计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2020,29(11):250−254 [doi: 10.15888/j.cnki.csa.007640]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

# 具有可维性的三维权限控制模块①

张荣荣[1], 甘清华[2]

[1](河南师范大学 软件学院, 新乡 453007)
[2](易思科讯 (深圳) 有限公司 研发部, 深圳 518057)
通讯作者: 张荣荣, E-mail: rflyingr@163.com

**摘　要**: 针对跨国跨地区的供应链和多公司集团企业, 在角色访问控制 (Role-Based Access Control, RBAC) 的基础上, 加入组织和角色组, 提出三维权限控制模块.该体系遵循 RBAC96 和 ARBAC97 的模式, 控制用户 Web 访问资源和业务执行的最小权限集合. 本文采用 Java 语言开发基于 MS SQL Server 2012 数据库的权限系统模块, 实现权限体系的可复用和可扩展.快速应对企业业务变化.

**关键词**: 三维权限控制; 最小权限集合; 组织; 控制单元; 角色组

引用格式: 张荣荣,甘清华.具有可维性的三维权限控制模块.计算机系统应用,2020,29(11):250–254. http://www.c-s-a.org.cn/1003-3254/7640.html

## Three-Dimensional Access Control Module with Dimensionality

ZHANG Rong-Rong[1], GAN Qing-Hua[2]

[1](College of Software, Henan Normal University, Xinxiang 453007, China)
[2](R&D, Ecvision Co. Ltd., Shenzhen 518057, China)

**Abstract**: For transnational, trans-regional supply chain and the group enterprise, on the basis of Role-Based Access Control (RBAC), adding the organization and role group, three-dimensional permissions control module is proposed, which follows RBAC96 and ARBAC97 mode and controls users minimum permission set of access to web resources and business implementation. Permissions system module is developed using Java language based on MS SQL Server 2012 database and can be reusable and extended. Therefor, it can response business change rapidly.

**Key words**: three-dimensional access control; minimum permission set; organization; control unit; role group

## 1　引言

随着 Internet 网络的普及, 信息安全是企业的头等大事[1]. 有效的权限机制是充分发挥系统功能的前提. 现代企业越来越体现为多公司、多工厂、多地点的集团化发展模式, 管理复杂, 涉及人员多, 职能多, 分工细致, 对权限控制的要求越来越高、越来越细, 而且企业的业务变化也变得越来越快. 因此, 具有可复用性和可扩展性的功能完善的权限机制是一个企业信息系统必不可少的部分. 近些年, 对于企业级别安全管理的研究得到普遍关注[2–4], 但是目前基于角色访问控制 (RBAC) 的授权模式权限体系, 大部分只能针对设定的组织内进行权限控制, 有的也可以在不同组织之间复制角色授权, 但是彼此之间缺乏联系. 当新增加业务涉及到新部门或者新第三方的时候, 这些授权模式就很难满足企业的要求. 本文在 RBAC 的基础上, 引入组织, 实现三维授权, 快速响应业务的变化.

## 2　三维权限控制的提出

权限管理主要有 3 种方法[4,5]: (1) 基于安全级别、集中管理的强制访问控制 (Mandatory Access Control,

① 收稿时间: 2020-03-12; 修改时间: 2020-04-12; 采用时间: 2020-04-21; csa 在线出版时间: 2020-10-29

MAC), 它的主要特征是对所有主体及其所控制的客体实施强制访问控制. 它为这些主体及客体指定敏感标记, 然后, 系统通过这些标记来决定一个主体是否能够访问某个客体, 因此, 系统可以防止特洛伊木马的攻击. MAC 对专用的或简单的系统安全保护是有效果, 但对通用、大型系统不太有效果; (2) 基于授权规则、自主管理的自主访问控制 (Discretionary Access Control, DAC), 它是指主体对客体进行管理, 由主体决定是否将客体访问的权限或者部分访问权限授权给其他主体, 因此, 主体定义自我客体的访问权限时, 不会影响到其他客体, 但是, DAC 为了最大程度的适应系统应用过程, 一般会对权限定义得较低, 用以保证任何主体在访问过程中不会出现无法访问的问题, 所以 DAC 一般适用于通用的、大型系统, 对于安全性要求不是太高的系统; (3) 基于角色的访问控制 (RBAC)[6], 其中 RBAC96 和 ARBAC97 是 RBAC 领域的基准模型, ARBAC97 提出了模型内自我管理和分布式管理的思想, 但是存在管理递归问题. SARBAC 和 ARBAC02 是针对 ARBAC97 改进的访问控制模型. SARBAC 模型提出了管理范围 (Administrative Scope) 的概念, 设计了专门用于管理角色层次关系的 RHA 系列, 包括 RHA1、RHA2、RHA3、RHA4; ARBAC02 保留了 ARBAC97 模型的主要特征, 增加了新的概念—组织结构, 改进了粗粒度授权. 然而, 目前很多企业的业务变化比较快, 需要迅速调整业务流程, 一般的基于 RBAC 的授权很难对新的业务流程进行管控.

