基于RBAC模型实现电子政务系统业务的柔性处理

吉同路[1],潘跃建[2],王立松[2]
(1.江苏省建设厅,江苏 南京 210013;
2.南京航空航天大学 信息科学与技术学院,江苏 南京 210016)

摘 要:电子政务的迅速发展,加大了业务处理的复杂度,先前的系统业务处理功能虽然丰富,但随着需求的不断变更和业务处理的不断重组,使得系统的适应能力已逐渐不能满足这种变化带来的柔性需求。文中根据电子政务系统存在业务处理流程中的"固化"的现象,引进基于角色的访问控制(RBAC)模型,从顶层设计的高度,利用基于数据字典的系统实现方法,实现了系统对业务的柔性处理,增强了业务处理的灵活性,从而提高系统的适应能力,进一步使得基于电子政务的政府机构办事效率提高。

关键词:电子政务;RBAC;数据字典;柔性管理
中图分类号:TP311 **文献标识码**:A **文章编号**:1673-629X(2010)02-0052-04

Implementation of Flexibility for Electronic Government System Based on RBAC Model

JI Tong-lu[1], PAN Yue-jian[2], WANG Li-song[2]
(1. Construction Bureau of Jiangsu Province, Nanjing 210013, China;
2. School of Information Science & Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China)

Abstract: With the rapid development of electronic government, the Business Process Systems(BPS) become more and more complex. Previous BPS can not meet the continuous improvement requirement and continuous restructured business process. In order to deal with this limitation of the "fixed model" in BPS, RBAC model, top-design method and data dictionary(DD) are introduced in this paper to design and implementation of E-government system. So its flexibility and adaptive capacity are greatly improved and do a good benefit to work efficiency of government.

Key words: electronic government; RBAC; data dictionary; flexible management

0 引 言

随着国家信息化战略不断深入,中国电子政务建设不断向深度和广度发展,电子政务业务涉面非常广泛,复杂度越来越大。为了更好地开发和维护电子政务系统,政务信息资源整合与应用研究愈发显示出在电子政务建设中的基础作用[1]。文中从顶层设计[2]的高度,基于资源整合的思路,构造一个柔性的业务处理体系,使得系统在这种柔性的体系下,不需修改代码直接能随着业务处理需求的变动而提供正确的业务处理功能;保证现有系统正常运行的情况下,实现对旧有功能的调整和新功能的添加,实现即配即用模式。

柔性的业务处理可以归结为对用户的业务功能的灵活配置,业务功能可以理解为系统的角色,配置过程就是角色的分配和回收等问题,所以可以用访问控制方法来实现此项功能。传统的访问控制机制对系统中所有用户进行直接的权限管理,权限操作复杂,授权方式不灵活,难以适应业务不断变化的高效电子政务系统的需求。而基于角色的访问控制模型(Role-Based Access Control, RBAC)[3~5]引入角色作为中介,将权限和角色相关联,通过给用户分配适当的角色授予用户权限,实现了用户和访问权限的逻辑分离,如图1所示。当用户岗位发生变化时,只要将该用户从一个角色移到另一个角色来实现权限的协调转换,完成业务流节点或业务段的交接。在组织机构中若进行业务流的重整时,系统只需要对角色进行添加或取消某些功

收稿日期:2009-05-08;**修回日期**:2009-08-30
基金项目:国家建设部资助项目(建标[2009]88号)
作者简介:吉同路(1966-),男,硕士,高级工程师,研究方向为电子政务、数据挖掘、软件工程;王立松,博士,副教授,硕士生导师,研究方向为安全数据库、软件工程、系统软件。

能的使用权限即可实现。这些特点使得RBAC具有无可比拟的灵活性和易操作性,改变了以往把业务流程"固化"在应用系统中的开发模式,实现了系统中业务的动态调整。

文中针对江苏省建设厅电子政务系统的具体需求[6,7],把RBAC96-3模型引进系统的设计和实现,满足了对业务柔性处理。

1 基于角色的访问控制模型(RBAC)

George Mason大学的Sandhu等人在总结前人研究成果的基础上,于1996年提出了基于角色的访问控制模型(RBAC)[3,4],第一次形式化地描述了基于角色的访问控制。并在1997年提出了RBAC的管理模型ARBAC(Administrative RBAC)。这两个模型是基于角色的访问控制模型中的经典模型,也被分别称为RBAC96模型和ARBAC97模型。

