

RBAC模型在B/S医院信息系统中的应用

黄静, 陈震, 危水根, 王凌

(南昌航空大学 计算机视觉研究室, 江西 南昌 330063)

摘要: RBAC(基于角色访问控制)的核心是利用角色建立用户与权限之间的联系,实现了用户与访问权限的逻辑分离,其优点是减少了授权管理的复杂性,降低管理开销,具有灵活、易用和高效的特点。针对医院信息系统(HIS)在实际运行中存在的权限管理的复杂性和数据的安全性问题,在分析传统RBAC模型的基础上,结合B/S模式医院信息系统的实际需求,设计了一个实用的、可靠的权限管理应用模型,分析了基于该模型的访问控制模块在医院信息系统中应用的合理性,并采用ASP.NET及SQL Server 2000等技术予以实现。

关键词: RBAC模型; 医院信息系统; 访问控制; 角色; 权限

中图分类号: TP309.2

文献标识码: A

文章编号: 1673-629X(2011)06-0246-04

Application of Role-Based Access Control Model in B/S Hospital Information System

HUANG Jing, CHEN Zhen, WEI Shui-gen, WANG Ling

(Laboratory of Computer Vision, Nanchang Hangkong University, Nanchang 330063, China)

Abstract: The core of RBAC (Role Based Access Control) is that the relationship between the permission and user is established by the role, so as to achieve the logical separation of user and permission, the advantage of this model is to reduce the complexity and the cost of authorization management. It is flexible, easy and efficient. Considering the actual demand of hospital information system (HIS) based on B/S model, designed a application model of permission management applied to the HIS based on the traditional RBAC model, to solve the complexity of privilege management and data security issues which were existed in the actual operation of HIS, and analysed the rationality of its application in HIS based on this model. Finally, the system is realized by ASP.NET, SQL Server 2000 and other technologies.

Key words: RBAC model; HIS; access control; role; permission

0 引言

医院管理对医院信息系统(Hospital Information System, HIS)有较高的安全性要求, HIS必须不间断地运行,既不允许数据丢失,也不允许数据泄密,需要较好的健壮性和保密性。系统应有严密的数据验证和身份认证,保证数据的准确和安全,同时还需要有详细的权限划分,以配合医院的实际管理制度。B/S模式虽解决了传统C/S模式的工作量大及不易维护等问题,但是由于其开放式和分布式的特点,系统对数据安全性的要求则更高,所以必须解决系统的权限管理问题。在权限管理中,访问控制是实现整个权限的核心内容,

它是实现数据保密性和完整性机制的主要手段^[1]。其中,基于角色的访问控制(role based access control, RBAC)是目前应用较为广泛的一种访问控制技术,是解决大型企业统一资源访问控制的有效方法^[2]。为了解决以往系统权限管理普遍存在的安全性较低、用户功能单一和授权灵活性差的问题,文中采用基于角色的访问控制技术来实现B/S模式下医院信息系统中的权限管理,从而增加系统的可靠性和安全性,防止非法用户的入侵和合法用户的非法操作造成的数据破坏。

1 基于角色访问控制(RBAC)模型概述

1.1 访问控制

访问控制是指防止对资源的未授权使用,即允许被授权的主体对某些客体的访问、拒绝向非授权的主体提供服务的策略^[3]。一个完整的访问控制系统一般应包括:1. 主体(Subject):发出访问操作、存取要求

收稿日期:2010-11-22;修回日期:2011-01-24

基金项目:国家自然科学基金资助项目(60963003);教育部科学技术研究重点课题(206080)

作者简介:黄静(1988-),女,江西上饶人,硕士研究生,主要研究领域为医疗信息系统、信息安全;陈震,教授,博士,主要研究领域为计算机视觉、生物影像处理、模式识别。

的主动方,通常指用户或用户的进程;2. 客体 (Object):被调用的程序或欲存取的数据访问;3. 访问控制政策:一套规则,用于确定主体是否对客体拥有访问权限^[4]。

