03.005
[6] 王家忙. 面向SaaS的工作流管理系统设计与实现[D]. 杭州:浙江大学, 2010
[7] 韩秋君,丁岳伟. SaaS模式下新型认证方案的设计与分析[J]. 计算机工程, 2011, 37(7):133–135. DOI:10.3969/j.issn.1000–3428.2011.07.044
[8] DEMCHENKO Y, NGO C, LAAT C. Access Control Infrastructure for On–Demand Provisioned Virtualized Infrastructure Services [C]//2011 International Conference on Collaboration Technologies and Systems. USA:IEEE, 2011:466–475. DOI:10.1109/CTS.2011.5928725
[9] 曾巧文, 陈新度, 吴磊. 基于SOAP消息SaaS平台应用访问控制模型[J]. 机电工程技术, 2010, 39(10):27–29. DOI:10.3969/j.issn.1009–9492.2010.10.007
[10] 申利民, 刘波, 邢元昌, 等. SaaS模式下可插拔访问控制框架的设计[J]. 小型微型计算机系统,2010, 31(6):1107–1111
[11] LI J, ZHAO G, CHEN X, et al. Fine–Grained Data Access Control Systems with User Accountability in Cloud Computing[C]//2010 IEEE Second International Conference on Cloud Computing Technology and Science, USA:IEEE, 2010:89–96. DOI:10.1109/CloudCom.2010.44
[12] JENSEN M, SCHAGE S, SCHWENK J. Towards an Anonymous Access Control and Accountability Scheme for Cloud Computing [C]//2010 IEEE 3rd International Conference on Cloud Computing, USA:IEEE, 2010:540–541. DOI:10.1109/CLOUD.2010.61
[13] LUO S X, LIU F M, REN C L. A Hierarchy Attribute–Based Access Control Model for Cloud Storage[C]//2011 International Conference on Machine Learning and Cybernetics, USA:IEEE, 2011(3):1146–1150. DOI:10.1109/ICMLC.2011.6016897
[14] TANG Y, LEE P, LIU J, et al. Secure Overlay Cloud Storage with Access Control and Assured Deletion[J]. IEEE Transaction on Dependable and Secure Computing, 2012, 9(6):903–916. DOI: 10.1109/TDSC.2012.49
[15] 张坤, 李庆忠, 史玉良. 面向SaaS应用的数据组合隐私保护机制研究[J]. 计算机学报, 2010, 33(11):2044–2054. DOI: 10.3724/SP.J.1016.2010.02044
[16] 孟健, 曹立明, 王小平, 等. XML文档的加密访问控制与传输[J]. 计算机应用, 2006, 26(5):1061–1063

作者简介

彭勇,广西科技大学网络与现代教育技术中心工程师;研究方向为云计算、信息安全等。

侯超平,广西科技大学网络与现代教育技术中心工程师;研究方向为云计算、分布式系统、高可用技术等。

童遥,中兴通讯股份有限公司工程师;研究方向为云计算、统一通信等。

申光,中兴通讯股份有限公司工程师;研究方向为云计算、统一通信等。