基于任务的 RBAC 模型设计与应用*

贾晓辉,韩玉民
(中原工学院 软件学院,河南 郑州 450007)

摘 要:由于软件开发过程中设计不科学而造成的软件不安全使用、软件维护工作量大等可维护性问题,是软件开发中经常遇到的问题。RBAC 减少了授权管理的复杂性,提高了访问控制的安全性,从而提高了系统的可维护性,是目前公认的具有发展潜力的访问控制技术。在 RBAC 模型研究的基础上,建立了 T-RBAC 模型,用户对信息对象的访问权限可随执行任务的上下文环境变化,具有很好的安全性,并应用于网络课堂应用系统,提高了系统的可维护性,具有一定的推广应用价值。

关键词:RBAC;T-RBAC;软件工程;软件维护
中图分类号:TP311 **文献标识码**:A **文章编号**:1674-7720(2014)02-0078-04

Designing and application of Task-RBAC model

Jia Xiaohui, Han Yumin
(Software College, Zhongyuan University of Technology, Zhengzhou 450007, China)

Abstract: Due to unscientific designing, problem such as insecurity software use and lots of software maintenance becomes more and more in software development. RBAC policies reduce authorization management complexity, enhance the safety of access control and improve system's maintainability consequently, then RBAC policies becomes the accepted potential access control technology. A model named T-RBAC is established based on the research of RBAC model in the paper, the access authority changes with the context which has better security, then the application of T-RBAC is discussed in net course system which can improve the system's maintainability and can be extended.

Key words: RBAC; T-RBAC; software engineer; software maintenance

近年来,随着电子信息技术应用的迅速发展,计算机应用软件不仅已经渗透到各个行业,甚至也在改变着普通百姓的思维模式,例如越来越多的人对于未知的东西,首先会想到去"百度一下"。计算机应用软件已经不仅仅是解决问题的介质,更多的时候已经被理解成为一种服务。

因为软件维护是软件生命周期时间最长、投入最多的一类活动,因此受到了越来越多的重视。软件的维护工作是否到位,直接影响客户对软件的评价,从而影响到软件的寿命。

软件的可维护性[1]是衡量一个软件维护容易程度的软件属性,通常从软件的可理解性、可修改性及可测试性 3 个方面进行定性分析,因此提高软件的可维护性就是要提高软件的可理解性、可修改性及可测试性。在软件开发初始阶段就要考虑软件的可维护性,以减少软件维护工作量为努力的目标。

现代企事业组织机构中,工作人员的流动性比较大,但是该机构中需要的角色则相对稳定,同时角色在该机构中拥有的权利和义务也基本相同,相比对于工作人员的管理,角色管理更加简单明了、易于执行。同样对于一个拥有大量用户的应用软件来说,引入角色的概念,采用角色进行访问控制同样能够极大地简化管理工作,而且易于维护。能为管理工作提供一个灵活实现安全策略的环境,符合现代企事业管理模式。

如何进行角色管理,成为角色访问控制的核心问题,访问控制的目的就是要防止非授权访问和非授权使用系统资源,同时保证合法用户在授权范围内使用系统。RBAC[2-3](基于角色的访问控制)是将不确定的用户赋予一个确定的角色,将对用户的直接管理转换为对角色的管理,通过对用户分配角色、角色授权实现对用户的管理,这种面向对象的权限分离思想提高了访问控制

* 基金项目:河南省教育厅科学技术研究重点项目(12A520051)

的通用性和可复用性，便于对应用软件的维护。

1 相关工作

RBAC96 自 Sandhu 等提出后，已经成为继自主访问控制(DAC)、强制访问控制(MAC)后出现的公认的具有发展潜力的访问控制技术，其基本思想是通过中间实体——角色实施访问控制策略，通过给用户分配合适的角色，将用户与访问权限相联系，使主要的管理工作变为对角色授权或者更改用户的角色，因此大大降低了管理开销，提高了系统的可维护性。用户、权限、角色之间的关系是：权限描述系统的基本关系，权限派生角色，角色决定用户，用户被赋予角色，权限赋予角色而不是用户，用户通过承担某些角色而获得对系统的访问权限，用户和权限通过角色关联起来。通过角色控制资源对用户的开放程度，将对大量的用户管理转变为少量的角色管理，其基本模型如图 1 所示，包含用户 users、角色 roles、目标 objects、操作 operations、许可权 permissions 5 个基本数据元素。权限被赋予角色，而不是用户，当一个角色被指定给一个用户时，此用户就拥有了该角色所包含的权限。会话 sessions 是用户与激活的角色集合之间的映射，RBAC 与传统访问控制的差别在于增加了角色层而带来了灵活性。