传统型访问控制策略分为两类:自主型访问控制 (DAC) 和强制型访问控制 (MAC) 策略。自主型的访问控制 (DAC) 是目前计算机系统中实现最多的访问控制机制,它是在确认主体身份以及它们所属组的基础上对访问进行限定的一种方法;而强制型的访问控制 (MAC) 是“强加”给访问主体的,即系统强制主体服从访问控制的策略^[5]。自主型访问控制模型灵活性较高,但安全级别较低;而强制型访问控制管理比较集中,但实现工作量太大,不适用于主客体经常更新的环境。传统的访问控制策略采用对系统中用户进行直接的权限管理模式,授权方式不灵活,权限操作比较复杂,难以适应业务管理不断变化的医院信息系统的需求。20 世纪 90 年代提出的 RBAC 技术能有效地克服传统访问控制技术的不足,RBAC 具有无可比拟的灵活性和易操作性,改变了以往把业务流程“固化”在应用系统中的开发模式,实现了系统业务的动态调整^[6]。

HIS 中的主体是使用医院信息系统的用户, HIS 要提供对用户使用医院信息系统功能的授权,从而使系统软件在一个合理的范围内被使用,保证了数据和系统的安全。因为 B/S 模式的医院信息系统是一个比较典型的企业信息系统,它具有比较复杂的功能模块,在实际使用上,由于存在多种用户类型 (医生、护士、系统管理员等),需要对不同的用户根据其身份进行访问控制,并考虑到网站系统的扩展性和可伸缩性问题,文中选择了 RBAC 权限管理机制,以实现用户对访问控制的动态管理。

1.2 RBAC 模型的基本思想

RBAC 模型中,在用户 (User) 和权限 (Permission) 之间引入了角色 (Role) 的概念,实现了用户和访问权限在逻辑上的分离,将对用户的授权分成两个部分,通过角色来联系用户和权限^[7],其模型如图 1 所示。一个用户可以被赋予若干角色,一个角色也可以被赋予给若干个具体用户,用户和角色之间是多对多的关系,用户添加到角色中,就自动继承了角色的权限;同样,一个角色可以具有多项权限,一项权限也可被赋予给多个不同的角色,角色和权限之间也是多对多的关系;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^[8]。RBAC 中用户不直接与权限关联,因此简化了权限的管理。RBAC 对访问权限的授权由管理员统一管理,根据用户在组织内所处的角色做出访问授权与控制,授权规定是强加给用户的,用户不能自主地将访问权限传给他人,这是一种非自主型

集中式访问控制方式^[9]。例如,在医院里,医生这个角色可以开处方,但他无权将开处方的权力传给护士。

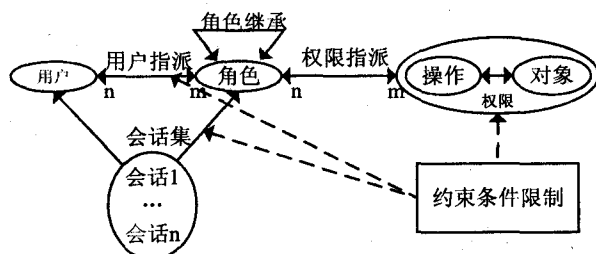


图1 基于角色访问控制框架模型

RBAC 的最大优点在于它能够灵活表达和实现组织的安全政策,使管理员从访问控制底层的具体实现机制中脱离出来,十分接近日常的组织管理规则。该模型解决了具有大量用户、数据客体和各种访问权限的系统中的授权管理问题,有效地克服了传统访问控制技术存在的不足,为管理员提供一个比较好的安全策略实现^[10]。基于角色访问控制模型的一个重要属性就是 RBAC 自身是中立于策略的^[11],所以各种不同的系统都可以根据自身的需要来调整策略,运用到实际的问题当中。

2 医院信息系统中权限管理的设计

2.1 权限管理的应用模型分析

文中结合 B/S 模式的医院信息系统的特点,以 RBAC 基本思想为基本模型,设计了一个符合医院实际需求的应用模型。运用 RBAC 模型来设计访问控制系统,主要的问题是研究用户、角色、权限管理以及它们之间的关系。

