

RBAC模型中角色互斥研究及应用

陈 胜, 娄渊胜, 张文渊

(河海大学, 江苏 南京 210098)

摘 要:应用系统的用户数量和系统角色越来越多,使得角色间的互斥也更加频繁。而角色互斥作为一种实施职责划分的有效手段,在基于RBAC模型的访问控制中具有非常重要的作用。目前关于角色互斥的研究还不够完善,为了更好地处理角色间的互斥关系,文中对RBAC下的角色互斥进行了研究,通过分析角色的本质列举了角色互斥的各种类型,并在此基础上设计了角色约束表,通过形式化的方法给出了角色约束表的组建和角色互斥撤销的方式。最后实现了一个带角色互斥检测的角色分配控制器,能够很好地根据角色互斥关系来进行角色分配,并成功应用到了一个简单系统中。

关键词:基于角色的访问控制;角色互斥;角色分配;互斥撤销

中图分类号:TP39

文献标识码:A

文章编号:1673-629X(2012)12-0021-04

Research and Application of Exclusion Role in RBAC Model

CHEN Sheng, LOU Yuan-sheng, ZHANG Wen-yuan

(Hohai University, Nanjing 210098, China)

Abstract: The number of users and system role in application system is more and more, making the characters exclusion more frequent. Mutually exclusive role as a kind of implementation function of duties separation is very important in the RBAC model. In order to study the types of role conflicts, it studies the role mutual exclusion based on this situation, through the analysis of the nature of role list various types of role exclusion, and on this basis the role constraints table is designed, through the formalized method give the role constraints table form and role exclusive undo way. Finally design a role distribution controller with role conflict detection that perform role distribution according to role exclusion relationship well, is applied to a simple application system successfully.

Key words: RBAC; role mutual exclusion; role distribution; mutual exclusion digestion

0 引言

各种网络环境下应用系统的不断增多,规模也越来越大,继而对访问控制也提出了更高的要求。基于角色的访问控制(RBAC)作为传统访问控制(DAC, MAC)的有前景的代替受到了广泛的关注^[1,2]。

基于角色的访问控制中,用户的授权是通过授予用户角色来实现的,一个用户可以承担不同的角色,从而实现授权的灵活性^[3]。只要用户属于某个角色,那么他就具有这个角色的所有操作许可,也就是这个角色拥有的权限。基于RBAC的系统能够动态地调整用户的角色分配,也可以动态地调整角色的操作许可(权限)^[4,5],使得基于RBAC的访问控制系统非常的灵活。随着角色、权限数目的不断增大,为了更好地在

RBAC模型中实现职责分离原则^[6-8],就要控制好每个用户的权限大小,即要定义角色之间,权限之间的约束^[9]。其中角色间的互斥可以由管理员自定义(比如A角色与B角色不能同时担任),也可以从权限互斥得到。

目前RBAC理论研究已经趋于成熟,但是对于RBAC中角色互斥的研究还不够完善。文中详细地分析研究了角色互斥的各种类型,其互斥来源和互斥撤销方案,并且设计了一个带角色互斥检测的角色分配控制器。

1 基于角色的访问控制

1.1 RBAC模型

RBAC的核心思想是将角色直接和访问权限相联系,通过把角色分配给用户,让用户可以进行相应的操作。

RBAC模型中比较著名的是RBAC96^[10]模型,该模型又可以分为RBAC0, RBAC1, RBAC2, RBAC3。其中RBAC0是基本模型,规定了任何RBAC系统所必须的最小需求,而RBAC3是在RBAC0上增加了角色继

收稿日期:2012-04-12;修回日期:2012-07-17

基金项目:河海大学中央高校基本科研业务费项目(2009B21614);
河海大学自然科学基金(工科类)资助项目(2009421211)

作者简介:陈 胜(1987-),男,硕士,主要研究方向为分布式计算;
娄渊胜,博士,副教授,CCF高级会员,主要研究方向为软件体系结构、分布式应用集成。

承和约束的概念,文中的研究正是基于 RBAC3 模型,其中 RBAC3 的模型图如图 1 所示。

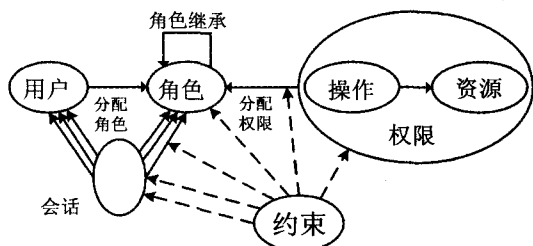


图 1 RBAC3 模型图

RBAC 模型中的一些定义如下^[11]:

