校园网访问控制系统的应用研究①

Application of Campus Network Security Authentication System

曹锦梅 孟祥娟 杨 芳 (新疆医科大学 高职学院 新疆 乌鲁木齐 830054)

摘 要： 身份验证和权限分配一直是网络应用中的核心问题。该文设计了一种基于角色的访问控制系统,，改变以往静态授权的缺陷，设计了一个基于 RBAC 的动态权限配置应用到校园网中，设置了授权信息表，根据角色的改变而修改访问权限，引入筛选条件对记录进行控制，实现了资源细粒度访问控制，比传统的访问控制方式更为严格,，也具有更大的灵活性和普适性，有效提高了安全性，可广泛应用到各类局域网中。

关键词： 校园网 RBAC 角色 授权 认证

目前高等院校网络基础设施建设已初具规模，但一般的方法是采用“用户名+口令”这种简单的传统认证方式，随着校园网的发展必将会存在诸多安全隐患，同时系统信息资源管理也将面临着重大安全隐患。

近年来在访问控制这个课题中，国际上在典型的自主访问控制与强制访问控制的基础上提出了若干种访问控制模型及其改进模型。Bertino, Sandhu 提出了具有否定授权功能的授权模型[1,2]， Sandhu 提出基于角色的访问控制模型[2]， Adam 提出了基于内容的访问控制模型[3]。

1 基于角色的访问控制

1.1 RBAC 模型

基于角色访问控制技术是当前研究的一大热点。RBAC 技术有效地克服了传统访问控制技术的不足，减少授权管理的复杂性，使指定和执行特定企业保护策略过程更加灵活。该模型通过在用户和权限之间引入角色这个中介，为用户授予角色，为角色授予权限，用户通过角色间接访问系统资源，实现了用户与权限的逻辑分离[4]。

1.2 RBAC 模型的优势

访问控制策略一般有 3 种:自主型访问控制方法(Discretionary Access Control,DAC)、强制型访问控制方法(Mandatory Access Control,MAC)和基于角色的访问控制方法(RBAC)。DAC 和 MAC 直接对用户授予或取消权限,但当用户数量巨大且关系复杂时,主体和客体的匹配以及权限的授予和管理会变得复杂而且困难。采用 DAC 和 MAC 访问控制模型很难灵活地管理权限。

采用 RBAC 模型的权限策略将权限授予角色而非用户,即访问控制的权限是由各个人员所担任的角色来确定的。用角色表示访问主体具有的职权和责任,可以灵活地表达和实现校园网的访问控制策略,使系统权限管理在校园网的组织视图这个较高的抽象集上进行,从而简化了权限的管理。

2 系统设计与实现

2.1 系统开发及运行环境

本设计的实现平台为：jdk1.4.2+ tomcat5.0.28+ SQL Server2000，操作系统为 windows2000。利用基于角色的访问控制机制，设计了一种基于角色的授权管理系统，以校园网图书管理为例进行实证研究。

① 基金项目:新疆医科大学大学生创新性实验计划项目(CX2008131)
收稿时间:2008-07-17

2.2 授权管理信息表的设计

本系统对用户访问表、记录、字段均是从授权信息表获取信息，然后对信息进行分析、综合而实现的；同时，授权管理中心为用户授予角色、为角色授予权限，也要根据这些信息表控制授权，防止重复授权，实现角色互斥等。

在本方案中授权数据库中设计了 7 个授权信息表，这些信息表分别存储用户信息、角色信息、用户/角色信息、角色约束信息、角色继承信息、字段映射信息以及访问权限信息。各信息表的详细设计如下：

(1)用户信息表（User_table）

此表是系统中用户基本信息的存储场所，作为身份验证的基本信息，只有在用户信息表中登记的用户才允许授予角色，允许访问数据库资源。结构如表 1 所示：

表 1　用户信息表的结构

编号	字段名称	数据类型	字段说明
1	User_name	char (20)	用户名，主键
2	Unit	char (100)	用户单位
3	E_mail	char (20)	用户 e-mail
4	ID_card	char (20)	身份证号
5	degree	char (40)	学历
6	Telephone	smallint	用户联系电话

这里将 user_name 定义为主键，既保证了用户信息表中用户信息的唯一性，同时，可被用户/角色信息表引用为外键，并定义为级联删除，当用户表中一个用户信息被删除时，用户/角色信息表中则相关信息被自动删除，确保了相关表数据的一致性、完整性。

(2)角色信息表（Role_table）

由管理员根据一个部门提供的职位建立，结构如表 2 所示：

表 2　角色信息表的结构

编号	字段名称	数据类型	字段说明
1	Role_name	char(20)	角色名，主键
2	H_set_no	smallint	继承角色集编号
3	E_set_no	smallint	互斥角色集编号
4	Con_num	smallint	角色授予用户数
5	User_num	smallint	角色已授予用户数

