

# 基于角色的 Web 系统安全策略研究

李 向, 郭晓兰, 严 烨

(中国地质大学 计算机学院, 湖北 武汉 430074)

**摘 要:**在基于 Web 服务器的访问控制技术研究与应用中, 后台数据库的安全性问题至关重要。而采用基于角色访问控制(RBAC)模型可以有效地解决数据库安全性问题。文中结合“选课选课”系统设计与实现, 详细论述了角色访问具体的安全机制, 通过限制系统中各种角色对系统的操作, 有效地解决了 Web 页面安全访问和控制数据库的问题。

**关键词:**RBAC; 安全; 权限

**中图分类号:**TP309.2

**文献标识码:**A

**文章编号:**1673-629X(2006)10-0155-02

## Research on the Role - Based Web Security

LI Xiang, GUO Xiao-lan, YAN Ye

(Computer School, China University of Geoscience, Wuhan 430074, China)

**Abstract:** The security in back database is very important, with the research and application of the access control based on the Web server. For this, taking measure of the role - based control model can solve it very well. Applies this idea in the choosing subjects or course system. It describes the RBAC security particularly. The system limits different roles operate it. It is good for the security at access control in the Web system.

**Key words:** RBAC; security; purview

### 0 引 言

传统管理是基于用户和组的概念模型, 自 Unix 系统开始就一直使用至今。用户组和角色在实现访问控制策略时的最大区别在于: 用户组仅是用户的集合; 而角色则还是权限的集合, 角色是两个集合之间联系的媒介。基于角色的访问控制将权限同角色关联起来, 而对用户赋予相应的角色, 用户所能访问的资源权限就是该用户所拥有的角色的权限集合的并集。根据机构中不同工作的职能可以创建不同的角色, 每个角色代表了一个独立的访问权限实体, 它们之间可以有继承、限制等关系, 然后在建立了这些角色的基础上根据用户的职能分配相应的角色。这样在用户机构变动时就可以很容易地将该用户从一个角色移到另一个角色去实现变更, 而操作对用户完全透明。另外, 还可以根据应用系统的需要对角色进行重新授权或取消某些权限, 这使得基于角色访问控制策略的管理具有无可比拟的灵活性和方便性。

基于角色的访问控制 RBAC<sup>[1]</sup> (Role - Based Access Control) 的概念是从 20 世纪 70 年代对在线的多用户、多应用系统的研究开始的。J. S. Park 和 R. S. Sandhu 研究了 Web 上 RBAC 的实现策略, 提出了利用安全 Cookies、智

能认证以及 LDAP 三种实现方法。许多大型数据库产品 (如 Oracle 8.0, Sybase 11.5, Informix 7.2) 以及操作系统软件产品 (如 Solaris) 都相继实现了基于角色的安全访问控制<sup>[2]</sup>。正因为基于角色访问控制策略<sup>[3]</sup>是一项成功的技术, 在大规模的 Web 网络应用环境中, 正需要用它来有效地增强对用户访问的控制和管理。目前, 全国高校都在进行管理工作的信息化, 而所有信息化工作中, 面临的最大问题就是要保持信息的一致性和安全性。目前高校里许多工作还是靠手工完成, 很大程度上造成了信息的不一致性, 而且对数据的安全性也不能很好地保障。因此对高校现行工作的信息化改良是十分必要的。文中设计的高校学生课程选择和毕业设计题目选择系统正是为了弥补这种不足, 但同时为了保证系统的安全性, 加强身份认证和访问控制, 采用基于角色的访问控制策略给出了一个相应的解决方案, 详细论述了角色访问(RBAC)具体的安全机制, 通过限制系统中各种角色对系统的操作, 有效解决了 WEB 页面安全访问和控制数据库的问题。

### 1 基于角色的访问控制模型

关系型数据库的访问控制模型主要有三种: 自主访问控制模型(DAC); 强制访问控制模型(MAC); 基于角色的访问控制模型(RBAC)<sup>[3~5]</sup>。RBAC 是美国 R. S. Sandhu 提出的, 它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。其中主要涉及用户、角色、访问权限、会话等

收稿日期: 2006-01-09

**作者简介:**李 向(1970-), 男, 重庆人, 讲师, 博士研究生, 研究方向为演化计算及其应用; 导师: 康立山, 教授, 研究方向为演化计算及其应用。

概念。用户、角色、访问权限三者之间是多对多的关系。角色和会话的设置带来的好处是容易实施最小特权原则。在 RBAC 模型中,将若干特定的用户集合和某种授权连接在一起。这样的授权管理与个体授权相比较,具有强大的可操作性和可管理性,因为角色的变动远远少于个体的变动。通过引入 RBAC 模型,系统的最终用户并没有与数据对象有直接的联系,而是通过角色这个中间层来访问后台数据信息。在应用层次上角色的逻辑意义和划分更为明显和直接,因此 RBAC 通常使用于应用层的安全模型。鉴于 MIS, DSS 在授权管理和访问控制方面的特点,文中的设计方案中采用了 RBAC 模型<sup>[4]</sup>。