本文在 RBAC 的基准模型基础上引入了组织和角色组, 增加授权的维度, 以求解决对新部门或者涉及新的第三方的权限授权问题.本文中组织区别于 ARBAC97 中引进的组织结构, 除了隔离权限, 还包括隔离业务流程和基础资料等, 并引入组织之间关系 (汇报关系, 上下级关系等), 增加一个组织就相当于增加了一套相对独立的业务系统. 这套系统又是跟其他组织之间存在着信息流、物流和资金流的同步和互通, 能快速地响应业务变化. 组织从微观讲是一个公司内的不同业务部门, 例如财务部门, 采购部门, 销售部门等; 从宏观来讲, 是不同的公司, 供应商, 工厂等, 组织起到隔离公司业务权限、流程和基础资料等功能, 方便子公司扩展和集团的战略调整. 角色组是多个互斥角色的集合, 能给小企业和个体用户在单用户下集中管理业务.

总的来说, 在 RABC 的基础上, 引入组织概念, 把角色、业务流等基本环境隔离到不同的维度, 可以快速地响应集团公司业务变化. 角色组则是把业务和角色集中到同一维度, 方便对小企业和个体用户的集中管理.

## 3 权限策略

权限策略的基本思路: 首先权限依赖于组织, 每个组织具有不同属性, 绑定不同业务, 对应不同的业务权限, 所以, 组织决定权限. 同时, 用户被组织所隔离, 用户在组织中行使权限, 因此, 角色组织中隔离、脱离了组织的角色是无意义的; 其次, 角色组, 角色, 用户和权限都是被组织分隔在不同的环境中的, 用户对应着角色或者角色组, 权限对应着角色或者直接对应着用户.

组织分为控制单元和业务单元, 控制单元是用于划分不同独立财务核算的公司或者子公司的操作单元. 每个控制单元隔离不同组织的财务核算; 业务单元是具有业务功能的组织单元, 对应相应抽象的业务权限, 每个单元下都有若干角色或者包含多个角色的角色组, 每个角色有若干权限, 同时每个单元下面又有可能有多个不同团队 (用户组), 每个用户组具有相应不同权限. 宏观的层次大概分为: 组织->权限、业务单元->权限、角色 (组)->权限、用户组->权限, 如图 1 所示. 下面从微观的角度分析角色之间关系, 组织和组织之间的关系, 角色与组织之间关系.

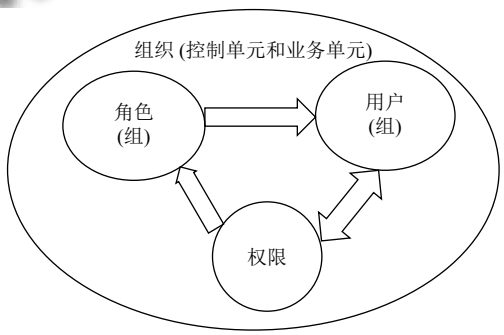


图 1 多维权限结构图

### 3.1 角色 (组) 的继承与互斥

角色的设计遵循 RBAC96 和 ARBAC97 的模式[7]:

(1) 角色之间存在父子关系, 但跟面向对象的继承有所不同, 父角色拥有子角色的全部公共权限, 但不能

访问子角色的私用权限.

(2) 一个用户可以拥有多个角色, 但是不能存在互斥的角色, 互斥角色就是防止用户作假, 例如审核员与采购员互斥, 财务会计与销售员互斥等.

(3) 角色组是一组角色的组合, 这是为需要多个角色的用户方便授权而设计的. 登陆到系统中只能有一个角色, 但是该用户可以自行切换到相应角色, 执行相应操作.

