文章编号:1671-4598(2020)08-0223-05 DOI:10.16526/j.cnki.11—4762/tp.2020.08.045 中图分类号:TP309.2 文献标识码:A

基于 RBAC 权限模型实现医院计算机信息管理的研究

董向文
(广西中医药大学 第一附属医院，广西 钟山 530023)

摘要：针对当前医院计算机信息管理系统遇到的安全性问题，将 RBAC（基于角色访问控制）基本思想融入了医院信息系统管理，有效地减少授权管理的复杂性；在文章设计的系统设计中，通过创建角色集合，能够有效地减少系统开销，进一步简化角色权限管理；该系统还对设计的数据库进行优化，能够使管理者根据设计目标和需求，在用户和角色之间、角色和权限之间构造一定的关联性，进而实现医院计算机信息管理系统的功能，减少其繁琐的应用步骤，进而满足健全医院计算机信息系统的需要；将角色权限访问模型应用到管理系统中，能够对医院用户进行角色分配，当用户被分配到适合的角色时，直接获得该角色本身拥有配套的权限，完成用户角色激活后，对各功能模型进行相应的操作，提高了安全性；实验表明，该方法比传统方法具有较高的数据管理能力。

关键词：基于角色访问控制；授权管理；计算机信息管理系统；角色权限访问；数据管理；数据库

Research on Hospital Computer Information Management Based on RBAC Authorization Model

Dong Xiangwen
(First Affiliated Hospital, Guangxi University of Traditional Chinese Medicine, Zhongshan 530023, China)

Abstract: Aiming at the security problems encountered by the current hospital computer information management system, Incorporate the basic idea of RBAC (role based access control) into the management of hospital information systems, effectively reducing the complexity of authorization management. In this system design, by creating a role set, the system overhead can be effectively reduced and the role authority management can be further simplified. This system also optimizes the designed database, which enables managers to construct a certain relationship between users and roles, roles and permissions according to the design goals and requirements, thereby realizing the functions of the hospital computer information management system and reducing its cumbersome application steps to meet the needs of a sound hospital computer information system. Applying the role permission access model to the management system can assign roles to hospital users. When a user is assigned to a suitable role, the role directly has the corresponding permissions. After the user role activation is completed, each function model is performed. Corresponding operation improves safety. Experiments show that this method has higher data management ability than traditional methods.

Keywords: RBAC; authorization management; computer information management system; role access; authorization management; data management; database

0 引言

随着现代的计算机技术不断升级，医院管理信息化程度越来越高，医院的管理信息类型繁多，需要耗费大量的时间进行处理，工作效率低。医院的信息管理不仅包括医生及患者信息、病案、医院设施、物资、人事、财务、药房及药物价格，还包括其他部门的信息交互，及时地了解相关的信息变动。目前，医院计算机信息管理系统面临最大的难题是信息安全保障[1-4]，为了解决问题，本文通过 RBAC 权限模型对医院计算机信息进行有效的管理[5-8]。

收稿日期:2020-01-03； **修回日期**:2020-02-16。
基金项目:广西省省级科技项目(050700KK52170236)。
作者简介:董向文(1977-)，男，广西钟山县人，大学本科，工程师，主要从事计算机管理与应用方向的研究。

1 RBAC 技术

随着我国的发展，各行各业的数据不断信息化，每个角色都有自己的数据库，任何角色都无权获取不属于自己的数据库相关的信息，而 RBAC 技术正是为了这个而提出的。RBAC 技术在各行业信息管理平台中比较广泛的应用，扩展性强[9]，RBAC 模型如图 1 所示，其主要思想如下：

首先创建角色集合，放在权限集合与用户集合中间，角色本身拥有配套的访问权限，具体用户不需要被直接授予系统中的访问权限，只需要被安排到合适的角色即可。在信息管理中，只需要角色授权信息，即可得到配套的访问权限，减少系统开销，简化角色权限管理[10]。

如图 1 所示，RBAC 模型由角色、用户、会话、权限构成。一个角色可分配到多个用户，同理，一个用户也可被赋予多个角色，角色与权限也同样如此。角色本身具有

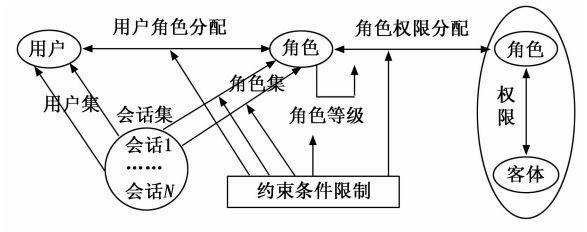

图 1 RBAC 模型

配套的权限，首先创建一个会话，在该会话中，当角色被分配到用户时，该用户自动获得相应的所有权限。

通过 RBAC 技术，使管理系统的工作效率提高，使用户授予权限的过程节省了不少的时间，有助于减少系统开销，提高安全性[11-12]。下面描述内容是 RBAC 技术的优势：

