带空间特性的角色访问控制研究

邹志文 陈昌乾 鞠时光
(江苏大学计算机学院 镇江 212013)

摘 要 以自主开发的内嵌式安全空间数据库管理系统SECVISTA为平台,研究带有空间特性的角色访问控制SRBAC(Spatial Role-Based Access Control)模型的特性。定义在空间环境下的空间对象区域范围约束、空间对象区域大小约束、空间对象责任分离约束和空间对象角色激活基数约束;对RBAC模型会话进行扩展,确定任一空间位置的无阻塞会话集合;讨论分析了空间环境下的角色继承关系;最终建立一个通用的、描述能力强的SRBAC模型。

关键词 信息安全,访问控制,空间数据库,SecVista
中图法分类号 TP309.2 **文献标识码** A

Research on Role-based Access Control with Spatial Character

ZOU Zhi-wen CHEN Chang-qian JU Shi-guang
(School of Computer, Jiangsu University, Zhenjiang 212013, China)

Abstract In order to strengthen the capability of safety expression for RBAC with spatial character, the secure spatial DBMS—SECVISTA was taken as platform to research spatial character of the Spatial Role-Based Access Control (SRBAC) model. First, the region coverage constraint of spatial object, duration constraint of spatial object, various spatial object separation of duty constraints and spatial object cardinality constraint of role activation were researched; after extending the traditional session, a non-blocked sessions set was confirmed at any spatial location, then the role hierarchy was discussed in spatial environment. So the theory of secure DBMS was optimized and afforded to build the stricter system.

Keywords Information security, Access control, Spatial DBMS, SecVista

1 引言

基于角色的访问控制RBAC模型的出现方便了系统权限管理[1]。许多研究者讨论了如何将RBAC模型应用于多级安全系统,包括:如何使用RBAC来模拟DAC与MAC[2];如何在不改变多级系统核心模块情况下使用RBAC[3];RBAC的角色图与MAC层次结构的关系等等[4]。在RBAC之中,权限被赋予角色,而不是用户。当一个角色被指定给一个用户时,此用户就拥有该角色所包含的权限。RBAC还规定了权限被赋予角色,或角色被赋予用户,或用户激活一个角色时所应遵循的强制性规则。RBAC访问控制模型不仅易于管理而且降低了复杂性、成本和发生错误的概率,因而近年来得到了快速发展。

目前已经建立了一些具有影响的模型:R. Sandhu等提出的RBAC96模型由于对RBAC进行系统和全面的描述而得到广泛认可。Sandhu在RBAC96模型中定义了4个概念模型,在RBAC97模型中讨论了角色管理,但由于对角色概念缺乏统一认识,因而始终没有提到在实际开发中对其如何划分、设置。美国国家标准与技术局(NIST)研究小组开发的RBAC2000模型[5]统一了人们对RBAC的认识。文献[6,7]对RBAC2000进行扩充,提出一个带有时间特性的角色访问控制模型TRBAC,该模型提出时间范围约束、时间长度约束等相关概念。文献[8]提出带有空间特性的角色访问控制SRBAC模型,但没有对带有空间特性的角色继承、约束和会话状态变化规律进行详细讨论。

随着现代通信技术的日新月异,尤其是光纤接入技术、第三代移动通信技术、蓝牙及超宽带等无线通信技术的发展,用户利用移动终端可以在任何地点使用网络信息和服务,这样也给系统带来了隐患。如在有些环境下,用户的访问请求会随用户位置变化而变化,这时,一个特殊的带有空间特性的约束就显得非常重要。鉴于此,我们以SRBAC模型为对象,讨论空间环境下的约束、会话状态变化、角色继承等特性,以提高SRBAC模型的安全描述能力。

2 SRBAC模型

SRBAC模型是对传统RBAC96模型的一个扩展。在SRBAC模型中,同一个角色在不同空间位置有不同权限。为了展开讨论,以下简要给出SRBAC模型定义。

到稿日期:2009-05-09 返修日期:2009-07-02 本文受国家自然科学基金(编号:60773049),江苏省研究生科研创新计划项目(编号:CX07B_125z),江苏省中小企业技术创新资金(编号:BC2008140),镇江市社会发展计划项目(编号:SH2008028)资助。
邹志文(1968—),男,副教授,CCF会员,研究方向为空间数据库,E-mail: zzw_yj@126.com;陈昌乾(1976—),男,硕士;鞠时光(1955—),男,教授,研究方向为信息安全、空间数据库。