### 3.2 角色与组织的关系

角色依赖于一个组织, 角色只能在某个组织 (公司) 下建立. 一般一个公司常用的组织有财务组织、采购组织、销售组织, 库存组织. 组织在这里起到隔离作用, 同样角色被隔离于不同的组织空间内, 它们之间互不干涉, 这对一些大型商务电子网站和多公司的集团公司比较重要. 由于使用的用户从属于不同的公司, 然而这些用户可能扮演着同样的角色, 但是相同角色的用户未必权限就相同, 这就需要组织来隔离.

### 3.3 组织与控制单元

对于大的集团公司来说, 旗下拥有不同的子公司, 因此需要不同的控制单元来进行划分他们之间财务核算和基础资料. 不同的子公司再在控制单元下划分相应的组织.

### 3.4 组织与业务单元

业务单元是具有业务功能的组织单元, 执行组织下的不同业务内容, 与对应的组织单元形成汇报关系或者上下级关系.

## 4 权限实现流程

在用户登录系统后, 首先通过控制单元隔离到对应的核算单元, 接着判断用户所处的业务单元, 限定业务权限范围. 如果组织下还存在细分的业务单元, 则再细分权限的范围, 在组织中一般会存在若干角色, 接着根据用户的角色 (角色组), 授予该组织的业务权限. 如果不存在对应角色, 则把该组织的全部业务权限授予用户. 登录的用户一般根据用户所处的业务单元、角色来决定的用户的完成业务的最小权限, 生成对应的操作菜单, 如图 2 所示. 本文采用 Java 语言实现权限的粗粒度控制和细粒度控制和基于 MS SQL Server 2005 的数据库设计.

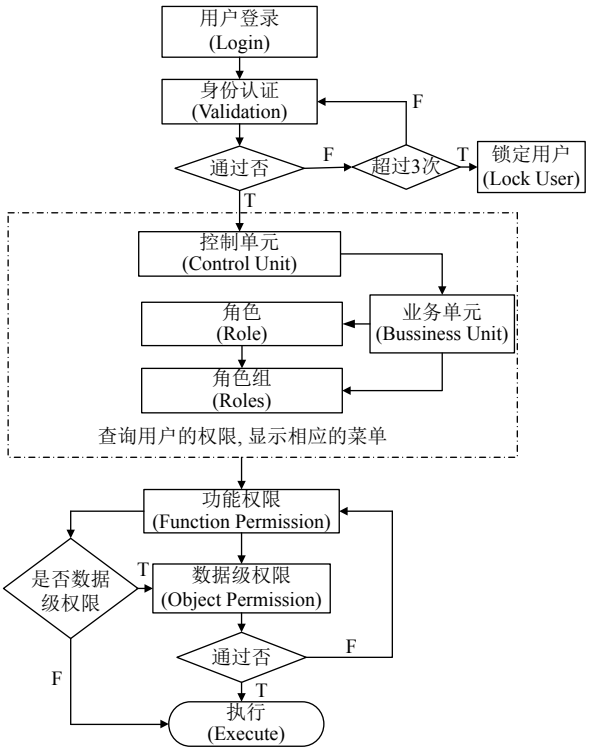


图 2 权限控制流程图

### 4.1 粗粒度和细粒度的权限实现

本文采用面向对象语言 Java 实现粗粒度权限和细粒度权限控制, 分别对应着功能权限和实体权限. 功能权限 (function permission) 给用户提供对单据的增加 (add)、删除 (delete)、修改 (update)、查看 (view) 和审核 (audit) 5 个基本权限, 共同实现功能权限接口 (ifunction permission), 开发人员可以根据需求实现功能权限接口开发其他功能权限. 实体权限 (object permission) 主要分为读权限 (read)、写权限 (write) 和锁权限 (lock), 读权限可以细分为对某些字段的可见和不可见; 写权限细分到对某个 (某些) 字段的可写或者不可写, 这在审核的功能权限中要经常使用到; 锁权限一般针对某个单据挂起的权限. 实体权限的共同接口是 IObjectPermission.

```
Public Interface IFunctionPermission {
Permission getFunctionPermission(User user,
Role role,
Organization org,
ControlUnit unit)
throws Exception;
Menu getAvailableMenu(Permission permission)
```

```
throws Exception;
    }
    Public Interface IObjectPermission {
    Permission getObjectPermission(User user,
    ICompositeObjectID objectID)
    throws Exception;
    Boolean checkAccess(User user,
    ICompositeObjectID object, int permission)
    throws Exception;
    }
```

考虑到 Internet 网络的及时性, 为提高系统响应速度, 专门设置常用数据管理服务器, 这些系统属性和用户权限常用数据将长驻内存, 会把所有业务用户的权限分配, 组织分配、角色分配和对应的菜单树, 在 Web Server 启动过程中一次性从数据库读到内存中, 用户登陆的过程中直接读取内存中准备好的实体对象数据.