这里将 role_name 定义为主键，既保证了角色信息表中角色信息的唯一性。同时，可被用户/角色信息表、访问权限信息表引用为外键，当这些表参照完整性定义为级联删除时，角色信息表中的角色信息被删除，则这些引用为外键的信息表中相关信息被自动删除，确保了相关信息表数据的一致性、完整性。

定义外键 h_set_no 和 e_set_no 参考 role_inherit 表和 role_con 表中同名列，由于这两个外键约束，限制了 role_inherit 表和 role_con 表中记录的删除，防止这两个表记录删除导致角色表的空指针现象，使这三个表的数据项保持一致性、完整性。

(3)用户/角色信息表（User_role）

此表是授权管理员为用户授予角色信息的存储场所。结构如表 3 所示：

表 3　用户/角色信息表的结构

编号	字段名称	数据类型	字段说明
1	User_name	char(20)	被授予角色用户名
2	Role_name	char(20)	角色名

定义外键user_name和role_name参考users_table表和role_table表中同名列，使这三个表的数据项保持一致性、完整性。定义user_name　role_name的组合唯一性约束，可防止对用户的重复授权。

(4)角色约束信息表（Role_con）

角色约束主要有角色互斥，另外还有授权的互斥、角色数量的约束，由于角色数量的约束通过在角色表中设置 con_num(角色授予用户的最多数量)、user_num(角色已授予用户的数量)两字段，并在授权中检查这两个字段来实现。因此，这里所提出的角色约束信息表存贮的是角色的互斥信息。互斥角色基数就是一个用户只能被授予互斥角色中的基数规定数量的角色。其结构如表 4 所示：

表 4　角色约束信息表的结构

编号	字段名称	数据类型	字段说明
1	E_set_no	smallint	互斥角色集编号
2	E_set	char(200)	互斥角色集
3	Base_num	smallint	互斥角色基数

定义 e_set_no 为主键，保证了互斥角色集的唯一性，并可作为角色信息表的外键。这种约束限制了角色约束信息表的记录随意删除，防止角色信息表中空指针，保证与角色信息表的完整性、一致性。

(5)角色继承信息表(Role_inherit)

主要存储角色之间的层次信息，由部门负责人提

供给授权管理员，一般保持不变。其结构如表 5 所示：

表 5 角色继承信息表的结构

编号	字段名称	数据类型	字段说明
1	H_set_no	smallint	继承角色集号
2	Role_name	char(20)	角色名
3	Down_role_set	char(50)	被继承角色集

采用直接继承角色集的表示方法，该方法在角色继承信息表中以该角色为根，按照树先序遍历的顺序，存贮直接被继承的角色(即儿子角色)，存贮元素以“ / ”开始和结束，每个角色间用“ / ”分开， 此方法可以减少角色继承信息表中记录的数量，节省存贮空间；便于继承角色的查找，在程序中容易实现对继承角色的搜索。

定义 h_ set_ no 为主键，作为角色信息表的引用为外键。定义 h_set_no 与 role_ name 的组合唯一性约束，保证了角色继承信息表中记录的唯一性。

(6)字段映射信息表（Field_map）

此表保存被访问的数据库中表的字段在该表中位置映射信息，由数据库结构搜索程序自动导入，位置编号由程序自动生成。数据库结构搜索程序是按照数据库资源树先序遍历的顺序，将字段与数值对应起来。字段映射信息表是字段访问控制掩码(FACM)转换成字段访问权限信息时使用的重要控制表。其结构如表 6 所示：

表 6 字段映射信息表的结构

编号	字段名称	数据类型	字段说明
1	Table_name	char(20)	目标数据库中表的名字
2	Field_name	char(20)	表中字段名
3	Pos_value	smallint	字段在表中位置映射值

table_ name, field_ name 组合作为唯一性约束，保证此表只能给每个用户访问的表字段赋予唯一的位置值。

(7)访问权限信息表（Access_perm）

此表是授权信息的存储场所，通过授权管理中心提供的界面管理此表。为了能对数据库资源实施细粒度访问控制，此表设置了对表、记录、字段访问控制。其结构如表 7 所示：

表 7 访问权限信息表的结构

编号	字段名称	数据类型	字段说明
1	Role_name	char(20)	映射角色，外键
2	Table_name	char(20)	表名
3	Op_type	check(10)	操作类型
4	Rd_condition	char(300)	可访问记录范围
5	Fd_access	Char(10)	可访问掩码表示
6	Sq_date	datetime	为角色授权时间

定义外键 role_name 参考 roles_ table 表中同名列，使这两个表的数据项保持一致性、完整性。定义 op_type 为 CHECK 类型约束，则使系统自动检查操作类型，使操作类型限制在 select, insert, update, delete, all 五种中，这样定义可保证操作类型的错误授权，授权时通过选择项选取相应操作类型即可。当操作类型为 all 时，表示该角色具有前四种权限。定义 sq_date 为缺省的时间值，实现在授权时自动取系统时间，简化了授权时输入时间的繁琐操作。

