

改进的基于角色的通用权限管理模型及其实现

李昕昕, 严张凌, 王赛兰

(四川大学锦城学院 计算机科学与软件工程系, 四川 成都 611731)

摘要:合理的权限管理能从根本上保证数据的安全,是所有 MIS 系统的核心内容之一。传统的基于角色的访问控制 RBAC(Role-Based Access Control)模型对角色的依赖度过高,常会导致业务系统的权限管理不够灵活。文中从提高权限管理的灵活性和通用性入手,提出一种新的 RUP(Role-User-Privilege)模型,并在此基础上设计了一个具有通用性的数据库。改进的基于角色的通用权限管理模型相较于以往的通用权限管理平台,具有管理粒度细化、分级授权和权限制约的特点,使其能更广泛地满足各种业务系统复杂、多变的应用需求。

关键词:权限管理;基于角色的访问控制;角色-用户-权限模型;业务系统;通用性

中图分类号:TP309

文献标识码:A

文章编号:1673-629X(2012)03-0240-05

A Modified Role-Based Permission Management Model and Its Implementation

LI Xin-xin, YAN Zhang-ling, WANG Sai-lan

(Department of Computer Science & Software Engineering, Jincheng College of Sichuan University, Chengdu 611731, China)

Abstract: A appropriate design of permission management can guarantee the security of data, which is the core of all MISs. The traditional role-based access control model depends highly on the role component that results many inflexibilities in permission management. To meet the demands in both flexibility and generality, it proposes a new role-user-privilege model and designs a database with generality. Compared with the traditional common rights management platforms, the modified role-based permission management model has more detailed granularity, hierarchical authority and privileges restricted features. It can meet the requirements of the wider variety of business complexity and application changes.

Key words: permission management; RBAC; RUP model; business system; generality

0 引言

随着计算机和网络技术的不断发展,开发信息管理系统已成为各行业进行信息化管理的一种基本手段。随着管理信息系统中所涉及的业务逻辑越来越复杂,对各类信息资源的访问与控制以及对用户权限和相关人员的管理也变得越来越复杂^[1]。因此,人们设计了各种权限控制模型,确保只有被授权的用户才能访问某些数据和信息。

访问控制决定了一个用户或程序是否有权对某一特定的资源执行某种操作^[2]。传统的访问控制一般被分为两类: DAC(Discretionary Access Control, 自主访

问控制模型)和 MAC(Mandatory Access Control, 强制访问控制模型)^[3,4]。二者都是主体和访问权限直接发生关系,根据主体/客体的所属关系或主体/客体的安全级别来决定主体对客体的访问权。但随着分布式数据库的快速发展, MIS(Management Information System, 管理信息系统)的规模日益增大,用户与日俱增,并且可访问的信息资源的结构也日趋复杂,如果仍使用上述访问控制机制,那么存取权限的管理将会变得十分复杂且难以满足越发复杂的企业环境需求^[5]。因此, Ferraiolo 和 Kuhn 在 1992 年提出了基于角色的访问控制(Role-Based Access Control, RBAC),并对此作了许多研究^[6,7]。RBAC,通过新增加“角色”,使用户与访问权限实现了逻辑分离,通过对角色的权限分配来最终达到访问控制的要求,如图 1 所示。

RBAC 模型定义了四个实体和两个分配关系:

(1) 会话 S(Sessions):指用户与系统的交互,用户与会话之间是一个多对多的关系^[8]。

收稿日期:2011-07-27;修回日期:2011-10-29

基金项目:中央高校基本科研业务费专项基金(2009QK17);可视化计算与虚拟现实四川省重点实验室基金(J2010N01);四川省教育科研基金(09ZC079);