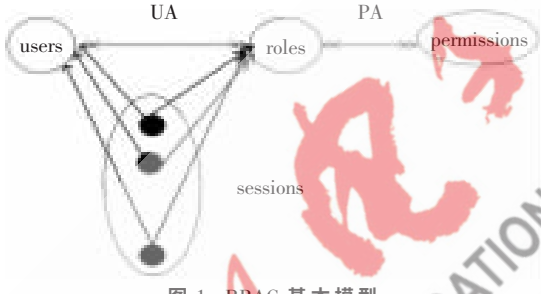

图 1 RBAC 基本模型

针对 RBAC96 模型的角色授权不灵活的问题，杨柳[4]的 ERBAC 针对 RBAC96 模型进行了改进，提出了对用户和角色混合授权的控制模型，如图 2 所示，实现了除角色授权外，同时对用户直接授权，混合授权的方法增加了用户授权的灵活性和可维护性，同时也增加了管理的复杂度；汪林林[5]对 ERBAC 模型进行改进，引入访问规则和模糊时间约束及模块与角色绑定的方法使授权更灵活、系统更安全，但是系统维护工作量大，而且模型针对某应用系统，通用性较差；贾笑明[6]的模型基于人工指定角色及权限而导致的成本高及权限分配不公问题，引入了完备信息系统的信息粒度度量的方法，对角色及权限信息的不确定性进行分析，为系统信息使用提供帮助，但是角色作为一个属性而不是实体，在使用中受限；赵卫东[7]通过引入属性约束及用户组的方法解决授权复杂、不灵活的问题，但是同样增加了关于用户组的分配等工作量，尤其在用户属于不同组时该如何取舍仍然取决于人为操作；李双[8]提出具有约束条件权限清晰的访问控制模型，其直接对权限集划分，降低了角色—权限的授权难度。

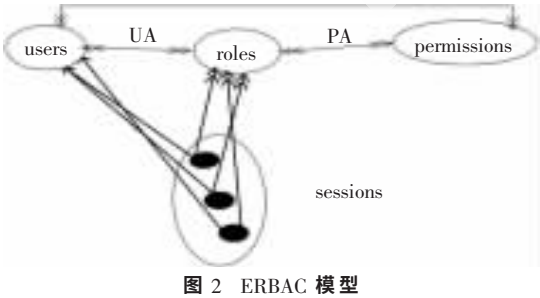

图 2 ERBAC 模型

2 T-RBAC 模型

在进行了大量 RBAC 研究的基础上，结合软件开发、软件维护等工作，考虑到数据与功能点一一对应的关系，以角色为基础，以功能点为资源，权限随着角色使用的功能而授予或者取消，以角色为基础围绕功能点建立安全模型和实现安全机制，在进行任务处理过程中，对信息对象的访问权限随着执行任务的上下文环境变化，提出了 T-RBAC 模型，保证系统使用安全的同时提高了系统可维护性，一定程度上降低了软件维护工作量。模型结构如图 3 所示。

