

DOI: 10.3976/j.issn.1002-4026.2011.06.021

# RBAC模型在中医药信息资源管理平台中的应用研究

李振阳,曹慧,马金刚,宋晓瑞

(山东中医药大学理工学院,山东 济南 250355)

**摘要:**采用基于角色的访问控制(role-based access control, RBAC)技术,构建了一个通用的中医药信息资源管理平台。在平台中引入角色这一中介,在统一身份认证的基础上,对不同的资源进行角色访问控制,每一个资源子模块定义为一个数据库角色,该角色具有子模块所拥有的权限,然后根据需要把这些角色授予各个用户。该平台安全、易于管理,有良好的可移植性和扩展性,获得了较好的用户体验。

**关键词:**中医药信息资源;基于角色的访问控制;权限管理

**中图分类号:**TP311      **文献标识码:**A      **文章编号:**1002-4026(2011)06-0084-04

## Application of RBAC model in a traditional Chinese medicine information resources management platform

LI Zhen-yang, CAO Hui, MA Jin-gang, SONG Xiao-rui

(School of Science and Engineering, Shandong University of Traditional Chinese medicine, Jinan 250355, China)

**Abstract:** We constructed a universal traditional Chinese medicine information resources management platform with role-based access control (RBAC) technology. We introduced the concept of a role, an intermediate, into the platform and performed universal identity authentication based role access control for different resources. We also defined each sub-module as a database role which had the same authority as a sub-module, and then distributed these roles to all users. The platform is secure, easy to be managed, and has good transferability and scalability. It therefore receives better favor from many users.

**Key words:** traditional Chinese medicine information resources; role-based access control; authority management

长期以来,我国在中医药研究及实践过程中积累了大量的科学研究和观察数据,但由于管理体制、历史渊源等原因,许多数据资源较分散,不能有效共享,形成了严重的数据壁垒,使得中医药行业工作者往往很难得到研究所需的数据资源,不能全面、及时地了解中医药发展动态,在很多情况下不得不进行重复工作,不仅造成了时间和资源的浪费,而且使得数据的可信度、完整度、权威性得不到保障。随着网络的快速发展,利用现代信息技术,整合和抢救离散的中医药数据资源,形成统一、有效的数据共享服务系统,有助于避免资源的流失及研究的重复浪费,也为挖掘和搜寻分散的数据资源提供了方便,是抢救数据资源的有力措施,这就对中医药信息资源的访问控制服务系统提出了更高的要求。

收稿日期:2011-08-30

基金项目:济南市科技局自主创新计划项目(200906007)

作者简介:李振阳(1984-),男,硕士,研究方向为生物医学信息处理与分析、虚拟现实技术。Email:1984060455@163.com

自 20 世纪 90 年代以来出现的基于角色的访问控制技术(role-based access control, RBAC),不仅有效地减少了授权管理的复杂性,而且为管理员提供了一个较好的实现安全政策的环境<sup>[1]</sup>。由于中医药信息资源管理平台资源是完全预知的,通过 RBAC 技术可以进行全局的权限规划<sup>[2]</sup>,本文利用此技术,在统一身份认证的基础上,对不同的资源进行角色访问控制,构建出一个通用的、完善的、安全的、易于管理的、有良好的可移植性和扩展性的权限管理模型。

### 1 RBAC 模型

在 RBAC 中,权限与角色相关联,用户通过成为适当角色的成员而得到这些角色的权限,在一个组织中,角色是为了完成各种工作而创造,用户则依据它的责任和资格来被指派相应的角色,用户可以很容易的从一个角色被指派到另一个角色。所谓“角色”就是一个或一群用户在组织内可执行的操作的集合<sup>[3]</sup>,可依新的需求和系统的合并而赋予新的权限,而权限也可以根据需要而从某角色中回收。RBAC 的基本思想就是,使用角色来管理用户的访问权,通过角色定义一组访问权限并将其分配给用户,从而将用户和访问权限在逻辑上分开,但是用户并不直接与权限关联,权限控制看似复杂,但也可以用极其简单的逻辑表达式来表达,即“WHO”对“WHAT”进行“HOW”操作,实质上是对资源的一种保护方法<sup>[4-7]</sup>。

