扩展的 RBAC 模型在数据共享服务平台中的应用

袁文礼，陈平华，熊建斌
（广东工业大学 计算机学院，广东 广州 510006）

摘　要：针对数据共享服务平台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，首先，分析了传统的 RBAC（基于角色的访问控制）模型，然后，结合数据共享服务平台的实际需求，对典型的 RBAC 模型进行了扩展，经过扩展后的模型对角色和客体进行了抽象，增添了“特征”的概念，粗化了权限和角色的粒度，有效地减少了角色、权限的数量。此方案已经在数据共享服务平台中得到应用，结果表明这种扩展的 RBAC 模型不但有效地降低了授权管理的复杂度，而且让系统的维护和扩展变得更方便。最后给出了该模型在数据共享服务平台中的应用实例。

关键词：RBAC 模型；数据共享；权限控制；角色
中图分类号：TP39　　**文献标识码**：A　　**文章编号**：1673-629X(2012)08-0221-04

Application of Extended Role-based Access Control Model in Data Sharing Service Platform

YUAN Wen-li, CHEN Ping-hua, XIONG Jian-bin
(Computer College, Guangdong University of Technology, Guangzhou 510006, China)

Abstract: On the basis of analyzing the traditional RBAC (Role Based Access Control) model, with the actual demand of the data sharing service platform, extended RBAC model, in connection with the complexity of rights management and data security issues in actual operation of the data sharing service platform. Extended RBAC model abstracted the role and object, added a "feature" concept, coarsened the granularity of permissions and roles, these can effectively reduce the number of roles and privileges. This program has been applied in the data sharing service platform, the result shows that this model can effectively reduce the complexity of authorization management, and makes it convenient to be maintained and extended. Finally, the application example of this model in the data sharing service platform was given.

Key words: RBAC model; data sharing; access control; role

0 引　言

随着计算机技术的发展，政府和企业管理的信息化越来越普及，在不同时期根据不同需求建立了各种各样的应用系统。然而这些系统之间往往是互不相通的，数据缺乏共享，这样容易造成系统重复建设、资源浪费等一系列问题。如何低代价、方便地将企业内部或企业间异构数据进行交换，从而实现大范围的跨企业实体的商务应用系统的对接，这是当前互联网环境下每个企业发展所面临的一个大问题[1]。

面向科技部门的数据共享服务平台的建立就是为科技部门各项业务系统提供一个信息共享的平台，为跨部门的信息共享和信息交换提供服务，促进信息资源的开发利用[2]。由于其开放式和分布式的特点，系统对数据安全性的要求比较高，所以必须有效地解决系统的权限管理问题。基于角色的访问控制[3]（Role Based Access Control，RBAC）是目前应用较为广泛的一种访问控制技术，它利用角色来联系用户与权限，简化了各种环境下的权限管理。RBAC 经典模型降低了安全管理成本和管理的复杂性，解决了传统访问控制和自主访问控制管理难度大的问题[4]。随着 Web 系统的日益复杂化，传统的 RBAC 模型已不能满足实际应用的需要，迫切需要构建一种授权灵活、安全性能好、通用性好的访问机制[5]。

文中针对数据共享服务平台的特点，从两个不同

收稿日期：2012-12-16；**修回日期**：2012-03-21
基金项目：广东省自然科学基金资助项目（9151009001000021）；广东省教育部产学研合作专项资金资助项目（2009B090300341）；广东省中国科学院全面战略合作项目（2011B090300041）
作者简介：袁文礼（1984-），男，湖南邵阳人，硕士研究生，研究方向为计算机网络与分布式信息处理；陈平华，硕士生导师，教授，研究方向为计算机组成与体系结构、嵌入式系统、基于 Web 的分布式信息处理系统。