作者简介:李昕昕(1981-),女,讲师,硕士,研究方向为软件工程、计算机网络和人工智能。

(2)用户 U (Users):指一个可以独立访问系统中的数据的主体^[9]。用户可以是人、计算机或一些组织。

(3)角色 R (Roles):指一个或一群用户在组织内可执行的操作的集合^[10]。

(4)权限 P (Privileges):指对系统中的一个或多个客体进行特定模式访问的操作许可。

(5)权限分配 PA (Privilege Assignment):指角色与权限之间按其职责范围获得权限许可的分配关系。

(6)用户分配 UA (User Assignment):指用户与角色之间按职责和权利进行分配的关系。

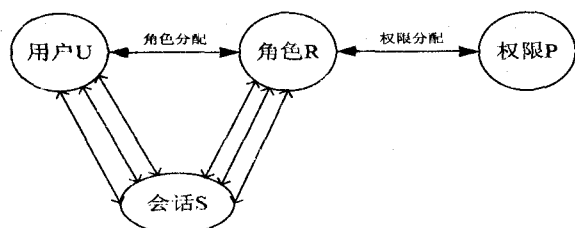


图1 基于角色的访问控制模型-RBAC96

由于 RBAC 模型实现了用户与访问权限的逻辑分离,更符合企业的用户、组织、数据和应用特征,已逐渐成为前面几个模型的最佳替代者。但是由于 RBAC 模型对角色的依赖度过高,常会导致业务系统的权限管理不够灵活,因此文中将从提高权限管理的灵活性和通用性入手,提出一种新的模型——RUP (Role-User-Privilege, 角色-用户-权限),并对其进行实现。

1 通用权限管理模型的总体思路

在传统业务系统中,权限设计通常是针对不同用户赋予不同的访问权限,因此,系统权限管理的范围较窄、粒度较粗、灵活性较弱、通用性较差,而通用权限管理模型则能够解决上述问题^[11]。

1.1 RBAC 模型的缺陷

虽然 RBAC 作为基于角色的访问控制方法可以减小授权管理的复杂性,降低管理开销;同时能灵活地支持企业的安全策略,并对企业的变化有很大的伸缩性,但是,它在针对不同需求、不同规模和不同开发环境的系统上应用仍存在以下问题:

(1) 灵活性弱。

当角色不存在时,系统管理员无法给某特定用户添加权限。如系统刚建成时,使用单位对于角色的划分尚不清晰;

(2) 通用性差。

系统角色过多、角色责任不明确。如对于某些权限并不对应一个明确的角色概念,或者某些权限只需要临时被赋予某用户的情况,为了能使用户使用到这些权限,还是得新建一个甚至多个角色。

(3) 可控粒度较粗。

权限只针对功能进行设置,作用范围较窄。比如同样是查询功能,系主任就可查询该系所有学生的信息,而组长就只能查询该班某个范围内的学生信息。

1.2 RUP 模型

RUP 模型是在 RBAC 模型的基础上,针对其作用范围较窄、粒度较粗、灵活性较弱、通用性较差的缺点设计出来的,见图 2。

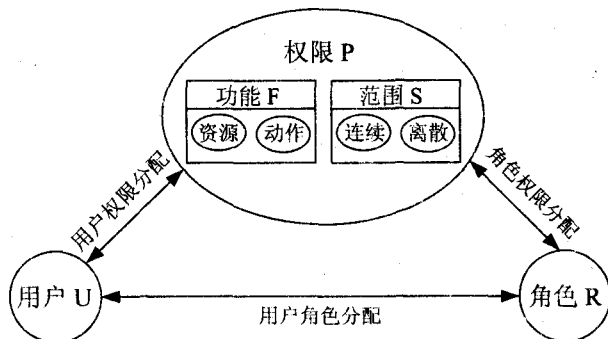


图2 基于“角色-用户-权限”的访问控制模型 RUP

RUP 模型的基本原理:在 RUP 模型中,权限 P 由功能 F 与范围 S 构成,系统管理员可以直接对用户或角色赋予权限。对角色进行权限管理可以较为方便地将一类具有相同权限的用户统一进行管理,简化了管理的复杂度;对用户进行权限管理则可以针对某些特殊的个体单独进行权限管理,提高了管理的灵活性。而用户与角色的对应关系则可以实现用户与角色间多对多的关系,使管理兼具粒度细、灵活性强以及通用性好的特点。

RUP 模型的概念:

(1)功能 F:指在系统中完成业务单元动作所需的资源访问权。其中资源指数据表、文件等系统元素;动作指增、删、改、查等;

(2)范围 S:指对资源访问的范围,是对功能的限制。如教务管理系统中管理人员、教务人员、辅导员、班长都被赋予了学生个人信息的访问权限,但不同的角色被允许访问的资源范围不一样。因此,在本平台中,设计了两类范围描述方式:连续范围、离散范围。