根据 NIST,标准 RBAC 模型定义了 4 部分组件——基本 RBAC 模型(Core RBAC)、角色分级 RBAC 模型(Hierarchy RBAC)、角色限制 RBAC 模型(Constrained RBAC)和统一 RBAC 模型(Combines RBAC)<sup>[8]</sup>,本文采用了 4 种 RBAC 组件模型中的基本 RBAC 模型,见图 1。在 RBAC 之中,包含用户(Users)、角色(Roles)、目标(Objects)、操作(Operations)、许可权(Permissions) 5 个基本数据元素,权限被赋予角色,当一个角色被指定给一个用户时,此用户就拥有了该角色所包含的权限,实质上角色访问控制,决定主体是否被授权对客体执行某种操作。

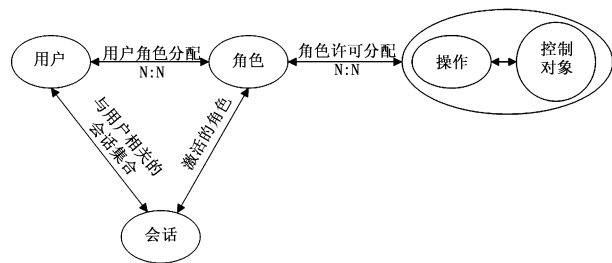


图 1 基本 RBAC 模型

Fig. 1 Basic RBAC model

### 2 中医药信息资源管理平台分析

中医药信息资源管理平台功能模块主要包括资源类别管理、资源管理、资源历史、资源版本对比、附件管理、资源审核、标签管理、资源搜索、评论功能等,每个模块又可以细化为若干子模块,见图 2。比如资源管理模块包含了资源的删除、添加、修改、查询等子模块。由于中医药信息资源内容丰富,在维护、管理、利用过程中难度大,所以采用基于 RBAC 模型的安全管理,通过角色将用户和权限联系起来,减小了授权管理的复杂性,以及权限管理的负担和代价,让系统简洁易懂、容易维护,提高了工作效率<sup>[9]</sup>。

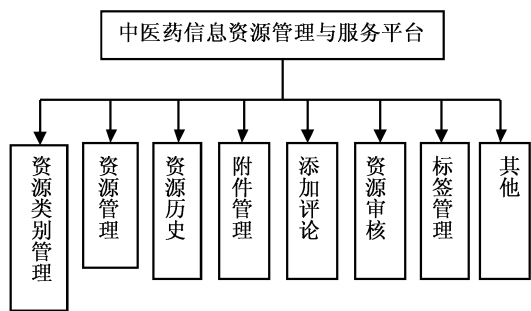


图 2 中医药信息资源管理平台功能模块

Fig. 2 Functional module of traditional Chinese medicine information resource management platform

### 3 RBAC 模型在中医药信息资源管理平台中权限管理的实现

中医药信息资源管理平台针对广大用户,提供查询并使用中医药相关信息,满足用户对中医药医疗服务的需求。根据需要为每一个资源模块的子模块定义一个数据库角色,角色具有相应子模块所拥有的权限,然后根据需要把这些角色授予各个用户。

### 3.1 用户权限模块的设计

在中医药信息资源管理平台中用户权限管理功能结构主要由用户信息管理、系统权限管理、角色管理三大模块组成,见图3。

(1)用户管理模块:用户是角色的实体,在创建用户时要为用户分配一个或多个角色,同一角色只属于一个部门,决定了用户也只属于一个部门,但在部门中,通过系统管理员的设置,一个用户可以有多个角色,其具体的权限由权限集来实现;

