第44卷　第3期
2025年9月

《新疆师范大学学报》(自然科学版)
Journal of Xinjiang Normal University
(Natural Sciences Edition)

Vol.44,No.3
Sept. 2025

一种支持否定授权的RBAC优化模型

李　峰
(湖北三江航天红峰控制有限公司 技术中心,湖北 孝感 432000)

摘　要:针对基于角色的访问控制(RBAC)模型在授权管理方面存在的不足,本研究对RBAC模型进行多维度整体性优化,构建了一种支持否定授权的RBAC优化模型。首先,采用组合化方法分别对RBAC模型用户端和权限端进行优化,简化了角色和权限的分配过程;其次,将用户属性及其规则表达式融入RBAC模型,增强模型的动态访问控制能力;再次,引入否定授权策略并具象化其实践方式,提高模型访问控制的灵活性和安全性;最后,为辅助角色和授权管理提出了一种基于该优化模型的角色查询方法。同时,给出优化模型的形式化描述,并对其授权和权限验证、权限获取过程进行详细分析和阐述。

关键词:角色;RBAC;否定授权;访问控制;优化;RBAC-OMSNA

中图分类号:TP309.2　　**文献标识码:**A　　**文章编号:**1008-9659(2025)03-0011-06

访问控制是保护信息系统中数据安全的关键技术,其通过定义系统中主体对客体访问权限的方式,限制用户对数据资源的访问能力和范围,防止信息的非授权访问[1-2]。基于角色的访问控制(Role Based Access Control,RBAC)模型在用户集合和权限集合之间建立角色集合,用户被授予适当的角色来获得角色所拥有的全部权限[1,3-5]。该模型因其安全性、灵活性、可扩展性等特点已成为目前应用最广泛的访问控制技术之一[4-6]。然而,对于复杂的访问控制环境而言,基于角色的访问控制模型仍存在不足之处:①RBAC模型具有用户角色分配和角色权限分配两组多对多关系,且均需进行人工配置,当用户数量和权限规模十分庞大且经常变化时,将产生权限分配困难的问题[1,3];②RBAC模型中的角色是静态指派的,无法动态进行用户权限分配[3,7-8];③RBAC模型基于肯定授权的封闭访问控制策略[9-11],在RBAC相关研究中很少提及否定授权,RBAC模型缺乏对否定授权的有效支持。

针对上述问题,本研究以RBAC模型为基础,提出一种支持否定授权的RBAC优化模型(RBAC Optimization Model Supporting Negative Authorization,RBAC-OMSNA),该模型对RBAC模型用户端和权限端以及用户角色的分配方式进行了优化,并在此基础上引入并实施否定授权策略,同时为提高角色和授权管理效率给出了一种基于RBAC-OMSNA模型的角色查询方法。

1　优化RBAC模型

RBAC是一种经典的访问控制模型,其模型元素包括用户、角色、会话和权限,四者之间有如下关系[1,12-13]:用户角色分配、角色权限分配和角色激活。

从上述RBAC模型概述及其存在的不足可知,在对RBAC模型进行优化时,首先从RBAC模型元素及元素间的关系入手开展优化,其次通过引入否定授权对RBAC模型单纯采用肯定授权的方式进行优化。针对RBAC模型元素中的用户和权限,通过构建相对独立的管理单元进行优化;针对RBAC模型元素间的关系,采用结合属性规则及其表达式的方法对权限分配方式进行优化。

1.1　优化用户端

针对用户端,采用在RBAC模型中用户与角色的映射关系的基础上,增加岗位与角色的映射关系,取代

[收稿日期]2024-07-02　　[修回日期]2024-10-26

[作者简介]李　峰(1981-),男,高级工程师,主要从事计算机应用技术方面研究,E-mail:1661888499@qq.com.

原有的单一用户与角色映射关系的方法进行用户端优化,构造出用户-岗位-角色或者用户-角色两类授权管理模式[13-15]。由于组织内岗位与人员相比相对稳定,为岗位分配相应角色后,该岗位所有人员均完成相应角色指派,即可自动建立用户与角色的映射关系,从而实现用户权限的实时更新。

