一种超细粒度权限模型研究与应用

陈占芳[1]，顾健[1]，张晓明[2]，马腾飞[2]，姜晓明[1]，郝明[1]
（1.长春理工大学 计算机科学技术学院，长春 130022；2.中国白城兵器试验中心，白城 137000）

摘 要：访问控制是保护系统安全的重要防护之一，对RBAC方法进行深入研究，通过对办公业务的分析与借鉴细粒度访问控制方法的思想，提出一种基于角色的超细粒度权限模型（SFG-RBAC），使角色管理更加方便快捷。在该模型中把角色与单位、部门联系在一起，使具有相同角色的不同的单位、部门访问不同资源的权限问题得到解决。

关键词：访问控制；权限模型；角色
中图分类号：TP301.6 **文献标识码**：A **文章编号**：1672-9870(2016)01-0088-04

Research and Application of A kind of Super Fine Grained Model

CHEN Zhanfang[1], GU Jian[1], ZHANG Xiaoming[2], MA Tengfei[2], JIANG Xiaoming[1], HAO Ming[1]
(1.School of Computer Science and Technology, Changchun University of Science and Technology, Changchun 130022; 2.Baicheng Ordnance Test Center, Baicheng 137000)

Abstract: Access control has important significance in the information platform. This paper has further studied model of RBAC, through the analysis of office business and reference the theory of finely granular access control, and put forward a kind model of super fine grained based on RBAC which makes the role management more convenient and quick. In the model, it makes the roles associated with the units and departments, that make questions which the same roles in different units and departments have permission to access different resources has been resolved.

Key words: access control; authorization model; role

Inheritance(继承)是类(class)之间的一种层次关系。在一般的面向对象语言中,类层次自动对应了一种类型(type)层次[1],这样,super-class和sub-class之间的关系自然是super-type和sub-type之间的关系。

保护系统安全离不开访问控制,其原理是通过特定途径显示的限制或允许用户访问的范围和能力,根本目的是解决合法用户非法访问系统资源和非法用户入侵系统的问题。其中有一种细粒度访问控制方法[1],思想是依据访问对象的粗细程度,把对象进行细化与区分,细化到不能再分解的按钮或链接。传统的访问控制有两种:自主访问控制(Discretionary Access Control,DAC)和强制访问控制(Mandatory Access Control,MAC)。另外还有一种访问控制类型,即基于角色的访问控制(Role-Based Access Control RBAC)。在20世纪90年代,RBAC技术被Ferraiolo和Kuhn提出的,该方法易被理解,易管理,灵活性好,逐渐成为大众的访问控制技术。

RBAC模型虽然使用范围最广,并能够实现访问控制权限,但是它仍然存在一些缺点:模型的最小权限约束粒度不够细化;权限集合与实际用户操作的权限集合不能完全相等;在权限管理中需要多次访问角色表、权限表和功能表,运行损耗比较大;具有相同角色的用户访问不同资源时难以控制范围。通过对实际生活中的单位与部门中的日常办公流程进行研究,为了满足其办公需求,对RBAC模型进行研究与改进,提出一种基于角色的超细粒度权限模型(Super Fine Grained-RBAC,SFG-RBAC)。在模型中引入单位和部门,减少角色分配的复杂度,并把角色的权限区分到超细程度。

收稿日期：2015-10-27
基金项目：吉林省政府重点工作项目（2012-CZ01）；吉林省科技发展计划项目（20105013）
作者简介：陈占芳（1980-），男，博士，副教授，E-mail：chenzhanfang@cust.edu.cn

1　RBAC访问模型

RBAC的权限管理和维护远远低于传统的访问方法，复杂性低但灵活性高，节省了系统的开销。在RBAC技术中，其最特别的地方就是引入了角色，把用户和权限这两个对象隔离开，解耦了两者之间的关系。把权限授权给角色，而不是用户，当用户想要获取某些权限时只需被赋予相对应的角色即可，使系统的用户–权限变化更加的方便。

