基于RBAC权限管理系统的优化设计与实现

信 科,杨 峰,杨光旭,马媛媛
(山东师范大学 信息科学与工程学院,山东 济南 250014)

摘 要:针对Web系统的特点及其对用户访问控制的特殊要求,在RBAC(基于角色的访问控制)模型的基础上进行了优化,设计并实现了分级的、细粒度的权限管理子系统。该子系统结合用户权限驱动的动态多级Web导航,在很大程度上提高了Web系统的易用性。系统的实现基于统一的基类,大大提高了代码复用,几乎无需修改现有程序就可以把本系统无缝地集成到现有Web系统中。实践证明此方案不仅可以满足大中型Web系统对权限管理的需求,而且能随组织结构或安全需求的变化而变化,具有很好的灵活性和可操作性。

关键词:访问控制;权限管理;RBAC
中图分类号:TP393 **文献标识码**:A **文章编号**:1673-629X(2011)07-0172-03

Optimum Design and Realization of Privilege Management Based on RBAC

XIN Ke, YANG Feng, YANG Guang-xu, MA Yuan-yuan
(School of Information Science & Engineering, Shandong Normal University, Jinan 250014, China)

Abstract: Aimed at the characteristic of Web system and its special demand in access control, it optimizes the classical RBAC(Role-Based Access Control) model and designs a hierarchical privilege management system. This system with a dynamic multi-level web-menu drived by privileges can enhance Web system's usability. The whole system's implementation is via base-class, so it can reduce code copying effectively. Practice proves that this scheme not only can appease complex Web system's requests for privilege management, but also can vary with institutional framework or security demand.

Key words: access control; privilege management; RBAC

0 引 言

权限管理是Web应用系统最重要的组成部分之一,担负着用户分级分类管理、系统和数据的访问控制等重要职责。基于角色访问控制(RBAC)[1]是一种极其重要的访问控制方式,是当前访问控制研究和应用的热点。RBAC经典模型降低了安全管理成本和管理复杂性,解决了传统访问控制和自主访问控制管理难度大的问题[2]。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、通用性好的访问控制机制。文中在RBAC模型的基础上优化设计并实现了细粒度的权限管理模型,并结合权限驱动的动态导航,组成了Web系统的权限管理子系统。该子系统继承了RBAC模型用户和角色混合授权的特点,并提出新的扩展方案,最后给出了设计与实现,使得基于角色的访问控制授权更加灵活、安全性更高、通用性更好。

收稿日期:2010-12-22;**修回日期**:2011-03-02
基金项目:山东省自然科学基金(ZR2010FM021)
作者简介:信 科(1985-),男,山东淄博人,硕士研究生,研究方向为嵌入式系统开发与设计、Web系统设计与开发;杨 峰,硕士生导师,教授,研究方向为嵌入式开发与设计、集成电路设计、信号与信息处理、Web系统开发与设计。

1 基于角色的访问控制(RBAC)

RBAC的基本原理是创建具有某些访问权限的角色,使权限和角色直接相联系,通过给用户分配合适的角色将用户与权限联系起来,用户只有通过激活角色才能获得访问权限,实现了用户和权限的分离[3]。RBAC中定义了4个主要实体对象,分别是用户集、角色集、权限集和会话集[4]。在此模型中,用户集是子系统中可以访问资源的主体;角色集是指一个组织或任务中的工作或位置;一个用户可以从属于一个或多个角色。权限是指对系统中的数据或其它资源进行访问的许可。权限与角色关联,一个角色可以拥有多个权限。当权限被指派到某个角色上时,就意味着这个角色拥有了这个权限,而从属于这个角色的用户也将拥有这个权限。会话则是一个运行时动态概念,即一个用户一定以某个角色的身份使用资源,这一特定的对

应关系就形成了运行时的一个会话[5]。由于在RBAC模型中,资源访问许可被封装在不同的角色中,用户通过角色间接地访问资源,所以可以解除用户与权限的耦合,提高权限管理的效率与灵活性[6]。

