第41卷 第6A期
2014年6月

计 算 机 科 学
Computer Science

Vol. 41 No. 6A
June 2014

基于RBAC的复杂信息系统中访问控制模型的设计

强振平[1] 何丽波[2] 陈 旭[1] 李 彤[2]

(西南林业大学计算机与信息学院 昆明 650224)[1] (云南大学软件学院 昆明 650500)[2]

摘 要 针对复杂信息系统中因角色数量多、用户职责属性经常动态改变等导致访问控制复杂的问题,在充分考虑用户的组织形式与授权关系的基础上,以用户所在机构、用户分组信息为角色分配主体,同时增加信息系统中资源访问操作权限范围限定,改进了RBAC模型并设计了实现改进模型的数据关系。实践结果显示,改进模型不仅可以方便地完成机构和用户组职责改变时对所涉及用户授权的修改,而且可以快速响应因人员职责属性改变引起的授权修改,同时能够灵活地完成资源访问操作权限的控制。

关键词 RBAC,访问控制,权限管理,资源管理,用户组

中图法分类号 TP311 **文献标识码** A

Design of the RBAC-based Access Control Model in the Complex Information Systems

QIANG Zhen-ping[1] HE Li-bo[2] CHEN xu[1] LI Tong[2]

(Department of Computer and Information Science, Southwest Forestry University, Kunming 650224, China)[1]

(National Pilot School of Software, Yunnan University, Kunming 650500, China)[2]

Abstract To the complexity control problems in a complex information systems which was usually caused by the management of large numbers roles and the dynamically changing of the user's responsibilities attributes, in this paper, we based on the full consideration of the relationship between the user's authorization and the form of the use's organization, used the organization and group as the main body to assigned the roles, and increasing the resource access permissions scope defined in information system, we proposed an improved RBAC model and designed the realized data relationships. Practical results show that not only can be easily complete the authorization which caused by the responsibilities changing of the organization and groups, and can quickly respond to the change of the property caused by the personnel duty, at the same time can flexibly achieve the resource access permissions.

Keywords Role-based access control, Access control, Authority management, Resource management, User group

1 引言

随着信息系统的快速发展,信息系统越来越紧密地与业务、财务等核心数据相关联,其中涉及的权限管理已经成为了整个信息系统的基础和核心,甚至影响到整个系统的正常运行,这使得信息系统安全、可靠的访问控制策略成为了一个大的挑战。

传统访问控制策略主要包括两类:1)自主访问控制策略DAC(Discretionary Access Control),通过主体自主授权给其他主体,在灵活方便的同时,往往因个别特权用户不受控的授权造成系统安全问题;2)强制访问控制MAC(Mandatory Access Control),通过主体与客体的安全级别判定主体是否具有访问客体的权限,这种严格的级别约束使得整个系统实现困难,同时不适宜存在变化的应用环境。这些缺陷使得传统的访问控制策略无法满足信息化系统的广泛应用,在此情况下,1991年Ravi Sandhu提出了基于角色访问控制模型的概念,并1996年在IEEE Compute上提出了"基于角色的访问控制模型(Role-based Access Control Models, RBAC)"的框架[1],一般称为RBAC96;2001年,David Ferraiolo, Ravi Sandhu进一步提炼、整理和标准化了该模型[2];2004年,美国国家信息技术标准委员会(ANSI INCITS 359-2004)将标准化的模型指定为美国的国家标准ANSI RBAC[3]。在此模型中,通过引入角色,将主体用户与客体权限进行了逻辑分离,具体授权过程通过两步完成,首先,系统的管理人员根据系统使用职责需求,定义不同的角色,对于不同角色分配不同的权限,建立角色与权限的关系;第二步,在用户授权时,给不同用户分配不同的角色,使得不同的用户具有了相应的权限。实际应用中,通过用户与角色的多对多的关系、角色与权限的多对多的关系方便地完成了权限的管理。即通过RBAC授权,就可以完成"谁(Who)对什么(What)进行怎样(How)的操作"的限定。

RBAC模型并不是一个非常完善的模型,存在许多问题,

本文受国家自然科学基金项目:云计算环境下双模型驱动的面向软件动态演化的建模与分析(61379032)资助。

强振平(1981—),男,硕士,讲师,主要研究方向为软件工程、数字图像处理,E-mail:zhenpingqiang@gmail.com;何丽波(1982—),女,博士生,主要研究方向为软件工程;陈 旭(1973—),男,博士,副教授,主要研究方向为软件工程、遥感图像处理;李 彤(1963—),男,博士,教授,主要研究方向为软件过程方法与技术、软件工程,E-mail:tli@ynu.edu.cn(通信作者)。