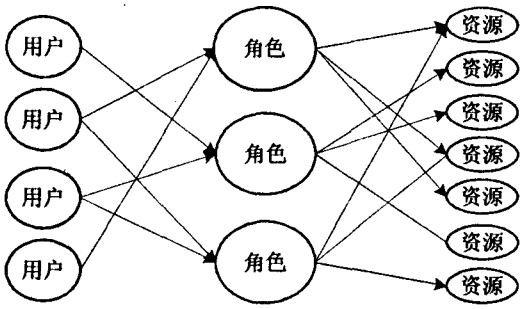

图1　基于角色的访问控制模型

在RBAC模型中,包含用户users(USERS)、角色roles(ROLES)、目标objects(OBS)、操作operations(OPS)、许可权permissions(PRMS)五个基本数据元素,权限被赋予角色,而不是用户,当一个角色被指定给一个用户时,此用户就拥有了该角色所包含的权限。会话sessions是用户与激活的角色集合之间的映射。

Sandhu提出的RBAC96模型是RBAC模型的基础,该模型包括4个部分:RBAC0、RBAC1、RBAC2和RBAC3。如图2所示,RBAC0是基本模型,定义了RBAC系统所需的最小需求;RBAC1在RBAC0的基础上添加了角色间的继承关系。继承关系可分为一般继承关系和受限继承关系。一般继承关系仅要求角色继承关系是一个绝对偏序关系,允许角色间的多继承;而受限继承关系则进一步要求角色继承关系是一个树结构。RBAC2在RBAC0的基础上添加了约束的概念。RBAC2的约束规定了权限被赋予角色时,或角色被赋予用户时,以及当用户在某一时刻激活一个角色时所应遵循的强制性规则。约束与用户-角色-权限关系一起决定了RBAC2模型中用户的访问许可。RBAC3包含了RBAC1和RBAC2,通过传递,也包含了RBAC0。由于篇幅关系,有关RBAC及改进的RBAC模型的详细信息可以参照文献[3,4]。文中根据RBAC96-3模型进行江苏省建设厅电子政务系统的设计和实现。

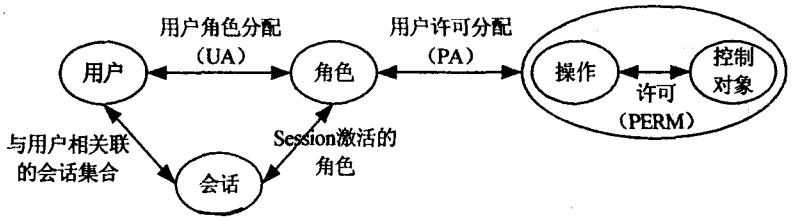

图2　RBAC模型

2 系统的设计

电子政务系统是多种信息技术的综合运用,是应用系统级别上的互联互通的系统。以往的系统由于条块分割、地域分割、部门分割导致形成"烟筒系统"和"孤岛系统"[2]。随着电子政务系统形态、结构和处理业务的复杂化,先前的设计已不能满足当前用户的业务需求。文中采用顶层设计的思想,从全局的角度出发,充分考虑系统的各个方面、各个层次、各种参与力量以及组织结构中客观存在的越位、缺位、空位等情况,进行整体技术结构的设计,优化业务的处理。

2.1 系统功能分析

根据用户的应用需求,系统划分为住房保障、公积金管理等五个子系统;系统面向的用户分为非行政部门和行政部门,行政部门分为街道、县(市)等四个等级,各个子系统可以通过接口对数据资源进行共享,各用户可通过各子系统进行业务处理,也可通过公用模块进行即时或非即时的信息交流。图3为本系统的宏观框架图。