1）该技术给用户赋予了本身拥有配套权限的角色，以便降低了开销，提高了灵活性和管理效率，大大节省了管理技术复杂的用户角色占据的空间。

2）职责分离，比如，为了提高安全性，防止发生欺骗现象，在支付平台中通过该技术将实际付款和授权付款分开进行，减少经济损失。

3）最小权限原则，为了避免有些用户利用职权进行滥用行为，利用技术给每个用户分配到该角色本身拥有的权利，该权利只能在自己工作范围内履行，不能超过角色本身权限范围，超出范围外的权利视为无效。

2 医院计算机信息管理系统

2.1 整体平台模块设计

随着科学技术发展，医院信息管理系统的权限体制越来越精细，增强了权限管理灵活性。医院信息管理系统设计思想是“谁拥有权利，职责是什么、应该做什么”，权限系统主要实现整体控制，业务逻辑主要实现局部控制。例如，在某个业务里，A 医生拥有删除本身创建的病历信息的权限，同时，拥有 A 医生角色权限的 B 医生只能修改 A 医生创建的病历信息，其他医生只能查看病历信息的权限，这就需要通过业务逻辑来实现这一要求。权限系统的主要问题是给医生赋予什么样的角色，同样角色本身自带配套的权限，同时利用业务逻辑根据独特权限要求通过编码实现其他的权限，建立健全的权限体系。

基于上述主要思想，现在设计出如图 2 所示的功能模块图，在该功能模块图中，将医院计算机信息管理平台划分为若干平台，比如，该模块分为界面客户端平台、网站查询平台、后台管理平台、手机客户端平台等[13-15]。为了论述的需要，将上述模块作为主要的平台进行论述。界面客户端平台主要通过主机进行访问不同应用功能，比如用户注册及登录。网站查询平台主要通过网站对应用功能进行访问。手机客户端平台通过手机进行访问医院信息。后台管理平台主要管理和维护医院计算机信息系统运行，以保障系统安全性。

通过上述模块设计，能够在医院计算机信息管理平台上实现界面登录、预约挂号、就诊呼叫、病例查询等功能。

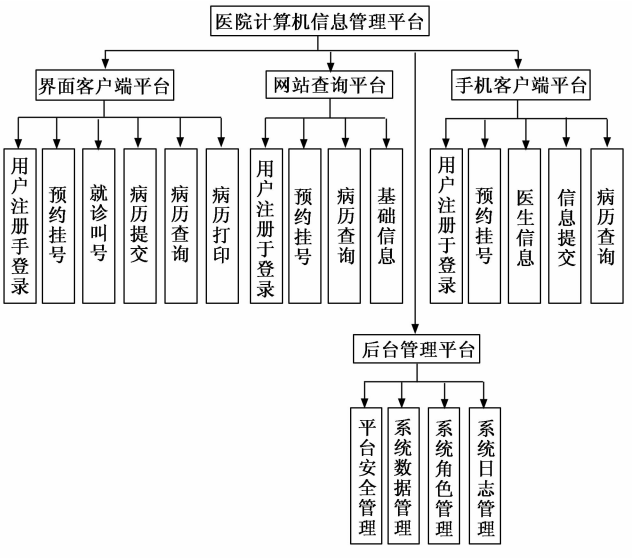

图 2 功能模块设计

用户还可以在后台管理平台实现各项功能的应用[16-17]，比如平台安全管理、系统数据管理、系统角色管理和系统日志管理等。在引入 RBAC 技术后，需要对数据库进行设计，下文将详细介绍。

2.2 数据库设计

下面对数据库进行重点说明，为了防止医院隐私信息泄露、外界非法入侵，在医院管理系统中引入了 RBAC 技术。首先设计数据库，对数据表进行定义[18-19]。在数据库中：

1）hx_user：表示用户表，其负责保存用户基本资料，包括 username，name，sex，department，id，position 和 userpass 等字段。