在文献[4]中对RBAC模型研究历程中的系列问题进行了分析，而在实现的使用中，特别突出的包括：(1)批量用户的授权，特别是信息系统中常存在同一部门的人具有相同的授权，但当部门的权限改变时，RBAC模型存在大量的授权操作；(2)功能与资源的统一授权问题，在信息系统中，往往存在相同角色的用户具有相同的功能权限，但是其可操作的用户数据或者资源对象的权限存在差异；(3)单点登录认证系统中不同业务系统的集中授权，通过RBAC模型需要定义不同系统中的角色，再进行统一管理角色、权限及用户，增加了系统的复杂度。此外，复杂系统中对于不同的任务、工作流过程存在不同的授权，而且授权操作会涉及不同的分布式系统，存在跨域的访问控制授权，以及存在不同时空相关的授权，这些在RBAC基础模型中都很难直接解决。前3个问题是本文研究解决的重点，后续问题在综述文献[5,6]中给出了解决方法。

本文通过对RBAC模型的研究，设计了基于RBAC的复杂信息系统中访问控制模型，并且通过实例进行验证。具体组织结构为：本文第3节介绍本文提出模型的设计，并结合实际应用案例分析本文模型解决前3个问题的具体过程；最后提出模型的特点及全文的总结，并给出下一步具体工作。

2 相关研究

RBAC模型自提出后，一直是访问控制领域内的一个研究热点，最初的RBAC96由用户(User)、角色(Role)、会话(Session)及授权(Permission)4个基本要素构成。大量研究人员基于RBAC96展开了研究。

一方面，为了更好地管理RBAC，Sandhu等相继提出3个RBAC的管理模型：ARBAC97(Administrative RBAC97)[7,8]、ARBAC99[9]、ARBAC02[10]。ARBAC97在RBAC模型中加入了管理员角色，强调了角色管理角色，即通过管理角色完成对规则角色的管理。ARBAC99在ARBAC97的基础上扩充了可移动和不可移动用户，增强了用户和权限分类处理的稳定性。ARBAC02在ARBAC99的基础上引进了“组织结构”的概念，作用于用户和权限池，取代了角色层次结构中的先决条件角色，同时，基于“组织结构”设计了一个自底向上的权限分配管理方案。这3个模型中都包括了角色范围及角色继承的管理，系统的安全性主要由管理员保证，但未考虑不同用户的差异、信息流控制机制等情况。随着系统规模、用户、功能的增加，系统中的授权管理越来越复杂，基于RBAC的授权管理在效率及安全性方面都面临严峻的挑战。另一方面，基于具体的应用系统需求，许多研究者完成了对RBAC模型的扩展。Xinwen Zhang等在文献[11]中提出在RBAC中增加灵活的委托模型(Permission-based Delegation Model，PBDM)，其本质是一种转授权，即通过用户将自己的权力转授给其他的用户，被转授的用户可以代替授权用户执行相应的权力。PBDM支持用户到用户、角色到角色的多级委托，同时清晰区分了安全管理和委托。考虑信息系统中不同任务对安全需求的不同，朱君在文献[12]中对委托授权模型进一步扩展，提出了基于角色和任务的转授权模型(Task and Role-Based Delegation Model，TRBDM)，支持了委托授权的时效性、职责分离的约束，同时考虑了角色层次、多级授权及授权回收策略等。

此外，用户的授权往往也会因部分环境属性的改变发生变化，如时间、地理位置、机构信息等动态属性，特别是基于SOA应用中的挑战，E Yuan等在文献[13]中提出了一种基于主体、客体及环境属性的属性访问控制模型(Attribute-Based Access Control，ABAC)，证明了其在动态信息访问过程中的优势。考虑RBAC中不采用基于角色的授权方式，在文献[14]中，J. Xin等提出了一种ABAC与RBAC联合的以角色为中心基于属性的访问控制模型(Role-Centric Attribute-Based Access Control，RABAC)，该模型中将角色作为一项属性，即将角色作为属性的一个成分完成授权，在确保RBAC安全优点的同时，避免了其实现的复杂，同时通过ABAC保证了实时环境改变引起访问控制改变的应用。Ed Coyne等进一步论证了ABAC与RBAC共存模型是一种可扩展的、灵活的和可审计监管的访问管理模型[15]，并且给出了RABAC中授权过程的处理流程。近年，随着移动设备在企业和政府机构信息系统中日益占据主导地位，需要更加细粒度的访问控制，Michael等[16]基于近场通信(Near Field Communication，NFC)技术确定用户请求位置信息及验证位置信息，提出了一种结合空间约束的增强型RBAC模型，支持了基于位置的访问控制策略。类似地，在文献[17]中，Kirkpatrick等提出了一种空间位置与邻近约束(A Proximity-based Spatially Aware RBAC，Prox-RBAC)模型，对于敏感资源，只有用户在受信任的位置才能访问，即要求访问用户在指定的位置才能获取与位置相关角色的权限。