2.1.1 用户管理

从医院的安全管理角度出发,系统的所有用户必须为能合法使用信息系统的员工,包括系统管理员和普通用户,系统管理员可以添加、修改和删除用户,还可以对普通用户的角色和权限进行分配。普通用户则只能在系统管理员的授权下才能进行相关的业务操作。

2.1.2 角色管理

角色管理主要是对于角色的添加、修改和删除操作,并负责给用户分配相应的角色以及给角色赋予相应的权限等。文中在实现系统访问控制模块时定义了系统挂号员、管理员、收费员、医生、护士等角色,且每个角色拥有的权限都是由系统事先进行约定,该模块还提供了相应的用户界面接口,管理员可以根据实际的需求来对各个用户进行角色和权限的分配及授予操作。

2.1.3 权限管理

权限管理则应保证授权过程中遵循最小特权原

则,即分配给用户的权限不应超过用户实际使用中完成工作所必需的权限^[12]。在该系统中,用户的权限分配是通过用户菜单来表示的,即为某一用户登录系统后,ASP 页面中显示的全部菜单项,这些菜单项转向的链接就是用户可以访问和操作的页面,也就是该用户的权限。在权限管理中操作对象即为系统的功能结构,当某个用户拥有对某个资源的可见权,则该系统将会为此用户链接此资源,反之,若资源对于该用户是不可见的,那么该用户也就没有相应权限的具体操作。

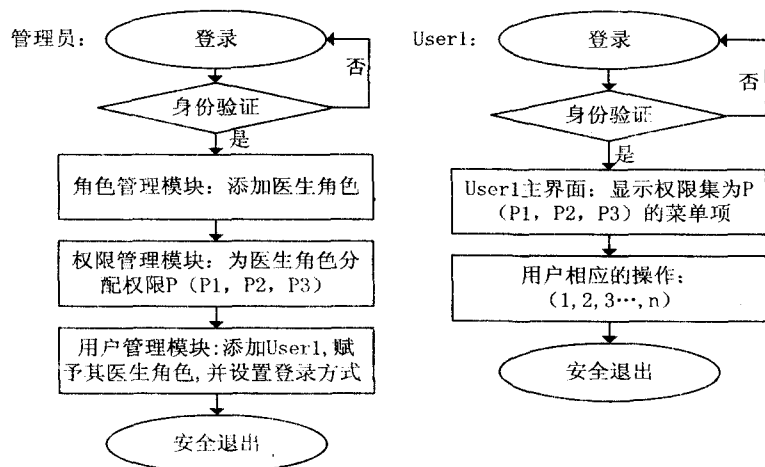


图2 权限管理应用模型的分析流程图

对该应用模型在医院管理中的具体分析过程可以以医生角色为例加以说明,如图2所示:首先,管理员登录系统后,在角色管理模块中为系统添加一个医生的角色;然后,在权限管理模块中选择医生的角色,对其进行权限的分配;最后,通过用户管理模块为系统新增一个普通用户,将医生这一角色分配给该用户并设置其可选的登录部门和单位;当该用户登录系统时,经身份认证成功,则进入到该用户的操作主界面,这时用户只拥有医生这个角色所拥有的权限菜单,其他的都对其不可见,从而避免了用户的越权操作。

2.2 权限管理的数据库设计

系统的动态权限管理是以数据库为基础的,为了实现基于角色的访问控制的授权思想,共设计了以下5张表:

(1) 用户表(User)。

本医院信息系统的用户表中保存了该系统所有用户的信息,系统管理员可以按照需要增加相应的用户。

(2) 角色表(Role)。

角色表中存储了系统所有的角色,角色按照部门单位和系统结构进行划分,由系统管理员(Admin)在角色管理功能模块当中录入。

(3) 权限表(Permission)。

本系统的权限表中储存了系统用户的所有权限,这些权限都对应于页面的相应菜单项目,根据指定的URL可以跳转到相应的页面。

(4) 用户-角色表(User-Role)。

用户-角色表记录了用户拥有的所有角色。当用户被赋予了某一种角色,则它就拥有了该角色所具有的全部权限。当分配给某一角色什么权限,被指派了这一角色的用户就会拥有相应的权限。