的方面对 RBAC 模型进行了改进和扩展，增强了系统权限维护的灵活性，降低了授权管理的复杂度，提高了系统管理的效率。

1 基于角色访问控制的 RBAC 模型

1.1 访问控制

访问控制是一种常用的资源保护手段，是安全技术的重要部分。通过限制对关键资源的访问，授予系统合法用户访问资源所必须的操作权限，防止非法用户的侵入或因为合法用户的不慎操作而造成的破坏。访问控制通常包括主体、客体和安全访问规则三个元素。当前比较流行的访问控制模型主要有三种：自主访问控制模型（Discretionary Access Contorl，DAC）、强制访问控制模型（Mandatory Access Contorl，MAC）和基于角色的访问控制模型（RBAC）。自主访问控制型允许资源的所有者自主地决定可存取其资源客体的主体，此模型的主要特点是授权灵活，缺点是权限可以传递，所以容易出现失控，从而引起信息泄露。强制访问控制是一种不允许主体干涉的访问控制类型，主体的权限和客体的安全属性都是固定的，由系统的安全管理员强制分配，授权方式不灵活，管理工作量大。基于角色的访问控制模型是一种可扩展的访问控制模型，也是目前公认的解决大型企业统一资源的访问控制的有效方法。

1.2 RBAC 模型

RBAC 模型的核心思想[6]是：在用户和权限之间引入了角色的概念，权限不再是直接赋予给用户，而是赋予给角色，再给用户赋予相应的角色，通过对角色的授权来控制用户对系统资源的访问。RBAC 模型的比较系统化的版本是基于 Sandhu 等工作提出的 RBAC96 模型[3]，RBAC96 模型框架中包含了四个层次的模型组成：RBAC0、RBAC1、RBAC2、RBAC3。

RBAC0 是基本的核心模型，由 5 个基本的元素组成：用户、角色、许可、客体、操作，此外还包括了会话和授权两个基本概念。RBAC1 和 RBAC2 都包含了 RBAC0，但两者之间并不存在包含和兼容的关系。区别是：RBAC1 模型是在 RBAC0 的基础上引入了角色间的继承关系，所以 RBAC1 也称作角色分级模型；而 RBAC2 模型是在 RBAC0 的基础上引入了约束的概念，它规定了权限被赋予角色时，或角色被赋予用户时，以及用户在某一时刻激活一个角色时所应遵循的强制性规则[7]，所以也称为角色限制模型。RBAC3 是由 RBAC1 和 RBAC2 复合而成，同时提供了角色分层结构和约束的概念[8]，所以被称为统一模型。这里给出 RBAC3 模型如图 1 所示。

2 扩展的 RBAC 模型

RBAC 模型是一种以主体为中心，对主体进行抽象，而对角色和客体的定义相对简单的一种访问控制技术[8]。由于对角色和客体并没有进行相应的抽象，这样就造成了只能根据具体的客体来制定权限，然后再依照相应的权限来设定角色，权限和角色的粒度太细，容易导致很大程度上的冗余[9]。针对这个问题，对传统的 RBAC 模型作出了相应的扩展和改进：一是增添了“特征”的概念，对角色和客体进行了相应的抽象，丰富了主体、角色和客体的语义表达。二是粗化权限和角色的粒度，把权限指定为按对象来划分的功能模块，即如果角色分配了该对象资源，它就同时拥有了该对象所具有的各种操作。

