基于角色和颗粒操作的自定义通用权限管理模型研究

赵 君[1]，熊燕妮[2]

（1.武汉设计工程学院 信息工程学院，湖北 武汉 430205；2.荆州理工职业学院 商学院，湖北 荆州 434000）

摘 要：权限管理系统是软件系统的核心部分，涉及到数据的安全和保密性。针对传统基于角色的访问控制RBAC（Role－Based Access Control）模型中角色管理不灵活、与其它系统耦合性高且通用性低的缺点，提出一种基于角色和颗粒操作RPO（Role－Particle－Operation）的自定义通用权限管理模型。该模型耦合性低，角色和颗粒操作完全可以由用户自定义，支持无限级权限，并独立于其它软件系统，具有高通用性，可以为几乎所有软件系统提供权限管理接口。

关键词：权限管理；RPO；无限级权限；高通用性

DOI：10.11907/rjdk.162122

中图分类号：TP301 **文献标识码**：A **文章编号**：1672-7800（2016）012-0014-02

0 引言

随着软件系统功能越来越多、规模越来越大以及模块化要求越来越高，管理信息系统对各类信息资源的访问与控制以及对各类用户群体的管理也越来越复杂。因此最初基于用户的权限管理被基于角色的访问控制RBAC（Role－Based Access Control）模型所替代，用角色代替用户是此模型的一大创新，减少了管理员在大量用户系统中要为每个用户分配权限的繁冗操作[1]，但是此模型的缺陷是对角色权限的划分比较模糊和僵化，粒度较粗。最为重要的是，当系统升级或者权限发生改变时，仍然需要修改系统的源代码，这与“高内聚低耦合”的软件设计理念相矛盾，会给软件升级和软件维护带来巨大的额外开销。因此提出一个通用的、可以为几乎所有软件系统提供权限管理接口的模型尤为必要[2]。

1 通用权限管理模型总体思路

1.1 传统模型的缺陷

权限管理的实质是系统根据用户U的权限来限定其能访问的资源R和进行的操作O，这里的U、R和O均为集合，其中$U=\{u_1,u_2\cdots u_i\}$，$R=\{r_1,r_2\cdots r_j\}$，$O=\{o_1,o_2\cdots o_k\}$，权限集合P可以定义为$P=O*R$，P中有$j*k$个元素，那么系统中可能出现的权限子集的最大数为$2*j*k$，包括空集（无任何权限）和P本身（具有所有权限）[3]。如果U集合中有i个用户，那么在基于用户的访问控制模型中，系统开发者要为i个用户设计和分配权限的最大工作量为$W=2*i*j*k$，这是一个艰巨的任务。最关键的是，在实际的用户访问控制中，i，j，k经常发生变化，系统开发者需要修改代码，给后期维护带来不便[4]。

RBAC是基于用户权限控制模型的升级版，在RBAC中，多个具有相同权限的用户被归并为同一个角色，这样由用户集合U延伸出角色集合R′，$R'=\{r'1,\ r'2\cdots r'm\}$[5]，$m\leqslant i$，改进之后的工作量虽然有所减轻，但是因为权限的定义固化在程序里，所以仍不能从根本上解决问题。

1.2 RPO模型的特点

如果要从根本上解决问题，则需要将权限设置交给客户，将权限管理模块从软件系统中剥离出来[6]。但是一个成熟的系统在使用上不能包含太多技术细节，所以这种设计的难点在于如何将以前只能由代码完成的复杂功能变成可以由鼠标点击完成的图形界面操作[7]。RPO模型即为完成这种转换设计的新型模型。

在RPO中，要想实现自定义权限的通用管理，必须首先将角色、资源和操作完全独立，并且充分颗粒化[8]，然后设定R′对O与R笛卡尔积的访问控制即可实现RPO模型，如图1所示。

作者简介：赵君（1980－），男，湖北荆州人，硕士，武汉设计工程学院信息工程学院工程师，研究方向为网络数据挖掘、大数据分析与处理；熊燕妮（1980－），女，湖北荆州人，硕士，荆州理工职业学院商学院讲师，研究方向为网络平台开发、云计算。

RPO 模型中，R′、O 和 R 均为用户自定义，不由系统开发者设计，这样才符合“自定义”的要求；但要做到“通用”，必须使 O 和 R 充分地颗粒化，即不可再细分[9]。

