基于角色的访问控制模型在保理业务中的应用①

Application of Factoring Management System Based on RBAC Model

张玲玲　祖向荣　(华北电力大学 计算机科学与技术学院 北京 102206)

摘　要： RBAC 模型是当前应用最广泛的一种访问控制机制。本文阐述了 RBAC 模型的基本原理，针对基于 Internet 的电力系统自身特点，提出一种加入组织结构的 RBAC 模型，并在系统授权时采用分级授权的方式，减轻管理员的负担，减少出错机率，增加权限管理的灵活性。给出了处理私有权限的方法，描述了用户登录和获得权限的过程；设计了访问控制数据库的结构；讨论了设计的合理性、适用性。

关键词： RBAC 模型　访问控制　组织　权限

1　引言

保理全称是保付代理，英文为 FACTORING。是指卖方（供应商）与保理商间存在一种契约关系，根据该契约，卖方将基于其与买方（债务人）现在或将来订立的货物销售/服务合同所产生的应收账款转让给保理商，由保理商为其提供下列至少一项的服务：信用风险控制与坏账担保、贸易融资、应收账款的催收或销售账管理。保理业务在国内正在迅速发展，由于保理业务中的数据都是需要极端保密的，因此系统的安全工作就显得异常重要。既要防止非法用法的侵入造成数据破坏，也要防止合法用户的非法操作带来的不良后果，甚至造成企业的重大损失。目前，基于角色的访问控制(RBAC)是一种比较适合在企业中实施的访问控制技术，可以简化权限管理，增加系统的可靠性。本文针对保理业务自身特点，在 RBAC 模型的基础上设计一种更加适合保理业务的 RBAC 模型。

2　RBAC 模型概述

RBAC 模型的基本原理是在用户层面和权限层面中间加入角色，用户与角色相关联，角色与权限相关联，通过将合适的角色赋给用户，使用户具有角色所具有的权限，实现了用户与权限的分离。在 RBAC 中涉及到以下几个主要概念：①USERS(用户),②ROLES（角色）,③PERMISSIONS（权限），④SESSIONS（会话）。

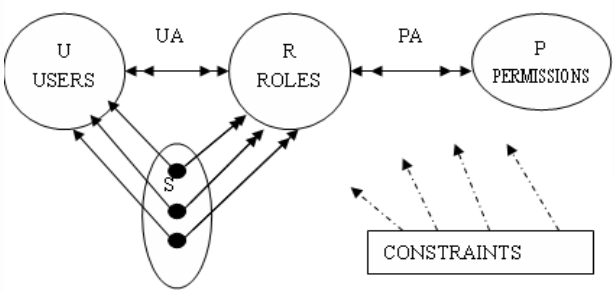

图 1　RBAC 模型各组成部分关系

图 1 描述了 RBAC 模型各组成部分的关系，一个用户(U)可以有多个角色(R)，一个角色也可以被分配给多个用户，用户-角色是一个多对多的关系；一个角色可以有多个权限(P)，一种权限也可以被分配给不同的角色，角色_权限也是一个多对多的关系；用户要对资源进行访问必须建立一个会话，一次会话只能对应一个用户，但是一次会话中用户可以激活用户具有的多个角色。

3　保理业务中的 RBAC

RBAC 的一个重要属性是 RBAC 自身是中立于策略的，即 RBAC 是用于表达策略而不是实现一个具体

① 收稿时间:2008-08-01

的安全策略[1]。这就为它适应各种不同的需要打下了基础，各种系统可以根据自己的需求来调整策略，使之具体化，详细化，从而实现系统的安全策略。由于本保理业务管理系统是基于 Internet 的，因此系统涉及到不同地理位置的用户。而且不同地理位置的用户还可能拥有相同的权限，只是各自属于不同的单位组织，比如，有两个子 Factoring 公司（F1,F2）的项目审核人，他们都可以对各自客户提出的保理项目进行审核，只是 F1 的审核人不能审核 F2 的客户提出的项目，F2 的审核人也不能审核 F1 的客户提出的项目。因此，保理业务管理系统中的 RBAC 模型引入了组织单位，在指定角色的同时指定相应的组织单位。另外上级角色不一定能继承下级角色的所有权限，为了解决私有权限问题，在系统中引入私有权限，公有权限，私有继承，公有继承等概念。

3.1 组织单位

保理业务管理系统通过划分组织结构来实现用户、角色和资源的层次性。系统中将用户分为内部用户与外部用户，内部用户指电力系统内部员工，而外部用户指电力公司的客户，外部用户通过此系统来实现与保理公司的业务来往。