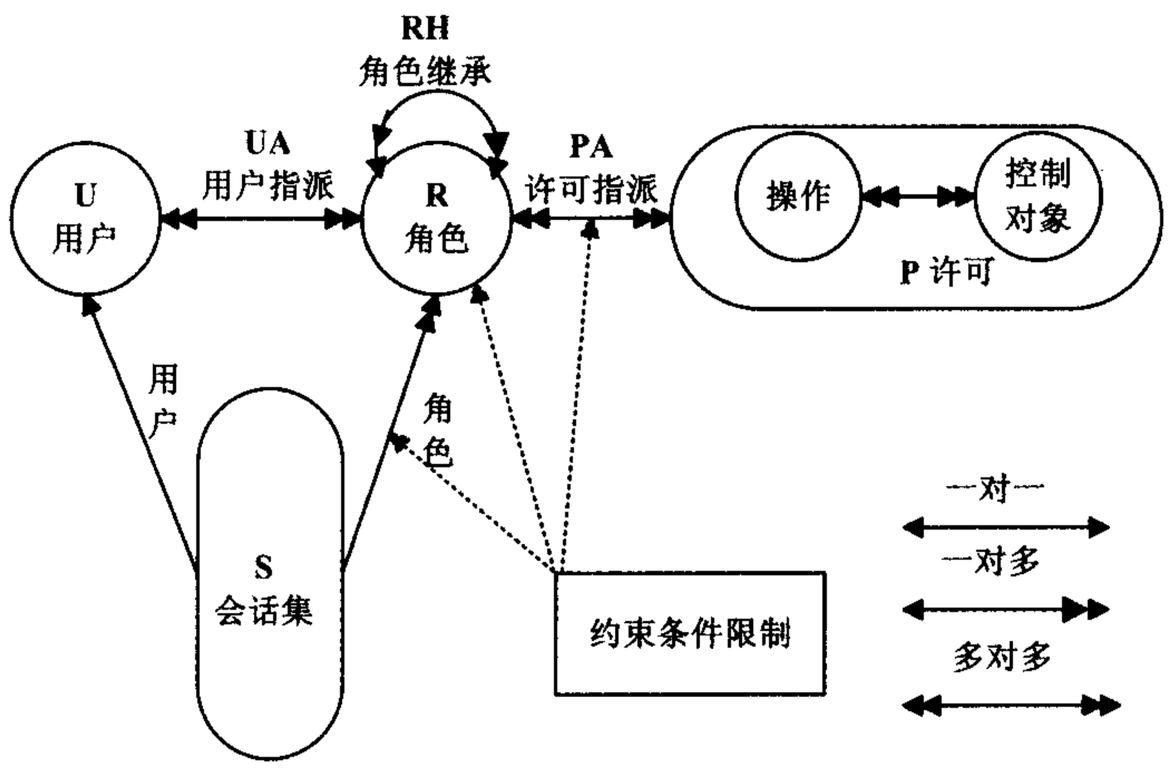

图 1 RBAC3 模型

对于第一点，在改进的 RBAC 模型中增加了特征这个属性，是以比传统的 RBAC 复杂为代价来大大减少角色和权限的数量，降低系统管理的复杂度。以数据共享服务平台为例，下属各个部门形成了一个典型的树形结构，按照传统的 RBAC 模型的，是以节点为单位来创建角色，然后再为各个角色设置相应的权限。然而这些角色和权限有的就仅仅只有部门不同而已，这样造成了角色和权限的极大冗余。表 1 和表 2 分别给出了服务审核这个权限在两个不同的 RBAC 模型下的设定。

表 1 传统的 RBAC 模型设定

用户	角色	权限
A 局审核员	A 局审核员	A 局服务审核
B 局审核员	B 局审核员	B 局服务审核
C 局审核员	C 局审核员	C 局服务审核

表 2 改进的 RBAC 模型设定

用户	角色	权限	特征（部门）
A 局审核员	审核员	服务审核	A 局
B 局审核员	审核员	服务审核	B 局
C 局审核员	审核员	服务审核	C 局

对于第二点，把系统资源按对象来划分成具有特

定功能的小模块,把这些功能小模块当做权限赋予给各个角色,如果角色分配了该对象资源,它就同时拥有了该对象所具有的各种操作。继续以共享服务平台下的服务审核权限为例,按照服务审核的整个流程设计出服务审核的功能模块,它具有查看、查询、审核、批量审核等相关功能,如果该用户具有审核员角色,则菜单栏里的审核功能模块就对其可见,而其能审核的范围就由其部门特征来决定。图 2 分别展现了传统的 RBAC 模型的权限集和改进后的 RBAC 模型权限集的情况。