定义 1 SRBAC 模型

$U=\{u_1,u_2,\cdots,u_n\}$，是所有用户的集合；$R=\{r_1,r_2,\cdots,r_n\}$，表示所有角色的集合；$Ob=\{ob_1,ob_2,\cdots,ob_k\}$，表示所有对象的集合；$Op=\{op_1,op_2,\cdots,op_k\}$，表示所有操作的集合；$S=\{s_1,s_2,\cdots,s_p\}$，表示所有会话的集合；

$P=2^{Op\times Ob}$ 是所有权限的集合；

$LOC=\{LOC_1,LOC_2,\cdots,LOC_n\}$，表示空间位置；

$UA\subseteq U\times LOC\times R$，从用户集合到角色集合的多对多映射，表示用户在某空间位置被赋予的角色；

$PA\subseteq P\times LOC\times R$，从许可集合到角色集合的多对多映射，表示角色在某空间位置被赋予的权限；

$RA\subseteq R\times R\times LOC$ 是角色集合上的一个偏序关系，称为层次关系。如果$(r_i,r_j)\in RH$，则定义为 $r_i \underset{(LOC)}{>} r_j$，表示在空间位置 LOC，r_i 继承 r_j 的权限；

$S=\langle U,R,UA,PA,C,ChangePosition,Op\rangle$，会话 S 是指用户与系统进行的一次交互。会话由 7 元组来描述，C 表示该会话在运行时必须满足的约束规则，$ChangePosition$ 表示会话状态发生变化时的空间位置，$Op\subseteq R\times S$，是指系统根据用户的任务要求所执行的指令，本文用到的 Op 有：

1)authorized(r,LOC)：使角色 r 在空间位置 LOC 处于授权状态。

2)assign_user(u,r,LOC)：在空间位置 LOC 给用户 u 分配角色 r。

3)assign_perm(r,p,LOC)：被用来在空间位置 LOC 给角色 r 分配权限 p。

4)get_role(u,r,LOC)：表示在空间位置 LOC 用户 u 激活角色 r。

5)get_perm(u,p,LOC)：表示在空间位置 LOC 角色 r 获得权限 p。

6)get_perm_role(p,r,LOC)：表示在空间位置 LOC，角色 r 获得权限 p。

7)session_role(u,s,LOC)：返回在空间对象 LOC 范围内用户 u 的会话 s 的相关角色。

8)session_perm(u,s,LOC)：返回在空间对象 LOC 范围内用户 u 的会话 s 的相关权限。

定义 2 空间位置左边关系

有两个空间位置 $L_i(X_i,Y_i)\in LOC$，$L_j(X_j,Y_j)\in LOC$，如果 $X_i<X_j$，则称 L_i 在 L_j 的左边，记为 $L_i<L_j$。

定义 3 空间区域

$LS=\{\langle L_i,L_j\rangle\mid L_i,L_j\in LOC,i<j\}$ 表示由 $\langle L_i,L_j\rangle$ 确定的空间区域。空间对象区域特征用对象最小包围矩形来表示。$LOCSet=2^{LS}$，表示由空间区域构成的集合。

同时规定一个角色状态可以为授权状态或非授权状态。用户只有被分配一个角色，并且这个角色处于授权状态时，用户才可以激活这个角色；而角色处于非授权状态时，则不能被激活。并且规定系统中每个会话都有一个优先级，记为 p，$(p,\leqslant)$是偏序的关系。

3 SRBAC 模型的约束

在提出的 SRBAC 模型中，首先定义了一个空间约束规则库。该规则库中把约束分为空间区域范围约束、空间区域大小约束、空间的角色激活基数约束和空间对象责任分离约束。这 4 种类型的约束全面反映了一个角色在空间区域特征维度上的访问控制规则，系统管理员可根据安全需要启用或禁用这些约束。

