基于 RBAC 的学校多媒体教学与管理系统的安全设计与实现

周卫东[1,2]，王翠玲[3]，王彩凤[1]
(1.西北师范大学 数信学院，甘肃 兰州 730070；2.兰州园艺学校，甘肃 兰州 730060；3.甘肃农业大学，甘肃兰州 730070)

摘 要：学校多媒体教学与管理系统的安全性是基于 WEB 的系统和基于角色的访问控制的来设计的。本应用系统采用了用户界面层、WEB 服务层、数据库层的三层结构。在设计时，从这两个方面考虑：一是对 WEB 访问的控制，另一个是对数据访问的控制；在实现时，我们将基于角色的访问控制模型中的用户、权限、角色及约束转化为关系数据库中表间关系，采用 SQL 语言来描述系统的约束策略，从而实现系统的访问控制和系统的安全的目的。

关键字：WEB 访问；RBAC；数据访问；B/S
中图分类号：TP139

1 引言

随着 Internet 技术的发展和基于 WEB 开发平台的推出，目前应用系统开始由传统的 C/S 模式向 B/S 模式转变。B/S 模式就是以 WEB 为中心，采用 TCP/IP、HTTP 传输协议、客户端通过浏览器访问 WEB 服务器，以及与 WEB 服务器相连的后台数据库。C/S 模式是一种网络模式，这种模式将应用一分为二，服务器负责数据管理，客户机完成与用户的交互任务。C/S 具有很强的数据操纵和事务处理能力，以及数据的安全性和完整性约束；但也存在明显的弊端：1、管理成本高，需要开发客户端软件；2、随着 MIS 软件越来越庞大，对硬件的要求也越来越高；3、移植困难。不同开发工具开发的应用程序，一般来说互不兼容，不能搬到其它平台上运行 4、新技术不能轻易应用。因为一个软件平台及开发工具一旦选定，不可能轻易更改[1]。而 B/S 模式简化了客户端，只需安装通用的浏览器软件，使安装简化、又简化了系统的开发和维护，只需把所有的功能都实现在 WEB 上；弊端是安全性较差[2]。可见 B/S 构架比 C/S 结构在开发上有更大的优越性。由于安全隐患，使得 WEB 站点与应用系统及后端相连的数据库安全性就显得尤为重要。为了保护系统中重要信息安全，我们构造了一种适合于我校特点的安全模式。

2 系统简介

我们在校园网上构建的多媒体教学与管理系统是基于 WEB 的系统，教学内容以 WEB 页面的课件形式出现在站点中，管理内容包括学生学籍、成绩、机要公文资料等；用户通过访问站点中的 WEB 页面来实现网上教学与管理。本系统由四个系统组成：教务管理系统、教学管理系统、自主学习系统和教学资源管理系统。在总体结构上是采用 3 层 B/S 结构，各类教学资源与管理资源向服务器提出请求，服务器通过中间件 ADO 与数据库 SQL 统一存放和组织；用户使用浏览器向 WEB 服务器提出请求，服务器通过中间件 ADO 与数据库链接，把请求服务的教学内容或管理内容以 WEB 页面形式通过浏览器反馈给用户。

3 系统安全控制与管理

由于该模式的安全隐患，使得 WEB 站点与应用系统及后端相连的数据库安全性就显得尤为重要。我们从用户界面层、WEB 服务层、数据库层的三层结构来设计应用系统，其安全控制分布在这三层结构的每个层面，在具体实现上从两个方面来考虑：一是 WEB 访问的控制；另一个是数据访问的控制[3]。

1)WEB 访问的控制与管理实现

当访问应用系统的资源时，系统要求用户输入用户名与口令以进行身份认证，若认证合法，根据合法用户登录的有关信息在 RBAC 数据库中查询出处于系统当前层的所有该用户有权执行的属于超链接的应用程序文件的 URL 地址和其中文描述，以及其在系统中所处的应用层次，根据查询结果在页面中动态生成超级链接菜单；否则返回注册页面。管理员事先将有不同权限的用户资料输入数据库，注

册提交后管理员建立会话请求授权时，将用户信息与基本信息数据库进行比对，若数据库中有资料的用户将会得到授权，然后返回登陆主页；若无则得到访客权。为防止非法用户直接以 HTTP 方式在浏览器请求执行某页面，在每个应用系统程序文件中需包含具有以下功能的代码：判断该用户是否登录并建立会话，如已建立会话，就检查该用户是否有该页面的执行权限。方法是先取得请求执行页面的路径，然后结合该用户保存在 Application 变量中的用户名、口令、用户属性等用户信息，在 RBAC 数据库中查询其是否有访问该页面权，有则显示相应访问界面，否则释放该变量并终止程序。见图 1：