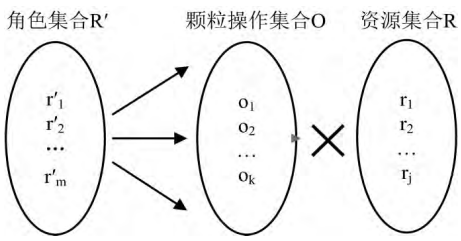

图 1　基于“角色和颗粒操作”的 RPO 模型

2　RPO 设计

2.1　角色集合 R′的定义

3 个集合中，R′的定义最简单，因为客户对业务逻辑中的角色最清晰[10]。角色的定义如表 1 所示。

表 1　角色定义

角色名	描述
Administrators	系统管理员组
班主任	对所辖班级有所有权限
物理教师	对所辖班级的物理科目有编辑权限

2.2　操作集合 O 的定义

操作即为用户在系统中可以执行的动作，在 RPO 中，操作必须是不可再分[11]或者是在本系统中不可再分的颗粒，比如“物理教师编辑学生成绩”中的动词“编辑”则不满足要求，因为“编辑”还可以细分为增加、修改和删除。所以 O 在定义上较 R′要复杂一些[12]。操作集合 O 的定义如表 2 所示。

表 2　角色定义

操作索引	颗粒操作
1	管理目录
2	管理颗粒操作
3	管理角色
4	管理角色用户
5	管理角色权限
6	查看学生信息
7	添加学生信息
8	修改学生信息
9	删除学生信息

2.3　资源集合 R 的定义

相对于 R′和 O，R 的定义最为复杂，因为 R′和 O 中的元素彼此之间没有关系，且都是颗粒性质不可细分的，用表 1 和表 2 中的二维表即可定义[13]。而 R 中的资源可能有多层包含关系，例如年级包含班级，班级包含学生，所以用二维表定义可读性差、维护困难[14]。本模型中设计的定义方式是目录树。在目录树中，所有资源，无论是集合还是元素都被定义为目录，这里充分应用了软件中抽象的思想[15]。目录的可多层包含性实现了权限的无限极特性，为本模型提供了良好的实用性和灵活性[16]。

3　RPO 通用权限管理模型调用

本模型总共包括 5 个功能模块：用户管理、角色管理、目录管理、颗粒操作管理[17]和角色权限管理。模型功能结构如图 2 所示。

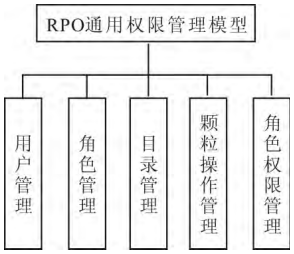

图 2　RPO 通用权限管理模型功能结构

因为所有功能均为自定义，且具有低耦合性，所以本模型可以独立于其它软件系统运行，并提供权限管理接口供其它系统调用。其它系统将加密后的信息通过网络发给本模型[18]，本模型处理后将结果加密后返回给其它系统，调用流程如图 3 所示。

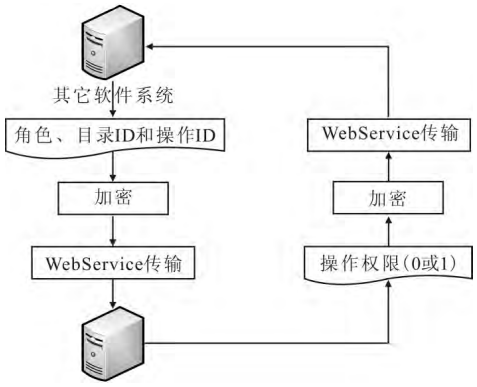

图 3　RPO 通用权限模型调用流程

本模型支持多系统调用，每个系统的角色、目录和操作均独立，管理员可以在自己的业务范围内管理角色、目录和操作，系统之间互不干扰，真正实现了调用的通用性。

4　结语

传统的权限管理模型将用户、资源和操作集成或者捆绑在代码中，虽然能够解决权限分配和系统安全的问题，但是在可维护和可扩展方面存在巨大弊端，改进后的 RBAC 模型将角色取代用户，降低了工作量，可是仍不能从根本上解决系统维护和扩展问题。本文提出了 RPO 自定义通用权限管理模型，该模型将角色、资源和操作从代码中独立出来，由之前的代码定义变为用户自定义，极大地提高了可维护性和可扩展性。并且该模型独立于软件系统，可以被其它系统方便地调用，真正实现了通用性。

参考文献：

[1]　李昕昕，严张凌，王赛兰.改进的基于角色的通用权限管理模型及其实现[J].计算机技术与发展，2012，22(3)：240-244.