尽管RBAC已经得到广泛应用,但传统的RBAC模型仍存在不足之处,主要有以下两个方面:

(1)访问控制不能满足实际应用的需要,Web应用系统需要更加细粒度的访问控制。

(2)该模型仅仅定义了访问控制的内部机制,并没有提出简单友好的访问控制实现方式,而对于Web系统的用户而言,友好直观的用户接口是系统必不可少的组成部分[7]。

2　对RBAC模型的优化

目前,基于RBAC的访问控制一般只能细化到页面资源的粒度,虽然一些访问控制子系统可以实现按钮粒度的访问控制,但是也会因为其缺乏通用性和灵活性而导致使用不便和扩展困难。在该系统的设计中,权限集又细分为访问集和操作集;对象集细分成数据对象集:

(1)访问集(ACC)= $(A_1,A_2,A_3,\cdots,A_n)$ 主要是指在Web系统中的功能导航,如发布通知、部门管理、人事管理等。

(2)操作集(OPS)[8] = $(O_1,O_2,O_3,\cdots,O_n)$ 主要是指在Web系统中功能的操作集,如查询、添加、删除、修改等操作。

(3)资源对象集(RES)= $(R_1, R_2, R_3,\cdots, R_n)$ 主要是指Web系统中的数据资源和页面资源,以上访问集和操作集分别针对页面资源和数据资源而产生。

通过以上定义,可以把访问控制模型形式化描述为五元组 URAOR[9] {Users, Roles, ACC, OPS, RES}。其中:Users代表用户集,Roles代表角色集。由ACC、OPS、RES共同组成的对系统资源的操作权限集可以有 $RES\times2^{ACC\times OPS}$ 种,它代表Web系统中对资源的访问许可集合即角色集。通过以上分析,该设计可以把权限控制粒度细化到对每个系统资源的具体操作,下面给出该子系统的实现。

3　Web系统中权限管理的实现

3.1　权限管理子系统的整体架构

该子系统在Asp. Net平台上设计并实现,在实现过程中,Asp. Net提供的Form验证以及基础的访问控制机制极大简化了该子系统的开发复杂度[10]。子系统架构分为四个模块:数据库模块、对象模块、. Net验证模块、权限管理接口,各模块之间相对独立使得子系统的修改和扩展易于实现。下面是各模块介绍:

(1)权限管理接口主要为管理员提供权限管理接口,其中包括用户管理界面、角色管理界面、权限管理界面。

(2). Net验证模块是Asp. Net中提供的基于角色、权限的Form验证机制和运行时会话集。

(3)对象模块包括用户、角色、资源、操作等实体对象[11]。

(4)数据库模块包括5个表:用户表、角色表、用户 & 角色关系表、权限表、角色 & 权限关系表。

3.2　相关数据库表的设计

用户表用来维护用户的信息,用户 & 角色关系表用来关联用户和分配给该用户的角色,角色 & 权限关系表用来关联角色和授予该角色的权限。以上三个表因比较简单仅做简要描述,下面给出实现该子系统关键的两个数据库表结构,见表1[12]、表2。

表1　角色表

字段名	数据类型	主键	含义
RoleId	int	是	角色编号
RoleName	nvarchar(50)	否	角色名称
Operations	nvarchar(20)	否	操作标识

表2　资源表

字段名	数据类型	主键	含义
ResId	nvarchar(50)	是	资源编号
ResName	nvarchar(50)	否	资源名
LinkAddress	nvarchar(100)	否	链接地址
LinkIco	nvarchar(100)	否	图标地址

(1)角色表除了维护角色的基本信息以外还有一个表示OPS的字段"操作标识",该字段由 n 个字符组成分别代表 $(O_1,O_2,O_3,\cdots,O_n)$ 中的对应位,每一位字符取1或0且分别代表拥有或不拥有该操作权限。把OPS直接与角色绑定的优点是细化权限粒度的同时又可以大大降低资源集的冗余度,如果直接与资源绑定,则会造成"资源表"中数据的指数级增长,为权限管理带来不便。

