知识管理系统中的角色-角色授权的实现研究

卿 竹[1,2]
(1.重庆工商职业学院,重庆 400052;
2.重庆大学 计算机学院,重庆 400044)

摘 要:在知识管理系统中,特别是文档管理系统中,为方便指派管理,多采用把用户分为用户组的方式进行用户-角色指派和权限组进行权限-角色指派,但其中的用户组和权限组在 RBAC 中无对应概念。ARBAC 模型包含 3 个子模型,其中的 RRA 可实现对用户和权限的分组管理。为了与 RBAC 统一,可采用 RRA 实现对用户和权限的分组管理。

关键词:知识管理;访问控制;RBAC RRA
中图分类号:TP311.131 文献标识码:B

Study on the realization of RRA in knowledge management system

QING Zhu[1,2]
(1.Chongqing Technology and Business Institute, Chongqing 400052,China;
2.College of Computer Science,Chongqing University,Chongqing 400044,China)

Abstract: RBAC has divided user and permission into different groups. There exist two methods of user-role assignment and permission-role assignment. So in knowledge management system, especially document management system, RBAC provides a convenient assignment management. ARBAC has three sub models, one of these three models is RRA which can be used for management of users and permissions with group. We can use RRA for this management in RBAC.

Key words:knowledge management; access control; RBAC RRA

知识文档管理是知识管理系统的重要组成部分。文档访问控制管理主要解决不同人对不同文档的访问权限问题,完善的访问控制体制能确保文档管理的高度安全性,保障知识文档信息的完整性和可靠性。由于文档管理系统中存在大量文档,系统中能够访问文档的用户数量庞大,因此如何有效地实现针对文档的访问控制是一个重要问题。本文主要针对文档管理中的用户和权限管理,探讨如何通过有效方便的用户管理,实现对文档的有效管理。

基于角色的访问控制技术——RBAC,作为信息完全领域的一种新技术,正不断受到重视。在 RBAC96 [1] 中与用户管理相关的是 RRA97[2]。RRA97 引入了 3 种角色概念:Abilities、Groups、UP-Roles,分别称为能力角色、组角色和混合角色。其成员分别由权限或其他能力角色、用户或其他组角色、权限和用户以及其他混合角色构成。3 种角色可分别记做 A、G 和 UPR。

RRA 定义了两种指派操作:can-assigna 和 can-assigng [3]。can-assinga 比照 PRA 定义的能力角色和权限之间的关系,实质就是将不可分割的权限组织成一个整体;can-assigng 是比照 URA 定义的组角色和用户之间的关系,对用户进行分组。相应地,定义了各自的 revoke 操作。参考文献[5] 涉及了如何对用户进行分组和对用户组管理。

1 RRA 的实现

1.1 RRA 基本操作

RRA 中,通过将用户和权限进行分组,分别指派给组角色和能力角色实现对用户和权限的分组管理。本文将实现 RRA 中的以下问题:用户-组角色指派与撤销、权限-能力角色指派与撤销、组角色-角色指派与撤销、能力角色-角色指派与撤销、组角色管理、能力角色管理。

用户-组角色指派与撤销过程的实质是将用户分配到合适的组角色中,并将用户从组角色中删除,实现用户的分组管理。借用 URA 定义,可将其过程定义为:

定义 1 用户-组角色指派关系 can-assignUG$\subseteq$AR$\times$CR$\times 2^{G}$。其中,AR、CR 含义同 URA,G 为组角色。CR 中的角色也为组角色。

定义 2　用户-组角色撤销关系 can-revokeUG⊆AR×2^G。其中，AR、G 含义同定义 1。

用户-组角色指派过程中存在指派先决条件，因而需要在 RRA 实现中体现出来，本文将考虑该因素。

权限-能力角色指派与撤销过程实质是将权限进行分组管理，通过将不可分离的权限组织成一个权限组来方便角色-权限指派。借用 PRA 可将其关系定义为：

定义 3　权限-能力角色指派关系 can-assignPA⊆AR×CR×2^A。其中，AR、CR 含义同 URA，A 为能力角色。CR 中的角色也为能力角色。

定义 4　权限-能力角色撤销关系 can-revokePA⊆AR×2^A。其中，AR、A 含义同定义 3。

定义 5　组角色-角色指派关系 can-assignG⊆AR×CR×2^R。组角色-角色撤销关系 can-revokeG⊆AR×2^R。其中，AR、CR 含义同 URA，R 为角色。

定义 6　能力角色-角色指派关系 can-assignA⊆AR×CR×2^R。组角色-角色撤销关系 can-revokeA⊆AR×2^R。其中，AR、CR 含义同 URA，R 为角色。