RBAC访问技术就是把用户和权限分开，角色是两者的链接枢纽，如图1所示，三者之间是多对多的关系。

图1　用户角色权限之间的关系

(1)用户(u)：计算机的使用者，访问计算机中的数据或管理计算机中数据的主体，一般情况下为人。

(2)角色(r)：是用户和权限的中间层，它表示的是功能与责任。

(3)权限(p)：表示的是操作的许可，例如对计算机中数据的修改、删除等。

(4)用户角色分配：也可被称作授权，即是给用户分配一个角色。

(5)权限分配：就是给角色分配权限，分配权限的规则以最小特权为主。

(6)会话：是一个映射，当用户和角色发生关系时就建立了一个会话。

在使用RBAC模型的时候需要遵守三个安全原则：

(1)最小权限原则：$\exists\ r\in$ROLE，且 $p(r)\in$PERMISSION，那么 p 一定为最小。也就是说当给某个角色分配权限时，这个权限一定是该角色可完成任务的最小权限，此原则是为了保护系统中数据的安全，防止角色拥有过多的权限而进行非法操作[1]。

(3)责任分离原则：$\exists\ r_1$、r_2，$r_1\cap r_2=\Phi$，那么 $\forall\ u\in(r_1\cap r_2)$。也就是说两个相互独立互斥的角色不能被一个用户所拥有。在这里责任分离可分为动态和静态的两种。

(3)数据抽象原则：数据抽象就是把数据按照同一类型特征进行分离，分离后的数据可作为操作的资源，当系统想要对数据进行读、写等操作时，只需要使用操作集[3]。

RBAC模型是目前访问控制管理中应用最多也是最广泛的模型，但是随之研究的深入和信息系统业务的创新，RBAC模型的缺点也逐渐暴露出来，RBAC模型具体的优缺点[4]如表1所示。

表1　RBAC模型的优缺点

优点	缺点
1.易被人理解； 2.易管理，灵活性好； 3.应用范围广，特别是在大规模的应用中； 4.适应的安全策略。	1.对主、客体的关注度不平衡； 2.对客体的管理方法不够； 3.对操作行为缺少管理。

2　超细粒度权限模型

2.1　多级复杂业务模型的分析与构建

通过对业务实际权利分配流向的考察与研究，提出一种多级复杂业务模型，模型中在五个等级，分别为高级、中上级、中级、中下级及下级，如图2所示。在模型图中，高级角色可以查看和管理中上级角色、中级角色、中下级角色和下级角色，但中上级角色、中级角色、中下级角色和下级角色只能向上查看高级角色，但不能管理高级角色。以此类推，可总结为上级角色可查看和管理下级角色，当下级角色只能查看上级角色而不能管理。在单位、部门业务办公中，每级单位都对应着许多部门，每个部门中存在许多的业务。处于不同层次的部门也具有相同的性质。因此利用模板技术对每个层次的部门建立一个模板。部门业务模板是处于同一个层次中的部门共同具有的属性和业务标准。不仅规定了这些部门的属性，同时也管理着不同层次的业务部门。对同一级的业务部门同一配置部门的角色和权限。