2.3 访问控制掩码（ACM，Access Control Mask）

访问控制掩码是一个多位的二进制，其位数与用户访问的表中字段的数量相等。掩码的每一位与相应操作权限对应，没有该权限时，对应位为 0，有该权限时，对应位为 1。字段位置编号体现在字段映射信息表中，FACM（Field Access Control Mask）二进制数据按顺序与字段一一对应。通过这种映射，FACM 中的每一位可与一字段相对应。管理员通过给 FACM 中与字段对应的位进行置位或复位操作设置权限。

3 用户、角色、权限管理的关键算法

3.1 用户角色管理

RBAC 方法引入了角色，这样用户与角色之间以及角色与权限之间就形成了两个多对多的关系。角色之间有继承关系，此关系反映了一个组织内部权力和责任的关系，提供了对已有角色的扩充和分类的手段，使定义新的角色可以在已有角色的基础上进行，扩充就是通过增加父角色的权限去定义子角色，分类通过不同子角色

继承同一父角色来体现.角色管理流程如图 1 所示：

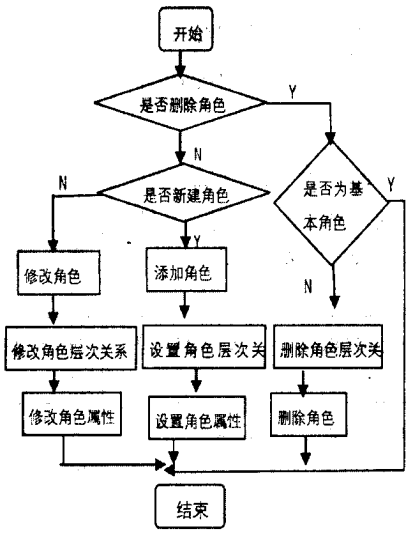

图 1　角色管理流程图

3.2 用户权限的验证

通过查询角色信息表和访问权限信息表，验证用户是否有权进行当前操作，并且确定对应的角色是否是有效登录，如果验证通过，则打开目标数据库进行相应的操作，否则给出错误提示，并中止当前操作。权限管理流程如图 2 所示：

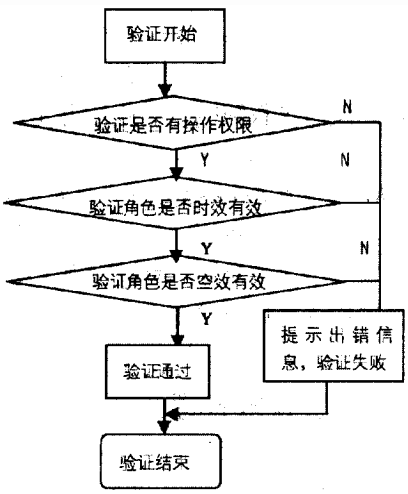

图 2　权限验证流程图

3.3 权限授予与回收

角色授予的完整性原则：

①权限授予以角色为单位进行。

②已拥有高级别角色的用户不能再授予低级别角色，除非在时效上和空效上没有重叠。

③角色授予过程中不能形成闭合环，即用户不能直接或间接对自己授予角色。

4　授权管理中心的设计

授权管理中心应具备以下特点：

(1)易操作。要求界面做到人性化，尽量简单。要屏蔽对后台授权信息表的繁琐操作。

(2)有效性。主要是针对数据库资源特点和基于角色策略进行设计。对用户信息表、角色信息表、角色继承信息表、角色约束信息表实施管理。按照数据库资源所属部门提供的用户信息、角色组织结构关系对各表进行管理。数据库表的操作主要有查询、插入、修改、删除四种对访问权限信息表进行管理。

5　结束语

通过对校园网系统中的用户权限的动态配置要求的研究及分析，采用基于 RBAC 技术，并与数据库紧密结合，实现了用户权限按照预定角色进行实施灵活的配置。它比传统的访问控制方式更为严格，也具有更大的灵活性和普适性，必将在未来计算机应用系统中获得越来越广泛的应用。在此基础上，本设计还有待进一步完善，对角色的继承和约束机制还需进一步深入研究。

参考文献

1 Bertino E, Samarati P, Jajodia S. A Temporal Access Control Mechanism for Database System. IEEE Transactions on Knowledge and Data Engineering. 2004, 8(1): 67–80.

2 Sandhu R. Access Control: The Neglected Frontier Proceedings of First Australasian Conference on Information Security and Privacy. 1996, 6(1): 23–26.

3 Adam N.R, Atluri V. A Content-Based Authorization Model for Digital Libraries. IEEE Transactions on Knowledge and Data Engineering.2005,14(2): 263–301.

4 孙群.多组织多用户条件下基于角色的访问控制.济南:山东大学[硕士学位论文],2005.

5 杨善林,吴涛.基于 LDAP 技术的协同商务认证与访问控制的实现.计算机应用研究,2005, 10.

6 杨湖,李凤蕾,王斌.SQL Server2005 数据库系统开发案例精选.北京:人民邮电出版社,2007.