当将岗位如同用户一样分配给角色时,角色实际上是与一个或一组特定工作岗位相关的一个权限集合。一个岗位可能会有多名组织成员,这样将岗位分配给角色,本质上是将一组用户同时指派给相应的角色,避免对相同岗位的用户重复进行用户角色指派。通过对岗位授予角色,可以快速使某一类用户具有相同的权限,简化了对用户端的授权操作。同时,在进行岗位角色指派之前,需要完成用户岗位指派,即完成人员定岗。人员定岗一般由企事业单位的人力资源部门负责,当组织成员的人事关系或工作岗位发生变化时,信息系统的管理人员无需再配置此用户与相应角色的映射关系,从而降低了用户端授权管理的复杂度。

1.2 优化权限端

针对权限端,采用在RBAC模型中角色与权限的映射关系的基础上,增加角色与权限组的映射关系,取代原有单一的角色与权限映射关系的方法进行权限端优化。进一步进行权限分组,形成权限组,即形成一组权限的集合,构造出角色-权限组-权限或者角色-权限两类授权管理模式,此时可对角色赋予一个或多个权限,也可对角色赋予一个或多个权限组。当为角色分配相应权限组后,该权限组所有权限均完成相应角色指派,即可自动建立角色与权限的映射关系,角色具有所属权限组中的全部权限。

将权限组如同权限一样分配给角色,本质上是将一组权限批量指派给相应的角色,避免对权限组内的权限重复进行角色权限指派。通过将权限组授予角色,可以快速完成一组权限的角色权限指派操作,简化了对权限端的授权。在进行角色权限组指派前,需要信息系统的管理人员完成权限组的定义以及对权限组中的权限进行初始化配置,当调整权限组中的权限时,只需要维护权限组与权限的映射关系,无需再配置角色与相应权限组的映射关系,所有拥有该权限组的角色将同步完成权限的动态更新,从而提高权限端授权管理的效率和实用性。

1.3 优化用户分配

RBAC模型需要对每一个用户静态指派合适的角色,无法动态匹配用户和角色的映射关系,当系统中的用户经常变动时,该模型无法实现实时、有效的授权管理。

针对这一情况,采用结合属性和角色混合访问控制的基本思路,将用户和角色的静态分配关系扩展为通过主体属性动态实现用户角色分配[7,11,16]。从实用性和实现成本角度考虑,RBAC-OMSNA模型只对常用角色优化用户分配方式。结合对用户端的优化,筛选用户的岗位属性信息,通过岗位属性集合子集的属性表达式自动决定常用角色的用户分配。由于在实际应用场景中用户的岗位等级与用户在信息系统中所拥有的权限具有直接关系,同时企事业单位常见的应用系统,如办公自动化(Office Automation,OA)、业务流程管理(Business Process Management,BPM)、企业资源计划(Enterprise Resources Planning,ERP)等系统中经常出现应用较为频繁的角色,如普通用户、部门领导、主管领导等,这些常用角色本身也体现出组织机构的岗位层次结构,可以将用户和上述常用角色的分配关系扩展为通过岗位等级构造的规则表达式进行动态匹配,无论用户的岗位如何变化,用户都可以自动成为相应角色的成员。

访问控制模型的扩展和应用需要充分考虑应用场景的特性,在基于属性的用户角色动态分配过程中,可根据具体应用场景选用合适的主体属性,建立单一或多维属性的规则表达式来优化用户角色的分配关系。当用户提供的属性满足设定的规则表达式时才可以被分配给相应的角色,这样使得访问控制模型不仅能够支持实时、动态的用户分配,而且显著降低了人工分配用户角色的工作量。

1.4 引入否定授权

为了避免访问控制模型中用户通过激活某些角色组合来绕过访问控制策略的情况,可以在模型中引入否定授权策略[9],同时支持肯定授权和否定授权易产生授权冲突。在RBAC-OMSNA模型中将采用否定授权优先策略[10],其否定授权可以分为两种形式:一种针对用户端,另一种针对权限端。

根据RBAC-OMSNA模型特点,针对用户端的否定授权可以分为对岗位的否定授权和对用户的否定授权。对岗位的否定授权是对分配给某角色的岗位进行否定授权,即对该岗位下的所有用户均进行否定授权,从而阻止该岗位下的全部用户获得通过与该岗位间接关联的角色所对应的全部权限;对用户的否定授

权是对直接分配给某角色的单个用户进行否定授权,只能阻止单一用户获得其所关联角色所对应的全部权限。

权限端的否定授权可以分为对权限组的否定授权和对权限的否定授权。对权限组的否定授权是对分配给某角色的权限组进行否定授权,即对该权限组所包含的所有权限均进行否定授权,从而阻止该角色关联的全部用户获得该权限组的全部权限;对权限的否定授权是对分配给某角色的单个权限进行否定授权,只能阻止该角色关联的全部用户获得该权限。

