维普资讯 http://www.cqvip.com

第28卷 第3期 计算机工程与设计 2007年2月
Vol. 28 No. 3 Computer Engineering and Design Feb. 2007

层次化动态权限控制模型的设计和实现

傅国强， 陈锐锆
(深圳职业技术学院 信息中心，广东 深圳 518055)

摘 要：对于业务管理层级分明、耦合度高、涉及用户多而分散的WebMIS，传统的基于用户或角色的访问控制方式难与实际管理模式吻合。结合RBAC的基本思想，提出了一种通过模块和角色分层定义，权限分布式逐级控制的模型，实现WebMIS与传统MIS管理模式无缝吻合，优化规范管理流程。在实现技术上，利用目录结构树使权限管理直观方便，简化了用户、模块和权限三者之间的配置。

关键词：管理信息系统；浏览器型；层次化；动态；权限管理；角色
中图法分类号：TP311.132 **文献标识码**：A **文章编号**：1000-7024 (2007) 03-0690-03

Design and implementation of dynamic access control of WebMIS based on hierarchy roles

FU Guo-qiang, CHEN Rui-hao
(Information Center, Shenzhen Polytechnic, Shenzhen 518055, China)

Abstract: It is difficult to implement the administration of information system privilege when the management is hierarchical and high coupling with too many scattered users to utilize the traditional access control. According to the basic theory of the RBAC. A model implement hierarchical privilege management by using hierarchical programs and roles is given. It makes privilege management convenient and visual, and easy to configure users, programs and permission.

Key words: management information system; web; hierarchy; dynamic; privilege management; role

0 引 言

WebMIS是随着Internet发展而出现的一种新技术，其优点时易于管理，零客户端维护，跨地域跨平台，方便使用。这项技术使越来越多的管理系统采用B/S结构，运行于Internet上，大有超过C/S之势。Internet跨地域跨平台使权限控制显得尤其重要，但由于其连接无状态使系统权限不易控制，同时多层次分级管理的实际业务模式，涉及用户多而分散，这又要求系统权限控制必须具有操作灵活、实现简便的特点。在RBAC基础上，根据实际应用需求提出一个模式，通过资源和角色分层定义，实现权限的分层控制，比较好地吻合了现实中的分层逐级管理模式，结合角色定义，使管理权限由一人管理权限变为多人分级动态控制。实践证明，通过分层动态控制模型在实训室管理系统的应用，系统可以通过层层管理、层层负责，降低了由系统管理员统一管理所有权限给系统运行造成各种风险、具体实现过程中的繁琐及时效性差等缺点。

1 RBAC的基本概念

权限往往是一个极其复杂的问题，可归纳为这样的逻辑表达式："谁对什么如何进行的操作"的逻辑表达式是否为真。针对不同的应用，需要根据项目的实际情况和具体架构，综合考虑维护性、灵活性、完整性，选择最佳的方案。在RBAC模型中，有以下基本概念：①用户：系统的使用者，一般指单位(如：事业、企业或公司等)的职员；②角色：对应于单位(如：事业、企业或公司等)中某一特定的职能岗位，代表特定的任务范畴，角色的例子有：会计、采购员、销售员等；③许可：表示对系统中的客体进行特定模式访问的操作许可，例如数据库系统中对数据的查询、修改和删除等，一般许可受到特定应用逻辑的限制，图1表示了用户、许可和角色三者之间的关系；④用户分配、许可分配：用户与角色、角色与许可之间的关系是多对多关系。用户分配是指根据用户在组织中的职责和能力被赋予对应各个角色的成员。许可分配是指角色按其职责范围

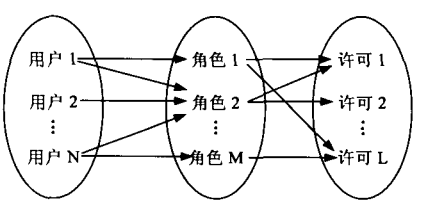

图1 用户、角色、许可关系

收稿日期：2006-06-23 **E-mail**：FREDFU@tom.com
基金项目：深圳科技局基金项目 (05kjh021)。
作者简介：傅国强 (1966－)，男，江西人，硕士，高级工程师，研究方向为数据挖掘、决策支持系统等；陈锐锆 (1977－)男，广东人，工程师，研究方向为网络编程技术、管理信息系统。