Hadoop 性能测试自动化研究

尤元建，吴洪学

（南京中兴软件有限责任公司 中心研究院，江苏 南京 210012）

摘 要：目前，越来越多的行业认识到大数据会带来新一轮的革命，而 Apache Hadoop 项目则是目前大数据平台应用的事实标准。各行业在建设大数据平台时，除功能外，性能指标也是考虑的重要因素。目前大数据平台性能评测工具多样，测试过程耗时、繁琐。鉴于此，讨论建设基于 BigDataBench 的 Hadoop2.5 大数据平台性能测试自动化系统，既提高工作效率，又减少人为操作差异化，实现版本间性能数据自动对比，保证了测试质量和数据准确性。同时对自动化测试工具的演进方向进行了规划。

关键词：Hadoop；大数据平台；自动化测试；性能测试

DOI：10.11907/rjdk.162030

中图分类号：TP302 **文献标识码**：A **文章编号**：1672-7800(2016)012-0016-3

0 引言

信息爆炸时代带来了信息数量的级数级增长，各行业也越来越认识到对大数据的掌控和分析能力会是未来竞争力的核心。行业决策也超越了以前依靠抽样调查的阶段，转而依靠大数据进行全面分析支持。

Apache Hadoop 是对 Google 的 GFS(Google File System)BigTable 的一个开源实现，具有高扩展性、高效性、高容错性、低成本以及易于虚拟化等特性，是目前行业事实的应用标准[1]。Apache Hadoop 大数据生态圈核心包括 HDFS、Zookeeper、Yarn、Hbase、Hive、Impala 等应用。

除功能外大数据平台性能处理能力是评测大数据平台的重要指标之一。目前，大数据平台性能测试存在的问题主要有：开源版本更换较快，需要频繁更换版本；测试条目较多，场景比较复杂、繁琐，手工操作容易出错或不准确；整个测试过程持续时间长。本文基于 BigDataBench 工具和 Apache Hadoop2.5 进行大数据平台性能测试自动

[2] 鲍可进，彭刨.一种扩展的 Android 应用权限管理模型[J].计算机工程，2012，38(18)：57-64.
[3] 李东，施懿闻，郝艳妮，毛基业.科学基金管理系统的用户权限管理模式研究[J].计算机技术与发展，2012，22(2)：159-164.
[4] 王少辉，王超，孙国梓.DroidDefence：细粒度的 Android 应用权限管理系统[J].四川大学学报：工程科学版，2014，46(6)：14-18.
[5] 王非，李凝，侯平路，等.基于角色权限管理的 B/S 与 C/S 模式相结合的教务管理系统安全体系的研究与设计[J].辽宁师范大学学报：自然科学版，2012，35(4)：488-492.
[6] 王居柱，侯彤璞，孙明柱.基于 Struts-Hibernate 架构的权限管理系统的设计与实现[J].计算机与数字工程，2011，39(4)：101-105.
[7] 张伟.基于逻辑程序的 RBAC 模型研究[D].北京：北京大学，2013.
[8] 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.
[9] 曾锡山，陈振洲.基于对象属性约束权限控制研究与实现[J].华南师范大学学报：自然科学版，2016，48(2)：111-115.
[10] 罗求，丁滟，陈松政.一种基于管理员分权的用户特权提升机制[J].计算机工程，2016，42(4)：27-36.
[11] 李天鸣，何月顺.基于 ExtJS 技术与 SSH 框架的权限管理研究[J].计算机应用与软件，2011，28(5)：165-205.
[12] 范明虎，樊红，伍孝金.ASP.net 中基于 RBAC 的通用权限管理系统[J].计算机工程，2010，36(1)：143-145.
[13] 吴波，王晶.基于基本 RBAC 模型的权限管理框架的设计与实现[J].计算机系统应用，2011，20(4)：50-54.
[14] 高丽丽，王琼.基于角色的访问控制在 OA 系统中的应用[J].软件导刊，2016，15(3)：157-158.
[15] 赵明斌，姚志强.基于 RBAC 的云计算访问控制模型[J].计算机应用，2012，32(S2)：267-270.
[16] 张磊，张宏莉，韩道军等.基于概念格的 RBAC 模型中角色最小化问题的理论与算法[J].电子学报，2014，42(12)：2371-2378.
[17] 蒋辉，李敬辉，魏巧玲.基于 RBAC 模型的通用权限管理系统分析与设计[J].软件导刊，2016，15(3)：120-123.
[18] CHE TIANWEI，MA JIANFENG，LI NA，et al.Security analysis of access control model in hybrid cloud based on security entropy [J].High technology letters，2015，21(2)：200-204.

（责任编辑：陈福时）

作者简介：尤元建(1974－)，男，山东临沂人，硕士，南京中兴软件有限责任公司中心研究院工程师，研究方向为通信网管理、大数据应用；吴洪学(1987－)，男，江苏徐州人，南京中兴软件有限责任公司中心研究院工程师，研究方向为软件测试自动化、大数据应用。