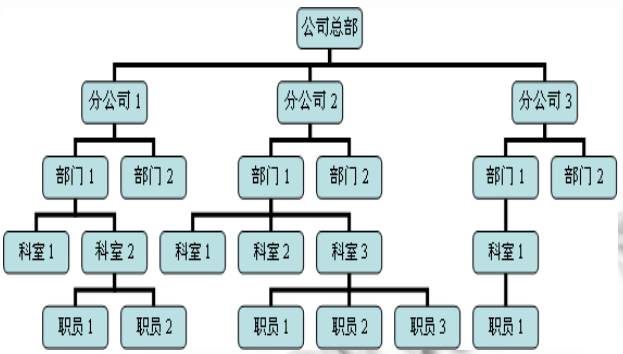

图 2　组织结构图

图 2 展示了基于 Internet 的保理业务管理系统的组织结构，公司分为总公司和分公司，总公司和各分公司都相对独立，总公司对各分公司有监督权利，但不能代替分公司做具体业务。

系统中的 Users：是所有使用此系统的用户，包括内部用户（Factor 公司）和外部用户（Factor 公司的客户）。内部用户均属于某个层次中的一员，即属于某个组织单位的一员。外部用户则没有组织结构。

Roles：是系统中的所有角色，内部角色的划分按照组织结构的层次来划分，与各层次的具体岗位对应，所以角色也具有层次性。上级角色不一定完全具有下级角色的全部权限，但是对下级角色有监督的权利，督促下级来完成相应的任务。外部角色是公司客户所具有的角色。所有客户都具有外部角色。

Permissions：是权限的集合，包括对方文件，数据的增、删、改、查、计算，申请，审批等。

Object：在系统中将操作对象分为两部分：一部分是系统的功能结构，表现为系统结构的菜单树，这部分资源是用来展现系统功能的。如果某用户具有对某资源的可见权，那么系统将为此用户展现此资源；反之，资源对于用户是不可见的，也就没有具体的操作权限。另外一部分是具体操作数据的按钮，如果用户对数据有操作权限则按钮是可使用的，反之，如果用户没有某操作权限，则相应按钮变为灰色，不可用。

3.2 系统的授权方式

系统采用分级授权方式来进行授权。由于系统是基于 Internet 的，用户众多且分散， 如果所有授权工作均由管理员来完成，那么管理员的工作将非常繁重，也增加了出错的机率。所以根据组织结构采用分层管理，各级负责的模式，更能提高效率。

图 3　分级授权示意图

如图 3 所示，管理员只负责公司总部内部的授权工作，而把分公司的授权工作交由分公司的管理员来做。分公司的管理员负责给各部门经理分配权限。而科室的权限则由部门经理来分配。这样上一级只负责给下一级的用户分配权限，并且只有科室以上层次才

可以给其他用户分配权限，每个用户在登录时，系统计算出他自己本身的权限，如果具有相应的权限，那么他才可以给他下一级的用户分配权限。

3.3 角色关系

在角色继承时，为了保证系统的安全性，在系统中上级角色不一定能继承下级角色的所有权限。在这里采用文献[2]中处理私有权限的方法，将权限分为公有权限和私有权限。公有权限可以被上级角色继承，而私有权限则不能被上级角色继承，是该角色特有的权限。对系统中的所有大主题、小主题进行权限标注，并将权限类型设为公有权限或私有权限，一个角色可以被付予多个权限（可以是公有权限也可是私有权限），上级角色在继承该角色时，通过判断该角色的权限类型来继承，该角色的所有公有权限均被继承，而私有权限则受到保护，不能被继承。上级角色在继承下级角色时，也分为公有继承和私有继承，上级角色公有继承下级角色时，下级角色的公有权限仍保持其公有的性质，还可被再上一级的角色继承；而上级角色私有继承下级角色时，下级角色的公有权限要转变为私有权限，再不能被其他角色来继承。这在某种程度上实现了角色继承的有限性，也就是说可以控制角色继承的深度。

对角色间的各种约束，则根据系统的结构层次和实际业务来描述，比如出纳和会计这两个角色就是冲突角色，一个用户不能同时具有这两个角色。对项目具有审核权限的角色必须是具有部长角色的用户才能被分配，这属于角色依赖。这些都是静态分配好的。

3.4 系统访问控制

在保理业务管理系统中，借助目录服务来实现认证策略。目录服务提供跨平台身份信息存储管理和认证支持功能。具体说，目录服务是指以一定的格式记录了大量企业资源信息，并将各种资源信息集中管理起来，以对象的方式予以记录，明确设定每个对象的“身份”和“位置”。目录服务提供用户身份认证和授权机制。

当用户登录系统时，系统根据用户输入的用户名，密码及用户的组织单位，通过用户信息表（USER_INFO）来判断用户是否属于合法用户，在用户信息表中保存了用户的详细信息，内部用户登录时必须输入自己的组织单位，以此来区分各个不同组织中的用户，如果是外部用户，则输入用户名、密码和用户类型（external），系统根据用户名、密码和用户类型来判断用户是否为合法用户。用户身份认证是为了避免非法用户登录系统造成危害。