连续范围:指用户/角色希望访问的数据在一个连续的范围段内。如:教务管理系统中,班长仅被允许查看他所在班级的同学信息,因此只需要给他指定一个连续范围,包含该班所有同学的学号即可。

离散范围:指用户/角色希望访问的数据在两个甚至多个数据段中。如:教务管理系统中,辅导员被允许访问他所带班级的同学信息。由于一个辅导员可能负责多个班,而这些班的同学学号未必是连续的,因此需要给辅导员指定一个离散范围,这里应该包含所有他带的班的学生学号。

(3)权限 P:由功能和范围组成,明确指定对一定

范围内特定资源的访问方式,如:教务管理系统中对学号为092801~092870的同学的添加操作。

(4)角色R:权限的集合,可以直接赋予用户。

(5)用户U:同基于角色的访问控制模型中用户的解释。

2 通用权限管理模型的设计与实现

在RUP模型的基础上,结合传统业务系统的特点,设计出了一个能够为绝大多数业务系统提供权限访问控制的管理平台。该平台具备以下特点:

(1)通用性强、可移植。

该平台适用于各种结构的系统,可以将其加入到任何需要进行权限管理的系统中。另外,该平台可以被重复利用,具有较好的可移植性。

(2)系统整合简单。

业务系统设计完成后,只需利用通用权限管理系统提供的接口,即可将平台的授权管理功能集成到该系统中,适合各类用户的需求。

(3)灵活的权限管理。

平台不仅允许管理员对业务系统的部门、用户、角色、操作、对象和权限信息进行自定义,还允许对拥有相同操作权限的不同个体设置其允许访问的范围,充分考虑了不同应用需求的特点,使其能更好地为各业务系统服务。

(4)分级授权。

如果用户拥有“授权”角色,则该用户还可为其他用户授权,这种授权可以是分级进行的,被授权者的权限范围不能超过授权者的权限范围,具体做法是:在用户表中添加“授权者”字段,可以表明该用户之权限继承自该授权者,从而使该用户的权限范围控制在授权者的权限范围之内,从而实现分级授权。每个用户都有一个授权者,顶级用户授权者为System。

(5)权限制约。

通常来说,授权管理模块中角色权限的变动都由系统管理员决定,有一定的随意性。而本系统将“授权”和“审计”两个角色分别授予不同的用户,使最终被授权的用户需要经过授权和审计两步以后才能真正使用自己的权限。以此实现了权限制约,提高了系统

的安全性。

2.1 平台架构

整个权限管理平台由两部分组成,如图3所示。

管理控制台:根据RUP模型原理,提供权限管理操作;

应用程序调用控制台:是一组共用模块构件,供业务系统各应用模块调用,根据权限管理模型完成对用户数据库数据的读写权限控制。包括:

(1)用户身份确认检查;

(2)权限控制服务:业务系统提出请求,根据用户身份确认检查提供的用户所属角色名,通过查询数据库取得该用户所拥有的功能权限,由权限管理平台返回是否可执行的指令;

(3)会话信息管理:用户登录后的会话信息、操作信息管理;