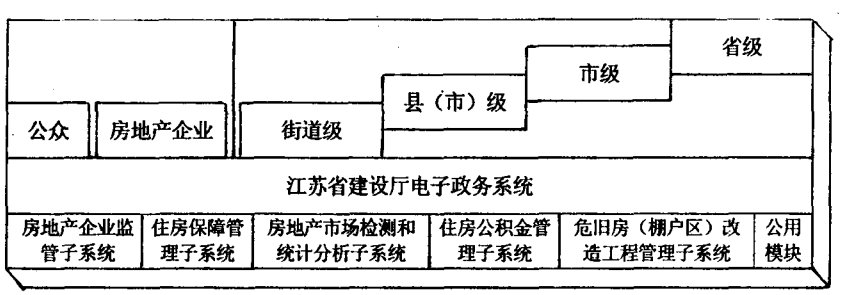

图3　电子政务系统宏观框架

用于篇幅关系,仅以住房保障子系统为例,进行下文的工作。

根据用户业务的需求，住房保障子系统可以划为保障审理请求、保障申请审批等功能，图 4 为本子系统的功能框架图。

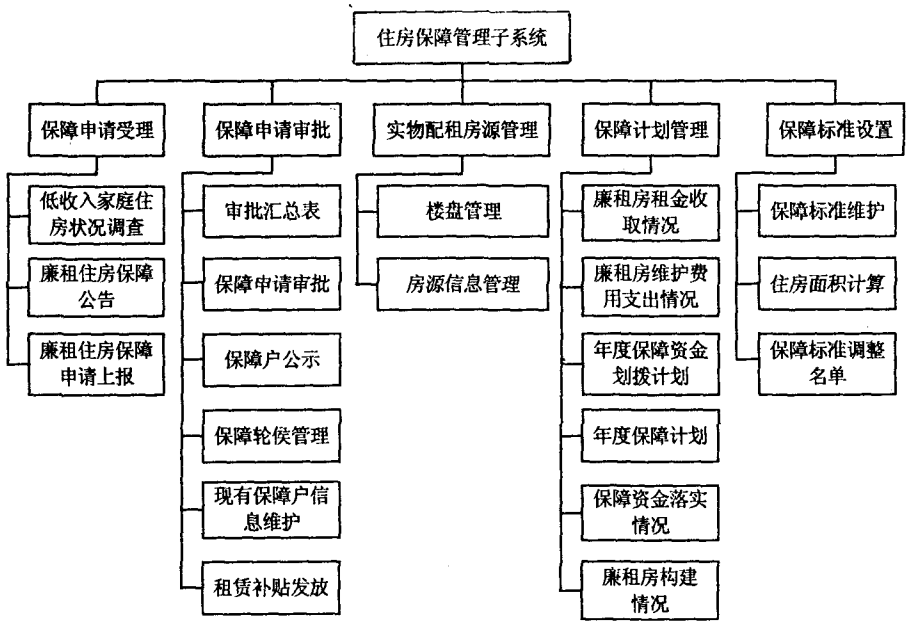

图 4 住房保障管理子系统功能框架

2.2 基于 RBAC96－3 模型系统设计

进行系统用户层的组织结构分析，是引入 RBAC 模型设计的前提。针对江苏省建设厅电子政务系统的具体情况，在总结全国各地电子政务系统建设规范的基础上，抽象出如下实体概念：结构、部门、人员、用户组、岗位。它们之间的关系可用图 5 表示。

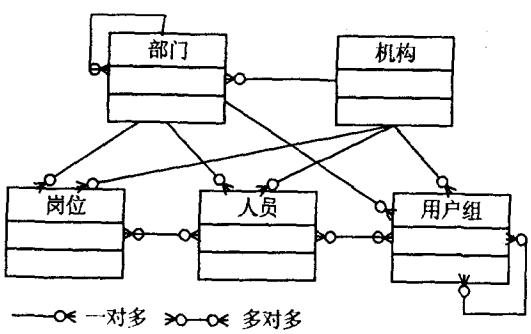

图 5 用户组织结构

在图 5 中可以发现：单个人员可以拥有多个岗位，也可以属于不同的用户组；一个组可以包含多个组，一个组也可以被多个组包含；一个部门可以拥有多个子部门，但一个子部门只能属于一个部门等。

权限管理是 RBAC 的思想的核心，由于本系统涉及功能和用户的复杂性，因此把用户主要集中在省级的层次（即江苏省建设厅）进行分析。在 RBAC 中，权限是指主体对客体（即受保护的资源）的操作。电子政务系统中有很多子系统，每个子系统又具有很多的功能模块。在文中，客体指各个功能模块，权限是指用户对各个功能模块的可操作权力，包括浏览、查询、添加、修改和删除等。权限的粒度可以根据不同需求发生变化，总体而言可分为两类，即模块级控制和数据级控制。角色如果具有模块级权限，就可以看到该模块操作界面；如果具有数据级权限，便可以对模块进行浏览、查询、添加、修改和删除等操作。权限的授予应满足最小特权原则，即用户所拥有的权利不能超过执行工作时所需的权限。在基于角色的访问控制中是指将只有角色需要执行的操作授权给角色，在角色不需要此权限时或长时间此角色没有操作时收回。