(5) 角色-权限表(Role-Permission)。

角色-权限表为角色添加具体的权限,角色和权限之间构成多对多的关系,通过该表建立动态的对应关系。

通过用户-角色表和角色-权限表就可以方便、灵活地建立用户和权限之间的对应关系,如图3所示。

3 医院信息系统中权限管理的实现

该医院信息系统的权限管理是基于B/S模型结构进行设计的,应用服务器层采用C#语言,Web服务器层服务器采用IIS6.0,数据库采用SQL Server 2000,并以Visual Studio 2005作为开发环境。

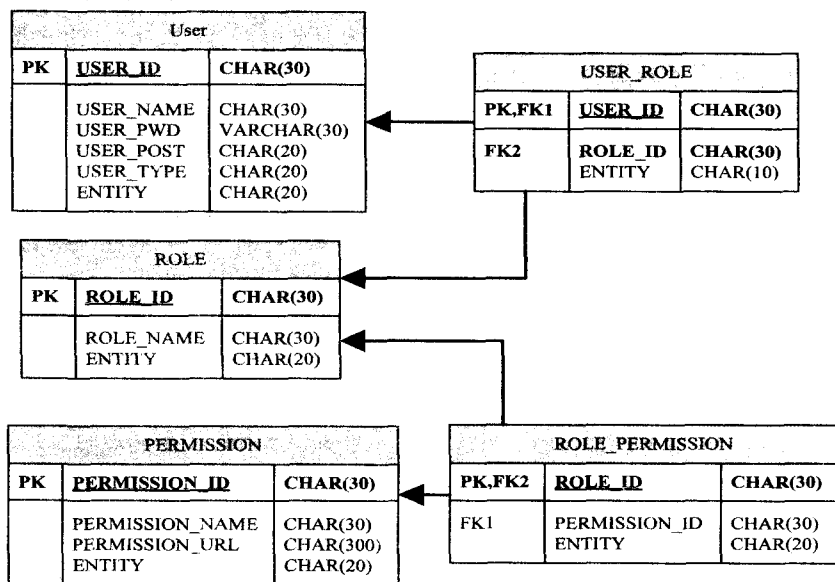


图3 权限管理中各表的关系图

当用户登录系统时,系统通过保存在session中的用户ID查询用户表,进行比较,再根据用户ID确定对应的角色ID,然后通过角色ID查找到与之对应的全

部权限名称,最后再和菜单表中的所有菜单项进行比较,找到所对应的菜单选项,这些菜单项对应的 URL 地址即为用户可以访问到的页面,这些菜单项中 URL 指向的所有页面就是该用户的权限。此时,比较中未对应的菜单选项则对该用户不可见,所以任何用户都不可能访问该用户菜单以外的内容。

为了保证其他用户的正常访问,基于安全性考虑,在程序设计过程中将 session-timeout 的值设置为 15 分钟,系统对于超过 15 分钟未进行任何操作的用户,会自动注销其登录状态,当用户再次进行操作时,系统会自动跳回到登录界面,用户必须重新登录。

