T-RBAC模型在ERP系统中的研究与实现

杨宗凯,李 琴,肖 宇,许 炜
(华中科技大学 电子与信息工程系,湖北 武汉 430074)

摘 要:ERP系统的动态权限控制已成为影响其应用与安全的重要问题。文中研究ERP系统中几种常用的权限控制模型,分析它们各自的优缺点。针对模型的动态性和角色的生命周期约束,结合RBAC与TBAC模型,采用T-RBAC模型,通过工作流程引擎实现了ERP系统的动态权限控制,并成功应用于东莞某印刷企业。

关键词:企业资源规划;基于角色的访问控制;基于任务的访问控制;工作流引擎
中图分类号:TP311 **文献标识码**:A **文章编号**:1673-629X(2007)01-0009-03

Research and Realization of T-RBAC Model in ERP System

YANG Zong-kai, LI Qin, XIAO Yu, XU Wei
(Electronic and Info. Dept., Huazhong Univ. of Sci. & Tech., Wuhan 430074, China)

Abstract: The dynamic access control of ERP system has become an important problem on application and security. Studies several different access control models, analyzes the advantages and disadvantages of them. Considering the dynamic characteristic of models and the lifecycle of roles, uses T-RBAC model which combines RBAC and TBAC model to implement the dynamic access control of ERP system by workflow engine. All these have been successfully applied in a printing enterprise in Dong Guan.

Key words: ERP; RBAC; TBAC; workflow engine

0 引 言

随着现代经济、计算机和信息技术的不断发展,实现企业资源调配与优化的ERP系统被迅速应用到企业活动的各个环节,给企业带来了极大的效益。一般地,ERP系统都具有若干子系统,每个子系统又具有若干功能模块。这些子系统、子模块分属不同部门、不同用户。ERP系统中将用户按级别分类,既有同级的并列关系,又有上下级的从属关系。随着企业规模的扩大、职责分工的细化,容易产生职权不明、管理困难等问题。解决这些问题的根本途径在于能够灵活、方便地为不同级别的用户赋予不同的操作权限。通过动态的权限控制机制,统一、可靠地保障系统的安全,是每个ERP系统/子系统都必须考虑的首要问题。

1 ERP系统的权限控制模型

1.1 自主访问控制模型和强制访问控制模型

自主访问控制(Discretionary Access Control, DAC)模型根据自主访问控制策略建立。它允许合法用户以用户或用户组的身份访问策略规定的资源对象(即权限控制的最小粒度),同时阻止非法用户访问资源对象。在该模型中,同一用户对不同的资源对象有不同权限;不同的用户对同一资源对象有不同的权限;用户能自主地将自己拥有的权限授予其他用户。DAC模型权限分配十分灵活,使其广泛应用于企业环境中。由于DAC模型可以任意传递权限,用户能间接获得本不具有的访问权限,因此DAC模型的安全性较低,不能给ERP系统充分的数据保护。为解决这一问题,强制访问控制(Mandatory Access Control, MAC)模型逐渐形成,并得到广泛的商业关注和应用。

MAC模型中,每个资源对象被赋予特定的密级,每个用户被授予特定的访问许可级别。访问时,系统先对用户的访问许可级别和资源对象的密级进行比较,再决定用户是否可以访问资源对象。用户不能改变自身和资源对象的安全级别,只有系统管理员或管理程序才能控制资源对象和用户的级别。MAC模型的优点在于用户权限的层次结构良好,存取控制相当严格;其缺点在于灵活性差。

1.2 基于角色的访问控制模型

基于角色的访问控制(Role-Based Access Control, RBAC)模型(如图1所示)引入角色的概念,根据企业中相对稳定的职能和责任划分角色,将角色与资源对象直接联系。RBAC模型通过系统管理员或管理程序给用户分配合适的角色,使角色成为用户和资源对象间的桥梁。用户与角色、角色与权限之间均是多对多的关系。

RBAC模型中,只有系统管理员或管理程序有权定义和分配角色。用户不能自主地将访问权限授予其他用户。这有效解决了DAC模型安全性较低、授权管理复杂的问

收稿日期:2006-03-17
基金项目:国家"十五"科技攻关项目(2001BA205A06-4)
作者简介:杨宗凯(1963-),男,湖北武汉人,教授,博导,研究方向为电子商务、信息集成和工作流技术。

题。RBAC 模型的角色具有不同等级,描述了用户和资源对象间的多对多关系。角色间存在继承关系,从而形成了角色间的偏序关系和层次结构,反映组织的结构和职权。RBAC 模型使角色关系具有相对稳定性和易维护性,无需多级安全需求,从而弥补了 MAC 模型灵活性差的缺点。