用户一旦通过身份认证，就应该对此用户进行授权，系统根据用户身份认证时记录下来的用户的信息，在用户–角色表(USER_ROLE)中来获得用户所具有的角色（r）.再根据授权表（PERMISSION）得出用户所具有的操作权限，因为角色可能是被多个分公司共用，所以在这儿要利用用户的组织单位来匹配 PERMISSION 表中的组织单位，只有组织单位与用户的组织单位相同的操作权限才能被赋给用户，然后将此记录在一个 Hashtable（相当于一个容器）中，此后在用户执行某项操作时，就检查此 Hashtable，看用户有没有执行此操作的权限，如果有,允许执行，否则，则说明用户不具有此操作权限，拒绝执行。这就保证了合法用户执行的是合法的操作，增强了系统的安全性。下面描述获取权限的过程：

```
// 1. 获得登录用户的角色
    List roleList = getRoleList(userId , userDep)
// 2. 在 PERMISSION 表中取得 roleId 的权限，将用户登录信息及权限放入 HT 中
Public Hashtable getUserAuth (roleId,userDep) {//根据角色和用户单位来查找权限
    Hashtable ht = (Hsshtable) getRolePerm(roleId,userDep);
  return ht;
}
```

4 系统的数据库设计

实现系统授权时，涉及到如下的几张表：

(1)用户信息表（USER_INFO）

用户信息表中保存了系统中所有用户的信息，初

始化时，系统只有管理员一个用户，管理员可以增加其他使用此系统的用户。

(2)角色表(ROLE)

角色表中保存系统中的所有角色，角色按照系统的组织结构，以及系统的功能来划分。所有角色均由管理员在角色管理模块中录入。

(3)资源表（OBJECT）

资源表中记录了系统中所有可用资源，对应了页面中的菜单树，菜单以及各种按钮，表中 OB_ID 字段是本表中的 ID，代表 ID 资源的上一级菜单。

(4)用户_角色（USER_ROLE）

用户_角色表记录的是用户所具有的角色，每个用户的所有角色均记录在此，用户的权限通过角色所具有权限来获得，角色有什么权限，那么被指派了这个角色的用户就具有什么样的权限。

(5)角色权限表(PERMISSION)

角色权限表为角色指定了各种权限，角色与资源的关系是一个多对多的关系，一个角色可能能对多个资源进行操作，多个角色也可能要对同一个资源进行操作，并且一个角色对同一个资源可能有多种操作权限，也可能只有一种操作权限，也可能没有操作权限。

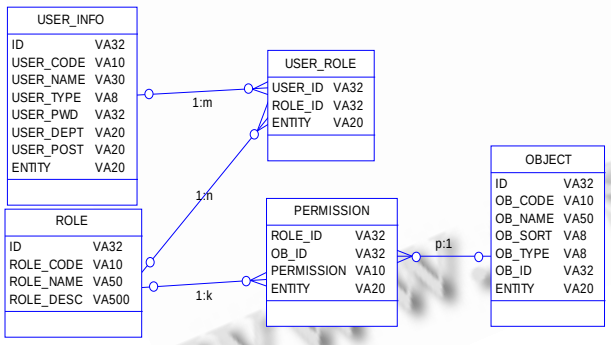

图 4　权限表关系

5　适用性

(1)按保理业务本身组织结构划分的角色，对应了实际应用中的岗位。按保理业务本身组织结构划分的资源，对应了实际应用中每个岗位要处理的对象。岗位的职能，就是角色对对象的处理权限.模拟实际情况设计的角色有更大程度的灵活性。

(2)由于系统基于 Internet,各分公司的结构大致相似，岗位角色可能重叠，在系统设计时为用户和资源都加上组织单位，那么重复的角色就可以在各分公司共用，只要在给角色分配权限时带上组织单位，用户在获取权限时用户的组织单位必须与资源的组织单位相同，这样就实现了角色的共用。

(3)分级授权原则更具有实际意义，也更符合实际情况。系统增加一个用户时，总是人事部门确定要增加，并把他分配到相应的部门，但是具体的工作则是由部门来具体安排，所以每个用户由上级来分配具体角色比统一由管理员来分配角色，更符合实际。

6　结束语

基于角色的访问控制是一种适合企业管理，提高企业系统安全的灵活有效的访问控制策略，它能够根据各企业的不同特点，建立适合的权限控制方式。本文根据 RBAC 模型的基本思想，结合保理业务管理系统基于 Internet 的组织情况，介绍了在设计系统时应该考虑系统的组织结构，以及如何处理组织中的角色关系；并给出了在系统授权中用到的数据表结构。文中加入组织结构的 RBAC 模型在保理业务管理系统的实际开发中已经在运用。

参考文献

1 Ferraiolo DF,Sanehu R. Proposed NIST standard: Role based access control. ACM Transactions on Information and System Security,2001, 4(3):224–274.

2 顾春华,肖宝亮.RBAC 模型层次关系中的角色权限.华东理工大学学报(自然科学版),2007,33(1):96–99.

3 Sandhu RS,Coyne EJ,Feinstein HL,and et. al.control models. Role 一 based IEEE Computer,1996,29 (2):38–47aCCesS.

4 王保义,于晓波.电力工作流中基于组织与任务的访问控制模型.电力系统自动化,2007,31(4):51–55.