一种基于角色的多约束动态权限管理模型研究

许 淳，王文发，李竹林，刘 芬
（延安大学 数学与计算机科学学院，陕西 延安 716000）

摘要： 在基于角色的访问控制模型(RBAC)基础上，引入访问终端、网络环境和接入方式等外部因素，提出了基于角色的多约束动态权限管理模型，依据外部因素的安全程度和资源可能带来安全风险分别对外部因素和资源进行量化，实现了用户、角色、资源和各种外部因素的统一。利用该模型可实现不同外部条件下，用户权限的动态管理，从而提高系统的灵活性和安全性。

关键词： 信息管理系统；RBAC 模型；角色；动态权限管理；外部因素
中图分类号： TN918.91 **文献标识码：** A **文章编号：** 1674-6236(2016)19-0031-03

A study on multi-constraint dynamic permission management model based on role

XU Chun, WANG Wen-fa, LI Zhu-lin, LIU Fen
(*College of Mathematics and Computer Science, Yanan University, Yanan* 716000, *China*)

Abstract: Based on the RBAC model, introducing external factor such as terminals, network environment and access styles, etc, an multi-constraint dynamic authority management model based on role is protested. According to safety degree of the external factors and security risks of resources, external factors and resources are both quantitative respectively, unifying users, roles, resources, and all kinds of external factors. Using the model we can realize dynamic management for user rights under different external conditions, and improve the flexibility and security of the system.

Key words: MIS; RBAC model; role; dynamic authority management; external factor
DOI:10.14022/j.cnki.dzsjgc.2016.19.010

随着信息化程度的不断提高，出现了各种信息管理系统[1-3]，用于实现数据的电子化和数字化管理，促进管理工作的规范化，甚至通过系统中数据的分析为各级管理人员提供决策支持，进而提高工作效率。从总体架构上系统大体可分为单机版和网络版两种。其中，前者属于早期的系统架构；后者是目前主流的系统架构，它可以更好地实现数据的共享及远程管理，但也给数据的安全性带来了挑战。此外，新型终端设备(如手机和平板等)的出现及无线技术的应用，突破了传统 PC 机终端的有线接入，终端及其接入方式的多样化一定程度上降低了数据的安全性。可见，安全性是任何信息管理系统开发过程中必须解决的一个重要问题。对于系统安全性，通常是在设计和实现过程中采取有效措施加以防范，如将用户的操作权限进行详细划分并严格控制，避免重要数据或敏感数据的非法篡改或泄露，从而提高数据的安全性。

针对终端类型、接入方式等外部因素的多样性，文中以 RBAC(Role Based Access Control，RBAC)模型为基础，提出一种基于角色的多约束动态权限管理模型。

1 基于角色的访问控制

基于角色访问控制模型最早由 Ferraiolo 和 Kuhn 提出[4]，目前出现了多种基于角色访问控制模型的扩展模型[5-8]。该模型主要涉及用户、角色和权限 3 部分，通过用户与角色之间、角色与权限之间分别建立多对多的对应关系，实现用户与权限之间的多对多关系。可见，角色是模型的核心，是用户(访问主体)和权限(受控对象)之间的桥梁。

该模型的大体操作过程：先建立合适的角色，再对每个角色授权，最后为用户赋予一定的角色。这样，用户就具有与其角色所对应的权限。其基本模型如图 1 所示。

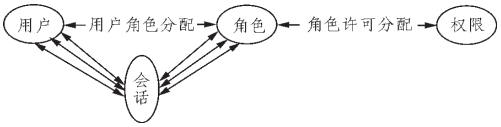

图 1 RBAC 基本模型图

由上述可知，RBAC 模型主要是从访问的主体出发，按照一定的规则对其进行分类，形成不同的角色并对其设置相应的访问权限。这种简单地从主体出发，仅考虑主体的角色，并不能有效提高系统的安全性。因为角色是相对固定的，不能随着访问系统的终端、系统接入方式、网络环境等的变化而变化。

2 基于角色的多约束动态权限管理模型

2.1 基本思想

一般地，外部环境通常会给系统带来一定的安全威胁，

收稿日期：2015-10-23 稿件编号：201510169
基金项目：延安大学校级科研项目(YDQ2014-48)
作者简介：许 淳(1981—)，男，陕西蒲城人，硕士研究生，讲师。研究方向：软件工程及数据库技术等。

合理考虑外部因素对系统的影响是必要的。权限最终表现为用户可使用的资源，资源有其敏感性，资源越敏感，安全风险就越大。因此，可将外部因素统一描述为影响系统安全的程度，并与资源的敏感度联系起来，形成一种基于角色的多约束动态权限管理模型。

该模型以 RBAC 模型为基础，对系统的资源的敏感度进行量化，通过评估外部环境可能带来的安全威胁，过滤该环境下系统中较敏感数据的操作权限，从而一定程度上保证数据的安全性，其模型如图 2 所示。