2）hx_department：表示部门表，负责保存部门基本资料，包括 id 和 department 字段。

3）hx_postion：表示职位表，负责保存职位数据，包含 id 和 postion 字段。

4）hx_node：表示权限表，负责保存权限基本资料，包含 id，name，moname，mname，aname 和 status 等字段。

5）hx_role：表示角色表，保存角色基本资料，包含 id，name，status 和 remark 等字段。

6）hx_tem_role：表示角色更新表，负责保存角色权限资料更新的列表，包含 id，name，status、remark 和 node 等字段。

7）hx_role_node：表示角色权限表，负责保存权限和角色的地址位置表，包含 rid 和 nid 字段。

8）hx_user_role：表示用户角色表：负责保存用户和角色的地址位置表，包含 rid 和 uid 字段。

9）hx_check：表示申报表，负责保存用户申报数据，包含 id，username，name，title 和 fankui 等字段。

10）hx_duty：表示员工值班表，负责保存员工值班基本数据，包含 id，username，name，department 和 time 等字段。

11）hx_book：表示公告表，负责保存公告基本资料，包含 id，title 和 replytime 等字段。

RBAC（role－based access control，对角色的访问控制），在数据库中，能够将角色与权限关联起来。简而言之，能够使一种用户拥有多个角色，各个角色拥有不同的权限。充分利用“用户－角色－权限”这种关联形式构建的授权模型[20-21]，进行进一步的计算其间的关联性，通过利用这种数据模型，使管理者在用户和角色之间、角色和权限之间根据设计目标和需求设计，进行操作计算机系统的各个需求功能。最后，结合医院需求和文化，对平台界面风格、配色、结构进行设计，创建出相关的网页。

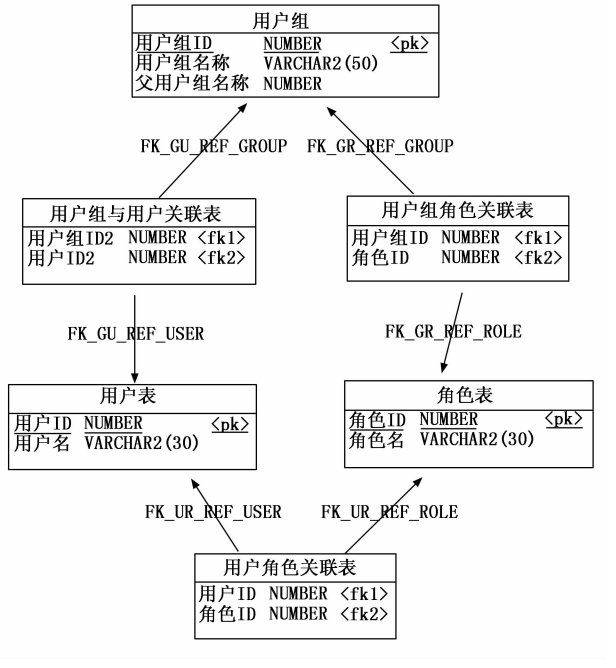

图 3　数据库功能模块示意图

在具体应用中，可以对各种数据模块进行分类，其分类的模式如图 4 所示。

在上述数据库中，充分利用了各种权限的作用，其中将“MENU”能够表示为对菜单的访问权限设置，将“OPERATION”表示为数据库中的功能模块的操作权限，而将“FILE”表示为文件的修改权限，将“ELEMENT”表示为页面元素中的可见性控制等[22-23]。

2.3　权限控制的业务逻辑

在对权限的功能模块进行了设计之后，控制的业务逻辑也是尤其重要。能否操作系统功能的模块决定了用户拥有的权限。只要用户拥有权限，不论访问的客体是否有资源，都可以进入系统操作对应的功能模块。利用非浸入式编程（aspect oriented programming，AOP）方法来隔离控制逻辑与业务，并在 Apache Shiro 安全框架中实现访问模型。通过 HashSet 对用户与角色本身拥有配套的权限进行授权，并在 Shiro 带来的 Realm 的 doGetAuthorizationInfo[24-25]中实现访问权限。