维普资讯 http://www.cqvip.com

与一组操作许可相关联。用户通过被指派到角色间接访问资源，进行许可分配时，应该遵循最小特权原则，即分配的许可集既能保证角色充分行使其职权，又不能超越其职权范围。

2 分层 RBAC 模型

RBAC 的一个重要属性是 RBAC 自身是中立于策略的，即RBAC是用于表达策略而不是实现一个具体的安全策略[3]。RBAC对一些安全规则(如最小特权规则、权限抽象规则、职责分离规则)提供支持，但是并没有说明这些规则怎样在系统中实施，甚至没有规定这些规则应该在系统中应用。要使用 RBAC 来实现精确的安全策略，必须对 RBAC 的各种部件进行详细地配置，如角色的定义、限制机制、对用户指定角色、为角色分配权限等。通过调整策略来满足一个组织内不断变化的需求能力是 RBAC 的一个重要优点。但是，如果按一般模式，统一由管理员定义各类角色的操作权，再将角色分配给各用户，这样对于系统复杂、特别用户众多且分散的情况下，实现极其困难。许多系统管理管理信息繁杂，用户多，如学校，学生上万人，教师也几千人，如果通过管理员垂直管理如此众多的用户几乎不可能。因此，本人提出的一种分层 RBAC 模型，增加了可操作性，可以直观并非常方便地控制权限。

2.1 对象的组织层次划分

根据单位的组织结构，可分为若干层，如3层、4层，首先，分为一级组织若干个，在每个一级组织下再分为若干个二级组织，依此类推，将整个单位按层次结构进行划分，生成一个树状结构，例如 4 层结构如图 2 所示。

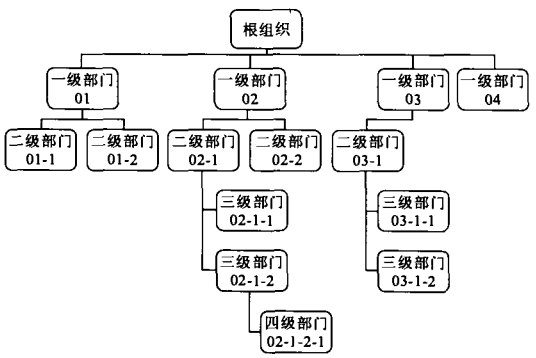

图 2 管理组织结构

按此组织结构，将人员和数据资源划分层次。如下定义：资源表(资源名，部门，传递)：建立组织机构与数据的关联。其中资源包括数据表、模块。这样任何资源都可以归属到某级组织上，全部资源便形成一个同样层次架构的分类图。角色分层结构：根据组织结构，可以在每层根据各层内资源的类别再分出 1~2 个角色，一般可以对各层次的职务，这样构成系统的角色分层结构。资源授权表：资源名，角色范围，操作权。人员授权表(人员，部门，角色)：建立组织机构与人员关联。操作权限值：这里用 1 代表查询，2 代表增加，3 代表删除，4 代表修改。这样就得到根据组织结构得到了分层的权限。用户、角色、资源控制关系如图 3 所示。

2.2 权限分层管理

权限从系统管理开始，将第一层权限授给第一批用户，所

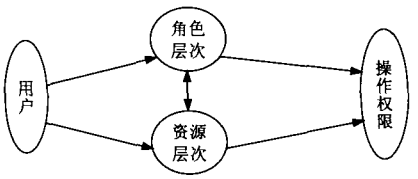

图 3 用户、角色、资源控制关系

以系统管理只管理第一批用户。这样，第一批受权用户可以将自己所属的管理范围根据实际职责需要，将第二级的权限授给第二批用户，第一批受权用户只管理自己单位内用户。依此类推，可以将各级信息的管理权授给相应的用户，每级用户只管理下一级用户，且用户只有拥有某级权限时才能将下一级管理权授出。用户授权时，系统首先计算用户本身所具有的权限，从而确定可以授出的权限。为了解决用户可能身兼数职的问题，用户也可以接收多个权限，甚至不同组织中的不同权限。

权限委托：对用户出差等的特殊情况造成用户不能及时由本人执行操作，可以通过权限委托的方式将工作零时委托给别人作。权限委托时仍然要受到自身权限的限制。

2.3 系统访问控制流程

WebMIS 的用户指的是任何一个对系统提出应用请求的主体，包括管理员和一般用户。当用户登录系统时，系统应根据每个用户登录系统的身份，分析得出其对于各种应用的权限，从而实现分类控制用户对系统资源的访问。系统的权限管理模块又可以分为两个子模块：用户身份认证模块和权限授予模块。