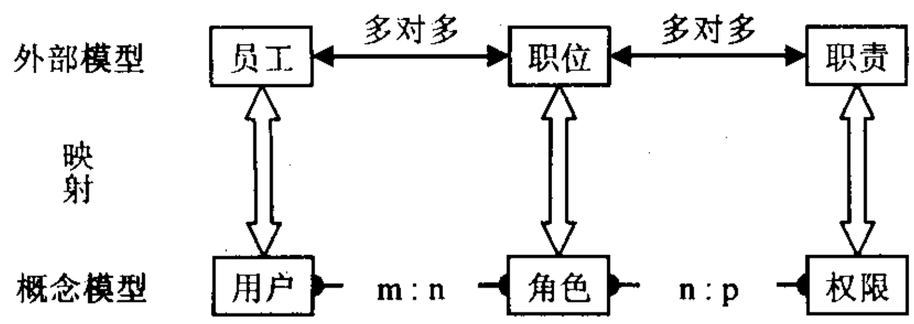

图 1 RBAC 模型示意图

RBAC模型在企业组织视图这一较高的抽象集上进行系统权限控制,较好地解决了 ERP 系统中用户数量众多、变动频繁的问题。与 DAC 模型和 MAC 模型相比,RBAC 模型是一种更有效的权限控制方式,因其授权管理相对简单、权限变更灵活、开销低和操作容易等,在 ERP 系统中得到了广泛应用。

然而实际的 ERP 系统中 RBAC 模型仍存在不足。在角色继承方面,支持角色的全部继承,使得复杂系统中角色粒度小、角色分配复杂、角色很难与实际的岗位职责相对应。在模型的动态性方面,不包含角色时间约束,使得模型很难适应随时间动态变化的需求[1]。在权限控制算法方面,大型企业中角色众多,系统中用户角色的分配工作往往由管理员一人承担,这必然造成权限控制的实现算法复杂、管理员负担重、用户角色的变更不够灵活。

1.3 基于任务的访问控制模型

DAC,MAC 和 RBAC 模型关注 ERP 系统的静态权限控制,从系统的角度(控制环境是静态的)出发保护资源。其授权一般用三元组(S,O,P)表示,其中 S 表示主体,O 表示客体,P 表示许可。如果存在元组(S,O,P),则表明 S 可在 O 上执行 P 许可。否则,S 对 O 无任何操作许可。三元组均预先定义,并静态地存放在系统中,且始终有效[2]。它们是被动安全模型,不能记录主体对客体权限的使用,权限没有时间限制。这类模型不能满足实际应用中随时间变化的动态权限需求,容易造成安全隐患。

基于任务的访问控制(Task - Based Access Control,TBAC)模型从应用出发,基于工作流建模。工作流是为完成某一目标而由多个相关任务(活动)构成的业务流程。数据在工作流中流动时,执行操作的用户改变,用户的权限也改变。

TBAC 模型的授权一般用五元组(S,O,P,L,AS)来表示,其中 S,O,P 的意义同上,L 表示生命期,AS 表示授权步。P 是授权步 AS 所激活的权限,而 L 则是授权步 AS 的存活期限。L 和 AS 是 TBAC 不同于其它访问控制模型的显著特点。在授权步 AS 被触发前,其保护态无效,其中包含的 P 不可使用。当授权步 AS 被触发时,其委托执行者开始拥有执行者许可集中的权限,同时其 L 开始倒记时。在生命期中,五元组有效。当生命期终止,即授权步 AS 被定为无效时,五元组无效,委托执行者所拥有的权限被回收[2]。

TBAC 模型依据任务和任务状态的不同,对权限进行动态管理,资源对象的访问权限随着执行任务的上下文环境发生变化[3]。TBAC 模型的优势在 ERP 系统的决策控制中得到充分发挥。但 ERP 系统中角色是一个非常重要的概念,TBAC 模型不支持角色的层次等级。

2 T-RBAC 模型的研究与实现

2.1 基于角色和任务的访问控制模型的研究

实际上企业环境中,既存在与角色绑定的静态权限,也存在因任务而产生的动态权限[4]。ERP 系统的访问控制存在被动形态,并非全为主动。RBAC 与 TBAC 模型各有优缺点,均不能完全适应 ERP 系统的需求。如前文所述 RBAC 模型未将任务从角色中抽离,缺乏动态性,无法操控任务的前后权责和时间。TBAC 模型忽略角色,不能体现组织结构和职权关系。