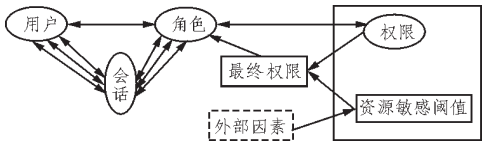

图 2　基于角色的多约束动态权限管理模型

上述模型中，用户最终权限大体可分解为两方面任务：由角色确定用户的初始权限；由外部环境确定高敏感资源所对应的权限。其中，前者主要以系统需求分析为基础，分别创建用户、角色和资源以及它们之间的对应关系，无需计算即可间接获取用户的权限；后者需要由外部因素计算出的资源敏感度阈值来确定。

2.2　模型描述

下面给出这种基于角色的多约束动态权限管理模型的形式化描述。首先给出一些的符号说明，具体如下：

u：表示某个特定的用户；

U：表示系统所有的访问主体，即用户的集合；

r：表示某个特定的角色；

R：表示访问主体所属类别的集合，即角色的集合；

s：表示某个特定被访问资源（或对象）；

S：表示系统中所有资源的集合；

n：表示外部因素的个数；

w_i：表示第 i 个的外部因素的权值；

v_i：表示第 i 个外部因素的取值；

$Max\ (v_i)$：表示第 i 个外部因素的最大取值；

L：表示资源敏感度的最大取值。

为了描述方便，这里引入两个多值函数和一个单值函数，具体如下：

$r=g(u)$　g 表示用户 u 所对应的角色 r

$s=f(r)$　f 表示角色 r 所对应的资源 s

$l=h(s)$　h 表示资源 s 所的敏感值 l

根据模型的基本思想，权限的管理可以看作是对资源的管理，即不同角色的用户在各种外部因素作用下所能获取的所有资源的集合 S''，具体如下式所示。

$S''=S'-\{s|h(s)>L',s\in S'\}$ 其中，$S'=\{s|s=f(g(u)),u\in U\}$，$L'=L\sum_{i=1}^{n}w_i(v_i/Max(v_i))$

2.3　模型实现

依据模型的基本思想，其实现过程为：1）获取用户激活角色所对应的系统权限；2）收集系统的外部环境并确定外部因素；3）计算外部因素作用下资源敏感度阈值；4）从 1）中所确定的权限中过滤大于资源敏感度阈值的所有权限，形成用户的最终权限。

下面以访问终端、网络环境、接入方式等 3 种外部因素为例，给出模型的详细实现过程，具体如下：

1）确定资源等级和分值，如 A-5，B-4，C-3，D-2，E-1，F-0，并根据其敏感程度打分，分值越大表明资源越敏感、破坏性越大；

2）创建用户和角色，为角色分配资源，为用户分配角色；

3）确定各个外部因素，并根据其安全程度及可能的取值分别确定权重、取值范围和取值。假设某个系统可能的外部因素及其取值范围、权重如表 1 所示。

表 1　外部因素的取值范围及其权重

外部因素	网络环境		接入方式		访问终端		
	内网	外网	有线	无线	PC 机	平板	智能手机
权重	0.6		0.3		0.1		
取值范围	{0，1，2}		{0，1，2}		{0，1，2，3}		
取值	2	1	2	1	3	2	1

4）根据 $L'=L\sum_{i=1}^{3}w_i(v_i/Max(v_i))$ 计算各因素的加权和即资源敏感阈值，并将其映射到资源的敏感度，为方便起见，这里引入无序对对访问者所处的外部环境进行描述。

（内网，有线，PC 机）：5*(0.6*(2/2)+0.3*(2/2)+0.1*(3/3))=5

（内网，无线，平板）：5*(0.6*(2/2)+0.3*(1/2)+0.1*(2/3))=4

（外网，无线，平板）：5*(0.6*(1/2)+0.3*(1/2)+0.1*(2/3))=2

5）获取由用户所属角色确定的资源，并从中去除值大于 L' 的资源项。假设某个用户同时拥有 A 级、B 级、C 级、D 级、E 级所有级别的部分资源，由 4）计算可知，第一种方式是相对最安全的方式，最终权限不受外部因素的影响；第二种情况下，该用户将不具有 A 级和 B 级资源的权限，第三种情况下，该用户仅具有 D 级和 E 级资源的权限。

2.4　模型的应用

分析上述模型，模型应用中将主要涉及用户、角色、系统资源、外部因素配置等 4 类基本信息的管理、系统外部环境采集模块以及最终权限的生成模块等的实现。其中，用户、角色和权限及其相互关系可以借助数据库技术加以实现；系统外部环境采集模块以及最终权限的生成模块需要通过应用程序代码加以实现。因此下面将从底层数据库设计和应用程序两个方面加以叙述。