2.3.1 用户身份认证

用户身份认证就是通过搜索用户信息表，对用户登录的用户名和密码进行鉴别，从而判定该用户合法还是非法。用户信息表定义了访问此系统的授权用户的详细信息，是用户管理模块中最主要的一张表。在这张表中，每个用户都有代号(UserID)和密码(Pass wd)属性，这是要实现防止非法用户登录系统所必需的。为了在不同平台之间实现单点登录，可将用户信息表在 LDAP 服务器上，将认证任务交给 LDAP 服务器完成。

如果用户身份认证，把 session 变量“valid”设为 1，表示已经成功登录。身份认证阶段记录下通过认证的合法用户的登录信息，如用户代号，所属部门，权限级别等等，定义一个类包含变量：用户的相应信息：“UserID”为用户代号，“DepID”为所属部门代号，“Level”为在部门的级别等，将类变量存在 session 中。在进入每个页面前，取出 session 中的类变量值，对其这个“valid”变量进行判断，如果不为“1”则自动切换到登录页面。

2.3.2 权限获取

权限获取阶段要做的就是：根据认证阶段记录下的用户信息，从数据库权限分配表中取出该用户对于在各组织和权限值(职务，通常采用数值化表示权限层次)，将这些记录在一个 hashmap 中。这样，当用户请求某一应用服务时，系统就根据应用对应的组织和需要的权限(职务)在hashmap中查找，根据查找结果来判断是否可以对应用进行操作。实现权限的配置主要是用一个函数 getPermission()，对数据库中与用户代号

维普资讯 http://www.cqvip.com

相关联的设置权限的表执行查询SQL操作，返回一个权限值，可以是True、False这样带有开关性质的值。

2.4 分层权限管理的优势

本系统只是基于角色权限管理模式的一个简化，因为实际的业务逻辑并不太复杂，所以每个用户固定了一个角色，而不能选择登录系统的角色。在一般的小型MIS系统中，应用这种简化的角色权限管理模式就可以满足业务需求，并且效率更高，权限逻辑更清晰。如果是在大型的网络信息系统中，则数据库设计时就需要有用户信息表、用户- 角色表、资源信息表、权限类型表、访问控制表。这样，系统主要就由访问控制表中的一个四元组(RoleID ,ResourceID , PermID ,PermValue)来实现权限访问控制，使一个用户可具有多个角色，各种资源拥有不同的权限类型集合，一种类型的权限可以授予多个角色。这样的系统具有更复杂的权限逻辑，适用于要求更高的业务需求，可以动态地管理用户权限。

总之，基于角色的权限管理模式有3个方面的作用：①简化了权限管理，避免直接在用户和数据之间进行授权和取消。研究表明，用户所具有的权限易于发生改变，而某种角色所对应的权限更加稳定；②有利于合理划分职责，用户只有其所应具有权限，这样可以避免越权行为，有关用户组的关系描述正是对此的支持；③防止权力滥用，敏感的工作分配给若干个不同的用户完成，需要合作的操作序列不能由单个用户完成。

3 模型的实现

本文提出的权限控制模型在实训室管理系统已得到具体应用，具体实现如下。

3.1 功能实现

(1)用户管理：管理用户基本信息库的管理，实现用户(添加用户、删除用户、修改用户信息)

(2)角色层次管理定义：角色管理(添加角色、删除角色、修改角色信息)根据相关单位的机构层次设置相应的角色间层次关系。根据组织结构，可以在每层根据各层内资源的类别再分出1-2个角色，一般可以对各层次的职务，这样构成系统的角色分层结构。

(3)资源管理：建立组织机构与数据的关联。其中资源包括数据表、模块。这样任何资源都可以归属到某级组织上，全部资源便形成一个同样层次架构的分类图。

(4)用户权限定义：角色分配(为角色分配用户和为用户分配角色)。

3.2 数据结构设计

系统实现权限控制的主要数据库有如下：用户基本基本信息表(UserID, Passwd)、单位组织表(DepName,DepID)、资源表(ResourceID,DepID)、角色分层结构(RoleID,DepID, Order)、资源授权表 (ResourceID, DepID, RoleID, Operation)、人员授权表：(UserID, DepID, RoleID)。其中DepID是按部门层结构编码，如三级层次单位则按：一级部门代码+二级代码+三级代码，010101。通过分级编码来表示部门的层次关系。