访问控制策略<sup>[3]</sup>体现在 RBAC 模型里是用户—角色、角色—权限和角色—角色之间的关系。采用 RBAC 的最大的好处在于将用户和它具有的权限分离开来,管理员可以将用户的授权和权限的划分进行分别处理,给用户授予角色来实现用户的授权操作。在集中式管理中,这些关系通常是由一个指定的管理员来进行分配。图 1 给出了 RBAC 的模型层次图, RBAC0 是任何支持 RBAC 系统需要满足的最低要求。RBAC1 和 RBAC2 都包含 RBAC0,但是分别有各自的特点。RBAC1 增加了角色之间可以相互继承访问权限的层次的概念,而 RBAC2 则对 RBAC 组件添加了限制条件的约束, RBAC1 和 RBAC2 相互独立。RBAC3 则同时包含了 RBAC1 和 RBAC2。在文中的系统中,对 RBAC 理论模型进行了组件化实现,使访问控制管理包含几个组件:可以控制细化到用于角色定义的管理员模块、定义角色间关系的模块及配置用户权限的模块。

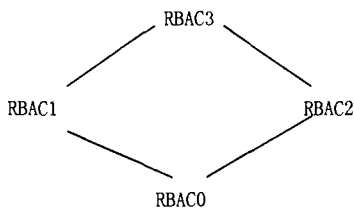


图 1 RBAC 模型的关系

## 2 系统的设计与实现

### 2.1 设计目标

在现有的应用信息系统中主要存在以下问题:

①面对大型数据库系统,如 Oracle, Sybase 等,应用系统的用户并非专业的数据库管理人员。由于大型数据库安全管理的复杂和专业化,使得普通用户在使用过程中很容易发生误操作,影响了 DBS 本身的安全性能。

②现有的一些数据库应用系统中虽然实现了数据库安全访问控制,但设计缺乏灵活性,在实际应用中,随时间和情况的变化,程序的适应能力差。为了解决上述问题,设计目标力求在保证后台数据库安全的前提下,提高软件的可用性,以及操作界面的友好性。

### 2.2 设计思想

首先,在解决后台数据库安全,减少用户使用过程中

误操作的问题上,方案采用了将应用程序和后台数据库管理系统紧密结合。通过在应用程序和 DBMS 之间建立相应的接口,使得用户能够通过简便、友好的界面对相关的数据信息进行安全的访问控制,保障用户操作的安全性。这样,就将后台数据库系统强大的安全管理机制引入了应用系统中。其次,采用动态管理机制提高软件的灵活性。RBAC 很好地解决了大量授权问题,但用户根据本单位的具体情况和实际需求,按不同的职务划分角色,随时间和应用的变化,会发生角色的增加、删除和权限的变化。如果在开发设计过程中事先规划好角色,不能再改变,则影响了程序的适应性和通用性。此外,应用系统功能模块的划分是通过菜单项来体现的。通过严格地对功能模块的授权访问,也保证了后台数据库中数据信息的安全。由于在实际应用中功能项还会发生增删改的变化,因此对功能项实行动态管理。

### 2.3 系统的实现

该方法采用流行 ASP + SQL2000 完成,系统运行于 IIS 5.0。这种 B/S (Browser/Server) 结构便于网络浏览,适合多学生、多教师和多管理员同时使用该系统。如图 2 所示。

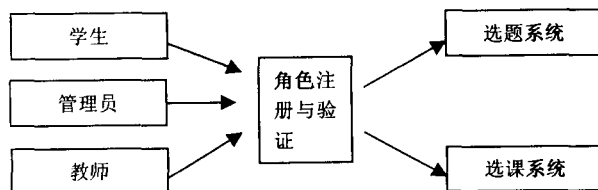


图 2 管理员、教师用户和学生用户角色

以学生毕业设计题目选择为例,首先教务管理人员以管理员角色初始化系统,如建立教师和学生用户,设置系统运行的各个阶段(第一阶段:教师命题;第二阶段:学生选题(第一志愿阶段;第二志愿阶段;第三志愿阶段);第三阶段:管理员根据志愿指派落选学生与落选题目);教师用户以指导教师的角色进行自己的信息维护、命题和选择学生;学生用户以学生角色进行自己信息维护和选择教师及毕业设计题目。

动态的用户、角色管理和角色授权用户管理包括对用户信息的增加、删除、修改。用户信息包含用户名、用户具体描述、加密后口令、创建时间及当前状态。在用户登录应用系统时,除对用户名和用户口令进行相符验证外,还需判断用户的当前状态。在建立用户信息时,将用户口令这样敏感的数据进行加密处理(加密算法采用单向函数加密算法),然后存放于用户表 user 中。在应用程序中建立一个用户后,在后台数据库系统中也创建相应的数据库用户。同样,应用程序角色的建立也和后台数据库中角色的创建一一对应。

在实际应用程序中,除了一个默认用户(应用系统管理员)事先赋予特权(DBA 角色)和功能模块的全部可视,其他普通用户创建、角色的授权都在应用程序中完成。对

(下转第 173 页)