在 ERP 系统中,整合 RBAC 和 TBAC 模型才能更好地满足动态权限控制的需求。角色和任务是两个独立而又相互关联的重要概念[5]。基于任务和角色的访问控制(Task - Role Base Access Control,T - RBAC)模型(如图 2 所示)应充分考虑到二者的联系,将之置于同等重要的地位。

文中结合 RBAC 和 TBAC 模型,采用集中管理的方式,在企业复杂的环境中研究并实现 T - RBAC 模型。其主要思想是:依据企业的层次结构和职权抽象角色[6],由系统管理员或管理程序关联用户与角色。从角色出发统一调度,分析企业活动中的工作流。对于与工作流无关的静态权限,利用图形化工具将资源对象授予角色,支持角色的全部和部分继承。针对动态权限,则采用工作流引擎将任务推送给角色。

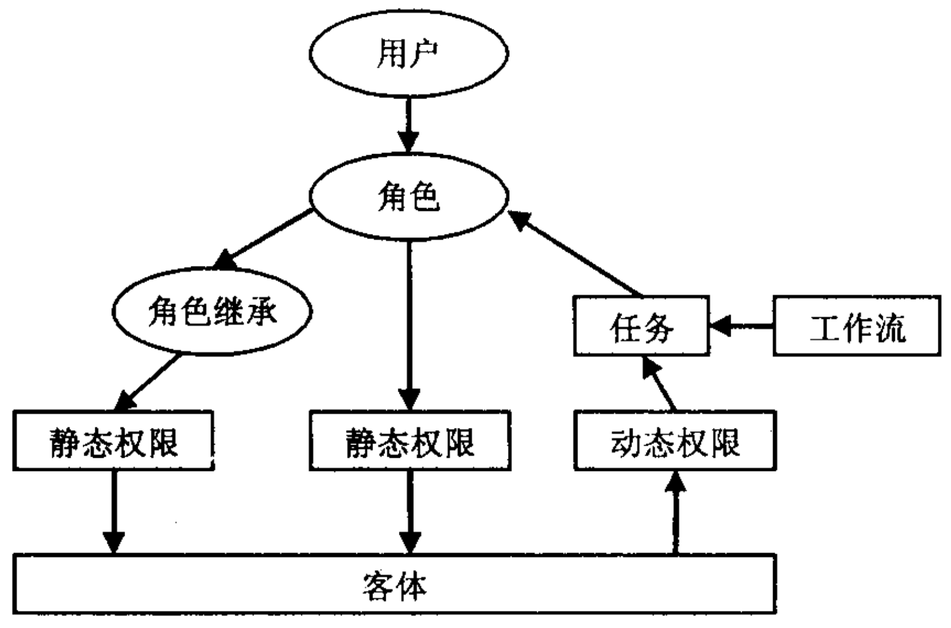

图 2 T - RBAC 模型

该 T - RBAC 模型层次分明、授权灵活、维护方便。它能反映企业和权限等级的特点,支持权限的全继承和部分继承。它同时支持被动和主动的访问控制。通过管理程序,它实现了大量用户和访问客体角色的分配。通过图形化工具,控制静态权限的分配。通过工作流引擎,完成任务的推送和动态权限的分配。

2.2　T－RBAC 模型的实现

文中在 B/S 架构的 ERP 系统上,结合静态授权工具和工作流引擎,实现了该 T－RBAC 模型,以满足企业客户的需求。

针对静态权限,设计四张表(角色信息、用户角色、页面信息和角色权限),用于存放角色的静态权限信息。

(1)角色信息表(AC_TRoleInfo)是系统的初始化设置之一。系统开放给用户注册前,系统管理员应依据本企业实际情况,通过相应模块将角色录入系统。角色依据职能划分,对应企业各部门的各个具体职位如表 1 所示。

表 1　角色信息表(AC_TRoleInfo)

字段名	英文标识	数据类型	说明
角色 ID	RoleID	INT	主键,自增长 ID
角色名称	RoleName	VARCHAR(20)	标识该角色
角色描述	RoleDescrpt	VARCHAR(50)	简介该角色职能
备注	RNotes	VARCHAR(250)	需要特别说明的其它事项

(2)用户角色表(AC_TUserRole)记录用户和角色的对应关系,如表 2 所示。系统管理员在审批用户时,通过管理程序将对应的角色分配给用户,并将对应关系和其它基本资料写入用户角色表。用户注册的具体信息写入用户信息表,因用户信息表不直接与权限控制联系,文中不赘述。

表 2　用户角色表(AC_TUserRole)