3.2.1 权限操作算法

(1)权限获取算法：我们假设用户已经通过了身份验证，进入了授权阶段，其权限获取的算法如下：①使用session变量“UserID”记录用户代号，session变量“DepID”记录用户所属部门，session变量“RoleID”记录用户所属的权限组。用户身份获取：由getRoles()在人员表找出用户在各部门中担任的角色，以一个Hash map保存查找结果，Hashmap记录了用户在各部门中担任的角色，(DepID,Role)，将此角色Hashmap存在session中。②当用户请求服务时，调用getPermission(Res, Op)函数判断该用户有没有此项权限。getPermission()的参数包含两个变量（资源，操作），资源代表要操作的模块或数据库。getPermission()函数首先取出session变量中角色hashmap表，这样可得到用户所有的角色(DepID, Role)，通过SQL语句，在人员授权表中查找具有的角色是否有对资源Res、操作Op的记录，如果有返回1，否则返回0。③对getPermission()得到的权限值进行判断。如果为0，则给出提示信息“用户没有对些资源进行此项操作的权限”。如果为2，代表权限为“操作所有”，则在后面要转向的页面中显示所有的业务信息。

(2)其它相关算法：权限授予setRoles(用户，数据源/组织，操作权，代理)，getRoles(人员) getRoles()在人员表找出用户在各部门中担任的角色，setRoles(人员)授予用户组织以下分支数据或某数据的操作权可以授予给其它用户。类似现实的岗位的职权授予。接收者可以委托授予。权限委托EntrustRoles(用户，数据源/组织，操作权，代理)，getRoles(人员)getRoles()在人员表找出用户在各部门中担任的角色。entrustRoles (人员)委托用户组织以下分支数据或某数据的操作权可以委托给其它用户。类似现实的岗位的职权委托。接收者不能再给其它人委托。

3.2.2 实例

在开发实训室管理系统中，系统采用Linux+J2EE+Oracle+LDAP平台，在开发过程结合Java和JavaScript语言，可以使用操作窗口化、菜单化，完全实现了权限的分层动态操作，通过权限控制，使现实管理模式在软件中得到很好实现。层次信息通过树形目录图形，操作简单直观。具体效果如图4所示。

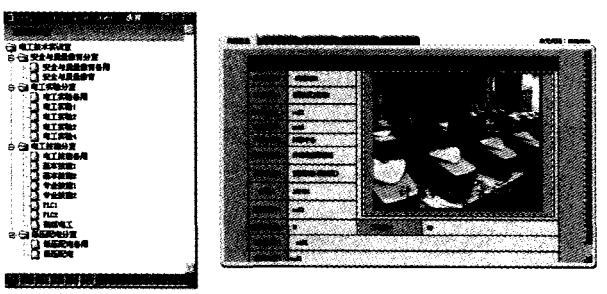

图4 系统实例

4 结束语

提出一个基于RBAC权限控制模式，通过资源和角色分层定义，实现权限的分层控制，比较好地吻合了现实中的分层逐级管理模式，结合角色定义，使管理权限由一人管理权限变为多人分级动态控制。实践证明对那些工作职能耦合度高，用户数较多，且有较多的岗位隶属层次关系，使得权限管理层次清晰，实现简单，比较好地吻合了现实中的分层逐级管理模式。

(下转第705页)

维普资讯 http://www.cqvip.com

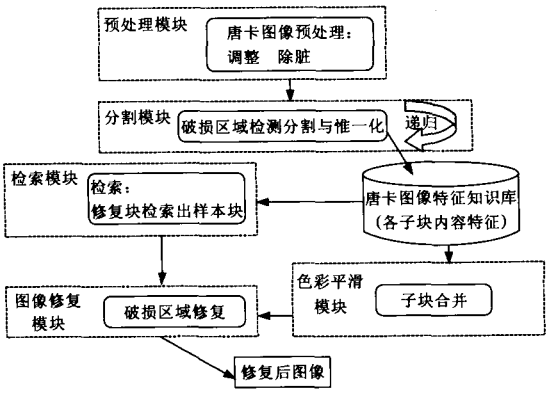

图 3 唐卡图像修复系统总体框架

破损图像修复系统为平台进行研究。破损大佛像唐卡的灰度图像修复结果：破损大佛像唐卡的灰度图像修复以图像灰度作为相似度计算的依据，图像在修复前作了高斯平滑处理和累积直方图均匀化处理，其修复结果是相当令人满意的，如图 4 所示。