- U, R, P, S : 分别为用户、角色、权限和会话。
- $PA \subseteq P \times R$: 给角色分配权限, 关系为多对多。
- $UA \subseteq U \times R$: 给用户分配角色, 关系为多对多。
- $RH \subseteq R \times R$: 角色继承, 是关于 R 的偏序关系。

1.2 RBAC 约束

RBAC 中约束的概念是指是否当前操作可以被接受, 只有被接受的操作才能够允许, 其中约束有很多种, 如下所示:

(1) 角色互斥。只允许同个用户使用互斥角色中的至多一个角色, 这样可以支持职责分离原则, 使得系统的安全性提高。还有由于角色的基数限制(一个用户可以拥有的角色数目受限)也能形成角色的约束。

(2) 先决条件角色。这个约束是因为要给用户分配某角色 B, 必须先要分配角色 A, 那么角色 A 就是角色 B 的先决条件角色。

(3) 运行时互斥。这是允许一个用户同时拥有两个互斥的角色^[4], 但是在运行时不能同时激活两个角色。这样动态的职责分离有利于用户角色的日后切换。

2 RBAC 角色互斥分析

2.1 角色互斥来源类型

角色互斥的类型按照是否角色之间自身存在冲突可以分为两类, 一类是由于达到了用户角色分配的上限引起的互斥, 比如当一个用户规定了他只能分配 10 个角色, 那么当给这个用户分配第 11 个角色的时候就出现了角色互斥。另一类是由于角色之间自身的互斥引起的, 这又可以分为三类:

(1) 管理员自己定义的角色互斥, 比如规定了角色 A 与角色 B 不能同时赋予同个用户。

(2) 来源于权限的互斥, 当权限 C 和权限 D 互斥的时候, 那么角色不能同时含有权限 C 和 D, 分别含有权限 C 和权限 D 的角色也相互互斥。

(3) 第三个是来源于角色继承的互斥, 角色 A 和

角色 B 互斥了, 那么角色 A 的所有继承角色也和角色 B 的所有继承角色互斥。

2.2 角色互斥表

为了方便在分配角色的时候查找到某个角色的互斥角色集, 需要设计一个角色互斥表, 所有的互斥角色都能够在角色约束表中找到。角色互斥表至少有 3 个字段组成, 其基本形式如表 1 所示:

表 1 角色互斥表基本形式

互斥 id	角色 A	角色 B	互斥来源
-------	------	------	------

根据一个角色就能知道其所有的互斥角色, 所以角色约束表最好设计成具有对称性, 如果有记录角色 A 与角色 B 互斥, 相应的也有角色 B 与角色 A 互斥。还有角色约束表里也必须定义好角色互斥的来源, 角色互斥来源于自定义的角色互斥或者是来源于权限互斥, 这样方便于在撤销权限互斥的时候判断是否撤销掉相应的角色互斥。

根据角色互斥的类型, 角色约束表主要也由三部分组成, 自定义的角色互斥, 继承的角色互斥, 还有来源于权限的互斥如图 2 所示:

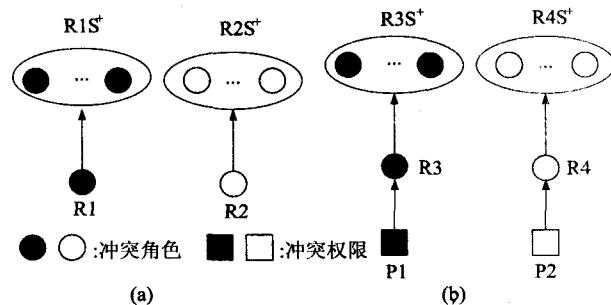


图 2 名称 角色互斥类型

图 2(a) 中 R1 与 R2 为互斥角色, 那么 R1 的所有继承角色和 R2 的所有继承角色之间也是互斥角色, 可形式化地用式(1)表示:

$$\text{If } (R1, R2) \in CR, \text{ Then } (R1S^+ \times R2S^+) \in CR \quad (1)$$