(2)资源表记录Web系统中功能导航所链接的页面资源,"资源编号"主要用来对页面资源进行访问控制,"资源名"、"链接地址"和"图标地址"是实现动态导航的关键字段。

3.3　系统的实现方法

为了把访问控制以及会话状态集放到Asp. Net容器中去管理,首先需要修改web. config文件,把系统的权限验证方式改为Form验证,并设置非法访问的登录转向页面,详细配置如下:

```
<authentication mode = "Forms">
        <forms timeout = "600" slidingExpiration =
"true" loginUrl = "Login. aspx"></forms>
</authentication>
```

然后创建类文件 UserPrincipal、UserIdentity 分别实现 Asp. net 提供的接口 System. Security. Principal. Iprincipal 和 System. Security. Principal. Identity[12]。

(1) BasePage 类:属性 ResID 表示用户当前访问的页面资源编号;OPS 代表操作集,该字段需要在构造函数中初始化,即从数据库取出用户角色的“操作标识”并赋值;OFlag 表示用户当前执行的操作。方法 IdentifyUser( )除了验证用户的登录信息以外,还会判断用户是否具有访问权限;方法 TestOPS( )验证用户是否有执行当前操作的权限。

(2) AspPage:代表系统中的 asp 页面,所有 asp 页面都需要继承父类 BasePage 并在方法 Page_Load( )中给 BasePage 的 ResID 和 OFlag 属性赋值。例如:用户当前访问的 asp 页面在数据库“资源表”中的编号为 12,则应该把 12 赋给 BasePage 类中的 ResID 属性,父类 BasePage 中的 IdentifyUser( )方法通过把 ResID 和用户拥有的“资源集”作比对来验证用户是否有访问当前页面资源的权限;如果用户当前执行的操作是 $(O_1, O_2, O_3, \cdots, O_n)$ 中的 O_3,则应该把 3 赋给 OFlag 属性,BasePage 通过验证当前用户角色的“操作标识”字段的第 3 位是否为 1,来判断用户是否有执行当前操作的权限。

(3) UserIdentity 类:该类是 Form 验证体系中的用户身份证,该对象依托 UserPrincipal 对象存在。

(4) UserPrincipal 类:该类是 Form 验证体系中的用户对象。

综上,该设计把访问控制细化到了页面、按钮的粒度,能够满足大中型 Web 系统对访问控制的需求。该子系统具有很好的可扩展性和通用性,只需要在现有系统中引入类 BasePage、UserIdentity、UserPrincipal,在数据访问层添加相应的数据访问方法,并在 asp 页面的 Page_Load( )方法中做少量的修改就可以把该子系统集成到现有 Web 项目中。

4 权限驱动的动态导航的实现

虽然以上设计可以实现系统内部对安全性的需求,但是在实际应用中,更加友好、直观的方式是根据用户拥有的权限来动态加载导航。在该子系统中,使用的是一种受权限驱动的基于模板的动态导航生成技术。该模块不仅能够根据用户不同的访问权限加载不同的导航菜单,并且能够控制导航的样式外观,极大地提高了 Web 系统的易用性。

数据库“资源表”中的字段“权限名”是链接在导航中的标题,字段“链接地址”存放该 asp 页面的 URL 地址,字段“图标地址”可以为每个链接设置不同的小图标,使导航菜单更加美观。为了实现多级导航,权限有如下编号规则:一级导航,用 2 位字符编号,范围从 00 ~ 99;以后每下一级导航,都在上一级导航的基础上增加两位。通过这种编码方式,每一个分支最多有 100 个链接,可以满足大中型 Web 系统对导航的要求。