以上基于RBAC及改进的RBAC模型的出发点都是制定标准通用的信息系统授权管理模型，但针对组织结构职责明确、用户数量巨大，存在功能授权、资源授权划分等的复杂信息系统，在保证安全的同时需要结合实际情况设计实用的授权管理模型。本文在RBAC模型的基础上，考虑实际信息系统授权与用户、用户组织机构、用户类型组、系统模块及系统资源等信息系统实体相关的特性，融入组织机构、用户组到系统授权管理中，并对数据资源设定所属机构及不同的访问域，增强对数据资源访问控制的管理。改进后的模型在实际的项目中得到了应用，模型的灵活性及可维护性得到了认同。

3 改进的RBAC模型

3.1 引入组织机构、用户组到RBAC模型

在RBAC模型中通过角色建立用户与权限的对应关系，突出了权限的集合，对于用户的组织方式考虑不足，而实际的行业系统中一般存在明显的用户组织方式，最突出的包括两方面：用户的组织机构及用户类型组，在大型信息系统中，每个用户本身的属性必然带有机构信息，对于分工明确的行业，用户具有明确的组信息。这些信息在实际业务处理过程中已经具有明确的权限及操作访问数据资源的范围，通过RBAC的访问控制未能充分考虑用户的这些属性，仅仅通过用户的不同角色进行授权，会使授权的过程非常繁琐，同时用户的机构信息本身就具有明确的权限等级，类似于角色的权限继承，通过对不同的机构设置不同的角色，可以方便地完成整个行业内的角色管理。

在RBAC模型中引入组织机构、用户组后，对于同一个组织机构、用户组可以设置不同的权限(实际本文改进模型中给不同的组织机构、用户组授予不同的角色)。在用户职位调动后，其机构、分组属性随即发生改变，其对应于机构、分组的

授权随用户机构、分组属性的改变而改变，大部分与机构、分组存在明确授权关系的业务系统不需要进行任何授权的修改；当行业业务发生调整时，通过修改不同机构及分组的权限，可以方便地完成整个机构、分组相关的用户权限的改变，从而大大简化授权的管理。

3.2 区分功能授权与资源操作授权

在大型企业信息系统中，存在多业务系统的集中统一授权管理，特别是在用户多、业务系统庞杂的综合管理系统中，如何有效地管理功能权限和操作访问资源权限也是一个非常现实的问题。通过 RBAC 模型解决这个问题，需要设置大量的角色进行权限管理，甚至同一个用户在不同系统中都需要根据不同的资源设置不同的角色，增加了系统授权管理的困难。本文基于 RABC 模型，引入系统管理、模块管理及与角色相关的授权管理，能够方便地完成不同业务系统模块功能的集中授权管理；对于资源操作的授权，根据实际系统使用中数据资源和机构一般具有实质的联系，一方面通过在资源中设置访问域或者机构属性，限定资源的访问范围，另一方面，对于保密要求高的资源，通过单独角色资源授权管理进一步限定授权。

3.3 改进的 RBAC 模型的设计

本文在 RBAC 的基础上，融入组织机构、用户组进行授权管理，同时对授权对象根据实际情况中属于同一角色的用户根据机构属性的不同对数据或资源对象的访问权限存在不同的情况，将授权对象划分为：资源权限、功能权限及管理权限，进行授权的分别管理，使得整个授权控制过程更加灵活安全。图 1 即为改进的 RBAC 扩展模型。