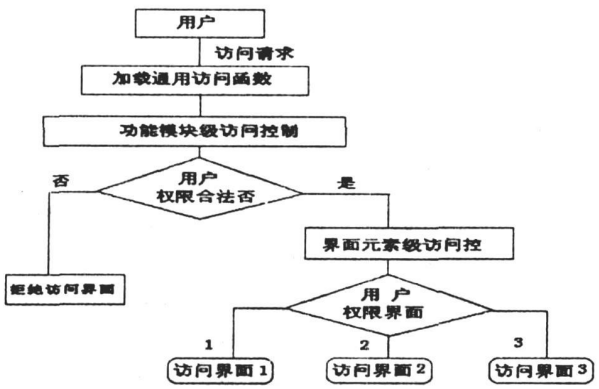


图 1 访问控制流程图

2)数据库访问控制与管理实现

数据库访问控制使系统安全的最后保障，也是最重要的一层；若该层出现问题，就意味着整个系统处于无保护状态[4]。保护数据库的完整性与可靠性为了保证数据的正确性，它涉及到数据库内容的正确性、有效性和一致性[3]。为了保证数据库中数据的确性，我们认为该部分的设计尤为重要。

(1)数据库设计与实现

安全信息表存放系统的各种安全信息，包括授权主体信息、授权客体信息和权限状态信息[5]。下面给出系统的安全信息表的数据结构。

①用户表(User_ table)：用户表具有用户号 User_ no、用户名 User_ name、用户性别 User_ sex、用户身份证号 User_ idcard、用户 password、用户地址属性 User_ addr、电话属性 User_ dh、邮编属性 User_ zip、个人网址属性 User wz、电邮属性 User_ email、单位属性 UT no 以及角色属性 User role。其中角色属性是网站管理员根据网站规定和安全策略分配的个人属性，注册后并取得会员资格的用户可以根据角色使用网站提供的会员级服务，比如查询功能。

②用户注册表(Reg_ Table)：用户注册表用于记录注册用户的原始信息，它具有注册用户 Reg_ no，注册用户名 Reg_ name、用户 Password、注册用户 Question、注册用户 Answer、注册用户 Reg_ realnm、注册用户身份证号 Reg_ idcard、注册用户 Reg_ sex、注册用户单位属性 Reg_ UTno。

③单位表(Unit Table)：单位表用于记录用户的单位属性，单位表具有单位编号属性 UT id，单位名属性 UT name、地址属性 UT dz、电话属性 UT dh、传真属性 UT cz、邮编属性 UT zip、网址属性 UT wz 以及电邮属性 email 。

④数据库对象表(DBobject Table)：各功能模块需要访问数据库服务器上的许多数据库对象，角色对功能模块的权限最终也是通过角色对数据库对象的授权来实现的。字段有数据库对象编号(DBobjectID)、数据库对象名称(DBobjectIDNM)、数据库对象类型(DBobjectIDTP)(可以取值 TABLE、VIEW、COLOUM、INDEX 等)。

⑤资源表(Resource Table)：资源表用于记录所有教学资源的属性，资源表编号 Rt id、资源名 Rt name、资源类型 Rt class、资源提供者 Rt tgz、资源应用范围 Rt yyfw 和资源属性 Rt sx。

⑥职工表(Officers Table)：职工表用于记录所有学校全体职工的属性，职工编号 Ot id、职工名 Ot name、职工性别 Ot sex、职工工作 Ot gz、职工部门 Ot bm、职工住址 Ot ad 和电话 Ot dh。

(2) RBAC 授权访问设计与实现

①根据设计数据库的工作可知，我们把访问网站的用户分为一般用户、会员用户和超级用户三类，一般用户是为学生级用户，只能获得网站一般共享信息，会员用户是教师级用户，它可以获得高级别的技术信息和资料。超级用户为网站管理员，负责整个数据库管理工作，有权修改数据库。在这一基础上，我们建立了具有角色属性的用户表。

1.建立角色——用户类别关系表

为了让所有的用户都能根据权限访问网站信息而又不危害信息安全，我们根据用户表中的角色属性对用户和数据库的关系进行了处理。首先，根据用户的类别，对用户表中的角色字段分一般用户(学生)、会员(职工、教师)和超级管理员分别设为数字 1、2、3 和 4；其次使用户和角色建立对应关系，即角色——用户类别关系表(见表 1)。