空间区域范围约束用来控制用户在某特定空间区域范围内能否建立会话，该会话可以给用户分配角色或给角色分配权限或改变角色状态。空间区域大小约束控制用户建立会话的空间区域的大小，该会话可以是给用户分配角色或给角色分配权限或改变角色状态。空间区域范围约束的起始位置是已知的，而空间区域大小约束的起始位置是未知的，其起始位置就是用户建立会话时所在位置。空间的角色激活基数约束是限制一个角色在某空间区域被激活的次数。空间对象责任分离约束用来控制冲突角色用在同一空间区域或同一角色用在冲突的空间区域上，它主要用于限制用户可实施的权限。

如表 1 所列：约束 a，b 是空间区域范围约束，a 表示管理员角色在办公室是授权状态，在家里是非授权状态；b 表示在办公室可以给小王分配管理员角色，在家里小王仅能被分配查询员角色。约束 c 是空间区域大小约束，在办公室小李被分配管理员角色，但是小李的活动范围仅有 100 平方米。约束 d 是角色激活基数约束，表示在办公室，最多可以有 5 个用户激活管理员角色，而小李在办公室仅能激活一次。

表 1

约束类型	带空间特性的角色约束
a	(办公室,authorized(管理员角色))
a	(家里,unauthorized(管理员角色))
b	(办公室,assign_user(小王,管理员角色))
b	(家里,assign_user(小王,查询员角色))
c	(办公室,assign_user(小李,管理员角色))
c	(100 平方米,assign_user(小李,管理员角色))
d	(办公室,5,active(管理员角色))
d	(办公室,1,active(小李,管理员角色))

4 SRBAC 模型的会话

假定系统中存在在空间位置 LOC_t 的会话集合 S，$S=\langle S(LOC_1),S(LOC_2),\cdots,S(LOC_t)\cdots\rangle$，$S(LOC_k)\in S$。系统中不同会话可能产生冲突，如有一个会话给用户分配角色 r，而有另外一个会话要取消给用户分配的角色 r，这样两个会话就产生了冲突。

4.1 冲突会话分类

1)同类会话冲突(类型 1)。会话是针对同一角色的同一类行为。如一个会话使角色从授权状态变为非授权状态，另一会话使该角色从非授权状态变为授权状态。

2)不同类会话冲突(类型 2)。会话是针对同一角色的不同类行为。如有一个会话激活一个角色，另一个会话使这个角色从授权状态变为非授权状态(非授权状态的角色是不能被激活的)。

4.2 冲突会话消除策略

定义 4 冲突会话消除策略

假设 S 是会话集合，$p:S$ 是优先级为 p 的会话，如果存在一优先级为 $q:Conf(S)$ 的会话，满足下面条件，则会话 q 阻塞会话 p。

1) 如果 $p:S$ 和 $q:Conf(s)$ 属于类型 1 冲突会话，并且 S 对应于表 2 的 S_1，$p\leqslant q$ 或者 s 对应于表 2 中的 S_2，$q>p$。

2) 如果 $p:S$ 和 $q:Conf(S)$ 属于类型 2 冲突会话，并且 s 对应于表 2 的 S_1。

3)存在相关约束禁止用户建立会话 S。假设规定角色 r 被激活的最大基数为 5，而在空间位置有 7 个用户激活角色 r，则其中 2 个用户建立的会话要被阻塞。

表 2

类型	S_1	$S_2=Conf(S_1)$	条件
1	authorized(r_1,LOC)	unauthorized(r_2,LOC)	$r_1=r_2$
1	assign_user(u_1,r_1,LOC)	unassign_user (u_2,r_2,LOC)	$r_1=r_2 \wedge u_1=u_2$
1	assign_perm(p_1,r_1,LOC)	unassign_perm (p_2,r_2,LOC)	$r_1=r_2 \wedge p_1=p_2$
2	get_role(u,r_1,LOC)	unauthorized(r_1,LOC)	$r_1=r_2$
2	get_role(u_1,r_1,LOC)	unassign_user (u_2,r_2,LOC)	$r_1=r_2 \wedge u_1=u_2$