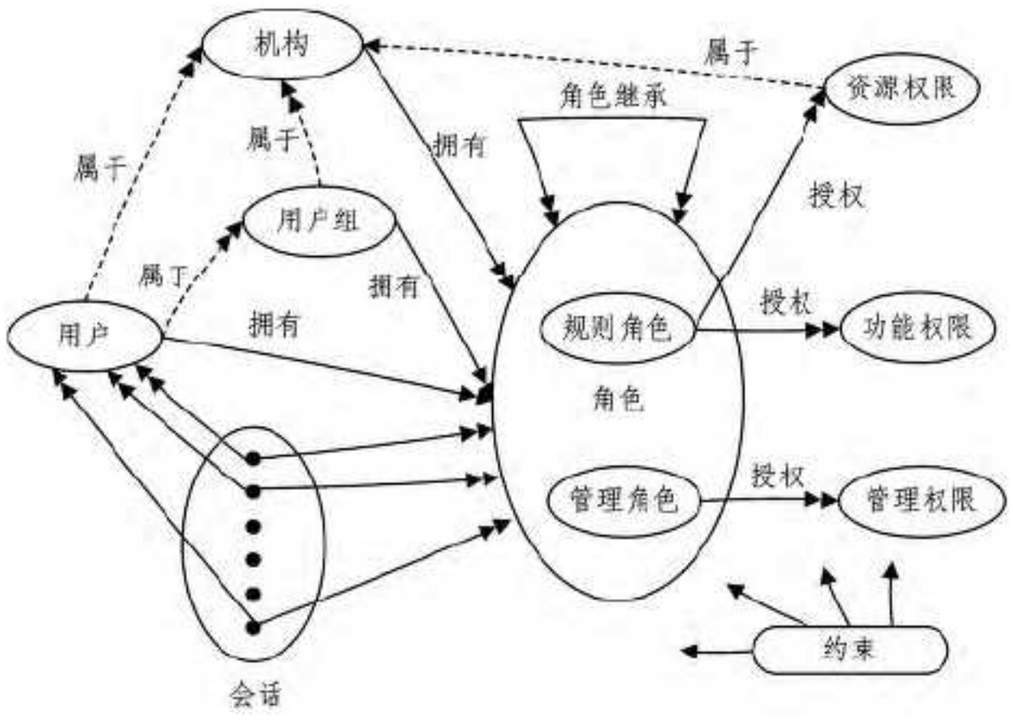

图 1 改进的 RBAC 扩展模型

在图 1 改进的 RBAC 扩展模型中，通过将用户归属于机构、用户组，授予机构、用户组不同的角色。定义模型中的元素：U 为用户集，R 为角色集，O 为机构集，G 为用户组集，UA 为用户角色分配表，$UA \subseteq U \times R$，OA 为机构角色分配表，$OA \subseteq O \times R$，GA 为用户组角色分配表，$GA \subseteq G \times R$。进一步定义：(1)R_1 为用户 U 拥有角色的关系；(2)R_2 为用户 U 属于机构的关系；(3)R_3 为用户 U 属于组织 G 的关系；(4)R_4 是机构 O 拥有角色的关系；(5)R_5 是组织 G 拥有角色的关系。则用户通过所属机构获得的角色为复合关系 $R_2 \circ R_4$，用户通过所属组织获得的角色为复合关系 $R_3 \circ R_5$。