(2)权限集管理模块:权限集是一个或者多个权限的集合体,可以灵活地对权限集加以修改而不必改动相应的单个权限,能灵活的操作相关权限,提高权限管理的效率;

(3)角色管理模块:在此模块中,系统管理员可自行添加需要的角色,并建立相应的用户与角色、角色与权限集的映射。

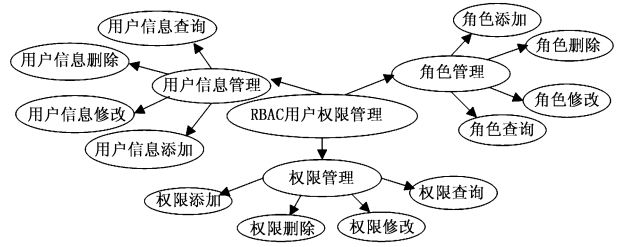


图3 基于RBAC的用户权限管理模块功能结构图  
Fig. 3 Structural-functional diagram of RBAC-based user authority management module

### 3.2 数据库模块

基于RBAC的中医药信息资源管理平台用户权限、管理权限、角色管理中的核心数据结构包括用户、角色和权限,与其他实体表的关系如图4所示。

### 3.3 数据表模块

为了管理系统的权限管理信息,在数据库的基础之上建立了基表,主要包括权限表、权限类别表、用户角色表、角色权限关联表、用户角色关联表和用户信息表。

(1)权限表:存放权限编号、列表编号、权限名信息。描述了系统中功能模块所用的具体权限。

(2)权限类别表:存放类别编号、类别名。权限类别是针对系统中功能模块的权限分类,和角色有所不同,只是为了方便维护管理权限而已。

(3)用户角色表:存放角色编号、角色名信息。角色是一个权限的逻辑分组,是针对具有相同权限用户的抽象定义。

(4)角色权限关联表:保存角色和权限的对应关系信息,从而说明每个角色具体拥有的权限。

(5)用户角色关联表:保存用户和角色的对应关系,主键是由User ID和Role ID组合构成的,用户有可能属于多个角色。

(6)用户信息表:存放用户的姓名、性别、联系方式、注册IP等相关信息。

### 3.4 系统实现的关键步骤

#### (1)数据的准备

中医药信息资源管理平台的总体及功能模块的设计;根据中医药资源的需要设立角色,并给各个角色分配权限;录入用户信息并把角色赋予用户。

#### (2)读入用户信息

用户登录时,首先判断用户名与密码,错误则给出出错信息,如正确,进一步去人员角色关系表中读取

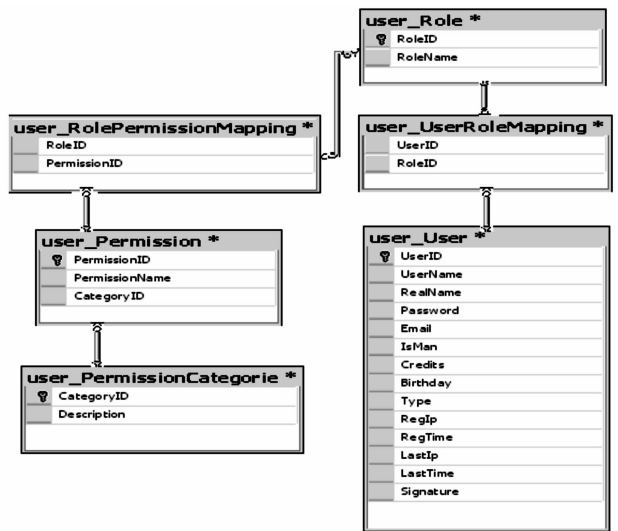


图4 权限角色管理实体表关系图  
Fig.4 Relationship chart of role management tables of authority