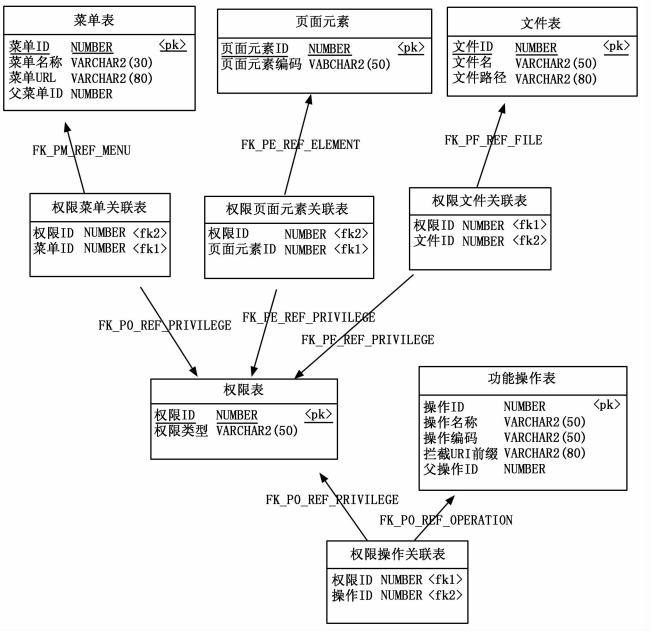

图 4　数据库分类结构示意图

为了对通用权限管理进行实现，本研究利用 AOP 编程方法对业务逻辑与权限判断进行分离。当用户访问时对用户的权限进行判断，必然会接触到访问的数据。我们可以在编程过程中添加约束条件集合语句，增加一些逻辑判断，以便在获取数据时，控制无权访问的数据。为了避免遭到外界入侵，在管理模块中只显示操作失败和空的结果，而不会出现操作越界的提示信息，具体实现方式如下：

1）为了查询数据库，对检索接口定义，设置额外检索参数，对用户、用户集对应的属性读写方式进行实现。

2）对权限和权限集对应的属性进行注解和标注。

3）利用 2）注解方法定义切面类。

4）为了增加一些约束条件，根据用户拥有的权限对用户、用户集对应的属性进行设置，以便在切面类中实现环绕通知。

下面的代码是业务逻辑与权限的分离过程：

```
List of masses Define MenusByCode
{
Back to ZhuMenu. Define MenusByCode;
}
Void AssignMenus of masses To Deptment Define string deptcode
{
AssignMenusToDept and ZhuMenu Define menuCodes, deptcode;
}
```

将 groupSet、groupId、userId 定义为类属性的实现代码，这些代码具备读写功能，检索数据接口的代码为 ResourceSearchMessage，实现业务层服务的注解为@ResourcePermission。如何判断检索到的参数（如 groupSet、groupId、userId），可通过实现环绕的切面方法，Resour-

cePermissionAspect 定义为切面类。定义 pGroupSet 为权限的组合集，由于医院部门类型繁多，各部门之间即联系又独立，可用 4 位编码来表示 groupSet、groupId、userId。如表 1 所示，O 代表存在，－代表不存在，组合集是否包含 groupId，可通过 Yes 或 No 来表示，比如 groupSet 非空且 groupID 非空时，根据 userId 情况显示的是 Yes 或者 No。为了防止没必要的连接或条件占据空间，在 Mybatis 动态 SQL 内可建立一个空的检索属性。

表 1 编码定义对应表

码值	userId	groupId	GroupSet	pGroupSet
0	—	—	—	—
1	非用户 ID	O	O	有值但不存在根组
2	用户 ID			存在根组

2.4 系统安全访问流程

用户在利用 RBAC 技术时，不仅仅能够防止医院的机密资料向外泄露，保护个人隐私，还能够大大节约用户的工作效率。其中 RBAC 权限访问模型工作原理如下：当对系统用户进行角色分配时，能够自动获得该角色相应的权限。用户一般指的是护士、护士长、医生、部门主任、院长等角色，每个角色都有自己配套的权限。如图 5 所示，RBAC 权限访问模型工作流程如下：