表 1　角色－用户类别关系表

User	一般用户	会员用户		超级管理
	员学	生职工	教师	
User－role	1	2	3	4

2.建立用户——角色关系表

根据用户表和角色－用户类别关系表,我们进一步建立用户一角色关系表。假设有 5 个用户 Userl,User2,User3,User4 和 User5,它们的 user_ no 分别为 6001,6002,,6003,,6004 和 6005,在访 Ip 系统时的角色分别为 Rolel、Role2 和 Role3。其中 Userl 为一般用户,User－ role 为 1;User2、User4 和 User5 为会员用户,User－role 分别为 2 或 3;User3 为超级用户,User_ role 为 4。我们对这 5 种用户建立的用户——角色关系表(见表 2)。

表 2　角色－用户关系表

User－no	6001	6002	6003	6004	6005
User－name	User1	User2	User3	User4	User5
User－role	1	2	4	2	3

3.建立角色——授权关系表

根据我们在建立数据库时对用户的分析,三种不同类别的用户在访问数据库时的角色是不同的。对应用户表,就表现为用户的角色数字和数据库中的各表之间不同的映射关系。同样,我们以上面 5 个用户为例研究它们的角色和数据库中的各表之间的关系,在数据库中建立的 8 个表,即用户注册表、用户表、教学资源表、部门表、单位表、职工表、文件资料表、学生表和课程表,分别用个位数字标记上述表,其对应数字依次为 1,2,3,4,5,6,7,8 和 9,如表 3 所示。

表 3　角色授权映射表

Table / role	注册表	用户表	资源表	数据库对象表	职工表	学生表	成绩表	文件档案表	课成表
	1	2	3	4	5	6	7	8	9
1	11	0	0	0	0	0	0	0	19
2	21	0	0	24	0	0	27	28	29
3	31	0	33	34	0	36	37	38	39
4	41	42	43	44	45	46	47	48	49

规定一般用户只可以访问注册表(受限访问,只可读写个人资料)、课程表和部门表;会员用户可以访问注册表(受限访问,只可读写个人资料)、教学资源表、部门表、单位表、职工表、学生表和课程表;超级用户可以访问和修改所有表。

这是一种多对多的角色授权映射关系。为了使这一映射关系能够用程序实现,我们将上述问题抽象为角色数字和数据库标识数字的关系矩阵,并用表的行表示用户角色,列表示数据库的表。在对应表的下面标注角色权限标识数字。角色权限标识数字由角色数字和对应表标识数字构成,当 User role ＝3 的用户可以访问注册表、数据库对象、教学资源表、部门表、文件档案、成绩表、学生表和课程表,由此 User_ role＝3 对应教学资源表的角色权限标识数字写为 33,同样,如 User_ role＝3 不能访问职工表表,对应的角色权限标识数字则为“0"。根据这个规则,结合角色－用户关系表和角色－用户类别关系表可以得到角色授权映射表。

4、子功能表:一个大的功能模块往往又包含若干子功能模块,字段有子功能编号(SFun ID)、子功能名称(SFun NM 年)、功能模块编号(Fun ID)。

5、功能_ 数据库对象关系表:功能模块和子功能模块是用来访问和操纵数据库服务器中数据对象的,功能模块或子功能模块是授权主体,数据库对象是授权客体。字段有功能模块编号(FunID)、子功能模块编号(SFunID)、数据库对象编号(DBobjectID)、检索有效标志(SelectV)、插入有效标志(InsertV)、删除有效标志(DelectV)、更新有效标志(UpdateV)、执行有效标志(ExectV)。

6、角色冲突约束限制表:是用来在对用户分配角色时防止角色冲突的产生,在往用户角色关系表插入一条新的授权记录时,用 SQL Server 中语句进行描述。

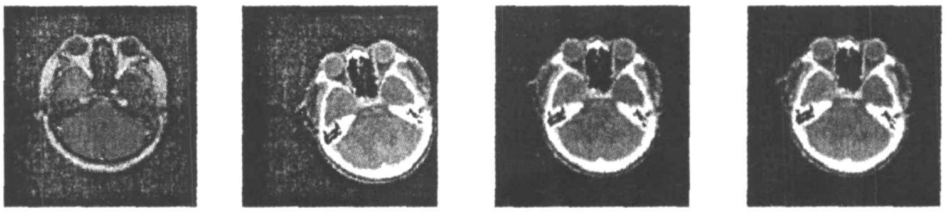
当角色唯一对一时,由以下语句控制:

```
SELECT USER－ID FROM USER－ROLE
 WHERE ROLE ID NOT IN
   (SELECT ROLE－ID FROM ROLE－
RELATION
   WHERE ROLE－ID＝"将要分配角色"
AND RELATION＝"1")
```