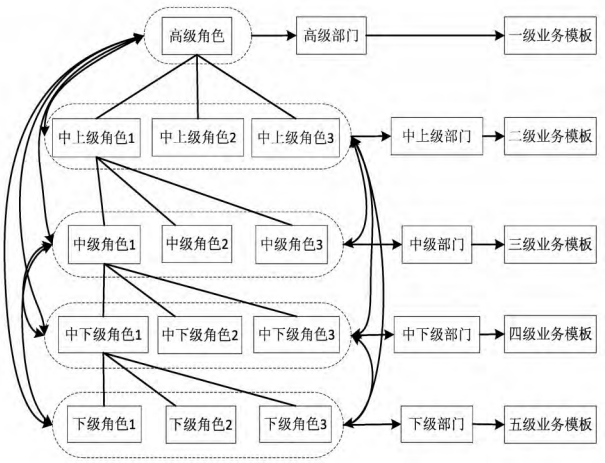

图2　多级复杂业务模型

2.2　超细粒度权限模型的分析与构建

在日常业务办公中，多数业务如多级负责业务

模型中所示，十分复杂，为了满足实际多级负责业务的需要，本文对功能权限进行进一步的细化，提出一种基于角色的超细粒度访问权限模型（Super Fine Grained–RBAC，SFG–RBAC），如图3所示。在该模型中，引入单位和部门组，让角色与单位及单位下的部门引起联系，并且由于在日常业务办公中涉及的上下级、部门的种类复杂、繁多，因此把功能权限的粒度划分的更加详细。

定义1 基于角色的超细粒度权限模型的基本要素为USERS、UNITS、DEPARTMENTS、ROLES、PERMISSIONS、Resources 和 SESSIONS，其中USERS为用户集，是对系统中的资源进行访问的主体，UNITS是单位集，PERMISSIONS是部门集，ROLES为角色集，是对系统中权限分配的载体，Resources为资源，即系统中被访问的数据，SESSIONS是会话集，代表了一次实例化的过程。

定义2 单位集（UNITS）单位是系统管理中最大的对象，单位的范围最广，包含的内容最多。

定义3 部门集（DEPARTMENTS）部门是单位的下属，许多个部门组成一个单位，一个单位可以包含多个部门，但一个部门只属于一个单位。

单位集UNITS=$\{u_1, u_2, u_3, \cdots, u_n\}$。

部门集DEPARTMENTS=$\{d_1, d_2, d_3, \cdots, d_n\}$。

用户集E=$\{e_1, e_2, e_3, \cdots, e_n\}$。

角色集R=$\{r_1, r_2, r_3, \cdots, r_n\}$。在此模型中角色与单位、部门向关联，因此角色$r_i$是一个三元组（$o_i$，$u_i$，$d_i$），其中$o_i$是角色，$u_i$和$d_i$为与角色有关的单位、部门信息。

在此模型中元素之间存在如下的关系和规则：

定义4 用户角色委派，在此模型中有两个委派集EU和ED，EU⊆E×U，就是给用户E分配一个与单位u有关的角色集；ED⊆E×D，就是给用户E分配一个与部门d有关的角色集。此时D⊆U即该部门是属于该个单位之下。

定义5 角色权限委派，在此模型中有两个委派集RU和RD，RU⊆R×U，即给与单位u有关系的角色一个权限集，RD⊆R×D，即给与部门d有关系的角色一个权限集。

规则1 $\forall u \in$UNITS，$\forall d \in$DEPARTMENTS，那么$\exists\{d_1, d_2, d_3, \cdots\} \subseteq u$，$\neg\exists\{d_1 \in u_1 \wedge d_1 \in u_2\}$。即一个单位可以包含多个部门，但一个部门只属于一个单位。

规则2 $\forall u \in$UNITS，$\forall d \in$DEPARTMENTS，那么$P(u) > P(d)$。即单位的权限集一定大于部门的权限集。

通过分析与比较，超细粒度权限模型与其他模型相比，具有更加精细的粒度划分功能，在该模型中把权限划分的更加的详细与准确，权利层次划分的深度也加大，使菜单下不具有再分的原子；角色管理更加的方便快捷，在该模型中把角色与单位、部门联系在一起，可以使具有相同角色的不同的单位、部门访问不同资源的权限问题得到解决，并且因此单位具有大的权利集合，因此在单位下的部门，只需要在该直属单位的权限集内再进行权限选择与划分，令权限分配更加的方便。

3 模型应用实例

高考信息化平台是基于SFG–RBAC模型而开发的，其办公业务符合多级复杂业务模型。在高考信息化平台中，五个角色可分别对应省招办、地区招办、县区招办、学校和班主任。