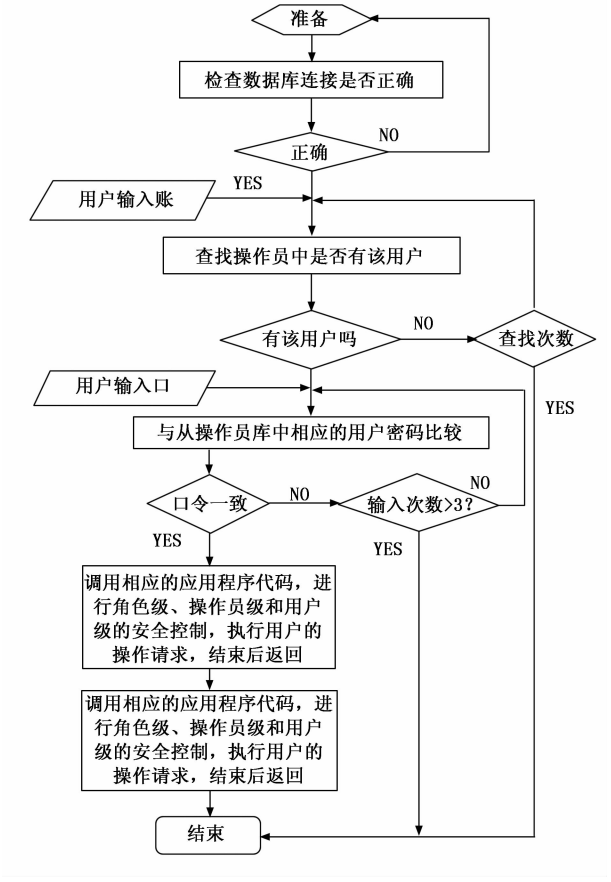

图 5 访问流程设计

1）用户注册时，对用户名进行定义，输入登录密码，完善个人资料，即完成注册。当用户在系统登录时，需要输入用户名及密码，将会通过验证方式进行验证，若通过验证，即将进入系统里面，反之将回到登录界面上。

2）完成登录后，用户在系统中被会话管理模块检索出角色信息，用户即将被安排到适合的角色。

3）用户被分配到角色后，为该用户新建会话窗口。

4）创建新会话窗口后，用户将得到该角色拥有配套的权限，即可操作相应功能模块。

5）管理人员需要等会话结束后，才能进行修改用户拥有的权限。

数据访问层设计代码如下：

```
//角色权限的获取过程//
List of masses Define MenusByCode
{
new List<string>() = List<string> menus;

"@code =select * Department code is defined as department menu" = string sql ;
SqlDataProvider = DataSet ds Define ResultBySql(CreateSqlParameter, SqlDataP－rovider, sql (code, VarChar, SqlDbType, "@ code"));
Array (Rows. Tables[0]. Data Row dr in ds)
{ Add(ToString. Func). menus
}
return menus;
}
/ /角色被分配到权限名称//
Void AssignMenus of masses To Deptment Define string deptcode
{
"@ deptcode =Remove deptcode from the b? " =Dept? Menu;
" Insert bs dept menu(menu－code, deptcode) values(@ menucode ,@ deptcode) " = string sql_ins;
ExecuteBySql. SqlDataProvider(CreateSqlParameter. SqlDataProvider. sql _ del (" dept－code, VarChar, SqlDbType, @ deptcode"))
Array (string mc in menuCodes)
{
ExecuteBySql. SqlDataProvider (CreateSqlParameter, SqlDataProvider, sql _ ins(dept－code, VarChar, SqlDbType, @ deptcode), CreateSqlParameter, SqlDataProvider(mc, VarChar, SqlDb－Type, "@ menucode")) ;
}
}
```

3 实验与效果分析

为了判断系统的有效性，本文对系统进行测试，下面利用读取方式对获取访问数据进行分析。在试验时，选择的操作系统为 Microsoft Windows 2010，64 位。主要开发工具为 Visual Studio 2015，OpenCV 3. 0。运行环境硬件参数为 CPU：inter （R） Core （TM） i7；主频为 2.

59GHz；内存 8G。在试验时，首先登录软件界面，其界面如图 6 所示，用户完成注册后，可在医院信息系统中输入用户名和密码后，完成登录。

图 6　用户登录界面图

在完成登录之后，如图 7 所示，当用户需要预约挂号，选择预约功能模块，直接进入预约管理系统，选择医院、挂号、时间和医生，完成预约挂号。

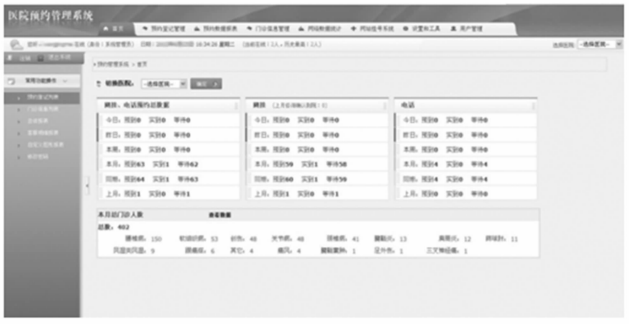

图 7　预约挂号管理系统图

然后调取数据库集中的数据，对数据进行计算。假设将 U 代表测试数据的集合，该数据集合包括数据源和数据访问记录。数据源有 A、B、C、D、E 五个子源，数据可由 a、b、c、d 四个表示，它们的分布关系如图 8 所示。A 子源包含 a 和 c 两个数据，B 子源包含 b 和 c 两个数据，C 子源仅包含 c 个数据，D 子源仅包含 d 个数据，E 为空集。