存在冲突的会话时，优先级高的会话阻塞优先级低的会话。如果两个会话优先级相同，采取“否定”优先原则。同时规定，如果同时出现类型 1 和类型 2 的会话，先消除类型 1 的冲突会话。因为用户激活角色依赖于用户是否被分配该角色和该角色状态，以确保先解决冲突类型 1 的会话。

5 SRBAC 模型的继承

首先定义 4 条规则：

1)$assign\_perm(p,r,LOC) \rightarrow get\_perm\_role(p,r,LOC)$，表示在空间位置 LOC，权限 p 被分配给角色 r，则通过角色 r 可以得到权限 p。

2)$assign\_user(u,r,LOC) \rightarrow get\_role(u,r,LOC)$，表示在空间位置 LOC，用户 u 被分配角色 r，用户 u 就可以得到角色 r。

3)$get\_role(u,r,LOC) \wedge get\_perm\_role(p,r,LOC) \rightarrow get\_perm(u,p,LOC)$，表示在空间位置 LOC，用户 u 被分配角色 r，权限 p 被分配角色 r，用户 u 就可以通过角色 r 得到权限 p。

4)$session\_role(u,s,r,LOC) \wedge get\_perm\_role(p,r,LOC) \rightarrow session\_perm(u,p,LOC)$，表示在空间位置 LOC，用户 u 建立会话 s 激活角色 r，权限 p 被分配给角色 r，则用户 u 建立的这个会话 s 就可以得到权限 p。

Sandhu 等把角色继承分为权限继承和激活继承[9]，激活继承是权限继承的一个扩展。

①权限继承($\geqslant$)。儿子可以继承父亲的权限，但是用户不可以激活父亲这个角色。

②激活继承($>$)。儿子不可以直接继承父亲的权限，但是被分配儿子的用户可通过激活父亲，得到父亲的权限。

在空间环境下，父亲、儿子在同一空间区域的状态可能不一样，因此在此基础上进一步将在空间环境下的继承分为松散继承和严格继承，以便能更好执行“最小特权”原则。

①松散权限继承记为 $r_i \geqslant_{\langle W,LOC\rangle} r_j$，表示只要 r_i 在空间位置 LOC 是授权状态，不管 r_j 是否为授权状态，r_i 都可以继承 r_j 的权限。

$\forall p(x \geqslant_{\langle W,IS\rangle} y) \wedge authorized(x,LOC) \wedge get\_perm(p,y,LOC) \rightarrow get\_per(p,x,LOC)$

②严格权限继承记为 $r_i \geqslant_{S,LOC} r_j$，表示 r_i，r_j 在空间位置 LOC 必须都是授权状态，r_i 才可以继承 r_j 的权限。

$\forall p(x \geqslant_{\langle S,LOC\rangle} y) \wedge authorized(x,LOC) \wedge authorized(y,LOC) \wedge get\_perm(p,y,LOC) \rightarrow get\_perm(p,x,LOC)$

③松散激活继承记为 $r_i \geqslant_{\langle W,LOC\rangle} r_j$，表示只要 r_j 在空间位置 LOC 是授权状态，被分配角色 r_i 用户就可以激活 r_j。

$\forall u(x >_{\langle W,LOC\rangle} y) \wedge authorized(y,LOC) \wedge session\_role(u,s,x,LOC) \rightarrow session\_role(u,s,y,LOC)$

④严格激活继承记为 $r_i \geqslant_{\langle S,LOC\rangle} r_j$，表示 r_i，r_j 在空间位置 LOC 必须都是授权状态，被分配角色 r_i 用户才可以激活角色 r_j。

$\forall u(x >_{\langle S,LOC\rangle} y) \wedge authorized(x,LOC) \wedge authorized(y,LOC) \wedge session\_role(u,s,x,LOC) \rightarrow seession\_role(u,s,y,LOC)$

对图 1、图 2，超级管理员角色在区域 1 是授权状态，而角色管理员 1 和角色管理员 2 分别在区域 2、区域 3 内才是授权状态。图 1 是松散权限继承，则被分配超级管理员的用户在区域 1 内可以继承管理员 1 和管理员 2 两个角色的权限。图 2 是严格权限继承，则在区域 1 内被分配超级管理员的用户就不能继承管理员 1 和管理员 2 这两个角色的权限。

