B/S 应用系统中的细粒度权限管理模型①

王成良 姜 黎 (重庆大学 软件学院 重庆 400044)

摘 要: 针对 B/S 模式下的油库网络信息系统的实际需求,为提高用户权限管理的动态性和授权访问的安全性,结合基于角色的访问控制原理,提出了一种在 B/S 应用系统中针对用户人员复杂、职务变动频繁特点的细粒度权限管理模型。该模型把资源的访问权限按细粒度分解,实现了由粗到细,不同级别的权限控制,既可进行角色授权也可直接用户授权,大大改善了用户权限管理的灵活性和可扩展性。

关键词: 角色;RBAC;权限;细粒度;面向用户授权

Fine-Grained Privilege Management Model and Its Application in B/S Application System

WANG Cheng-Liang, JIANG Li (School of Software Engineering, Chongqing University, Chongqing 400044, China)

Abstract: To meet the actual demand of oil network information system in B/S model, and to improve dynamics of users' authority management and security of authorized access, this paper presents a fine-grained privilege management model combining the role-based access control principle for the fact that users are complicated and they change jobs frequently in B/S application system. This model decomposes the access privilege of sources by fine-grained, and realizes access control of different levels from coarse-grained to fine-grained, and this model cannot only authorize the role but also authorize the user directly, which greatly improves the flexibility and scalability.

Keywords: role; RBAC; privilege; fine-grained; user-oriented authorization

近年来,随着互联网的普及,基于 B/S 模式的信息管理方式以其可扩展性和可维护性成为 MIS 应用的方向。具有一定规模的 B/S 模式下的信息系统以集成性和多用户为特点,完善的权限管理可以有效保护应用系统的操作安全性以及明确系统操作人员的岗位权责。目前,在企业环境中的访问控制方法一般有三种:自主型访问控制方法、强制型访问控制方法、基于角色的访问控制方法[1](RBAC)。其中,自主型访问控制方法通常采用的一种安全机制是访问控制表(ACL),这使授权管理处于较低层次,管理复杂、代价高、易于出错。强制型访问控制方法是根据客体中信息的敏感标记和访问敏感信息的主体的访问级对客体访问实行限制的一种方法,这种访问控制的缺点是访问权限不能由用户修改。RBAC 是目前公认的解决大型企业的统一资源访问控制的有效方法。其显著的两大特征是:1)减少授权管理的复杂性,降低管理开销; 2)灵活支持企业的策略,并对企业的变化有很大的伸缩性[1]。但一般的 RBAC 访问控制方式在权限管理方面,存在以下几个方面的不足:

(1) 权限维护复杂。在传统的基于角色权限管理模型中,权限分配统一由管理员角色实施。但在大规模分布式环境下,完全依赖管理员集中式管理将给工作带来很大困难。

(2) 灵活性差。在大型企业中,部门众多,人员复杂。系统用户因职务需要,权限变化频繁,导致角色的过度细分,从而失去角色存在的意义。

(3) 授权力度粗。不同用户的访问层次不同,对于具体到控件级别的权限控制,传统模型实现困难。

由于传统 RBAC 访问控制方式很难满足大型信息系统权限管理的需求,根据 RBAC 模型,本文提出了一种在 B/S 应用系统中可二次权限分配的细粒度权限管理方法,并在实际项目油库网络管理系统中得到了

① 收稿时间:2009-10-16;收到修改稿时间:2009-11-12

很好应用。

1　基于角色的权限控制模型

RBAC(Role Based Access Control)模型即基于角色的访问控制模型，它包括三个实体：用户、角色和权限。在 RBAC 中，用户就是一个可以独立访问计算机系统中的数据或资源的主体。角色是指一个组织或任务中的工作或者位置，它代表了一种权利、资格和责任。权限就是允许对一个或多个客体执行的操作。RBAC 引入了角色的概念，目的是为了隔离用户和权限。角色作为一个用户与权限的代理层，解耦了权限和用户的关系，所有的授权应该给予角色而不是直接给用户，从而实现了用户与访问权限的逻辑分离。传统通用的基于 RBAC 基本思想的数据库 ER 关系图如图 1 所示。这种方案是最常见也是比较简单的方案。