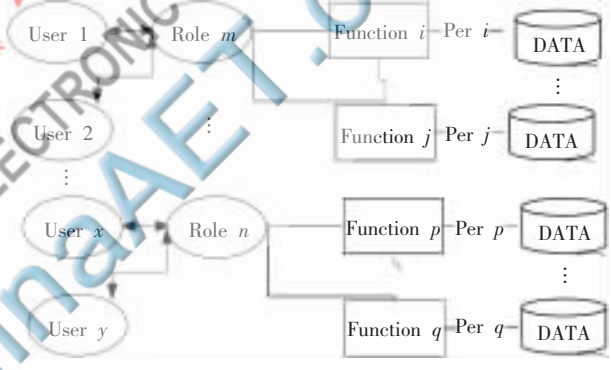

图 3 T-RBAC 模型

T-RBAC 实现了分析和设计的无缝连接，是面向对象分析和设计方法的有效应用。T-RBAC 是对 RBAC 模型的改进，因其提升了系统的安全访问控制而被关注研究，包括用户、角色、资源、用户和角色、角色与资源的关系，T-RBAC 模型比较适合增量开发，其中资源是设计的关键，不需要修改系统代码，即可随不同角色的使用而展现不同的用户界面，有效降低了系统的维护工作量，从而提高了系统的可维护性。以下将介绍 T-RBAC 在网络课堂系统中的分析和设计，并利用 UML 对其进行建模。

3 T-RBAC 模型的应用

3.1 功能分析

网络课堂系统一方面考虑到远程教育能够降低学习成本，另一方面考虑分区办学现状，可以充分利用师资等教学资源，因此得到了高速发展。学生通过网络课堂，可以在课外时间利用网络继续学习，教师利用网络课堂及时了解学生的学习情况，师生可以利用该系统实现在线交流等。基于该系统中涉及到学生、教师、课代

表、教学管理者及系统管理者等不同角色的关于系统的不同使用权限，采用了 T-RBAC 进行访问控制，利用 UML 对网络课堂系统进行分析与设计，通过建模得出权限部分的用例图，如图 4 所示。

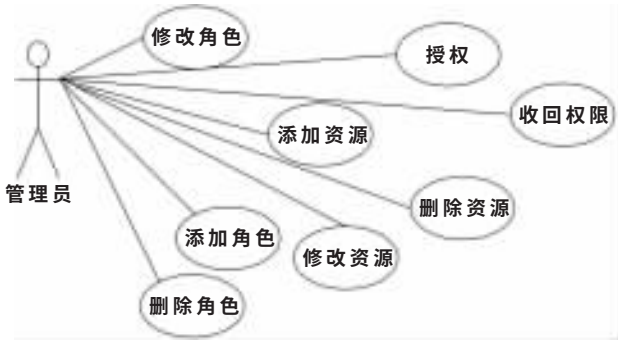

图 4 T-RBAC 用例图

3.2 类设计

网络课堂系统涉及的类比较多（如课程、教师、学生、管理员等），类之间的关系也相对复杂，关于权限部分的设计类图如图 5 所示，主要有 register（注册用户）、role（角色）、source（资源）和 permission（权限），其中角色即系统中的参与者，代表业务工人类型；资源即系统的功能点，根据其上下文关系需明确其父资源；权限即参与者是否拥有对用例的访问权限，其中数据代表某个角色拥有该资源的使用权限，用户对资源的使用权限根据其对应角色是否拥有该资源而变化。网络课堂系统将对学校成千上万的学生管理转变为对各种角色的管理，有效提高了系统使用的灵活度，降低了系统维护的工作量，提高了系统安全性。

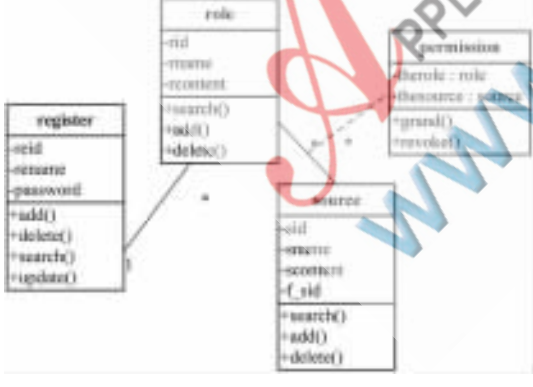

图 5 T-RBAC 类图

3.3 数据库分析设计

T-RBAC 基于关系模型，如图 6 所示。核心是角色（role）、用户（user）、资源（source）之间的关系，其中 role 和 user、role 和 source 的关系都是多-多关系，因此需要第三张表来保存两个表之间的关系。其中表 1 是角色表（角色 ID、角色名称、角色描述等字段，角色 ID 为主键），表示了系统中所拥有的角色集合。表 2 是资源表（资源 ID、资源名称、资源描述、父资源 ID，资源 ID 为主键），表示系统所具有的功能集合，资源之间具有自关联的关系。表 3 为权限关系表（角色 ID、资源 ID、是否拥有该权限），表示了某角色是否拥有对某个资源的访问权集合。表 4 为用户角色表（用户 ID、角色 ID），表示了用户所属于的角色。