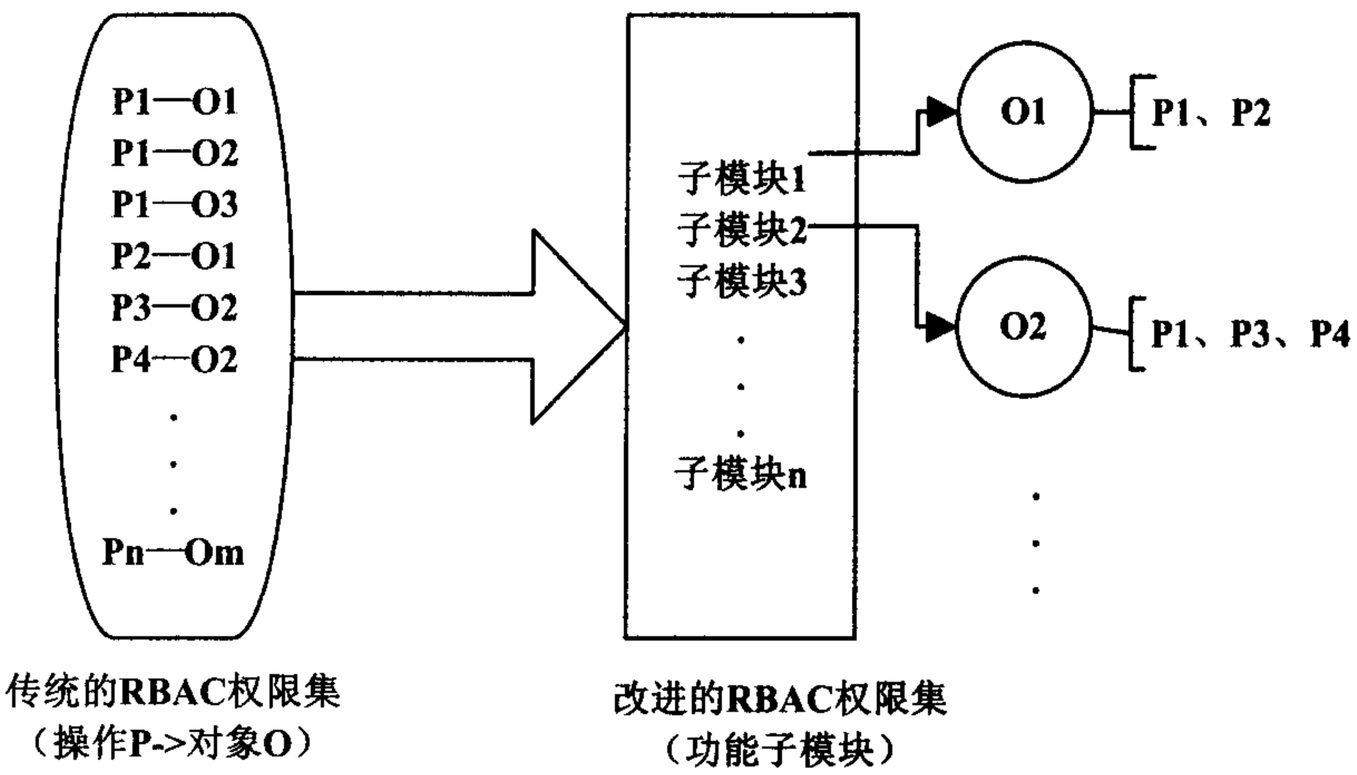

图 2　RBAC 模型的权限集

3　数据共享服务平台中权限管理的设计与实现

运用上述改进的 RBAC 模型来设计数据共享服务平台的访问控制系统,主要研究的问题是用户管理、角色管理、功能管理(权限管理)及三者之间关系[10]。

3.1　用户管理

数据共享服务平台的用户主要包括系统超级管理员、普通管理员和客户端普通用户。超级管理员管理对普通管理员和普通用户进行管理,普通管理员则可以根据超级管理员的授权,对其范围内的普通用户进行管理,普通用户就只能在其对应的管理员的授权之下才能进行相应的业务操作。

数据共享服务平台的用户管理主要由两个部分组成:一个是用户信息管理模块,负责对用户信息的查看,启用和禁用用户以及用户的增加、修改和删除等操作;一个是用户角色管理模块,负责给用户分配相应的角色。