整个权限控制流程如图 4 所示。

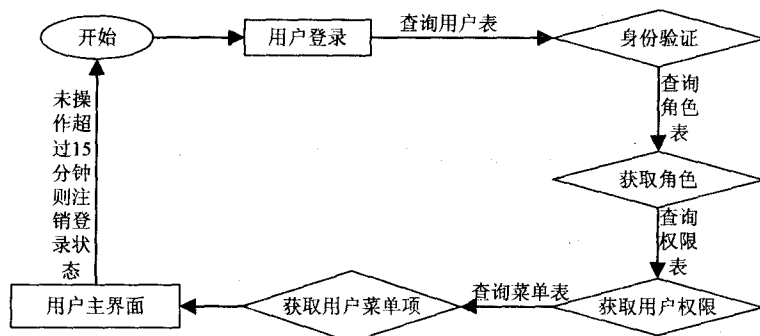


图 4 用户权限控制流程图

当用户登录系统时,身份验证成功后,就进入访问控制流程中,系统通过将在数据表中获得的用户 ID 最终找到对应的全部权限后,再将这些权限与保存在 Application 中的所有 MenuData 进行比较,若一致则将其显示在用户界面的菜单中,以此方法得到该用户的权限。访问控制模块的所有功能可以封装在一个独立的动态库中,访问控制模块主要包括 4 个类:身份认证类、数据库操作类、RBAC 访问控制管理类、角色管理类。下面给出了用户访问控制过程的主要实现代码:

```

操作员 ← Session["操作员"]
SqlText ← "select url ,mc, bh ,jb, bhsj from menu"
执行 SqlText 数据库查询语句, 获得菜单列表
MenuData[1...]

SqlText ← "select * from jsmx"
执行 SqlText 数据库查询语句, 获得角色菜单列表
RoleMenuData[1...]

for i ← 0 to length[ MenuData ]-1
    if( 操作员. 名称 == "admin" ) then
        do 显示输出 MenuData[i]. 名称、MenuData[i]. URL
    continue

for j ← 0 to length[ RoleMenuData ]-1
    if( 操作员. 角色编号 == RoleMenuData[j]. 角色编号 and MenuData[i]. 菜单编号 == Role-
```

```
MenuData[j]. 菜单编号) then
```

```
do 显示输出 MenuData[i]. 名称、Menu-
Data[i]. URL
```

```
continue
```

4 结束语

在医院信息系统开发中,加入角色权限管理模块,保障了系统操作的安全性,且具有较大的灵活性,实现了权限的协调转换,降低了权限管理和系统维护的复杂性。RBAC 模型的权限管理思想符合医院信息系统的应用要求,并能很好地适应医院信息系统的安全策略,且便于控制,是一种非常重要的安全保障措施。在实际应用过程中,能保证医院管理和患者信息的安全,具有重要的应用价值。

参考文献:

- [1] 林 磊, 骆建彬, 邓 宪. 管理信息系统中基于角色的权限控制[J]. 计算机应用研究, 2002, 20(6): 82-84.
- [2] Sandhu R S, Coyne E J, Feinstein H L, et al. Role-based Access Control Models[J]. IEEE Computer, 1996, 29(2): 38-47.
- [3] 李建东, 张 铁, 王中文, 等. 角色访问控制技术在放射治疗中的应用[J]. 计算机工程, 2008, 34(10): 269-270.
- [4] 戴祝英, 左永兴. 基于角色的访问控制模型分析与系统实现[J]. 计算机应用研究, 2004(9): 173-175.
- [5] 刘宏波, 罗 锐, 王永斌. 一种采用 RBAC 模型的权限体系设计[J]. 计算机技术与发展, 2009, 19(9): 154-156.
- [6] 古同路, 潘跃建, 王立松. 基于 RBAC 模型实现电子政务系统业务的柔性处理[J]. 计算机技术与发展, 2010, 20(2): 52-55.
- [7] 周锦程, 张佳强, 冷文浩. 可扩展系统中基于 RBAC 模型的访问控制[J]. 计算机工程, 2009, 35(14): 145-147.
- [8] 姜宇锋, 付 钰, 吴晓平. 基于 RBAC 的权限系统设计与实现[J]. 计算机与数字工程, 2009, 236(6): 98-101.
- [9] Sandhu R S, Bhamidipati V, Munawer Q. The ARBAC97 Model for Role-based Administration of Roles[J]. ACM Transactions on Information and System Security, 1999, 2(1): 105-135.
- [10] 王 月, 高虎明. 扩展式基于角色的访问控制模型的研究[J]. 计算机工程与设计, 2008, 29(2): 309-311.
- [11] Ferraioli D, Sandhu R S, Gavrila S, et al. Proposed NIST Standard for Role-based Access Control[J]. ACM Transactions Information System Security, 2001, 4(3): 224-274.
- [12] 杨官平, 陈鸿伟, 李永华. B/S 模式的电厂耗差分析系统权限管理的实现[J]. 计算机工程与设计, 2006, 27(3): 497-499.