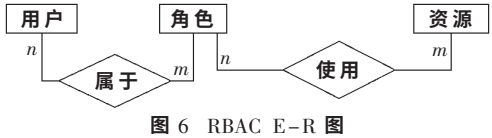

图 6 RBAC E-R 图

表 1 角色表

角色 ID（PK）	角色名	角色描述
001	教师	留作业、改作业、上传资料等
002	学生	交作业、提问、回答等
003	课代表	完成教师交给的任务
004	系统管理员	维护角色、资源等

表 2 资源表

资源 ID（PK）	资源名	资源描述	父资源 ID
0001	注册课程	注册一门课程，拥有对该课程的所有资源	1001
0002	上传资料	教师上传课件等资料	1002
0003	维护个人信息	用户可以修改个人信息	1002
0004	评价作业	教师给学生的作业打分	1003
0005	我的作业	与教师的课程作业相关内容	1003

表 3 权限表

角色	资源	备注
001	0001	教师角色有权注册课程
001	0002	教师角色有权上传资料

表 4 用户角色表

用户 ID	角色 ID	描述
1001	001	张丁的角色是教师，拥有教师对于系统的所有使用权限

3.4 系统实现

网络课堂系统中，注册用户通过系统主页可以登录、进入论坛、下载软件等，系统主页同时显示最新通告及精品课程，如图 7 所示。

图 7 系统主页

系统管理员根据系统需要可以创建角色，同时为角色授权。该角色在使用系统时，可以具备相关权限的使用，授权过程如图 8 所示。

图 8 创建角色

系统管理员通过角色管理为用户指定一个角色，同时也可以为该用户删除某个角色的定义，指定角色如图 9 所示。

图 9 分配角色

T-RBAC 采用功能点作为系统的资源控制粒度，通过权限关系规则实现对系统的安全访问控制，用户对信息对象的访问权限可随执行任务的上下文环境而变化，不同于页面访问控制粒度，也不同于属性访问控制粒度，有效提高了用户对系统的安全使用，同时管理员根据需要指定用户的角色及相关权限，增加了系统的灵活性，有利于系统的维护。该系统适用于层次管理模式的企事业单位或部门。网络课堂平台中使用 T-RBAC 模型后，在对用户的管理上更加有效。

在下一步工作中，将考虑角色的权限继承、同一用户的不同角色权限划分等约束机制，更好地解决系统的安全使用问题。

参考文献

[1] Shi Jimin, Gu Chunhua, Zheng Hong. Software engineering: principles, methods and applications(3rd Editiong)[M]. Beijing: Higher Education Press, 2009.

[2] SANDHU R S, COYNE R, FEIMTEIN H L, et al. Role-based access control models[J]. IEEE Computer, 1996, 29(2): 38-47.

[3] FERRAIOLO D F, KUHN D R. Role-based access controls [C]. 15th National Computer Security Conference, Baltimore, 1992: 554-563.

[4] 杨柳，危韧勇，陈传波. 一种扩展型基于角色权限管理模型(E-RBAC)的研究[J]. 计算机工程与科学，2006，28(9)：126-128.

[5] 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，2009，26(10)：3929-3937.

[6] 贾笑明，韩道军，王宝祥. RBAC 中基于概念格的角色评估[J]. 河南大学学报(自然科学版)，2013，43(1)：85-90.

[7] 赵卫东，毕晓清，卢新明. 基于角色的细粒度访问控制模型的设计与实现[J]. 计算机工程与设计，2013，34(2)：475-479.

[8] 李双. 一种扩展的基于角色的访问控制模型[J]. 计算机工程与应用，2012，48(19)：54-60.

(收稿日期：2013-09-30)

作者简介：

贾晓辉，女，1972 年生，硕士，副教授，主要研究方向：数据库，软件工程。