根据图 5 的用户组织模型，设计如图 6 所示的用户层级结构。

在电子政务系统中，设置了一个超级管理员，他把相应权限分配给其中某些部门，这些部门分配的权限可能不一致。在此引进权限域的概念，所谓的权限域是指一个封闭的管理范围。如图 6 把实物配租房源管理操作权限赋给房地产业处，那该部门的用户拥有了操作实物配租房源管理模块的权限，同时设置了部门级别的管理员，如图 6 中填充黑色标记的用户，即部门负责人。由此可知，用户角色可分为三类：系统管理员、部门管理员、普通用户。系统管理员分配较大权限给部门，部门在权限域内把权利分散给普通用户。这样设计分散了系统权限管理，大大提高了系统的灵活性，为实现业务柔性处理提供了保证。

2.3 业务柔性处理

由上文分析可知，基于 RBAC 模型可以实现电子政务系统业务的柔性处理。如图 6，如住房保障办公室主任“人员 4”因病不能参加日常工作，而系统处理业务的流程不能因此间断，而其他用户又不拥有“人员 4”的权限，如进行域内的权限管理。此时可由“人员 4”本人通过权限管理模块向系统管理员发出权限移交申请，系统管理员批准后把主任岗位拥有的权限赋给副主任“人员 5”，此权限在主任“人员 4”申请权利回收且系统管理员批准处理完成之前均有效；对于结构组织发生人事的变更时，系统管理员只需要进行相应用户角色增加、删除、替换即可；同理当系统或者子系统增减功能时，通过权限管理模块只需进行简单的角色