### 4.2 数据库设计

数据库是系统运行的基础, 权限系统模块成功的关键. 在本文中的权限系统模块涉及到权限项表 (T_Permission), 组织权限表 (T_OrgPermission), 角色权限表 (T_RolePermission), 业务权限 (T_Bussiness Permission); 用户实体涉及用户角色组织关系表 (T_UserRoleOrg)、角色表 (T_Role)、用户表 (T_User)、用户组表 (T_UserGroup)、控制单元 (T_ControlUnit)、组织表 (T_Org); 字段级数据控制涉及数据对象权限表 (T_DataObject Access), 字段权限控制策略表 (T_FieldAccessStrategy). 用户角色组织关系建立起用户、角色、组织的关系, 控制单元起到隔离各个组织 (公司). 权限项衔接组织、角色、业务, 组织链接角色, 用户属于组织, 分配角色. 图 3 为各个主要表的概念模型.

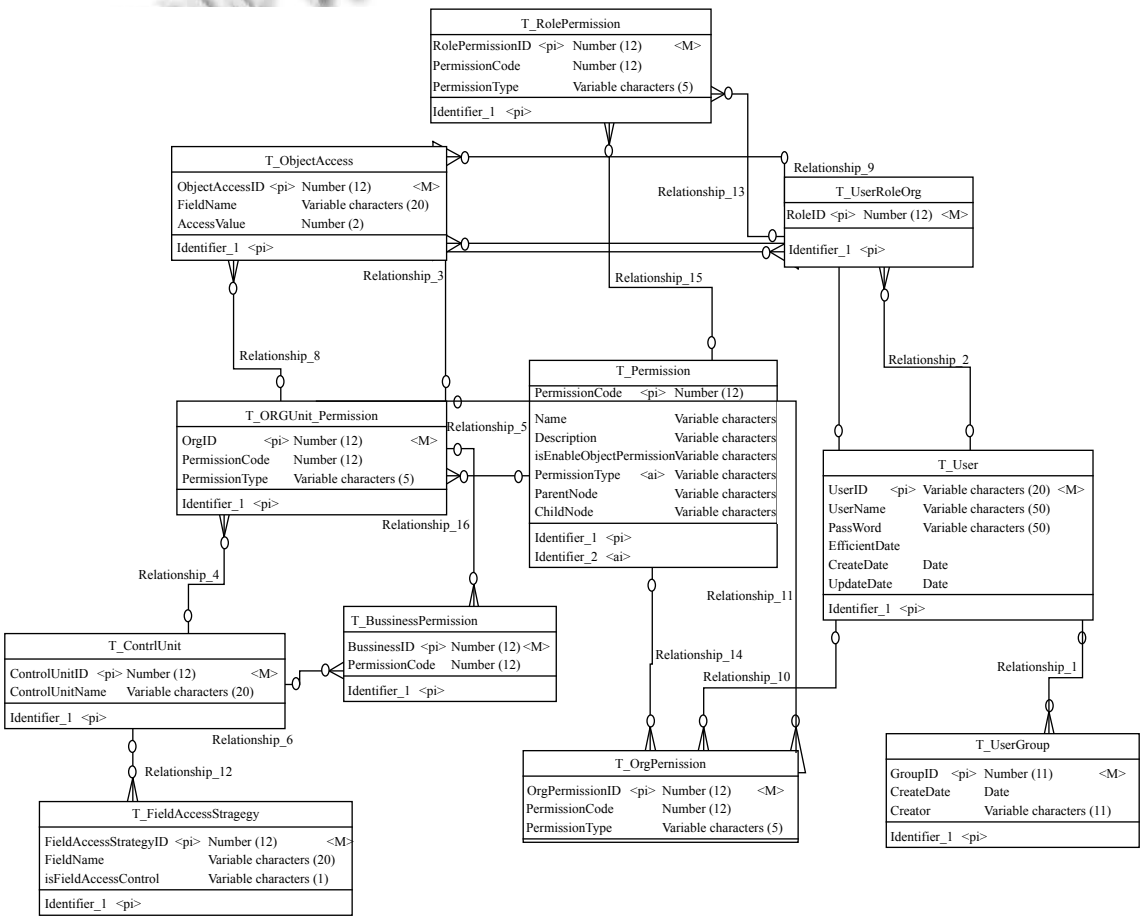


图 3 概念模型

### 4.3 权限模块的实例应用与验证

本权限模块已经在制造和零售行业的 ERP 系统中得到应用, 权限模块主要分为: (1) 组织单元管理; (2) 角色 (组) 管理; (3) 用户管理; (4) 访问控制规则管