(4)用户视图控制:根据权限控制理论的“最小权限”原则,通过对用户身份的判定为其自动定制相应的视图,既满足用户对功能的需求,又无法越权操作。

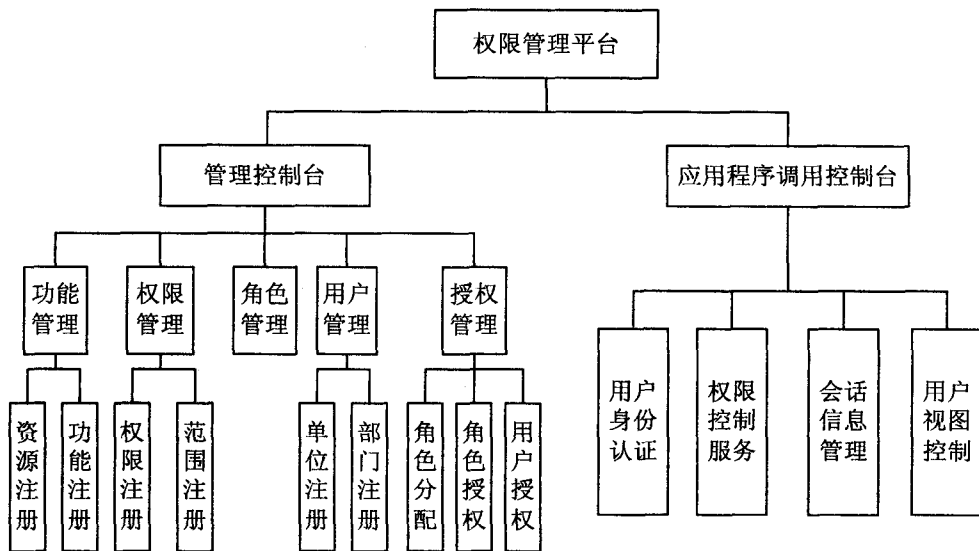


图3 权限管理平台功能结构

2.2 数据库设计

系统数据库设计的宗旨是能满足以下条件:

(1)清晰、合理、简洁地表述出用户—角色—权限三者之间的关系;

(2)便于扩展应用规模和附加的业务功能,要能体现出系统的通用性;

(3)权限管理变动与业务无关。

本系统涉及的数据表较多,不一一列举,这里主要列举其中比较重要的几个表:

①权限表:描述系统中完成业务单元动作所需的资源访问权以及资源访问的范围。权限表具有三个外键,分别对应“功能表”、“连续范围表”、“离散范围表”的主键。见表1。

②用户表:描述用户所属单位/部门信息,以及它在系统访问期间的关键数据操作记录。用户包括两个外键,分别对应部门表、单位表的主键。将单位和部门分开,是针对业务需求的实际情况,可以将行政区划及隶属关系和业务口进行分类管理。见表 2。