小一样的二值缺陷图像。凡是在缺陷图像中出现灰度值为 0 的情况,即已有图像像素点达到废品阈值,该待检图像应该被认为是废品。但是在实际检测中不能将包含单缺陷点的图像判定为不合格图像,因为高精度图像的分辨率很高,例如一般钞票印刷检测系统采集的图像中一个像素点所要求代表的实际大小为  $0.4\text{mm} \times 0.4\text{mm}$ , 这样人眼不可能敏锐地感觉到图像上的一个像素点大小的错误,也就没有必要使图像检测的精度超过人眼的视觉精度。如果把印刷检测精度设定得过于精确,会不可避免地产生很多误检错误。

在缺陷检测过程中,会有两个,或多个相距很近的缺陷区(比如两个缺陷点在图像上只有一个像素距离),通常认为它们同属一个缺陷区。因此,检测前需要先把它们合并成一个缺陷区,可以采用数学形态学的膨胀算法<sup>[6]</sup>。如需将不同缺陷分类的话,还要再经过腐蚀、膨胀、再腐蚀等一系列操作,将缺陷图像的边缘形状提取出来,以便进行进一步的分析和判断。

## 5 结束语

目前的印刷机械和印刷工艺虽然已经应用了很多高科技成果,其自动控制程度达到了相当高的水平,但它对操作人员本身的技能要求还很高,仍然需要操作人员有丰富的印刷质量控制经验,才能保证印刷品产品的合格。用

机器视觉识别系统代替人工进行印刷品质量检测,具有实用价值。文中讨论了一种对印刷品的缺陷进行自动检测的初步方案,能大大减少印刷品质量控制的人为干预,提高印刷质量检测效率,为真正实现印刷质量在线检测提供了可能。

下一步需要解决的问题有:

(1)较之外观缺陷要困难得多的如色差、套印不准等缺陷的检测与识别问题。

(2)要满足实际生产线检测的实时要求,根据目前微机的性能指标,除要对图像匹配算法进行优化以外,还须借助硬件才有可能。

## 参考文献:

- [1] 容观澳,数字图像处理[M].北京:清华大学出版社,2000.
- [2] 邢军.基于 Sobel 算子数字图像的边缘检测[J].微机发展,2005,15(9):48-49.
- [3] 章毓晋.图像工程(上):图像处理和分析[M],北京:清华大学出版社,1999.
- [4] 王熙法.C语言图像程序设计[M].合肥:中国科学技术大学出版社,1994.
- [5] 汪孔桥,沈兰荪,邢昕.一种基于视觉兴趣性的图像质量评价方法[J].中国图像图形学报,2000(4):300-303.
- [6] Gonzalez R C, Woods R E. Digital Image Processing[M].北京:电子工业出版社,2003.

(上接第 156 页)

角色授予功能项的权限为:功能项可视或不可视。对于普通用户,经常使用的是数据库中的表及视图,因此,在安全设计中仅对系统角色进行表级授权。首先,为角色授予数据库系统权限(Connect 权限),然后再授予所需对象权限(Select 权、Update 权、Insert 权、Delete 权)。角色所需权限分配好后,便可以为用户分配角色。在应用程序中进行授权,方便了数据库管理员的操作,提高了安全性。用户登录通过系统身份验证,连接数据库通过 check.asp 来验证,实现了安全管理机制。为管理用户和角色信息及功能项授权,在具体实现中,创建如表 1 所示的主要应用系统表。

表 1 系统中建立的基本表

学生班级表:	Stu_class	学生年级表:	Stu_grade
学生信息表:	Stu_infor	教师信息表:	Teach_infor
学生课程表:	Stu_course	初选结果表:	First_result
发布信息表:	Infor_issue	题目信息表:	Obj_infor
选课结果表:	Select_course	最终结果表:	Last_result

系统管理人员便可以通过应用程序的界面跟踪监视后台数据库中数据对象的使用情况,及时发现问题,确保数据库安全。

## 3 结束语

文中主要论述了在基于 Web 的选课选题系统中利用

不同用户角色的授权管理和自主访问控制(DAC),从而达到强制访问控制(MAC)的方法,防止信息流从高密级流向低密级和实现多级安全访问控制。文中论述的数据库角色访问控制方法为多角色软件开发提供了一种解决数据库安全访问控制问题的新方法。增加 RBAC 模型里职责分离等约束条件,从而以完整的基于角色的访问控制机制实现用户自定义的访问控制策略是下一步研究的工作。

## 参考文献:

- [1] Sandhu R S, Coyne E J, Feinstein H L, et al. Role-Based Access Control Model[J]. IEEE Computer, 1995, 5(3): 127-130.
- [2] Sandhu R S, Bhamidipati V, Munawar Q. The ARBAC97 Model for Role-Based Administration of Roles[J]. ACM Transactions on Information and System Security, 1999, 2(1): 31-36.
- [3] 宋志敏,南相浩.数据库安全的研究与进展[J].计算机工程与应用, 2001(1):85-87.
- [4] 林东.网络信息安全 & PGP 加密[M].北京:清华大学出版社,1998.
- [5] Tari Z, Chan Shunwu. A role-based access control for intranet security[J]. IEEE Internet Computing, 1997, 1(5): 24-34.