对图 3，角色超级管理员在任何区域都是授权状态，角色管理员 1、角色管理员 2 在区域 1 是授权状态，由于是松散激活继承，在区域 1 内被分配超级管理员角色的用户，可以激活管理员 1 角色和管理员 2 角色。

对图 4，角色超级管理员在区域 1、区域 2 内是授权状态，角色管理员 1、角色管理员 2 分别在区域 1、区域 2 是授权状态。由于是严格激活继承，被分配超级管理员的用户，在区域 1 可以激活管理员 1 角色，在区域 2 可以激活管理员 2 角色。

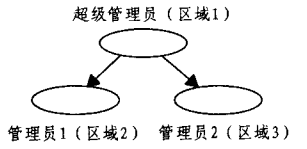

图 1 松散权限继承

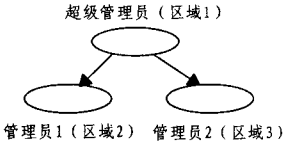

图 2 严格权限继承

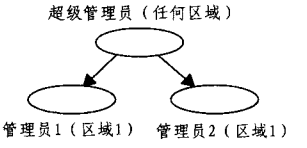

图 3 松散激活继承

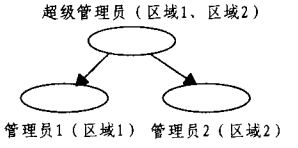

图 4 严格激活继承

6 应用

SecVista 是我们自主开发的内嵌式安全空间数据库管理系统，其已有的安全功能包括用户身份认证、自主访问控制、强制访问控制、审计跟踪、三权分立等。由于空间数据库系统庞大，而且还在不断发展之中，因此对安全管理模块的维护性和扩展性提出很高要求，所以我们在 SecVista 上实现了 SRBAC 模型。

SecVista 的 SRBAC 模型控制子系统主要有 RBAC 管理服务、身份认证服务、会话管理服务、访问请求决策服务和约束管理服务 5 个组成部分，5 个模块都由 RBAC 数据库提供数据支持。它们之间的关系见图 5。

例如表 1 所列的是 SecVista 系统中带有空间特性的角色约束，对约束 b，小王在办公室可以查询河流和通信塔的信息

（下转第 196 页）

证明:算法的时间复杂度是由 Σ 中异常最大化 XSMVD 的个数决定的,即为 n,所以整个算法的时间复杂度为 $O(n)$。

结束语 关于不完全信息环境下的 XML Schema 规范化理论,作者目前还没有查到国内的相应文献。本文针对此问题提出了存在 XML 强多值依赖的 XML Schema 规范化理论。基于 XML Schema、符合 XML Schema 的不完全 XML 文档树、子树信息等价和子树信息相容等概念提出了 XML 强多值依赖的定义。给出了弱键路径(集)和 XML 强多值依赖弱范式的定义,通过实例分析了 XML Schema 中数据冗余的原因,提出了转换规则,给出了规范化算法。本文的理论研究和实例分析表明,若 XML 文档存在大量不完全信息,一般情况下,此规范化理论只能减少数据冗余,不能完全消除数据冗余;若达到完全消除数据冗余,XML 文档不能出现大量不完全信息,从而表明数据冗余的多少与不完全信息的量存在着相互制约的关系。在未来的工作中,我们将对不完全信息环境下 XML 文档的查询进行研究。

参 考 文 献

[1] Vincent M W, Liu Jixue. Multivalued dependencies and a 4NF for XML[C]// International Conference on Advance Information Systems Engineering. Klagenfurt, Austria, 2003

[2] Vincent M W, Liu Jixue, Liu Chengfei. A redundancy Free 4NF for XML[C]// The first International XML Database Symposium. Berlin, Germany, 2003

[3] Vincent M W, Liu Jixue, Liu Chengfei. Strong functional dependencies and their application to normal forms in XML[J]. ACM Transactions on Database System, 2004, 29(3): 445-462