③用户权限分配表:描述用户表与权限表之间的对应关系。用户权限分配表有两个外键,分别是用户

表的主键和权限表的主键。见表 3。

④角色权限分配表:描述角色与权限之间的对应关系。角色权限分配表有两个外键,分别是角色表的主键和权限表的主键。见表 4。

⑤用户角色分配表:描述用户与角色之间的对应关系。用户角色分配表有两个外键,分别是角色表的主键和用户表的主键。见表 5。

表 1 权限表

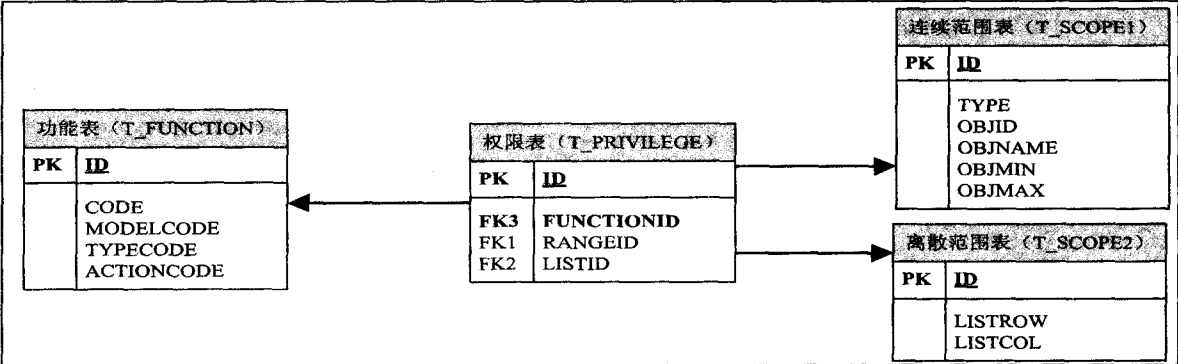


表 2 用户表

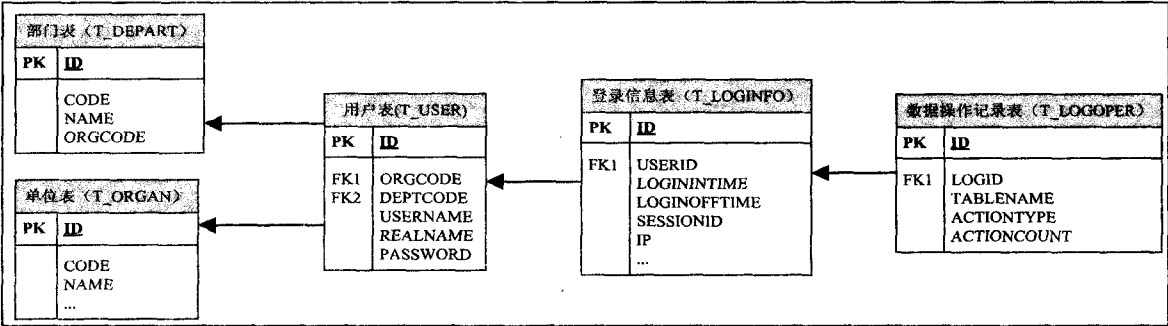


表 3 用户权限分配表

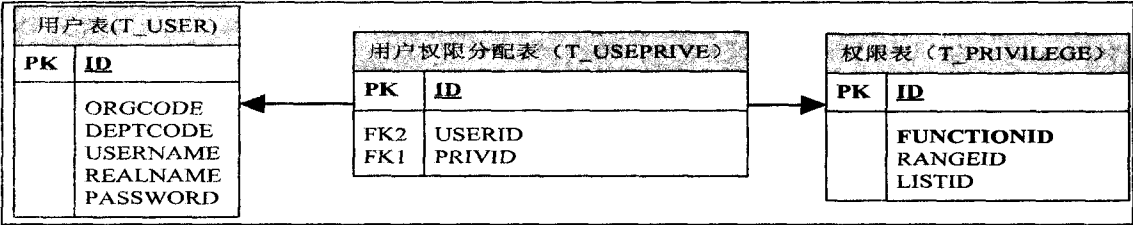


表 4 角色权限分配表

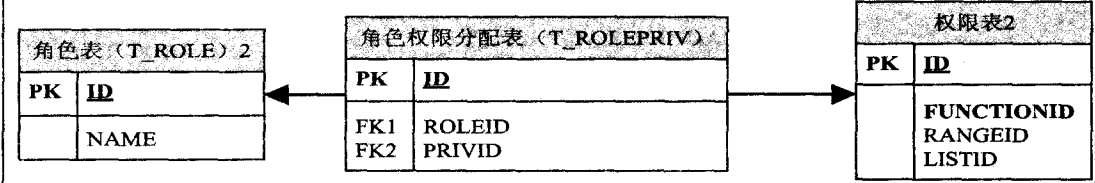
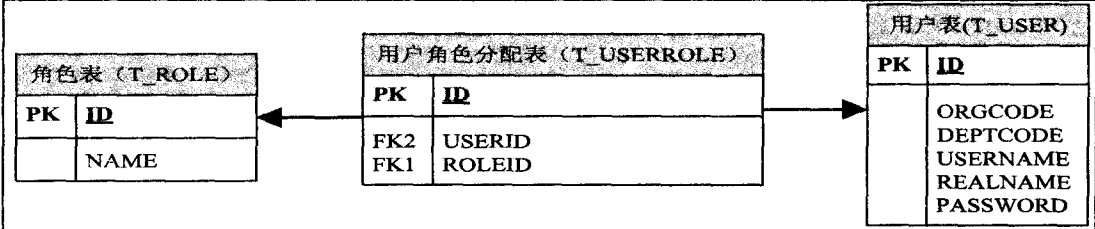


表 5 用户角色分配表



3 结束语

RBAC 模型通过将用户和角色相联系,降低了授权管理的复杂性,解决了具有大量用户和权限分配的系统中管理复杂性问题^[12]。但是由于该模型对角色的依赖性过大,限制了系统访问授权管理的灵活性和可变更性。因此,文中提出了一种改进的基于角色的通用性权限管理模型——RUP 模型。该模型在继承了 RBAC 优点的基础上着重强调了通用性和授权灵活的特点。最后,基于 RUP 模型设计并实现了一个通用的权限管理平台,该平台相较于以往的通用权限管理平台,具有管理粒度细化(即将系统资源分为功能和范围两部分,可以分别进行管理控制)、分级授权和权限限制的特点,使其能更广泛地满足各种业务系统复杂、多变的应用需求。

参考文献:

- [1] 蒋永,蒋玉明,彭思达.基于工作流用户权限管理模型的研究与设计[J].计算机技术与发展,2009,19(1):161-164.
- [2] 欧阳星明,张华哲.大型网络 MIS 系统中基于角色的权限管理[J].计算机工程与应用,2000,36(4):138-140.
- [3] 曹晟,杨浩,孟庆春.基于 PMI 的系统访问安全管理研