其中 $R1S^+$ 和 $R2S^+$ 分别为 R1 和 R2 的继承角色集, CR 为互斥角色集。R3 与 R4 也同理, 只是 R3 与 R4 的互斥来源于权限之间的互斥, 图 2(b) 中权限 P1 与权限 P2 之间互斥。

2.3 角色的互斥消解

为了使权限控制, 角色分配更加的灵活, 必须使得角色权限的互斥可以手动地撤销, 在撤销互斥的时候按照角色约束表的结构可以表示成下面的三种情况:

①如果角色 1 和角色 2 之间的冲突消解, 那么角色 2 和角色 1 之间的冲突也消解;

②如果角色 1 和角色 2 之间的冲突消解, 那么角色 1 和角色 2 继承角色集之间的冲突也消解;

③如果权限 1 和权限 2 之间的冲突消解, 那么角色 x 和角色 y 之间的冲突来源于权限 1 和权限 2

之间的冲突,消解 x, y 之间的冲突。

可形式化地用下面 3 个式子来表示:

(1) If (Role_1, Role_2) cancel from CR, Then (Role_2, Role_1) cancel from CR.

(2) If (Role_1, Role_2) cancel from CR, Then $\forall (Role_x, Role_y) \in (Role_1S^* \times Role_2S^*)$ cancel from CR.

(3) If (Permission_1, Permission_2) cancel from PR

For Permission_1 $\in \forall Role_x$, Permission_2 $\in \forall Role_y$

If (Source(Role_x, Role_y)) from PR, Then(Role_x, Role_y) cancel from CR.

Else return.

角色约束表的角色互斥具有对称性,即有角色 A 和角色 B 互斥的记录,就有角色 B 和角色 A 的互斥记录,可以用情况(1)表示,那么在撤销的时候也要把两条记录都去掉。PR 指的是互斥权限集,当权限 A 和权限 B 的互斥撤销后,就去角色约束表里查找分别含有权限 A 和权限 B 的互斥,如果该互斥是来源于权限互斥的,那么就把它撤销,否则继续查找下一条记录,可以用情况(3)表示。互斥角色 A 和 B 撤销后,也按照系统的要求是否同时撤销其继承角色集之间的互斥,可以用情况(2)表示。

3 角色分配控制器的设计

有了角色约束集,就可以设计一个带角色互斥检测的角色分配控制器^[12],当给用户分配新角色的时候,系统可以先查找该用户已经分配的角色集,然后把新分配的角色和已经分配的角色集作为角色分配控制器的输入,通过角色分配控制器后,可以检测出角色中的互斥部分和非互斥部分,其中互斥部分可以根据系统的需求来选择撤销分配或者忽略互斥。其角色分配控制器的设计图如图 3 所示:

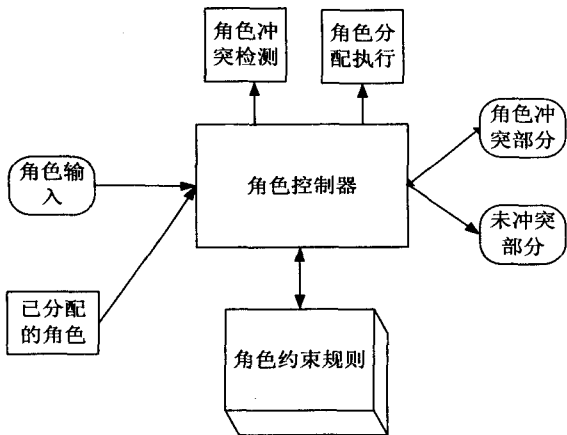


图 3 角色分配控制器

下面给出了给一个已知的用户分配新角色通过角色控制器过程的伪代码。

```
role_new[] = 用户新分配的角色;
role_old[] = 用户已经分配的角色;
i=0;
Set set;
//set 中的元素形式是二元组,分别代表了互斥的两个元素
且这两个元素前后没有顺序,set 最后存放的是该用户角色互斥
部分的部分互斥角色对
for(i=0;i<role_new.length;i++)
{
    role_conflict[] = table(role_new[i]);
    //在角色约束表查找 role_new[i]的互斥角色集
    result[] = compare(role_conflict,role_new+role_old);
    //返回输入角色中的部分互斥集
    set.add(result);
    //将部分互斥角色对放入到互斥角色集合中
}
return set;
```