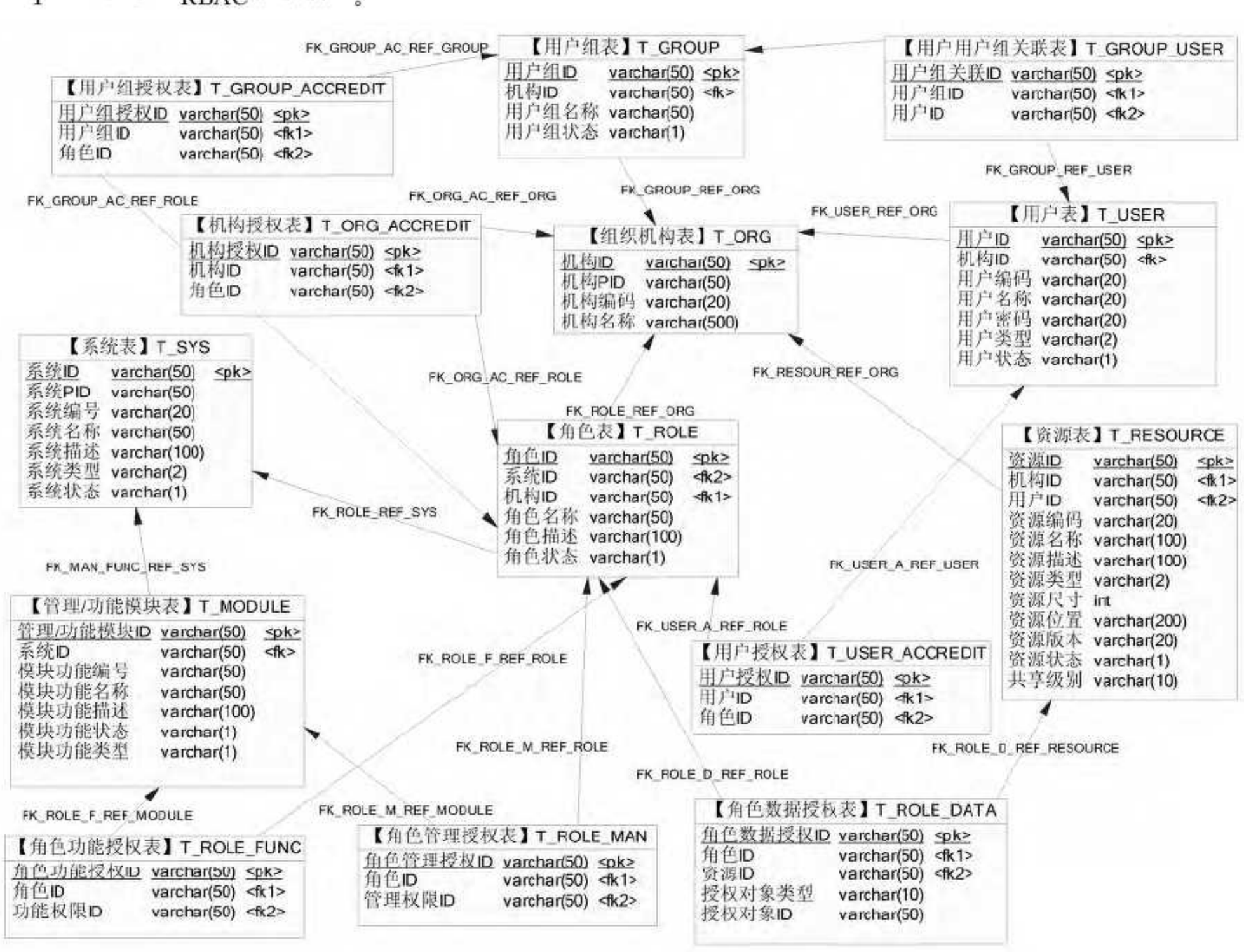

图 2 改进的 RBAC 扩展模型数据关系设计表

通过以上定义，在改进的 RBAC 扩展模型中，用户得到授权的角色为：$R_1 \cup R_2 \circ R_4 \cup R_3 \circ R_5$。

改进模型的实际应用中，一般不直接设置用户与角色的关系，用户的授权都是通过对用户所在机构及用户组授予角色，管理用户与功能、资源的访问控制关系，对于资源访问控制，通过限定资源所属机构、资源共享或者操作级别进一步限定，通过角色数据授权完成对资源操作的管理。

访问控制管理的实现需要对模型中的数据进行存储、检索等各种操作。图 1 扩展模型设计思想的应用，必须设计和实现一套有效的模型数据访问控制接口，用于对模型相关数据的操作。图 2 为改进的访问控制模型的数据表设计图。具体包括了 14 张数据表。

基于图 2 设计的数据关系表，课题组以 JAVA 为开发语言，数据库采用 Oracle 11g，设计实现了某集团企业内部资源管理、办公自动化系统、项目信息管理等信息业务系统的集中授权管理，对授权管理中涉及的系统根据机构使用特点设定了各系统角色，整个系统中未对任何用户进行直接角色分配（主要通过新增虚拟分组方式完成了对用户的管理，如系统管理员通过设定隶属于信息中心的管理员虚拟分组进行角色分配）。在系统试运行中，通过角色新增、修改、删除等基本操作，使得整个授权管理很好地适应了集团内部人事、职责等动态变化，同时在新系统投入使用时，通过新增数据库中系统表、管理/功能模块表及资源表记录，修改角色授权表记录（必要时需要新增角色）完成新增系统的统一授权接入管理，增强了对用户授权的灵活管理及系统扩展维护管理。

3.4 改进的 RBAC 模型的应用分析

针对本文引言部分总结的 RBAC 模型的突出问题，对于组织机构庞大、人员数量多的系统，通过对机构、用户组授权分配角色，尽量避免直接对用户分配角色。一方面，在机构、用户组权限发生改变时，可以避免对大量用户授权的修改；另一方面，在人员发生调动、隶属关系发生改变时，也可以避免授权的修改，有效解决了用户、机构的动态变化对系统带来的影响。通过设计系统表、管理/功能模块表及资源表将各种业务系统统一授权管理，并且对于资源限定其所在的机构及共享或操作级别，属于相同角色但属于不同机构的用户在相同系统功能操作界面中只能访问属于自己机构的数据。