属于他的角色信息列表,如果列表为空,表示该用户无权访问中医药信息资源管理系统并给出出错信息,不予登录。虽然一个用户可以拥有多重角色,但在某一个时刻,只能拥有其中一个角色的权限,如果需要行使其他角色的权限,可以通过列表更换身份。

### (3) 确定显示菜单

根据当前用户的默认角色,从角色与功能模块关系表中读取该角色所拥有的权限,根据功能模块与菜单的对应关系可以逆推当前用户显示哪些菜单。

### (4) 菜单响应

用户点击菜单时,根据菜单编号,从菜单与功能模块关系表中读取该菜单的功能模块的信息列表,通过RBAC模型的访问控制方法可以灵活高效地实现中医药信息资源管理系统中的权限控制。

## 4 结论

访问控制是保障信息系统安全的一个重要环节,本文通过RBAC技术,在中医药信息资源管理平台中引入角色这一中介,在统一的身份认证的基础上,对于不同的资源进行角色访问控制,在很大程度上简化了对信息资源访问控制的管理,使得该系统管理易于实现且效率更高,具有界面友好、方便、灵活、开销低等特点,减轻了管理员的权限维护工作量,提高了系统的安全性,可以很好地在各大医院、医学院校、基层社区卫生院等医疗单位使用。

## 参考文献:

- [1] 欧晓鸥,王志立,魏建香. 基于RBAC与GFAC架构的访问控制模型[J]. 计算机应用,2008,8(3):612-614.
- [2] 李南妮,张璟,李军怀. 一种基于树型结构的B/S系统权限控制方法[J]. 计算机应用研究,2005,22(10):128-130.
- [3] 夏志雄,张曙光. RBAC在基于Web管理信息系统中的应用[J]. 计算机应用研究,2004,21(7):198-199.
- [4] 张晓艳. RBAC模型在物资管理系统中的应用[J]. 电脑知识与技术,2008,4(4):997-999.
- [5] 沈磊,张媛,蒋平. 基于RBAC的权限管理在Web中的设计与实现[J]. 计算机时代,2010(10):49-51.
- [6] 吴波,王晶. 基于基本RBAC模型的权限管理框架的设计与实现[J]. 计算机系统应用,2011,20(4):50-54.
- [7] 甘剑,施荣华. 一种基于角色的动态访问控制模型的研究及应用[J]. 微计算机信息,2010,26(33):160-162.
- [8] 郑培旭,吴德雄,罗键,等. 基于RBAC的构件权限控制的研究与实现[J]. 电脑知识与技术,2010,6(28):8063-8065.
- [9] 周志烽,王晶. 基于RBAC的安全管理模块的设计与实现[J]. 电信工程技术与标准化,2010(10):84-88.
- [10] 董理君,余胜生,杜敏,等. 一种基于环境安全的角色访问控制模型研究[J]. 计算机科学,2009,36(1):51-59.
- [11] 吴新松,贺也平,周洲仪,等. 一个环境适应的基于角色的访问控制模型[J]. 计算机研究与发展,2011,48(6):983-990.
- [12] 唐为民,彭双和,韩臻,等. 一种基于角色的强制访问控制模型[J]. 北京交通大学学报,2010,34(2):95-100.
- [13] 王宇新,田佳,郭禾,等. 基于模糊的RBAC模型研究与优化[J]. 计算机工程,2010,36(13):137-139.
- [14] 张黎明,李玉龙. 基于角色的权限代理模型及其实现[J]. 计算机应用研究,2009,26(2):730-732.
- [15] 杨萍,李杰,胡芳. 基于资源的RBAC模型的研究与分析[J]. 计算机测量与控制,2008,16(2):231-232.
- [16] 廖尔崇,徐晓飞,刘旭东,等. 扩展的角色访问控制模型及其应用[J]. 计算机工程与设计,2008,29(7):1608-1611.
- [17] 樊金生,关保灿,李晓东. 基于角色的访问控制扩展模型及其实现[J]. 计算机工程与设计,2008,29(18):4718-4720.