(上接第 239 页)

达到持续完善信息安全管理的目的。

信息安全管理体的建立与实施,能从根本上强化员工的安全意识,规范信息安全行为,可以有效的降低和避免企业的信息资产安全风险,增强了企业的竞争优势。而且管理体系是在动态的技术环境中进行的,以预防为主的方式使企业以最低的成本支出达到可接受的信息安全水平。因此,建立完整的信息安全管理体系是为企业发展提供可靠的保障。

4 结束语

企业应以战略目标为指导,以风险管理为核心,以技术手段为支撑,严格按照以上四个阶段构建一套完善的信息安全管理体系,保障企业信息资产的安全。

参考文献:

- [1] ISO/IEC27001:2005. Information Technology—Security Techniques—Information Security Management Systems—Requirements[S]. Geneva: International Organization for Standardization, 2005.
- [2] ISO/IEC27006:2007. Information Technology—Security Techniques—Requirement for Bodies Providing Audit and Certifica-

研究与设计[J].计算机工程,2007,33(24):141-143.

- [4] Snyder L. Formal Models of Capability-based Protection Systems[J]. IEEE Transactions on Computers, 1981, 30(3): 172-181.
 - [5] 赵志明,江楠,王力斌. J2EE 平台下权限管理的研究与实现[J]. 郑州轻工业学院学报(自然科学版), 2009, 24(3): 9-12.
 - [6] Sandhu R, Coyne E J. Role-based access control models[J]. IEEE Computer, 1996, 29(2): 38-47.
 - [7] Abrams M D, Eggers K W, La Padula L J. A generalized framework for access control: an information description[C]// Proceedings of the 13th National Computer Security Conference. [s. l.]: [s. n.], 1990: 135-143.
 - [8] 戴祝英,左永兴. 基于角色的访问控制模型分析与系统实现[J]. 计算机应用研究, 2004(9): 173-175.
 - [9] 李仲,杨宗凯,刘威. 一种基于 RBAC 的实现动态权限管理的方法[J]. 计算机技术与发展, 2006, 16(10): 1-4.
 - [10] 沈海波,洪帆. 访问控制模型研究综述[J]. 计算机应用研究, 2005(6): 9-11.
 - [11] 顾丽娜,郭炎,宋焱森. 一种通用权限管理系统的设计研究[J]. 科技咨询导报, 2007(28): 116-116.
 - [12] 季小明,汪家常. 基于 .NET 动态用户权限管理模型的设计与实现[J]. 计算机技术与发展, 2006, 16(10): 202-204.
-
- tion of Information Security Management Systems[S]. Geneva: International Organization for Standardization, 2007.
 - [3] 奇峰. COBIT 在企业信息安全管理中的应用实践[J]. 计算机应用与软件, 2009(10): 282-285.
 - [4] 孙强,陈伟,王东红. 信息安全管理: 全球最佳实务与实施指南[M]. 北京: 清华大学出版社, 2004.
 - [5] Saint-Germain R. Information Security Management Best Practice Based on ISO/IEC 17799[J]. Information Manage Journal, 2005(7-8): 60-66.
 - [6] 赵昌伦,武波. 基于 .NET 的军队计算机网络信息安全对策[J]. 计算机技术与发展, 2009, 19(1): 150-153.
 - [7] 万东,曹木恒. 基于 ISO27001 的 IDC 信息安全管理体[J]. 信息安全与通信保密, 2009(1): 75-77.
 - [8] 李力. 信息安全建设和管理的生命周期[J]. 信息安全, 2006(9): 54-56.
 - [9] 黄松,夏洪亚,谈利群. 基于模糊综合的信息安全风险评[J]. 计算机技术与发展, 2010, 20(1): 189-192.
 - [10] 黄水清,朱晓欢. 基于 ISO27001 的数字图书馆信息资产风险评估[J]. 图书情报工作, 2006(11): 79-82.
 - [11] 罗佳,杨世平. 基于嫡权系数法的信息安全模糊风险评估[J]. 计算机技术与发展, 2009, 19(10): 177-180.
 - [12] 杨晓明,罗衡峰,范成瑜,等. 信息系统安全风险评[J]. 计算机应用, 2008(8): 1920-1923.