组角色更多的是反映用户的组织结构，因而存在着组角色之间的上下级和包含关系，为了和 RBAC 统一，可将这种关系看作继承关系。

定义 7　组角色 G 之间的继承关系 GH⊆G×G 为组角色 G 之间的偏序关系。

相应地，能力角色之间也存在着上下包含关系，同样可用继承关系定义。

定义 8　能力角色 A 之间的继承关系 AH⊆A×A 为能力角色 A 之间的偏序关系。

在实际应用中，组角色、能力角色的创建与维护由系统管理员完成。

1.2 主要表结构及其之间的关系

1.2.1 用户 – 组角色及组角色 – 角色之间的关系

用户、组角色及组角色、角色之间的关系如图 1 所示。其中，各表的含义分别为：

User：用户基本信息，主要是用户编号、用户名和密码。

Role：角色基本信息，主要包括角色编号、角色名。

UserRoleAssignment：用户-角色指派关系，主要是用户编号和角色编号之间的对应关系。

UserGroupAssignment：用户-组角色指派关系，主要是用户编号和组角色编号之间的关系。

GroupRoleAssignment：组角色-角色指派关系，主要是组角色编号和角色编号之间的关系。

GroupRole：组角色基本信息，主要是组角色编号，组角色名和组角色之间的继承关系。

URA-CR：用户-角色指派时应当满足的指派先决条件。

UGA-CR：用户-组角色指派时应当满足的指派先决条件。

1.2.2 权限 – 能力角色及能力角色 – 角色之间的关系

权限、能力角色及能力角色、角色之间的关系，如图 2 所示。其中，各表的含义分别为：

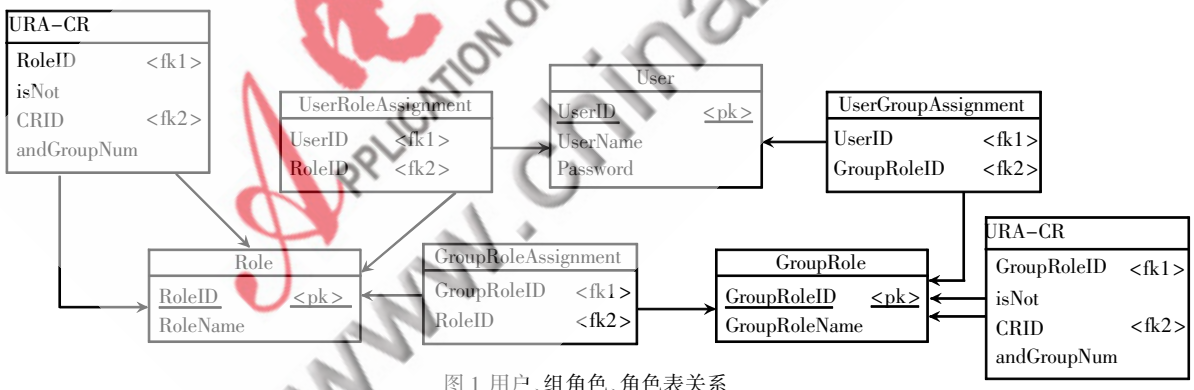

图 1 用户、组角色、角色表关系

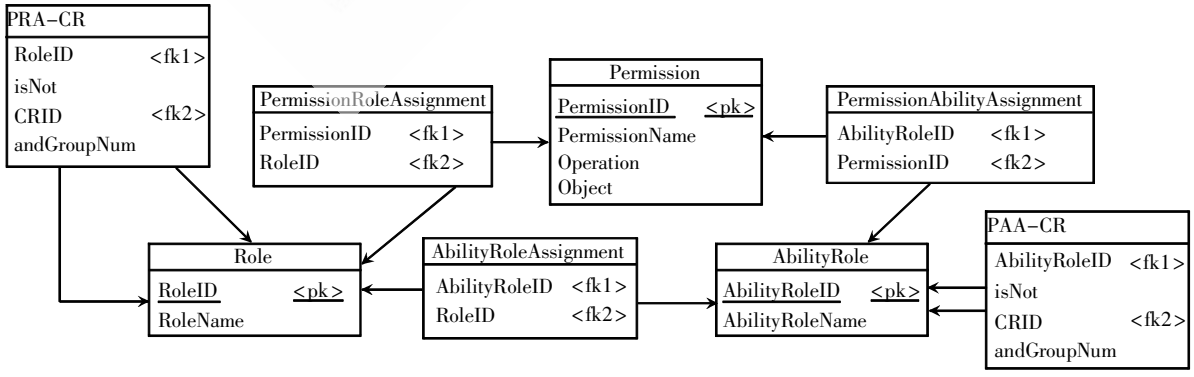

图 2 权限、能力角色、角色表关系

Permission：权限基本信息，主要是权限编号、权限名、该权限对应的操作和针对的对象。

Role：角色基本信息，同上小节。

PermissionRoleAssignment：权限-角色指派关系，主要是权限编号和角色编号之间的关系。

PermissionAbilityAssignment：权限-能力角色指派关系，主要是权限编号和能力角色编号之间的关系。

AbilityRole：能力角色基本信息，主要是能力角色编号、能力角色名和能力角色之间的继承关系。

AbilityRoleAssignment：能力角色-角色指派关系，主要是能力角色编号和角色编号之间的关系。

PRA-CR：权限-角色指派先决条件，字段含义同上小节。

PAA-CR：权限-能力角色指派先决条件，字段含义同上小节。

PRA-CR，PAA-CR 表中数据的关系同 UGA-CR 和 URA-CR 表。

2 实际应用

在规划局的知识管理系统中实现了利用 RRA 实现对用户和权限的分组管理。系统结构如图 3 所示。

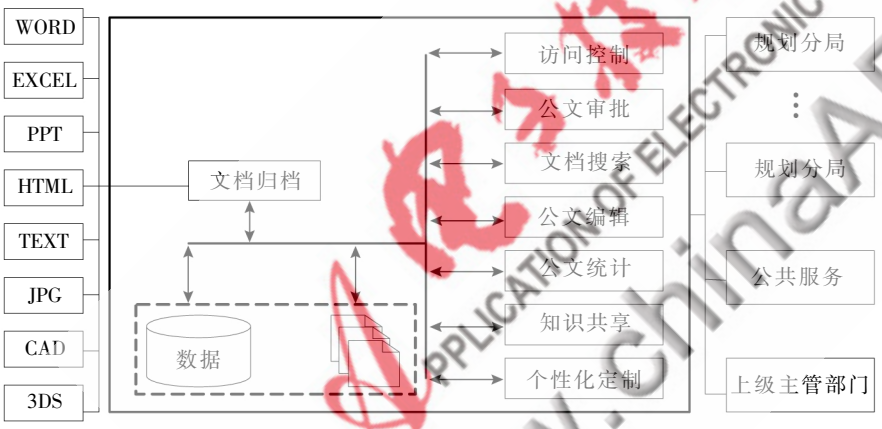

图 3 知识管理系统模块结构

2.1 用户分组管理