3.2　角色管理

角色管理是对用户的所属角色信息进行管理。它也包括了两个子模块:一是角色管理模块,负责对角色信息的查看,启用和禁用角色以及角色的增加、修改和删除操作;一个是角色功能管理模块,负责对系统的角色进行功能绑定。

3.3　功能管理

功能管理是对系统功能信息进行管理,包括了查看、修改、删除和新增操作,以及启用和禁用功能。在本系统中,通过用户的功能菜单来实现对用户的权限分配,当某用户通过验证成功登录后,JSP 页面中显示的全部功能菜单即为该用户所拥有的权限。用户通过这些菜单链接到自己可以访问和操作的页面。

3.4　数据库设计

数据库设计是动态权限管理的基础[11],本系统设计了 5 张表来实现基于角色的访问控制:

(1)系统用户表(T_USER)。

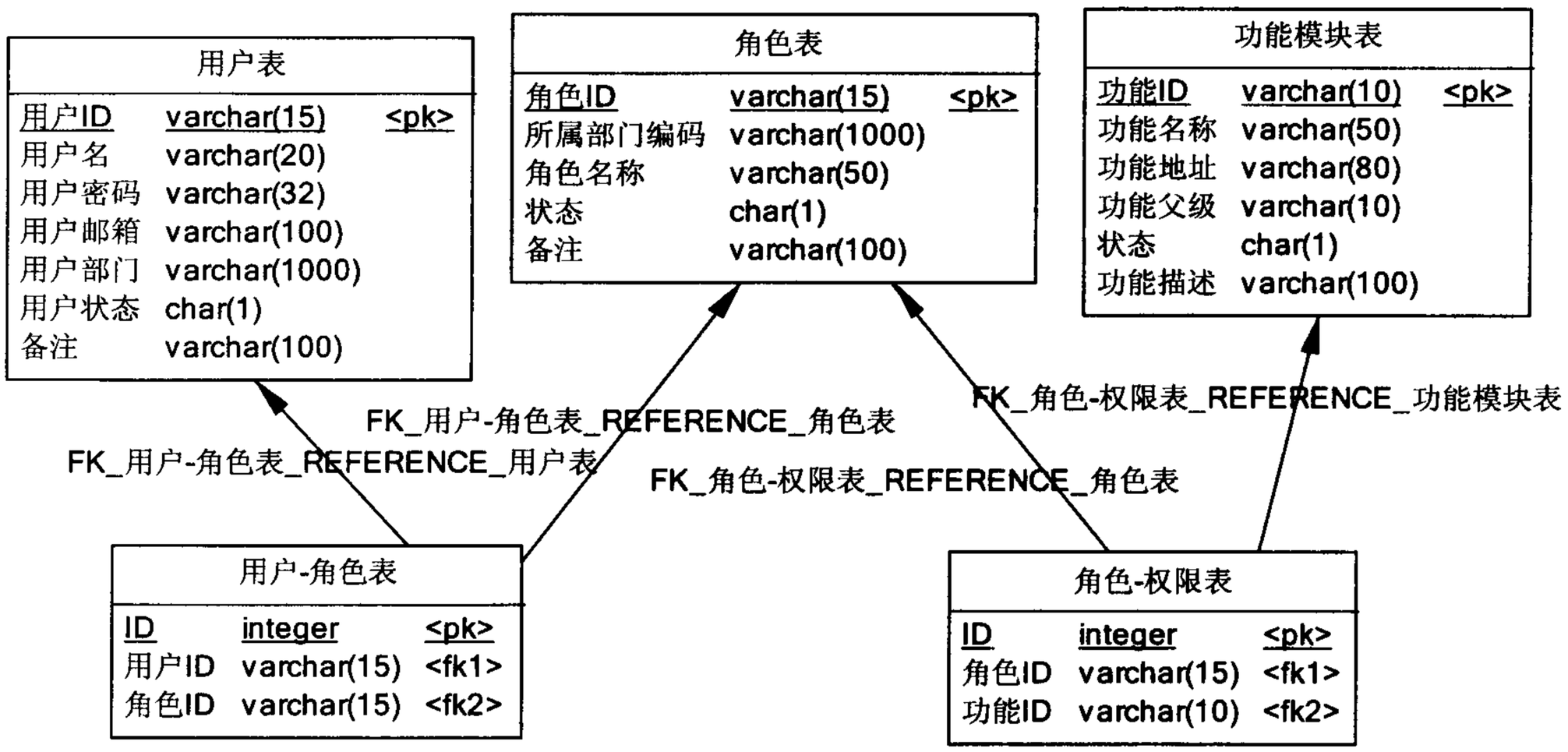

图 3　权限管理中各表的关系

存储该系统所有用户的基本信息、所属部门、登录信息等。

(2)系统角色表(T_ROLE)。

按部门存储该系统所有角色的基本信息。角色的录入和删除是由系统的角色管理模块来完成的。

(3)功能模块表(T_SYS_FUNCTION)。

该表存储了本系统的功能菜单上所拥有的所有功能的详细信息,包括功能名称、链接地址、父节点等。系统管理员可以通过功能管理模块来动态地新增、删除和修改功能。

(4)角色-权限表(T_ROLE_FUNCTION)。

存储角色所拥有的功能模块,通过该表使角色和功能建立动态的对应关系,这种对应关系是多对多的。

(5)用户-角色表(T_USER_ROLE)。

存储用户所拥有的角色,一个用户可以拥有多个角色。如果用户拥有某一角色,那么该用户就相应地拥有了这个角色所具有的所有功能模块。

通过用户-角色表和角色-权限表把系统用户表、系统角色表、功能模块表联系起来。各表的对应关系如图 3 所示。

3.5 实 现