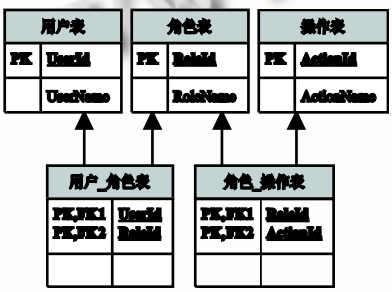

图 1　基于 RBAC 的传统模型

2　RBAC权限管理模型的改进

在以往的 B/S 模式系统中，权限管理通常只精确到页面级别，即甲角色有权访问 A、B 页面，乙角色有权访问 C、D 页面。考虑这样一种情况，某油库网络管理系统中，开票作业室部门拥有开票室主任和开票员两个角色，均可访问系统中的业务管理模块并进行一定操作，由于两个角色的职责不同，开票室主任可以在发油管理页面下进行发油开票、退单、季度/年度发油记录报表浏览、打印等操作，而开票员虽也能进入发油管理页面，但只能进行发油开票、退单操作。所以，为了满足上述不同角色在同一页面中拥有不同操作权限的需求，需要一个更细粒度的权限访问模型。

一个 B/S 模式系统中，最小的(也即不可再分的)功能单位是页面中的控件，如文本框、按钮、超链接等。而不同的操作权限归根到底是能够对不同页面上的功能控件进行操作。如果在页面控件级别进行权限的划分与分配，这样的权限管理就是最小粒度的权限管理。

2.1 模型系统概述

分析某公司油库网络系统的需求，油库分多个部门，每个部门拥有多个职位，相同部门的不同职位之间以及不同部门的不同职位之间，可能都有权访问同一功能模块的同一页面，只是在页面上的操作权限不同；有时，一个职位可能会被临时赋予更大的操作权限。如果将职位看做权限管理中的角色，那么一种改进后的 RBAC 模型可以满足上述需求，该模型所对应的数据库 ER 关系图如图 2 所示：

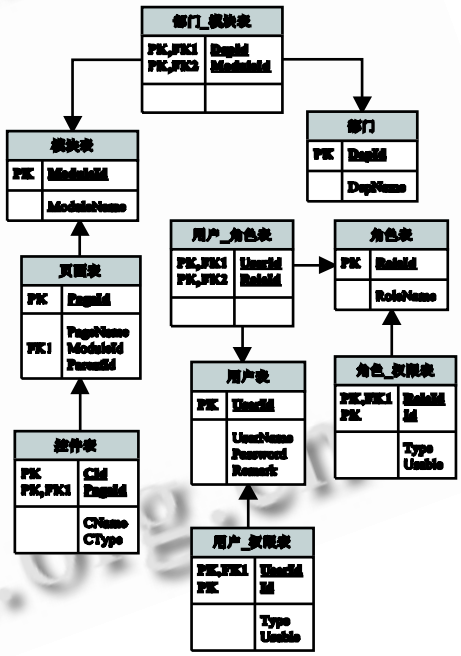

图 2　基于 RBAC 的细粒权限管理模型

改进后的 RBAC 模型包括以下四个实体：

* 资源：系统中资源，主要是各种业务对象，通常表现为页面、菜单、按钮等界面元素，包括功能模块中的所有页面和功能控件。

* 操作部门：访问资源的角色所在的部门，如销售部、财务部等。

* 用户：应用系统的操作者，每个用户都可以拥有一个或多个角色，用户具有该角色对应的操作权限。

* 角色：根据权利和职责而划分的在任务中的工作或位置，是一组功能权限的集合。例如系统管理员、

销售部门管理员等。一个角色有若干个功能权限。

2.2 功能权限的实现

与传统的设计相比，保留了用户表、用户角色表、角色表和角色权限表。对 RBAC 模型的改进过程包括：

(1) 细化权限系统的控制粒度。将要进行访问控制的系统资源分为三个层次：功能模块、页面、功能控件。功能模块是系统页面集合的一个划分，所有功能模块构成系统页面的全集，而任两个模块的交集为空。页面与控件是拥有关系，一个页面可拥有多个控件，而一个控件只能属于一个页面。因此在数据库设计中，对应的设计三个表，即模块表、页面表、控件表，保存模块划分信息、页面信息(包括页面与模块的关系)、控件信息(包括控件与页面的关系)。如此设计，可使系统在权限控制的粒度上拥有很大的伸缩性。