当角色为多对一时,由以下语句控制:

```
SELECT USER－ID FROM USER－ROLE
 WHERE ROLE ID ＝“启动角色的用户"
 EXCEPT
  SELECT ROLE－ID FROM SESSION
   WHERE USER－ID＝"启动角色的用
户"AND SESSION－STSTUS＝"1"
    AND ROLE－ID IN
   (SELECT ROLE－ID FROM ROLE－
RELATION
   WHERE ROLE－ID＝SESSION－ROLE
－ID AND RELATION＝"2")
```

(下转第 13 页)



(a) MRI 图像　(b)待配准 CT 图像　(c)粗配后的 CT 图像　(d)细配后的 CT 图像

图 2　配准前后的 MRI 和 CT 图像

的混合配准策略,从而在配准速度和精度上都得到了很大提高。但本文的算法也主要针对的是刚性、轮廓清晰的医学图像,有许多方面还需要改进和发展。

参考文献:

[1] Zitona Barbara,Flusser Jan.. Image registration methods:a survey. Image and Vision Computing, 2003, 21 (11):977-1000.

[2] 赵芹,周涛等,基于特征点的图像配准技术探讨,红外技术.2006,6,327-330.

[3] Dai X L, Khorram S. A Feature—based Image Registration Algorithm Using Improved Chain—code Representation Combined with Invariant Moments[J]. IEEE Trans on Geoscience and Remote Sensing. 1999, 37 (5):2351-2362.

[4] Wachowiak MP,Smolikovar, Idurassi GD,eta1. Generalized mutual information aimilarhy metrics formuhimodal biomedical image registration[A]. Engineringin Med icine an d Biology. 24tll Annual Conference and theAnnual Fall Meting ofthe Biomedical Enginering Society[C]. Houston. Texas. USA:The Institute of Electrical andElectronics En gine～, Inc. 2002, 2:1005-1006.

[5] Pluim J P W. Information and gradient information [J]. IEEE Transactions on Medical Imaging. 2000, 19 (8):809-814.

[6] 徐东,李升辉,互信息医学图像配准研究与局部极值的克服,计算机工程与应用.2007,43(3):217-219.

[7] 姜晓彤,罗立民等,一种改进的基于互信息和梯度特征的图像配准方法的研究,仪器仪表学报.2006.91141-1146.

[8] 周永新,罗述谦.基于形状特征点最大互信息的医学图像配准.计算机辅助设计与图形学学报.2002,14(7).

[9] Maes F,Collignon A,Vandermeulen D,et al. Multi modality image registration by maximization of mutual information[J]. IEEE. Tran Med Imaging ,1997,16(2): 187-198.

(上接第 25 页)

②根据用户表和角色授权映射表,当用户访问数据库时,系统将根据用户表的角色数字查询角色授权映射表,然后根据角色数字对应的角色权限标识数字来判断用户是否具有这种权限。身份认证通过后,角色权限标识数字作为参数要传递到角色数据库表接口模块,这个接口模块具体实现角色的授权情况。为了实现角色数据库表接口模块,可以将"角色—授权映射表"放到认证服务上的数据库中。每次要获得授权,只需根据角色数字到数据库中去查找角色权力标识数字,若查找到就获得了相应授权。

4　结束

我们以 WEB 模式的 B/S 三层结构进行本系统安全模式的设计过程。依据安全访问控制实现了前后台控制的一致性,把直接作用于客户端的安全信息转化为服务器的权限控制,使客户端的权限得到真正实现。在数据访问控制,通过建立 RBAC 授权数据库及采用 SQL 语句来描述系统的约束限制策略,使得基于角色的存取控制机制在系统中得以有效执行,从而实现了整个系统的安全,在实际应用中效果良好,得到了校方认可。

参考文献:

[1] 李仁玲.C/S 与 B/S 结合的图书馆管理系统设计[J].情报杂志,2006.1,102-104.

[2] 曹 莉,赵文静.基于 B/S 结构网上选课系统的设计与实现[J].自动化技术 :2006.3,92-93.

[3] 赵战生,冯登国.数据库和操作系统的安全[J].中国金融电脑,1999,(5):58-64.

[4] 宋志敏.数据库安全的研究与进展[J].计算机工程与应用,2001,(1):85-87.

[5] 张小英,张灯银,刘国祥.大型关系数据库安全机制的设计[J].南京邮电学院学报, 1996.16(4):59-62.