4 互斥检测的应用实例

为了更好地说明角色分配的执行过程,文中设计了一个应用系统,包含了数据库的设计和角色的设计。

4.1 数据库设计

根据 RBAC 的模型,确定了该系统应该包含用户、角色、权限、资源等基本表,因为用户和角色,角色和权限之间又是多对多的关系,所以应该包括用户角色关系表、权限资源关系表两张关系表。应用了该角色分配器后,由于角色的互斥有可能来源于自定义的角色互斥、权限间的互斥等,所以该数据库表中还应该包含自定义的角色互斥、自定义的权限互斥,整个权限管理系统的数据库设计如图 4 所示。

其中 User 为用户表,Role 为角色表,UserRole 为用户角色表,Permission 为权限表,Resource 为资源表,PermissionDefined 为自定义的角色互斥表,RoleDefined 为自定义的角色互斥表,RoleConflict 为最终的角色互斥表,角色控制器查找角色互斥的时候就是从该表中查找互斥的。

4.2 角色间的关系

为了方便说明,设计的角色组列表如下:学生,女学生,男学生,学生班长,党员学生,团员学生,讲师,副教授,教授。

首先管理员按照要求自定义了以下的角色互斥,存入 RoleDefined 表,分别是女学生与男学生之间互斥,班长,讲师间互斥。而权限可以是给一个学生打成绩,给一个学生赋予党员投票等等,然后再给相应的角色授予不同的权限,权限中的自定义互斥会引起角色间的互斥,但是为了限制的复杂性,本应用既没自定义

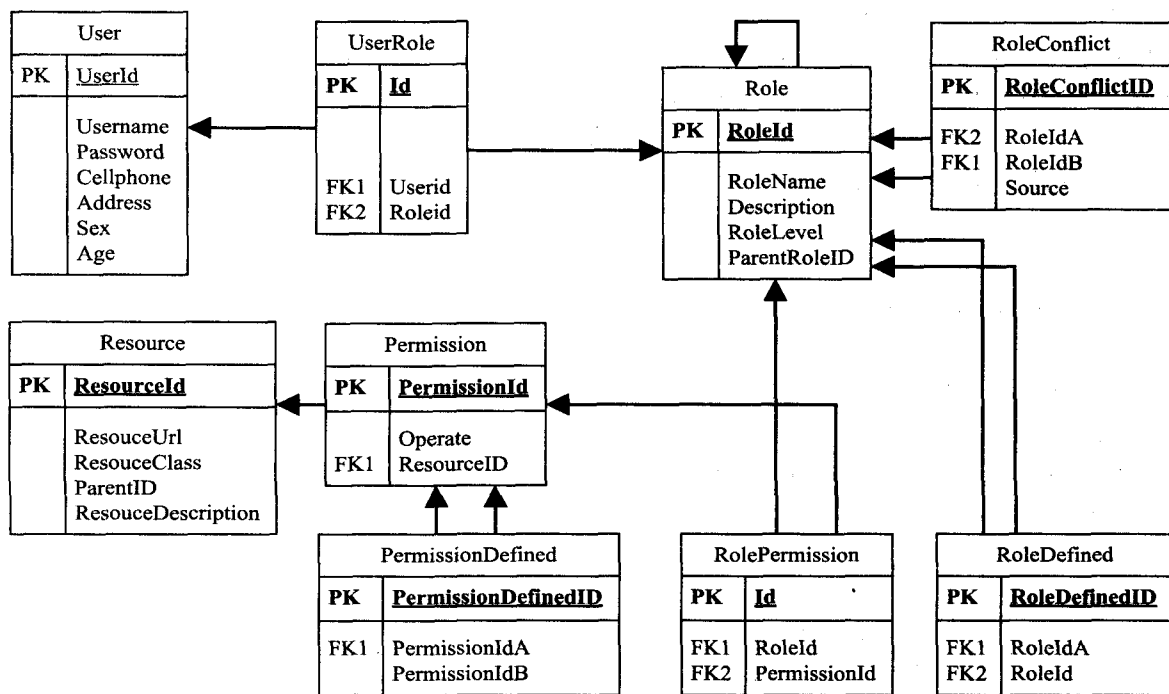


图 4 权限管理部分的数据库设计

权限间的互斥,也不限定一个用户拥有的角色数目和一个角色拥有的权限数目。

角色间的互斥构成,来源于前面自定义的角色互斥,以及来源于互斥角色的继承,又根据前文所描述的设计的角色互斥表具有对称性,可以导入角色间的互斥如表 2 所示:

表 2 角色间的互斥表

互斥 id	角色 A	角色 B	互斥来源
1	女学生	男学生	自定义角色互斥
2	班长	讲师	自定义角色互斥
3	班长	副教授	角色互斥继承
4	班长	教授	角色互斥继承
5	男学生	女学生	自定义角色互斥
6	讲师	班长	自定义角色互斥
7	副教授	班长	角色互斥继承
8	教授	班长	角色互斥继承

4.3 角色分配

角色分配包括两个部分,新分配角色以及重新分配角色。

1. 当为一个姓名为甲某的用户新分配角色的时候,甲某本来有党员学生这个角色,分配的时候忽略了角色等级比党员低的角色。经过该角色分配器后,角色分配器按照上面表 2 中的自定义互斥,返回互斥结果。

2. 重新分配角色,此时管理员可以给用户重新分配所有的角色,只是已分配的角色可以用其他颜色来标注,管理员选择相应的角色集一起作为角色分配器的输入点而忽略了用户已经分配的角色。整体的分配

角色与 1 类似,唯独不同的是分配的界面不同和角色分配器的输入角色集不一样。

如果要进行互斥角色的消解,可以按照 2.3 节中的三个式子进行处理,根据互斥来源的类型来决定是否消解角色的互斥。

5 结束语

文中主要对角色互斥的类型和互斥撤销的方式进行了分析,并且设计了一个角色分配控制器,该控制器可以根据现有的角色约束和输入的角色集自动地输出角色的互斥部分和非互斥部分,并且设计了一个简单的应用来进行测试和说明。但是角色分配控制只是给出了现有的角色互斥情况,并没有自动地给用户分配出最合理的分配方案,仍需要用户手动地进行交互。这个可以通过预设一些智能的互斥分配方案让控制器自动地给出最优的方案。

参考文献:

- [1] 王 婷,陈性元,张 斌. 基于互斥角色约束的静态职责分离策略[J]. 计算机应用,2001(7):1884-1886.
- [2] 程相然,陈性元,张 斌,等. RBAC 策略冲突及其检测算法的研究[J]. 计算机工程,2010,36(18):135-137.
- [3] 孙小林,卢正鼎,李瑞轩,等. 角色访问控制中基于描述逻辑的角色互斥实现[J]. 计算机工程与科学,2007(9):37-40.
- [4] Feng Xiaosheng, Ge Bin, Sun Yang, et al. Broadband Network and Multimedia Technology (IC - BNMT) [C]//2010 3rd IEEE International Conference on Digital Object Identifier.

(下转第 28 页)

4 实验结果

通过对 8M 的 Bi-gram ARPA 格式的语言模型的压缩试验,压缩结果为 1.4M,压缩率达到 0.175。查找效率方面,同样以此语言模型文件进行理论上的分析。该语言模型统计的一元词有 7165 个,二元词有 458382 个。

由于词是按照其 utf-8 编码进行排序的,所以可以采用近似的二分查找方法进行匹配搜索。假设每个元素的查找是等概率的,则二分查找成功的平均比较次数为 $\log_2(n+1)-1$ ^[11],其中 n 为树的结点数。在语言模型中,由于 n 取值比较大,所以近似为 $\log_2 n - 1$ 。所以压缩之前采用平均比较次数为:

$$N_1 = \frac{n_1}{n_1 + n_2}(\log_2 n_1 - 1) + \frac{n_2}{n_1 + n_2}(\log_2 n_2 - 1 + \frac{1}{2} \times \frac{n_2}{n_1})$$