数据共享服务平台采用 Java 作为开发语言,基于 SSH(Struts, Spring, Hibernate)框架下进行开发,以 Tomcat 为 Web 应用服务器,以 CXF 为 Webservice 服务器,以 ActiveMQ 为 JMS 服务器,采用 Oracle 10g 作为数据库,以 MyEclipse 作为开发环境。

数据共享服务平台的安全管理方式是结合 Spring Security 2.0 来实现的。Spring Security 是由一组 filter 来进行统一地过滤,不同的 filter 进行相应的权限过滤功能,通过配置 web.xml 和 applicationContext-security.xml 来整合 Spring Security。系统实现了的安全管理方式主要有:所有页面与数据均需要登录后才能访问;登录时需要验证验证码;登录时需要验证用户名和密码;登录后的所有系统的访问 URL 都需要授权;多个用户不能使用同一个账号同时登录等。

当用户登录系统时,输入用户名之后,系统通过 Ajax 查询数据库中得用户角色表,得到该用户所拥有的角色名称,并显示在登录页面上的用户角色输入框里,这样以便当用户具有多个角色时选择其中一个进行登录,如果系统无该用户,则角色输入框显示为空。当用户选择完角色之后,点击登录按钮,系统首先根据用户名称查询用户表进行用户的身份验证,验证成功之后,再根据用户的角色查询角色权限表,获取该用户所具有的全部功能,然后利用 Xtree 树形显示功能菜单到 JSP 页面中,功能菜单所对应的 URL 地址就是该用户具有访问权限的页面。该功能菜单既可以用来判定用户的操作权限,又可以作为系统过滤器用来过滤用户的 URL 请求[12]。流程图如图 4 所示。

用户访问控制过程中数据库访问的主要实现代码如下:

(1)获取用户所对应的角色列表:select ROLENAME, ROLE_ID from T_ROLE where ROLE_ID = (select F_ROLEID from T_USER_ROLE where USER_ID = (select USER_ID from T_USER where USERNAME = "+username+"))。