字段名	英文标识	数据类型	说明
用户 ID	UserID	INT	主键,自增长 ID
用户名称	UserName	VARCHAR(20)	该用户注册时录入的用户名
用户密码	UserPassword	VARCHAR(20)	该用户自定义的密码
用户角色	UserRole	INT	外键,受角色表约束
备　注	UserNotes	VARCHAR(250)	需要特别说明的其它事项

(3)静态权限的最小粒度通过 JSP 页面的 Tag 值反映。页面信息表(AC_TPageInfo)用于记录同一 JSP 页面的不同功能,由静态授权工具维护,如表 3 所示。一个 JSP 页面可能包括多个功能,比如客户信息页面包括录入、修改、详细显示等功能。不同角色具有不同的静态权限:业务组员能够录入和修改客户信息;生管组员只能查看,但不能修改客户信息;制造组员能够查看客户的简要而非详细信息。通过 JSP 页面的 Tag 标签,能将同一 JSP 页面的不同功能区分开来,实现对静态权限最小粒度精确地访问控制。为提高代码的可读性,通常在文件头部的注释中说明不同 Tag 值对应的功能。静态授权工具自动读取 JSP 页面的 Tag 标签等系列信息,并将之写入页面信息表。

表 3　页面信息表(AC_TPageInfo)

字段名	英文标识	数据类型	说明
页面 ID	PageID	INT	主键,自增长 ID
页面名称	PageName	VARCHAR(100)	JSP 页面的名称
页面 Tag	PageTag	INT	Tag 值
Tag 功能	TagFunc	VARCHAR(100)	Tag 值对应的功能
备注	PageNotes	VARCHAR(250)	需要特别说明的其它事项

(4)角色权限表(AC_TRoleAccess)记录角色能够访问的页面功能,即角色对应的静态权限的最小粒度,由静态授权工具维护。用户访问页面时,通过查询角色权限表,即可获得关于静态权限的三元组信息(S,O,P)。如表 4 所示。

表 4　角色权限表(AC_TRoleAccess)

字段名	英文标识	数据类型	说明
角色 ID	RoleID	INT	外键,受角色信息表约束
页面 ID	PageID	INT	外键,受页面信息表约束
页面名称	PageName	VARCHAR(100)	
页面 Tag	PageTag	INT	

针对动态权限,抽象企业环境中的工作流,采用工作流引擎,将任务推送至用户的个人工作台。文中企业环境中的工作流用简化的 BPEL4WS 语言描述,某印刷企业的工作流由以下 XML 文件所示:

```
<? xml version="1.0"encoding="gb2312"? >
  <process name="物料出库审批流程">
    <sequence>
      <action name="原料仓组员填写物料出库表单"
          ztmc="仓库审批否决"
          ztbh="3"
          role="41"
          fileURL="YL_05\MaterialOutUpdate.jsp? tag=
502"/>
        <action name="原料仓组长提交审核意见"
          ztmc="待审批"
          ztbh="1"
          role="18"
          container="button"
          fileURL="YL_05\MaterialOutDetail.jsp? tag=
501"/>
        <switch name="原料仓组长审核">
          <case name="原料仓组长同意"condition="同意"
>
            <end ztmc="仓库审批通过"ztbh="2" ></end
>
          </case>
          <otherwise name="原料仓组长不同意">
            <redo ref="原料仓组员填写物料出库表单"/>
          </otherwise>
        </switch>
      </sequence>
  </process>
```

因篇幅所限,工作流引擎的工作原理文中不再赘述。

3　结束语

ERP 系统的动态权限控制已成为影响其应用与安全的重要问题。文文研究 ERP 系统中几种常用的权限控制

(下转第 32 页)

式中，R 为NBC在验证集上的分类精度，D 为NBC在验证集上的差异度，λ 为决定差异度影响的系数。

(3)GABC 算法。

① 采用分层随机取样方法将数据库分成训练集和验证集；

② 随机生成 S 个随机属性子集；

③ 将 S 个随机属性子集对应的 NBC 作为初始种群，采用遗传算法优选；

④ 调整 λ，重复步骤③。

算法中，交叉算子采用两点交叉，即交换父本两个基因位间的部分，产生相应的后代；选择算子采用轮盘赌选择法。另外，每一代遗传群体中适应度最好的 5% 个体不参加交叉和变异，自动保留到下一代。

4 实 验

实验在 4 个数据集(来自 UCI 机器学习数据库)上进行[6]。对每个数据集，采用分层随机抽样，训练集数据占 70%，验证集占 30%。所谓分层随机抽样，就是从每个类的实例中随机抽样，以便结果集中实例的类分布与初始集大致相同。这种方法常常比简单随机取样有更好的精度评估[7]。