当角色只需要粗粒度的权限分配，比如部门管理员角色拥有其所在部门的所有功能模块的操作权限，那么对该部门管理员分配权限时只需勾选对应模块，即将所选模块下的所有页面、所有功能控件的操作权都赋予给该部门管理员。

当角色需要较细粒度的权限分配时，比如属于某一部门的普通操作员角色，只允许其访问该部门对应功能模块下的某一些页面。对该角色分配权限时则只需勾选相应的模块、页面，即将指定的页面访问权限赋予给该角色。

有时候不同的角色都能够访问同一页面，但在同一个页面的操作权限不一样。比如，角色 A 能在页面中进行查询、添加、删除、修改操作，而角色 B 在页面中只能进行查询、添加操作，不能进行修改、删除操作，这时候就需要细化到控件级别的权限分配。在权限分配时需要勾选相应的模块、页面、控件。

对角色的权限分配数据存放在角色权限表中，当用户访问系统时的后台逻辑分为资源过滤与越权阻挡两个步骤。首先，用户输入 ID 与密码登录，系统在验证了用户合法性后提供一个界面让用户选择其登录角色，随后即根据登录角色从角色权限表中取出其对应的可访问资源来构建系统导航菜单以及页面显示，角色无权访问的模块与页面不会出现在导航菜单中，角色无权访问的功能控件不会显示在页面上。这样就过滤掉了对该角色无关的信息。其次，在用户点击导航菜单打开某一页面或者点击某一功能控件时，系统后台逻辑会进行一次权限判断，若是合法用户才能让其继续操作。经过这两个步骤，便能有效地防止用户的越权行为。

(2)增加部门表与部门模块对应表，实现可二次授权管理的功能。权限的细粒度分配往往带来一个弊端，就是角色冗余问题会非常严重。很多角色可能拥有大量的相同权限，其被创造出来只是为了体现在某一细节上存在区别。如果只由一个管理员来管理潜在数量很大的角色群体是不现实的，很容易出错。解决这个问题的方法之一是实现权限可二次分配。

在角色表中有一个 roleType(角色类型)字段，该字段数据为：系统管理员、部门管理员、普通操作员。在权限系统中默认存在一个系统管理员角色，该角色拥有所有资源的访问权限。每个部门有一个部门管理员角色。系统管理员只负责创建部门管理员角色，部门管理员拥有本部门所有资源的访问权，负责添加属于本部门的普通员工角色并对其进行权限配置。

实际应用中，每个部门并不需要和所有的模块都发生联系，往往只操作几个模块。为了提高授权安全性，需要限制部门的权限，建立一个部门模块对应表来存放部门与模块之间的对应关系。系统中的角色都是属于具体部门的角色，无游离于部门之外的角色。图 2 中角色表中的 deptID 字段存放该角色所属的部门编号。当部门管理员创建一个新角色时，系统逻辑根据该部门管理员所属部门拥有的模块访问权限，在用户界面上构建一个权限列表，该部门无权访问的模块被过滤掉。这样使部门管理员只能创建出该部门权限范围内的角色，防止出现被创建者权限高于自身的情况。

部门模块对应表的另一个作用是在用户登录时，系统逻辑根据用户登录的角色获取该角色所属部门有权访问的模块，以这些模块为根结点生成用户界面导航菜单，不属于角色权限的功能模块与节点将不会在导航列表(或菜单)上出现。