该模块包括两个文件:Left. htm 文件是导航菜单的模板,文件中包含 html 页面的框架,包括 html、head、body 等标签元素,并且在 body 元素中放置字符串“ $ MenuContents”;Left. ashx 是生成动态导航的功能页面,它首先读取 Left. htm 文件内容,然后根据用户角色拥有的权限生成相应的导航内容,最后把“ $ MenuContents”替换为该导航内容。当用户请求 Left. ashx 时,返回给用户的是生成好的 html 导航页面。在系统中集成该模块,只需要把 Left. ashx 文件通过 frame 的方式引入主页,就可以为系统构建一个权限驱动的多级动态导航菜单。

5 结束语

文中在充分利用 ASP. net 提供的 form 验证的基础上,结合实际应用设计并实现了一个较完善的基于 RBAC 的权限管理子系统。该子系统不仅具有 RBAC 的优点而且细化了权限粒度,结合直观友好的动态导航,在保证了 Web 系统的安全性的同时提高了系统的易用性。除此之外,由于该子系统的设计和实现基于统一基类,所以具有很好的通过性和可扩展性,降低了在项目开发中对权限管理子系统的重复设计与开发带来的资源浪费。

参考文献:

[1] Ravi S, Edward J, Hal L, et al. Role-Based Access Control Models[J]. IEEE Computer, 1996, 29(2): 38-47.

[2] 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.

[3] 黄 刚,王汝传,田 凯. 基于 RBAC 策略的可信网格访问控制模型[J]. 计算机应用研究, 2010, 27(4): 1432-1495.

[4] 汪林林,张玉林,张学旺. ERBAC 模型的改进与实现[J]. 计算机应用研究, 2005, 22(10): 3932-3937.

[5] 范明虎,樊 红,伍孝金. ASP. net 中基于 RBAC 的通用权限管理系统[J]. 计算机工程, 2010, 36(1): 143-145.

[6] 佘江峰,冯学智. 基于 ASP. NET 的受权限驱动的多级动态 Web 菜单系统[J]. 计算机应用与软件, 2006, 23(10): 55-64.

[7] 孔令富,孔海娥,冯建周. 基于角色-页面的协同设计[J]. 计算机工程与科学, 2009, 31(9): 5-7.

[8] Andreas S, Jonathan M, Jeremy J. The Role-Based Access Control System of an European Bank [C]//SACMAT. [s. l.]: [s. n.], 2001: 9-11.

(下转第 249)

向量 x_1, x_2, …, x_N 的似然值为:

$$p(x_1,x_2,\cdots,x_N \mid M) = \sum_{s_1,s_2,\cdots,s_N \in s,} \prod_{i=1}^{N} p(x_i \mid s_i)p(x_i \mid s_{i-1}) \quad (9)$$

其中,P 为相对应的状态的概率,$S = \{1,2,3,4\}$ 表示状态的集合。

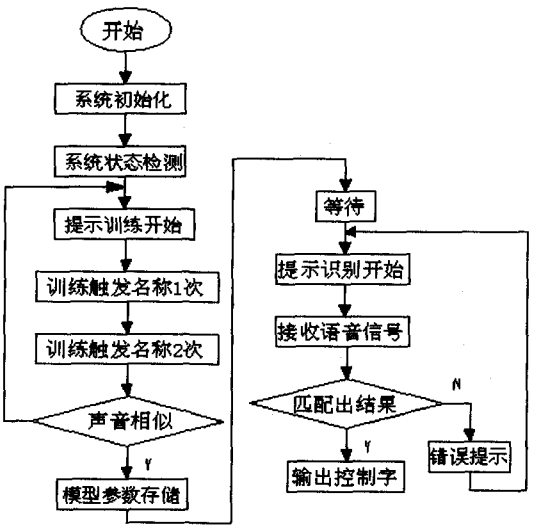

图 4　系统程序流程图

3　实验分析

文中在实验室条件下,使用麦克风单声道来录制采集 10 人说话的语音数据。采样率为 16kHz,每个说话人中 10 个语音段成为训练样本集,其中 6 个语音段作为训练测试集。对语音信号进行特征提取时,选取语音帧长为 410 个采样点,帧移为 160 个采样点,并且对语音帧进行预加重和加汉明窗处理,预加重系数为 0.97。语音信号经过语音训练、HMM 模型匹配识别后,分别提取 LPCC、MFCC、MFCC +△MFCC 的特征参数,由图 5 可见,该 10 人语音识别的识别率为:LPCC 为 88.52%、MFCC 为 91.56%、MFCC +△MFCC 为 92.54%。比较得知识别率以 MFCC +△MFCC 特征提取为最高。由此可知,MFCC +△MFCC 相结合的方法能有效地适用于语音特征参数的提取。