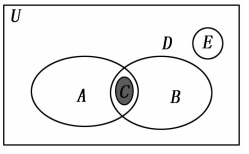

图 8　数据源分布关系

根据分布关系对用户的角色权限进行划分，有 A，B，C，D，E 五个读取权限。角色权限的分配结果如表 2 所示，○ 代表该存在拥有配套权限的用户，╳代表该存在不拥有权限的用户，—（空白）代表不存在该用户。ID 表示不同类型的用户，根据全部数据、A 子源数据，B 子源数据。

根据上述测试，为了试验本系统的管理能力，与传统医院计算机管理系统比较，对系统管理能力的实验效果进行分析，如图 9 所示。

实验结果可知，在相同环境中处理相同的数据情况下，与传统系统相比，基于 RBAC 权限模型的医院计算机信息管理系统的管理能力较高，大大减少系统开销。

表 2　测试结果

ID	U	A	B	C	D	E	全部查询	A 查询	B 查询
0	○	—	—	—	—	—	全集	{a,c}	{b,c}
1	╳	—	—	—	—	—	无权限	无权限	无权限
2	—	○	○	—	—	—	{a,b,c}	{a,c}	{b,c}
3	—	○	╳	—	—	—	{a,c}	{a,c}	{}
4	—	╳	╳	—	—	—	无权限	无权限	无权限
5	—	—	—	○	—	—	{c}	{}	{}
6	—	—	—	╳	—	—	无权限	无权限	无权限
7	—	—	—	—	○	—	{d}	{}	{}
8	—	—	—	—	—	○	{}	{}	{}

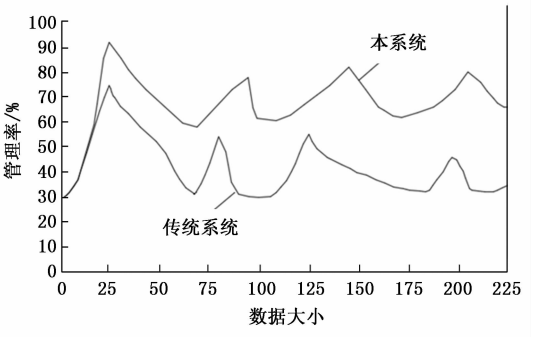

图 9　仿真结果对比图

4　结束语

在医院中的各种设施、人资、物资、财务、药房及药物价格等信息中，融合了各种信息。本文 RBAC 模型利用角色建立用户与权限之间的关系，使得用户能够在用户数据和访问权限数据之间实现数据分离，不仅能够减少数据授权管理的复杂性，还能够降低医院日常运营的成本开销。通过角色权限访问技术，根据职位和级别，将用户分配到适合的角色，使得用户获得该角色本身拥有配套的权限，对相应的功能模块进行操作，实现预约挂号、病历查询等功能，提高了安全性。基于 RBAC 模型的权限管理观念在医院信息系统中能够得到很好的应用，为后期在医院管理和患者信息安全方面提供重要的价值参考。

参考文献：

[1] 信　科，杨　峰，杨光旭，等. 基于 RBAC 权限管理系统的优化设计与实现 [J]. 计算机技术与发展，2011（7）：172－174.

[2] 刘晓玲，郭　龙. 基于 RBAC 的用户权限管理的研究与实现 [J]. 电脑知识与技术，2013（7）：1487－1490.

[3] 岳　兵. 基于 RBAC 的用户权限数据模型在信息系统的研究与设计 [J]. 医学信息，2015，28（7）：3－4.

[4] Chadwick D W，Otenko A. The PERMIS X. 509 role based privilege management infrastructure [J]. Future generations computer systems：FGCS，2003，2（2）：2－52.

[5] 白晋国，胡泽明，孙红胜. 基于 RBAC 模型多级角色的 SQLite3 安全访问控制 [J]. 计算机系统应用，2015，24（5）：177－182.

（下转第 232 页）