2.4.1　底层数据库设计

根据模型的要求，必须存储的信息主要包括：用户（用户编号、用户姓名、密码）、角色（角色编号、角色名称）、资源（资源编号、资源名称、资源对应的 URL、资源的层级、上层资源编号、资源敏感阈值）、外部因素配置（编号、因素名称、所属类别、取值范围、权重）等 4 个实体信息。此外，还需两个关系表：用户-角色（编号、用户编号、角色编号）、角色-资源（编号、

角色编号,资源编号),分别用于实现用户和角色的多对多联系,角色与资源的多对多联系。

限于篇幅且考虑到模型的通用性和关系型数据库的主流地位,此处以关系型数据库为例给出相关的表设计及其它们之间的联系,具体设计如图 3 所示。

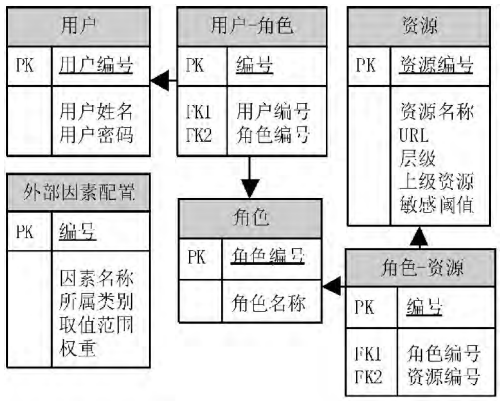

图 3　数据库表设计

2.4.2　关键的功能模块

在应用程序方面,主要是外部环境信息的采集、相关基础信息的管理以及最终权限的生成。其中,外部环境信息的采集和最终权限的生成是模型实现的关键,下面将分别给出它们的实现流程。

1)外部环境采集模块

该模块主要实现网络环境、客户端接入方式、系统访问终端类型等信息的采集,并将采集到的信息以参数的形式传递给权限生成模块。其中,网络环境信息主要可以通过获取客户端的 IP 地址端来确定;接入方式需要以终端类型为基础分别采取不同的方法来确定;系统的访问终端可以通过 JavaScript 进行判断。为了便于实现,可以按照以下流程进行实现:

a.判断系统访问终端的类型(含平台及浏览器信息等);

b.结合 a 中获取的信息,针对不同的访问终端判断其接入系统的方式;

c.获取设备的 IP 地址,并确定其是否与应用服务器的 IP 处于同一网段,如果是则为内网,否则为外网。

2)最终权限生成模块

最终权限的生成依赖于用户的角色和外部因素来确定,并通过系统操作菜单体现出来。其大体可以分为两大阶段,这里从系统登录页面开始给出最终权限确定流程。具体如下:

a.输入合法的用户身份信息;

b.通过用户信息的获取该用户的角色信息;

c.通过角色信息获取角色对应的资源信息;

d.获取所有的外部因素,根据外部因素设置信息计算其加权和;

e.对于 c.中获取的每一项资源,过滤其敏感值大于 d.中计算的加权和的资源项;

f.根据资源的层级关系,生成分级的操作菜单。

3　结束语

基于角色的多约束动态权限管理模型以传统的 RBAC 模型为基础,将用户权限的确定从仅依靠用户拓展到以用户为主、以各种外部因素为辅,并对这些外部因素和系统中的资源进行量化;同时,从外部因素对系统的安全程度和资源可能带来安全风险的角度,将外部因素以较为合理的方式引入最终权限的确定过程中。该模型具有通用性强,方便灵活,安全性高等特点,由于以传统 RBAC 模型为基础,因而也具有强的可行性和一定的应用价值。

参考文献:

[1] 台德艺,王昆仑,郭昌健.高校科研信息管理系统的设计与实现[J]. 计算机工程与设计,2009,30(9):2339-2341.

[2] 刘明举,郝富昌. 基于GIS的瓦斯预测信息管理系统[J]. 煤田地质与勘探,2005,33(6):20-23.

[3] 郑晓东.工程设计企业管理信息系统的开发研究[J].计算机技术与发展,2011,21(4):246-249.

[4] Ferraiolo D, Kuhn R. Role -based Access Control [C]// Proceedings of 15th National Computer Security Conference, 1992.

[5] 郝小龙. 改进的RBAC模型在电网视频监控平台中的应用[J].计算机技术与发展,2014,24(12):212-220.

[6] 宋万里,吴炜峰.基于改进的RBAC模型的系统用户权限控制研究[J].计算机与现代化,2014,9:49-54.

[7] 于小兵,郭顺生,杨明忠.扩展RBAC模型及其在ERP系统中的应用[J].计算机工程,2009,35(24):165-167.

[8] 陈军冰,王志坚,艾萍,等.关于RBAC模型中约束的研究综述[J].计算机工程, 2006, 32(9):1-3.