理. 其中组织单元管理包括建立组织单元、公司, 添加对应的业务单元, 用户组, 人员以及组织之间的关系; 角色管理主要是建立对应的角色, 添加对应的用户, 下面以采购员授权为例说明.

首先创建采购员所在的组织单元—采购组织, 这样就限定了采购员的业务权限, 接着创建该人员的角色—采购员, 进入访问控制规则管理模块创建规则, 如图 4 所示的授权界面, 其主要包含业务对象、授权对象和权限动作, 采购业务对象是复合数据集, 因此选择复合数据集; 授权对象包含成员、角色组和组织, 用户可以选择多维度授权: (1) 可以选择角色直接授权; (2) 选择通过组织获取的业务权限进行授权; (3) 通过成员, 选择对应的用户和相应权限动作授权.

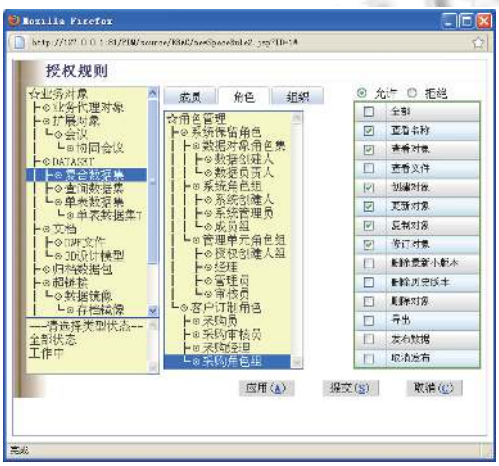


图 4 授权操作界面

基础资料, 业务流程, 角色等基本环境是可以通过组织隔离和封存, 通过三维授权模式, 用户很容易根据新业务, 复制和删除已有的业务模块, 形成新的业务模块和授权机制. 因为这样就很容易实现对新业务控制了, 极大提高软件可复用性, 减少开支.

## 5 结束语

为了满足跨国跨地区的供应链和多公司集团企业中分工的精细化, 集中控制, 分层管理的需求, 本文探讨和开发了独立的权限管理模块. 该模块采用 RBAC 模式作为基础, 实现业务权限最小化, 增加了组织和角色组, 能快速地管理新的业务流程, 降低授权的复杂度和管理难度. 采用组织进行业务环境的隔离, 很好地支持集团公司的扩张, 能够很容易地控制新的业务; 采用角色组使小型企业粗粒度管理, 减少人员管理. 总的来说, 三维权限控制提高了系统的适应性和安全性.

## 参考文献

1 王凤英, 程震. 网络与信息安全. 北京: 中国铁道出版社, 2006.
2 栗松涛, 李春文, 孙政顺. 一种新的 B/S 系统权限控制方法. 计算机工程与应用, 2002, 38(1): 99–101, 235. [doi: 10.3321/j.issn:1002-8331.2002.01.032]
3 戴莹莹, 希凡. 基于角色的访问控制在 B/S 模式中的研究与实现. 交通与计算机, 2006, 24(2): 124–127.
4 吴耀华, 李宁. 适用于 B/S 结构的 RBAC 模型研究及实现. 计算机应用, 2004, 24(S2): 84–87.
5 杨薇, 杨永国, 陈雪. B/S 模式下访问权限控制的研究与应用. 计算机安全, 2009, (7): 78–80. [doi: 10.3969/j.issn.1671-0428.2009.07.025]
6 Sandhu RS, Coyne EJ, Feinstein HL, *et al*. Role-based access control models. Computer, 1996, 29(2): 38–47. [doi: 10.1109/2.485845]
7 Schaad A, Moffett J, Jacob J. The role-based access control system of a European bank: A case study and discussion. Proceedings of the 6th ACM Symposium on Access Control Models and Technologies. Chantilly, VA, USA. 2001. 3–9.