4　结束语

文中介绍了一种基于动态特征参数的 MFCC+△MFCC 相结合的语音特征提取方法,并将此方法应用于嵌入式语音识别系统,与传统的 MFCC 方法比较,

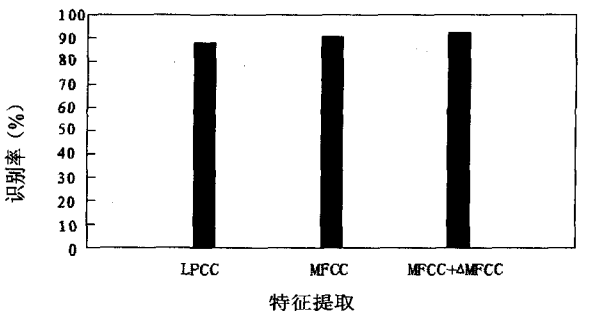

图 5　实验结果分析图

识别性能有较大提高,此方法在语音识别领域中有很好的应用前景。系统硬件结构上采用以 ARMS3C2410 为核心的处理器,加快了系统的处理速度[12],相对提高了语音识别的实时性。

参考文献:

[1] 徐　敏,邹　莹,魏洪兴.一种嵌入式语音识别控制模块的设计与实现[J].厦门理工学院学报,2008,16(4):44-47.

[2] 王坤卿.HMM 模型在语音识别研究中的应用[J].电脑知识与技术,2008,14(7):1966-1968.

[3] 杨　毅,杨　宇,余达太.语音增强及其消噪能力研究[J].微电子学与计算机,2006,23(7):203-208.

[4] 魏　星,周　萍.语音识别系统及其特征参数的提取研究[J].计算机与现代化,2009(9):228-243.

[5] 李弼程,邵美珍,黄　洁.模式识别原理与应用[M].西安:西安电子科技大学出版社,2008:72-98.

[6] Fakhr W,Salam A A,Hamdy N. Enhancement of mismatched conditions in speaker recognition for multimedia applications [C]//IEEE International Conference on Acoustics, Speech, and Signal Processing. [s. l.]:[s. n.],2004.

[7] Rabiner L,Juang Biing-Hwang. Fundamentals of Speech Recognition [M]. [s. l.]:Prentice Hall, 1992.

[8] 韩纪庆,张　磊,郑铁然.语音信号处理[M].北京:清华大学出版社,2004.

[9] 张军英.说话人识别的现代方法与技术[M].西安:西北大学出版社,1994.

[10] Rabiner L E. A Tutorial on Hidden Markov Models and Selected Application in Speech Recognition[J]. Proceedings of The IEEE,1989,77(2):257-286.

[11] 韩　普,姜　杰.HMM 在自然语言处理领域中的应用研究[J].计算机技术与发展,2010,20(2):246-252.

[12] 周立功.ARM 嵌入式系统基础教程[M].北京:北京航天航空大学出版社,2005.

(上接第 174 页)

[9] Richard D,Edward J,Timothy R. Adding Attributes to Role-Based Access Control[J]. IEEE Computer Society,2010(6):79-81.

[10] 陆庭辉,文贵华.B/S 结构下的用户访问控制方法[J].计算机工程与设计,2010,31(7):1433-1436.

[11] 杨　云,刘　军.Web 安全设计之道[M].北京:人民邮电出版社,2009.

[12] 李天平.NET 深入体验与实战精要[M].北京:电子工业出版社,2009.