本实验使用 VC++6.0，在内存为 512MB，CPU 为奔腾 1.7G 的微机上进行。实验中，遗传种群的规模为 100，遗传算法执行的最大代数为 150。实验结果如表 1 所示。

表 1 GABC 与 NBC 分类精度的比较

数据集	记录数	属性数	NBC	GABC		
				$\lambda=0$	$\lambda=0.5$	$\lambda=1$
Kr-vs-kp	3 196	36	74.75%	80.36%	80.17%	79.65%
Mushroom	8 124	22	73.49%	79.76%	80.57%	74.86%
Blance	625	4	69.45%	71.57%	69.87%	68.98%
Breast-cancer	286	9	70.84%	73.59%	72.07%	71.45%

由表 1 可知，GABC 在大多数的情况下，都能比传统的 NBC 取得较好的效果，只有在 Blance 和 Breast-cancer 等属性数较少的数据集中，两者的分类精度相近，这说明基于遗传算法的朴素贝叶斯分类是很有效的。而且，对同一个数据集而言，GABC 的分类精度随着 λ 的变化而不同，并从数据集 Mushroom 的实验结果来看，有时适当地考虑差异度的影响，可进一步提高分类能力。

5 结 语

基于遗传算法的朴素贝叶斯分类方法不仅避免了属性约简对分类精度的影响，而且充分考虑了分类误差在实例空间中的分布程度。实验表明，与传统的朴素贝叶斯方法相比，该方法具有更好的性能。下一步的研究方向应是：

(1)如何在一个给定领域里自动选取 λ 的优化值问题。

(2)先对遗传算法进行改进，再和朴素贝叶斯相结合。

改进方法主要包括：改进遗传算子；将遗传算法与其他优化算法相结合，构造混合遗传算法；使用并行遗传算法等方法。

参考文献：

[1] Written I H, Frank E. Data Mining: Practical Machine learning Tools and Techniques with Java Implementation[M]. Seattle: Morgan Kaufmann Publishers, 2000: 265-314.

[2] 史忠植. 知识发现[M]. 北京：清华大学出版社，2002.

[3] 朱 明. 数据挖掘[M]. 合肥：中国科学技术大学出版社，2002.

[4] 王小平，曹立明. 遗传算法——理论、应用与软件实现[M]. 西安：西安交通大学出版社，2002.

[5] 武兆慧，张桂娟，刘希玉. 基于模拟退火遗传算法的关联规则挖掘[J]. 计算机应用，2005，25(5)：1009-1011.

[6] Blake C L, Merz C J. UCI repository of machine learning database[EB/OL]. 1998-12-30[2002-09-28]. http://www.ics.uci.edu/mlearn/MLRepository.html.

[7] Kohavi R. A study of cross-validation and bootstrap for accuracy estimation and model selection[C]//Mellish C. Proceedings of IJCAI95. San Mateo: Morgan Kaufmann, 1995: 1137-1143.

(上接第 11 页)

模型，分析它们各自的优缺点。与 DAC 和 MAC 模型相比，RBAC 模型具有明显的优势，然而仍存在动态性不强等缺陷，TBAC 模型恰可弥补这一缺陷。针对模型的动态性和角色的生命周期约束，文中结合 RBAC 与 TBAC 模型，提出了一种 T-RBAC 模型。该 T-RBAC 模型层次分明、授权灵活、维护方便。结合静态授权工具和工作流程引擎，实现了 B/S 结构 ERP 系统的动态权限控制，并成功应用于东莞某印刷企业。

参考文献：

[1] 徐日佳，赵敬中. 一种改进的 RBAC 模型的研究与应用[J]. 微机发展，2005，15(8)：95-97.

[2] 邓集波，洪 帆. 基于任务的访问控制模型[J]. 软件学报，2003，14(1)：76-79.

[3] 沈海波，洪 帆. 基于企业环境的访问控制模型[J]. 计算机工程，2005，31(14)：144-146.

[4] SEJONG O H, PARK S. An Improved Administration Method on Role-Based Access Control in the Enterprise Environment [J]. Journal of Information Science and Engineering, 2001, 17: 921-944.

[5] 金稼玲，杨材堂. 基于 T-RBAC 的企业权限管理方法[J]. 计算机工程，2004，30(19)：93-95.

[6] 王军强，杨宏安. 管理信息系统权限控制的组件化研究与实现[J]. 计算机工程与应用，2005(5)：173-175.