权限可二次分配能有效降低系统管理员的负荷、降低工作出错的可能，也更符合企业部门的实际管理方式。

(3)增加用户权限对应表。该表使用户权限配置更加灵活。解决角色冗余问题的方法之二是面向用户授权。

在企业中，系统用户的职责有时会变化，用户权限也要随之变化。因为业务需求灵活多变，系统的功

能可能不断地增加或更新，角色的权限就要随着业务的调整经常发生变化。很多时候就因为这些不断的变化，创造出很多拥有细微权限差别的大量角色。有时当拥有某角色的用户需要被临时分配某种操作，而属于同一角色的其它用户并不具有该项权限，此时也需要添加一种新的用户角色，但在此工作完成后，该项权限将被收回，新添加的角色将被删除。这样操作起来过于繁琐。因此增加用户权限表来支持直接对用户进行授权操作。系统不再需要预创建大量只有细微差别的大量角色，当有权限变更的需求时，管理员可以将权限直接授予需要的用户。变更取消时，管理员直接取消用户的特定权限。

以上功能权限控制的扩展设计还是以角色授权为主，辅以对用户授权，有效地弥补了 RBAC 角色授权机制管理相对生硬的缺陷，使得权限管理变得更灵活和安全有效，同时符合现代化企业组织结构的管理特点。

3　细粒度权限管理模型的应用

某公司的油库网络信息系统是有多个应用平台、应用系统、功能节点组成，是一个集数据采集、自动控制、安全监控、业务处理、综合管理、决策支持等功能于一体的大型综合集成应用系统。其中涉及权限管理方面的是系统管理平台，它包括：模块管理、页面管理、角色管理、用户管理等，该平台面向系统管理员围绕用户部署与权限配置，有效管理系统资源，为用户提供系统管理、部署、维护、扩展等功能，实现系统的一体化管理。

在实际应用中，用户进入登录页面，输入用户名和密码以及验证码，如果输入正确则从用户_角色表中读取出属于他的角色信息列表。如果登录用户只有一个角色，则登录成功后直接进入系统主界面。当登录用户有多个角色时，将出现角色选择界面进行角色选择，然后进入系统主界面。获得用户所属的角色后，再根据角色_权限表和用户_权限表获得该角色拥有的权限，推出对该用户显示的界面。当用户调用某功能时，通过查看用户的权限集合能够准确地判断用户是否有权操作。图 3 是系统权限管理的流程图。

4　结语

实践证明，改进后的 RBAC 权限管理方法具有较好的效果，体现了安全性和完整性的设计概念。在维持 RBAC 模型基本框架不变的基础上，增加了权限可二次分配与面向用户授权，丰富了传统模型对功能权限的控制，提高了授权管理的可操作性，有效解决因为细粒度权限控制带来的角色冗余问题。同时将角色分属于不同部门，使授权管理符合企业的安全策略。与通常的 RBAC 权限控制系统相比，本文采用的细粒度 RBAC 权限管理模型保证了被授权用户安全达到对特定资源操作的目的。

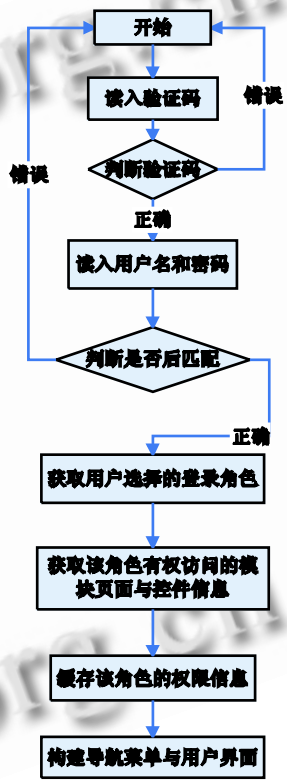

图 3　权限管理模块流程图

参考文献

1　周文峰,尤考军,何基香.基于 RBAC 模型的权限管理系统设计与实现.微计算机信息, 2006,22(5-3):35－36.
2　林伟炬,刘列根,张宁.一个通用的权限管理模型的设计方案.微计算机信息, 2009(15):7－9.
3　李璇,刘杰,吴岳辛.一种细粒度下的基于角色的访问控制模型.电信科学, 2008(8):86－89.
4　吴江栋,李伟华,安喜锋.基于 RBAC 的细粒度访问控制方法.计算机工程, 2008,34(20):58－60.