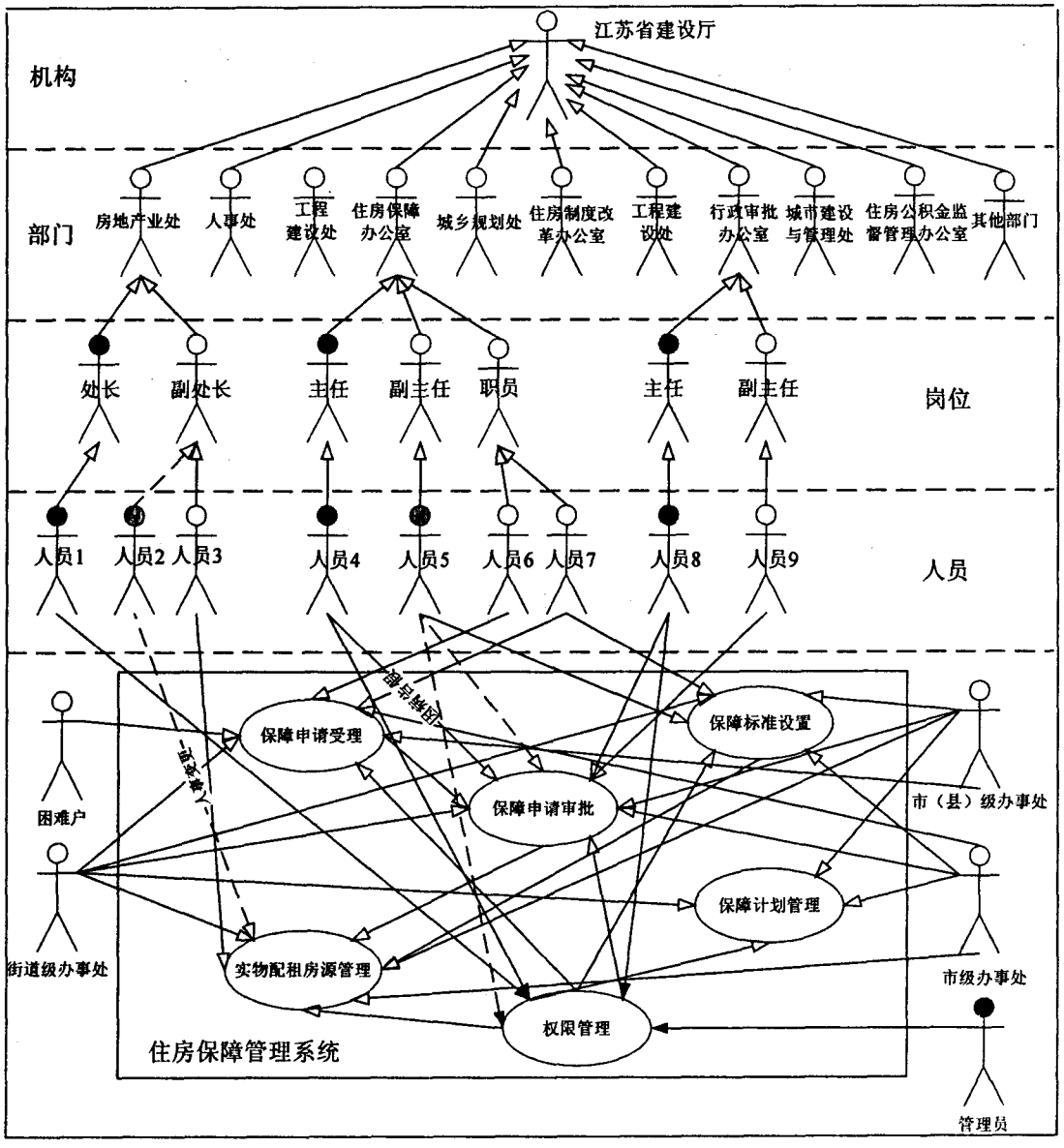

图6　住房保障管理系统用例图

设定即可。由此可知,基于RBAC模型的系统设计,可在代价最小的情况下保证业务的正常运转,提高政府机构的办事效率。

3　基于数据字典的系统实现

数据库管理系统的实现技术[8]中很重要的核心技术就是数据字典,也称为元数据,用以描述系统中所有的数据信息。本系统的实现方法就是采用数据字典来描述系统中所有数据的结构、数据的更新情况、数据间的依赖关系等,并且用其来实现数据转换、操作、管理。所以通过数据字典,使得本系统提供了一个系统应用平台,不仅实现了用户定义和业务重组的柔性,而且还具有灵活的可扩展性。数据字典在系统运行的过程中,根据业务需求的变化,系统管理员或系统开发人员可以随时对数据字典进行修改或增加新的属性,用以实现新的功能。本系统实现的数据字典的主要类型包括:数据存储和展现类、用户角色管理和系统安全类、业务管理类、数据交换类等。

4　结束语

电子政务的高速发展,导致现有的电子政务系统不能满足复杂业务的处理需求,寻找一种灵活的业务处理机制迫在眉睫。在这样的形势下,笔者把RBAC模型引进江苏省建设厅电子政务系统的建设,从顶层设计的视角实现了系统业务的柔性处理。

目前江苏省建设厅电子政务系统的房地产企业监管子系统、住房保障管理子系统、房地产市场检测和统计分析子系统已经实施成功。实践表明,把RBAC模型引入电子政务系统建设能成功实现业务的柔性处

(下转第59页)

光信息,RE2 二个光口都下电转换成从端口。在下一个周期的 REC 光口扫描中,RE1 将光口 1 下发的 HOP 数加 1 再从它的主端口发出。由于 RE1 到 RE2 的链路断开了,RE1 收不到有效信息,就将 HOP 为 1 的扫描结果回送到光口 1。光口 1 知道了现在连在这个光口上可达的 RE 只有 RE1 了。光口 2 下发的扫描信息到达 RE4 后,RE4 将再将 HOP 为 1 的扫描信息发送出去。RE3 收到扫描信息后再将 HOP 数加 1 发送出去。由于 RE2 的二个端口均为从端口,可以接收到 RE3 发送的光信息。RE2 获取到了 HOP 为 2 的信息将左端口置为主端口并把 HOP 为 3 的信息从主端口发送出去。同样由于断路 RE2 在主端口收不到有效信息,便向 REC 发送 HOP 为 3 扫描结果报告。REC 在光口 2 上获得 HOP 为 3 的信息后建立链路。到达 RE2 的链路从光口 1 的第二跳变成了光口 2 的第三跳。经过链环倒换后 REC 的主控单元的链路信息是 RE1:链路 1;RE2:链路 13;RE3:链路 12;RE4:链路 11。RE2 同样连上了一个 REC 从而能够正常的通信(见表 2)。