由于系统中用户较多，同一科室的工作人员的权限稍有不同。由于 RBAC 本身要求在进行角色设置时（此处的角色指 PRA 过程中的角色）尽量减少角色数量，以便简化角色继承关系的管理，而在本系统中的角色设置时考虑到用户实际组织结构的设置、角色名与职位名相同。在实际工作中，某些工作人员可能暂时具有不属于该科室的权限。此时可先建立一个用户组角色，为该组角色指派相应的角色，然后将该组角色指派给多个工作人员。由于用户组角色不进入角色继承系统，因而对原有角色继承关系不需要修改。同时利用组角色进行用户-角色指派，由于对多个工作人员只需要进行一次用户-用户组角色的指派操作，而不需要进行多次用户-角色的指派操作，因而当用户组中用户较多时，此法可减少用户-角色指派操作数量。

2.2 权限分组管理

该系统中，用户具有对知识管理系统中操作文档的权限，而操作权限可进一步细分为查询、录入、修改、打印等权限，需将这些权限作为一个整体指派给角色，不宜分开指派。此时可将这类不能分开的权限指派给能力角色，再将能力角色指派给角色即可。将权限指派给能力角色后，不同能力角色之间可形成继承关系。

针对知识文档管理系统中，通过将用户和权限进行分组，方便地实现用户-角色指派和权限-角色指派管理。对用户-组角色指派、权限-能力角色指派和撤销关系作了定义。设计了实现 RRA 需要的表，并给出了表之间的关系。同时，实现了指派先决条件的表示和存储，该指派先决条件可实现角色之间的互斥约束关系。最后，给出了一个具体的例子说明 RRA 的应用。

参考文献

[1] RAVI S. Role-based access control models [J]. IEEE Computer, 1996, 29(2):38-47.

[2] RAVI S, VENKATA B. The ARBAC97 model for rolebased administration of roles [J].TISSEC, 1999, 2(1):105-135.

[3] RAVI S, QAMAR M. The RRA97 model for role-based admini stration of role hierarchies[C]. In Procee-dings of 13th Annual Com puter Security Application Conference, Scottsdale, AZ, December 7-11, 1998.

[4] 何海云，张春，赵战生.基于角色的访问控制模型分析[J].计算机工程，1999，(8):39-44.

[5] OSBORN S. GUO Y.Modeling users in role-based access control[M]. ACMRBAC,2000.

(收稿日期：2009-02-24)

(上接第 49 页)

[3] SONKA M, HLAVAC V, BOYIE R.图像处理分析与机器视觉[M].艾海舟，武勃，译.北京：人民邮电出版社，2003.

[4] PREWITT J, MENDELSOHN M. The analysis of cell images[J]. Annals of the N.Y. Academy of Sciences,1966, (128):1035-1053.

[5] 姚敏.数字图像处理[M].北京:机械工业出版社, 2006.

(收稿日期：2009-07-13)