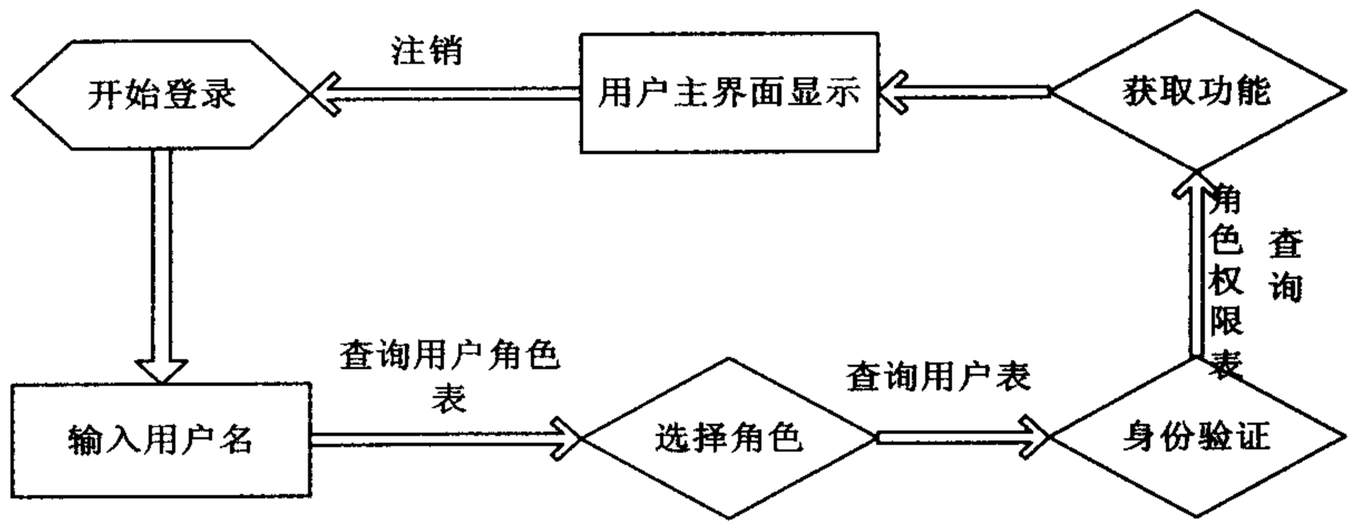

图 4 权限控制流程图

(2)查询用户进行验证:select USERPASSWORD from T_USER where USERNAME ="+username+"。

(3)根据用户登录时选择的角色名称获取用户的功能列表:select * from T_SYS_FUNCTION where FUNCTION_ID in (select distinct F_FUNCTION_ID from T_ROLE_FUNCTION where F_ROLE_ID = "+roleid +")。

4 结束语

文中结合数据共享服务平台中权限管理的实际需求,对传统的 RBAC 模型进行了扩展和改进,设计并实现了一个比较完善的权限管理子系统。该子系统引进了"特征"的概念,粗化了权限和角色的粒度,能够有效地保障系统的安全性,提高系统管理的效率。该方案是基于权限分配不是很细化的情况,可以应用于大部分的 Web 系统中,具有一定的可扩展性和可移植性,但对于细粒度的访问控制参照意义不是很大。

参考文献:

[1] 胡能发,唐为萍. 基于 XML 的通用异构数据交换模型[J]. 计算机工程与设计,2010,31(8):1743-1749.

[2] 林瑞锋,陈平华. 面向科技管理的数据共享平台关键技术研究[J]. 现代计算机,2009(9):104-105.

[3] Sandhu R S, Copne E J, Feinstein H L, et al. Role-based Ac-

(下转第 228 页)

```
Cbuffer = UIaddress&0x00ff;
Writedata( Cbuffer) ;
UIaddress>>=8;
Cbuffer = UIaddress&0x00ff;
Writedata( Cbuffer) ;//地址位先发
Writedata(0xe0) ;//高位控制位后发
ISDCS = 1;
    }
//////位控制码(11110)+11 位地址//////////////
voidPlay( unsigned int UIaddress) //PLAY 命令
{
unsigned char Cbuffer;
Cbuffer = UIaddress&0x00ff;
Writedata( Cbuffer) ;
UIaddress>>=8;
Cbuffer = UIaddress&0x00ff;
Writedata( Cbuffer) ;//地址位先发
Writedata(0xf0) ;//高位后发
ISDCS = 1;
    }
//////////音量增大//////////////
void Increase( )
{
DS1600CS = 0; //片选
Re_Delay(9) ;
DS1600UD = 1; ///U/D 置位
Re_Delay(9) ;
DS1600INC = 0;//INC 清零
Re_Delay(9) ;
DS1600INC = 1; //INC 置位
Re_Delay(9) ;
DS1600CS = 1;
}
```