将数据代入公式,得到平均比较次数约为 47.617。

采用在压缩过程中引入多级索引技术后,无需再在二元词中进行搜索,通过一元词的索引可直接定位。所以平均比较次数为:

$$N_2 = \frac{n_1}{n_1 + n_2}(\log_2 n_1 - 1) + \frac{n_2}{n_1 + n_2}(\log_2 n_1 - 1 + \log_2 \frac{n_2}{n_1} - 1)$$

代入数据得平均比较次数为 16.714。搜索语言模型时所需要的平均比较次数是原来的 0.35。当采用 Tri-gram 语言模型时,多级索引技术所带来的搜索效率上的提高将更加显著。

5 结束语

文中借鉴 K-means 聚类思想和多级索引方法,提出一种基于聚类和多级索引技术的 ARPA 格式的 N-gram 语言模型压缩方法。

根据 ARPA 格式 N-gram 语言模型的特点,对其组织方式进行了优化。对概率值进行聚类较好地解决了 ARPA 格式的 N-gram 语言模型所占空间过大的问题,而且多级索引技术的应用使模型获得了优良的检索效率。通过实验也验证了该方法的有效性和实用性。

参考文献:

- [1] 李晓光,王大玲,于戈. 基于统计语言模型的信息检索[J]. 计算机科学,2005,32(8):124-127.
- [2] Manning C, Schutze H. 统计自然语言处理基础[M]. 苑春法,李庆中译. 北京:电子工业出版社,2005.
- [3] 殷芳刚,吴建国,吴海辉. Windows Mobile 平台下智能手机输入法研究[J]. 计算机技术与发展,2011,21(5):75-78.
- [4] Rosenfeld R. The CMU Statistical Language Modeling Toolkit [C]//Proc of ARPA Spoken Language Technology Workshop. [s. l.]:[s. n.],1995.
- [5] Jelinek F, Mercer R L. Interpolated Estimation of Markov Source Parameters from Sparse Data[C]//Proc of Workshop on Pattern Recognition in Practice. Amsterdam: North-Holland, 1980.
- [6] Lafferty J D, Sleator D, Temperley D. Grammatical Trigrams: A Probabilistic Model of Link Grammar[C]//Proceedings of the AAAI Fall Symposium on Probabilistic Approaches to Natural Language. Cambridge, MA: [s. n.], 1992:89-97.
- [7] Ye Z X, Berger T. Information Measures for Discrete Random Fields[M]. Beijing: Science Press, 1998.
- [8] Kaufman L, Rousseeuw P J. Finding group in data: an introduction to cluster analysis[M]. New York: Wiley, 1990:83-88.
- [9] 段小斌,林雯,阮百尧,等. 一种基于三级索引词库结构的中文分词方法研究[J]. 计算机与数字工程,2007,35(7):47-49.
- [10] Brown P F, deSouza P V, Mercer R L, et al. Class-based n-gram models of natural language[J]. Computational Linguistics, 1992,18(4):153-157.
- [11] 王海涛,朱洪. 改进的二分法查找[J]. 计算机工程,2006(5):60-62.

(上接第 24 页)

- [s. l.]:[s. n.],2010:677-683.
- [5] Habib M A. 2010 International Conference on Internet Technology and Secured Transactions (ICITST) [C]. [s. l.]:[s. n.],2010:1-6.
- [6] Li Ninghui, Wang Qihua. Beyond separation of duty: An algebra for specifying high-level security policies[J]. Journal of the ACM, 2008,55(3):1-4.
- [7] 胡金柱,陈娟娟. RBAC 模型中角色的继承与互斥问题的研究[J]. 计算机科学,2003(11):160-163.
- [8] 付志峰,张焕国. RBAC 系统中职责分离的实现[J]. 计算机工程,2003(6):61-63.
- [9] 张雷,向宏,胡海波. 基于语义的 RBAC 模型权限冲突检测方法[J]. 计算机工程与应用,2011(26):74-78.
- [10] Sandhu R, Coyne E, Feinstein H, et al. Role-based Access Control Model[J]. IEEE Computer, 1996,29(2):38-47.
- [11] 段隆振,文锋,黄水源,等. 一种描述 RBAC 角色层次关系和互斥关系的模型及实现[J]. 南昌大学学报(理科版),2006(6):601-604.
- [12] 卢昱,王宇,吴忠望. 信息网络安全控制[M]. 北京:国防工业出版社,2011.