五个角色的权限分别为：

省招办：根据招生工作安排，完成系统信息设置

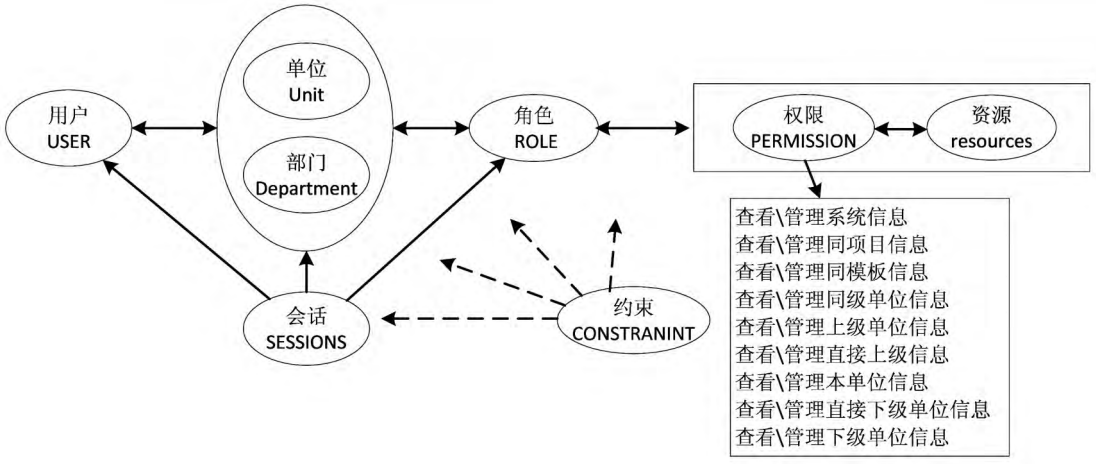

图3 SFG–RBAC权限控制模型

图4　单位业务关系

和基础数据初始化工作；对地区招办提交的数据进行检查、汇总、导出并归档；

地区招办：对所管辖的县区进行录入、管理和配置，并对县区招办用户进行授权控制；对县区提交的数据进行核实，无误后提交数据到生招办；

县区招办：对所管辖的学校进行录入、管理和配置，并对学校进行授权控制；图像信息的采集和上传；对学校提交的数据进行核实，无误后提交数据到地区招办；

学校：录入、统计班级信息，包括班级的个数、人数等；生成考生报名序号及密码；以班级为单位打印用户名和密码；在考生确认的基础上进行核实并确认，无误后提交数据给县区；

班主任：与考生讲解网上报名的步骤、注意事项及时间安排等，并确认考生的基本信息。图4显示的为高考平台中单位之间的业务关系。

4　结论

本文对访问控制和RBAC模型进行了研究，分析其优缺点。通过对办公业务的调研，设计出一种通用的多级复杂业务模型，并通过对此模型的研究，提出一种基于角色的超细粒度访问权限模型（SFG–RBAC），该模型把权限划分的更加的详细与准确，权利层次划分的深度也加大，减少了角色配置的复杂度。该模型在高考信息化平台中进行了实际应用，实现了权限管理和配置的灵活性，可以满足其在各种信息化平台中的应用。

参考文献

[1]　吴江栋，李伟华，安喜锋.基于RBAC的细粒度访问控制方法[J].计算机工程，2008，34(20)：52–54.

[2]　刘建生，彭行顺.控制模型综述[J].计算机与数字工程，2010(7)：115–117.

[3]　张晓明，韩冬松，马腾飞，等.基于角色访问控制模型的研究与改进[J].长春理工大学学报：自然科学版，2012，35(4)：122–124.

[4]　张小勇.基于角色的访问控制模型在Web信息系统中的设计与实现[D].南京：南京理工大学，2011.