4 结束语

本故障诊断系统利用传感器技术,将淋浴箱组工作过程中容易出现的故障及时反馈给控制器,控制器根据信号类型判断具体故障,及时切断自吸泵和锅炉并语音报警以提示工作人员及时维修,保证了锅炉安全、稳定、有效的正常工作。本系统经过反复调试和运行,达到了实际要求。

参考文献:

[1] 周 林,赵宗花. 锅炉常见故障处理办法[J]. 云南电力技术,2011(4):84-85.

[2] 史革盟. 锅炉监控系统的设计[J]. 现代制造技术与装备,2010(4):36-38.

[3] 盛水平,冯维君. 中小锅炉爆炸事故规律分析与研究[J]. 中国安全科学学报,2009(12):85-91.

[4] 郭奎建. 2007 全国特种事故及分析[J]. 中国特种设备安全,2008,24(4):51-53.

[5] 罗艾民,刘 骥. 锅炉 BLEVE 爆炸能量及其效应研究[J]. 中国安全生产科学技术,2006,2(5):29-32.

[6] 张兴容,马永慧. 我国工业锅炉的爆炸事故与预防对策研究[J]. 安全健康和环境,2003,3(1):9-11.

[7] Birk A M, Cunningham M H. Liquid temperature stratification and its effect on BLEVE and their hazards[J]. Journal of Hazardous Materials, 1996, 48(1-3):219-237.

[8] 周立功. LPC900 系列 FLASH 单片机应用技术[M]. 北京:北京航空航天大学出版社,2004.

[9] Fei Jiyou, Zhou Mo. The Design of the Small and Low-power LED Display System Based on Infrared Serial Communication [J]. Applied Mechanics and Materials, 2011, 43:480-483.

[10] Li Dongming, Zhang Jing. An Automatic Voice Query System for Bank Based on Telephone Network[C]//2008 International Symposium on Information Processing. [s. l.]:[s. n.], 2008:629-632.

[11] 梁子伊. ISD4000 系列语音芯片的单片机控制技术[J]. 单片机与嵌入式系统应用,2002(5):15-18.

[12] 林 琴,张道信,吴小培. 一种基于改进谱减法的语音去噪新方法[J]. 计算机技术与发展,2007,17(7):63-66.

(上接第 224 页)

cess Control Models[J]. IEEE Computer, 1996, 29(2):38-47.

[4] 张文涛,常红星. 基于 ASP. NET 的 B/S 架构下的项目管理系统的网络安全模式设计[J]. 计算机科学,2008,35(2):101-108.

[5] 信 科,杨 峰,杨光旭. 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,2011,21(7):172-174.

[6] 杨贯中,曾 熠. 一种扩展的 RBAC 模型-ERBAC[J]. 计算机系统应用,2009(11):84-86.

[7] 黄 建,卿斯汉,温红子. 带时间特性的角色访问控制[J]. 软件学报,2003,14(1):1944-1954.

[8] 孙尚辉,曹宝香,王廷蔚. 扩展 RBAC 模型在文档管理中的应用[J]. 计算机技术与发展,2007,17(3):210-213.

[9] 胡 昊,李 茜. 扩展的 RBAC 模型在政府机关中的应用[J]. 计算机工程与设计,2010,31(24):5236-5239.

[10] 黄 静,陈 震. RBAC 模型在 B/S 医院信息系统中的应用[J]. 计算机技术与发展,2011,21(6):246-249.

[11] 方卫青. 细粒度角色访问控制[J]. 计算机系统应用,2011,20(2):125-129.

[12] 暴志刚,胡艳军,顾新建. 基于 Web 的系统权限管理实现方法[J]. 计算机工程,2006,32(1):169-170.