[4] 吕腾,顾宁,施伯乐. XML DTD 的一种范式[J]. 计算机研究与发展,2004,41(4):615-620

[5] 谈子敬,施伯乐. DTD 的规范化[J]. 计算机研究与发展,2004,41(4):594-600

[6] Arenas M, Libkin L. A normal form for XML documents[C]// Proceedings of the 21th ACM SIGA-CT-SIG-MOD-SIGART Symposium on Principles of Database Systems Madison. Wisconsin, USA: ACM Press, 2002: 85-96

[7] 邱威,张立臣. 存在多值依赖的 XML DTD 规范化研究[J]. 计算机科学,2007,34(2):149-152

[8] 郝忠孝. 空值环境下数据库导论[M]. 北京:机械工业出版社,1996

[9] 殷丽凤,郝忠孝. XML 强函数依赖的推理规则[J]. 计算机科学,2008,35(9):165-167

[10] 殷丽凤,郝忠孝. XML 强闭包依赖的研究[J]. 计算机科学,2008,35(11):591-594

(上接第 191 页)

(见图 6),而在家里,他仅可以查询河流的信息(见图 7)。

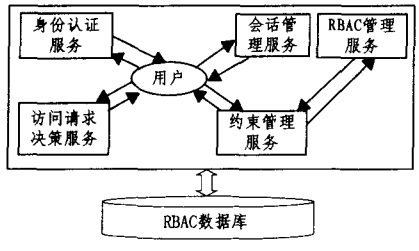

图 5 访问控制子系统的系统结构

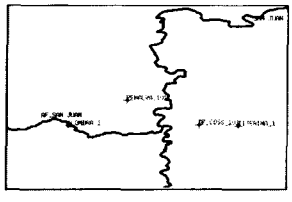

图 6

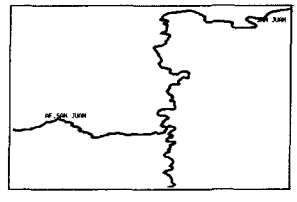

图 7

结束语 SRBAC 是在 RBAC96 基础上作空间特性的扩展。引入空间特性后的 SRBAC 模型有着更全面、更具体的安全描述能力。SRBAC 对传统的约束、会话和系统状态进行空间扩充,解决了空间约束、会话状态转变和角色继承问题,但在系统一致性维护方面仍有很多工作需要进一步研究。

参 考 文 献

[1] Sandhu R S, Conye E J, Feinstein H L. Role_Based Access Control Models[J]. IEEE Computer, 1996, 29(2): 38-47

[2] Osborn S L, Sandhu R, Munawer Q. Configuring Role-Based Access Control to Enforce Mandatory and Discretionary Access Control Policies[J]. ACM Trans. Information and System Security, 2000, 3(2): 85-106

[3] Kuhn D R. Role based access control on MLS systems without kernel changes[C]// Proc. of the third ACM Workshop on Role-Based Access Control. Fairfax, Virginia, United States, October 1998: 25-32

[4] Osborn S. Mandatory access control and role-based access control revisited[C]// Proc of the Second ACM Workshop on Role-Based Access Control. Fairfa, Virginia, United States, November 1997: 31-40

[5] Ferraiolo D F, Sandhu R, Gavrila S. Proposed NIST standard for role-based access control[J]. ACM Transactions on Information and System Security, 2001, 4(3): 224-274

[6] Joshi J, Bertino E, Latif U, et al. A Generalized Temporal Role-based Access Control Model[J]. IEEE Trans. Knowl. Data Eng, 2005, 17(1): 4-23

[7] Bertino E, Bonatti P A, Ferrari E. A Temporal Role-Based Access Control Model[J]. ACM Transactions On Information and System security, 2001, 4(3): 191-223

[8] Hansen F, Oleshchuk V. Spatial Role-Based Access Control Model for Wireless Networks[C]// Vehicular Technology Conference, VTC 2003-Fall. 2003 IEEE 58th: 2093-2097

[9] Sandhu R. Role activation hierarchies[C]// Proceddings of 2rd Acm Workshop on Role-based Access Control. Fairfax, Virginia, October 1998: 65-79