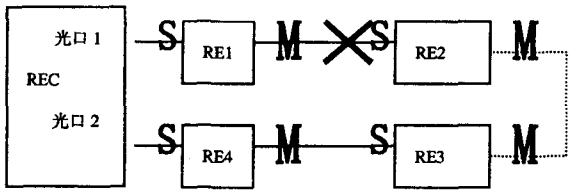

图 2　拓扑链路状态图(注:M:主端口,S:从端口)

表 2　倒换后的路由表

RE ID	光口号	HOP 数
RE1	1	1
RE2	2	3
RE3	2	2
RE4	2	1

4　结束语

文中针对 CPRI 的拓扑结构,基于光口上的"主端口－主端口"冲突特性,提出了一个链环拓扑结构有效的建链方法。此方法可以在断链的情况下自动的进行链路倒换,这种"自愈"能力对于 CPRI 拓扑结构的链路的可靠性有一定的研究价值。由于链环中总会存在一个"M－M"点,整个环相当于在这个点上分成两条链路。"M－M"点的位置是在竞争过程中形成的,上电后不确定。CPRI 状态的控制由 FPGA 执行,完全不受软件的控制。如果物理上实际的组网与预期的配置不一致,由于环的"M－M"点的不确定性,当发生链环倒换时,会导致一个 RE 的 ID 在不同情况下对应的物理设备不同。对于此问题,具体有效的方法还有待进一步的研究。

参考文献:

[1] 乐黎黎,孟利民. TD2SCDMA 分布式基站射频拉远模块的研究和设计[J]. 浙江工业大学学报,2008,36:166－168.

[2] Ericsson A B, Huawei Technologies Co., Ltd, Nec Corpoaration, et al. CPRI Specification V4.0[EB/OL]. 2008－06－30. http://www.cpri.info/downloads/CPRI_v_4_0_2008－06－30.pdf.

[3] 胡鹏程,戎蒙恬. 模块化的 3G/4G 基站传输接口－CPRI 及其特征与使用[J]. 黑龙江科技信息,2007,23:64－65.

[4] 钟显成,王宏伟. CPRI 协议分析仪的硬件开发与实现[J]. 世界电子元器件,2007(6):54－56.

[5] 王　彦,倪　琰. 3G 数字基站射频拉远 CPRI 规范的实现[J]. 移动通信,2007(Z1):107－109.

[6] 梁延峰. RRU 基本原理及应用分析[J]. 电信工程技术与标准化,2007(3):51－55.

[7] 陈岳林,石江宏. 数字直放站中 CPRI 协议的 FPGA 实现[J]. 现代电子技术,2009(4):31－34.

[8] 罗健强. 基于 CPRI 标准的 WCDMA NodeB 射频光纤拉远接口 FPGA 设计[D]. 成都:西南交通大学,2006.

(上接第 55 页)

理,满足日益变化的业务处理需求。

参考文献:

[1] 国家信息化领导小组. 国家电子政务总体框架(国信[2006]2 号)[S]. 北京,2006.

[2] 谢力民. 顶层设计——电子政务向纵深发展的标志[EB/OL]. 2004－12. http://it.sohu.com/20041217/n223538010.shtml.

[3] Sandhu R, Coyne E, Feinstein H, et al. Role－Based Access Control Models[J]. IEEE Computer, 1996, 29(2):38－47.

[4] Ferraiolo D F, Sandhu R, Gavrila S, et al. Proposed NIST Standard for Role－Based Access Control[J]. ACM Transactions on Information and System Security, 2001, 4(3):224－274.

[5] Ahn G J, Sandhu R S. Role－Based Authorization Constraints Specification[J]. ACM Trans on Information and System Security, 2000, 3(4):207－226.

[6] 蒋海琴,阎国年,蒋文明,等. 房产管理信息系统[M]. 北京:科学出版社,2007.

[7] 吉同路. 政府资源计划(GRP)初探[J]. 哈尔滨工业大学学报,2003,35(sup):132－136.

[8] 周龙骧. 数据库管理系统实现技术[M]. 武汉:中国地质大学出版社,1990.