改进的 RBAC 扩展模型通过避免对用户的直接角色分配，避免了因用户自身属性改变引起访问控制系统的修改。同时，在机构职责改变过程中能够快速完成涉及人员的授权修改，增强了 RBAC 模型中的授权管理能力，提高了整个授权管理的效率。通过对授权管理系统、模块、资源的统一管理，在一定程度上使得访问控制系统独立于业务信息系统，保证了整个模型的重用性。

结束语　本文设计模型从用户的有效组织为出发点，在 RBAC 模型中以用户的机构、分组信息为用户角色分配的主体，提高了模型使用的稳定性，降低了安全管理人员的授权复杂度。另一方面，增加信息系统内资源操作权限的管理范围约束，在统一资源管理的基础上方便了资源的有效利用。

RBAC 模型的研究及应用不仅涉及到信息系统领域，同时与管理、工作流等领域存在密切联系，但本文模型应用中未涉及随业务流程、任务过程、管理方法而发生的角色改变问题，及基于用户身份的细粒度访问控制问题，未考虑用户身份未改变但因接入位置、方式不同引起的授权差异等复杂的安全控制问题。这些问题的解决需要在模型中引入动态访问控制矩阵、控制域，甚至引入动态信任阈值机制等访问控制模型进一步完善。此外，RBAC 模型中存在许多部件，可以分割来进行管理：用户角色指派、角色权限指派、角色继承、约束限定等等，这些管理工作需要系统对管理员进行分工约束，这些方面还需要做进一步的研究工作。

参 考 文 献

[1] Sandhu R, Coyne E, Feinstein H. Role-based Access Control Models[J]. IEEE Computer, 1996, 29(6): 38-47

[2] Fereaiolo 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

[3] ANSI. American National Standard for Information Technology—Role Based Access Control[C]// ANSI Int'l Committee for Information Technology Standards. Feb. 2004: 359

[4] 刘强，王磊，何琳. RBAC 模型研究历程中的系列问题分析[J]. 计算机科学，2012，39(11)：13-18

[5] 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

[6] 李凤华，史国振，马建峰. 访问控制模型研究进展及发展趋势[J]. 电子学报，2012，40(4)：805-813

[7] Sandhu R, Bhamidipadi V. The URA97 Model for Role-Based User-Role Assignment, Database Security XI: Status and Prospects[J]. Chapman & Hall, 1998

[8] Sandhu R, Bhamidipati V, Munawer Q. The ARBAC97 model for role-based administration of roles[J]. ACM Transactions on Information and System Security, 1999, 2(1): 105-135

[9] Sandhu R, Munawer Q. The ARBAC99 model for administration of roles[C]// Proceedings of the Annual Computer Security Applications Conference. Phoenix, USA, 1999

[10] Sandhu R, Munawer Q. A Model for Role Administration Using Organization[C]// Proceedings of the SACMAT'02. Monterey, California, USA, 2002: 155-162

[11] Zhang Xin-wen, Oh S, Sandhu R. PBDM: A Flexible Delegation Model in RBAC[C]// Proceedings of SACMAT'03. Como, Italy, 2003: 149-157

[12] 朱君. 角色协同中群体感知和访问控制技术研究[D]. 广州：中山大学，2009

[13] Yuan E, Tong J. Attributed based access control (ABAC) for Web services[C]// 2005 IEEE International Conference on Web Services, 2005 (ICWS 2005). 2005: 11-15

[14] Xin J, Krishnan R, Sandhu R. A Role-Based Administration Model for Attributes[C]// Proc. 1st Int'l Workshop Secure and Resilient Architectures and Systems. ACM, 2012: 7-12

[15] Coyne E, Weil T R. ABAC and RBAC: Scalable, Flexible, and Auditable Access Management[J]. IEEE Computer Society, IT Professional, 2013, 15(3): 14-16

[16] Kirkpatrick M S, Bertino E. Enforcing Spatial Constraints for Mobile RBAC Systems[C]// Symposium on Access Control Models and Technologies-SACMAT. 2010: 99-108

[17] Kirkpatrick M S, Damiani M L, Bertino E. Prox-RBAC: a proximity-based spatially aware RBAC[C]// Proceedings of GIS. 2011: 339-348