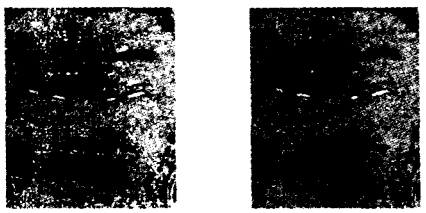

图 4 破损大佛像唐卡的灰度图像修复结果

破损大佛像唐卡的彩色图像修复结果：破损大佛像唐卡的彩色图像修复，以 R、G、B 各分量的相似度的均值作为总相似度计算的依据，图像在忠于修复前图的基础上作了相应的修复，其修复结果如图 5 所示。可以看到，修复后的图保持了大佛像唐卡原有的风格及其古香古色，总体上来说是成功的。

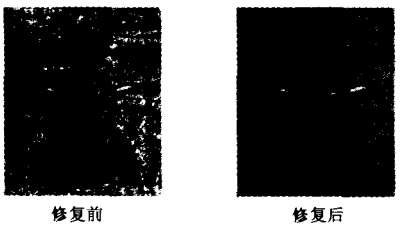

图 5 破损大佛像唐卡的彩色图像修复结果

5 结束语

通过唐卡破损区域的检测与标识，修复块优先级即基于同色线强度优先级的计算，最佳样本块的搜索与对应修复块的填充等理论探讨和工程实践，在唐卡图像复杂破损区域的修复方面取得了一定的成功，这是图像修复技术在实际工程中的典型运用。但由于目前将图像修复技术运用于实际工程的实例并不多，工程技术上还不很成熟，特别是古唐卡中的变色引起的误修复(见图 5 修复后)等都是今后要解决的问题。

参考文献：

[1] 丁晓华. 唐卡藏族艺术的瑰宝[N].中国商报, 2003-03-13.

[2] 祝君.试论唐卡的保护研究[C]. 中国文物保护技术协会第二届学术年会论文集, 2002.13-14.

[3] 白云飞,杜华.如何修复破损唐卡[N].人民日报海外版, 2004-05-29(8).

[4] Kokaram A C, Morris R D, Fitzgerald W J. Interpolation of missing data in image sequences [J]. IEEE Transactions on Image Processing, 1995, 11(4):1509-1519.

[5] Bertalmí o M, Sapiro M, Caselles V. Image inpainting[C]. New Orleas,Lu: Proceedings of SIGGRAPH, 2000.

[6] Fu-Li Wu,Chun-Hui Mei, Jiao-Ying Shi. Method of direct Teture synthesis on arbitrary surfaces[J].Comput Sci and Technol,2004, 5(19):643-649.

[7] Marcelo Bertalmio,Luminita Vese,Guillermo Sapiro,et al. Simultaneous structure and texture image inpainting[J].IEEE Transactions on Image Processing, 2003,8(12):882-889.

[8] 唐仕喜,王维兰.基于 W.M.A. 的藏族唐卡图像检索研究[J]. 香港:计算机科学与实践, 2005,(9):167-170.

[9] 刘昕,唐宝玲.基于样本的图像修复[J].西安:西安理工大学学报, 2005,(1): 1-54.

[10] 魏宝钢,李向阳,鲁东明,等.彩色图像分割研究进展[J].计算机科学, 1999,26(4):59-62.

[11] 吴振宇,王朔中.基于区域分割的损伤图像修复[J].上海:上海大学学报, 1999,(1): 54-55.

[12] Criminisi A,Pérez P,Toyama K.Region filling and object removal by exemplar-based image inpainting[J]. IEEE Transactions on Image Processing, 2004,13(9):1200-1212.

[13] Margaret H Dunham. Data mining introductory and advanced topics[M].Prentice Hall,Wilson:Pearson Education, 2003. 90-91.

(上接第 692 页)

参考文献：

[1] 季永志,阎保平.基于角色的访问控制框架的研究与实现[J].微电子学与计算机, 2005,(11): 100-103.

[2] 林磊,骆建彬.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,(6): 82-84.

[3] David F Ferraiolo, Ravi Sanehu. Proposed NIST standard: Role-based access control[J]. ACM Transactions on Information and System Security, 2001, 4(3): 224-274.

[4] 王毅彦.基于授权管理基础设施的授权及访问控制机制[J].计算机应用, 2005,(9): 22-25.

[5] 丁胜,陈建勋. 基于 RBAC 模型的安全访问机制建模研究[J].计算机应用与软件, 2005,(11):115-117.

[6] 刘一冰,王若烨. 运用 RBAC 策略实现权限管理[J].计算机工程与应用, 2005,(31):105-108.

[7] 李帆,郑纬民. 基于角色与组织的访问控制模型[J].计算机工程与设计, 2005,26(8):2136-2140.

[8] 景凤宣,连红. 基于角色的授权管理模型的研究[J].武汉大学学报(理学版), 2005,(12):134-138.