在实现RBAC-OMSNA模型中的否定授权时,能够以“黑名单”的形式进行呈现,即对某角色进行权限配置后还可配置黑名单。黑名单包括四种类型:用户黑名单、岗位黑名单、权限黑名单和权限组黑名单,分别对应对用户的否定授权、对岗位的否定授权、对权限的否定授权和对权限组的否定授权。根据实际权限配置场景和需要,选择合适的黑名单类型进行配置,即可快速在应用RBAC-OMSNA模型进行访问控制的信息系统中完成基于角色的否定授权操作。

2　支持否定授权的RBAC优化模型

2.1　模型形式化描述

RBAC-OMSNA模型在RBAC模型的基础上分别对用户端和权限端进行优化,同时引入否定授权机制,本质上相当于对RBAC模型中的用户集和权限集进行分类和细分。分类是指将RBAC模型中的用户集和权限集分别划分为两类,一类是进行肯定授权的用户集和权限集,另一类是进行否定授权的用户集和权限集;细分是指将RBAC模型中的用户集和权限集在分类的基础上再分别进行细化操作,其中用户集细分为用户集和岗位集,权限集细分为权限集和权限组集。这样RBAC-OMSNA模型的用户端包括用户集、岗位集、黑名单用户集和黑名单岗位集,权限端包括权限集、权限组集、黑名单权限集和黑名单权限组集,其模型如图1所示。

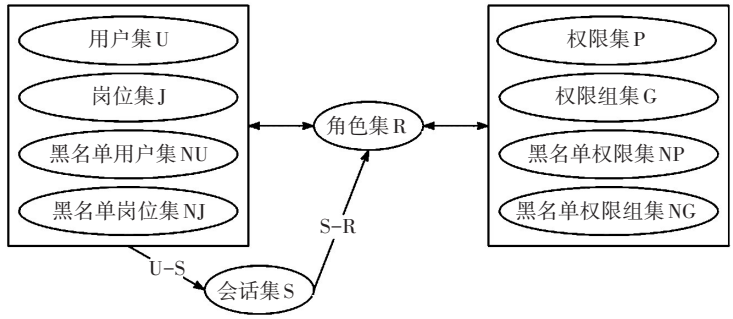

图1　RBAC-OMSNA模型

RBAC-OMSNA模型元素中的用户集U、权限集P、角色集R和会话集S同RBAC模型中相应元素定义相同,其余元素定义如下:

(1)岗位集J:是在组织中具有一定职务、责任和权力的集合。形式化描述为:J={j1,j2,jn}.

(2)黑名单用户集NU:是禁止访问系统中资源的主体集合,是禁止对访问对象进行操作的主体。形式化描述为:NU={nu1,nu2,…,nun}.

(3)黑名单岗位集NJ:是执行否定授权策略的岗位集合。形式化描述为:NJ={nj1,nj2,…,njn}.

(4)权限组集G:是对权限进行分组,不同的权限分组形成不同的权限组合。形式化描述为:G={g1,g2,…,gn}.

(5)黑名单权限集NP:是禁止对系统中的资源进行访问的权限集合。形式化描述为:NP={np1,np2,…,npn}.

(6)黑名单权限组集NG:是执行否定授权策略的权限组集合。形式化描述为:NG={ng1, ng2, …, ngn}.

RBAC-OMSNA模型中的函数关系UA(用户角色分配)和PA(角色权限分配)同RBAC模型中相应函数关系定义相同,其余主要函数关系包括:

(1)JA:岗位角色分配,表示岗位和角色多对多的映射关系;

(2)NUA:黑名单用户角色分配,表示黑名单用户和角色多对多的映射关系;

(3)NJA:黑名单岗位角色分配,表示黑名单岗位和角色多对多的映射关系;

(4)GA:角色权限组分配,表示角色和权限组多对多的映射关系;

(5)NPA:角色黑名单权限分配,表示角色和黑名单权限多对多的映射关系;

(6)NGA:角色黑名单权限组分配,表示角色和黑名单权限组多对多的映射关系。

2.2 授权和权限验证

RBAC-OMSNA模型的访问控制授权分为两个过程:肯定授权和否定授权,但进行肯定授权和否定授权的操作没有先后之分,并且可以只选择其中一个过程进行授权。其中肯定授权分为用户端分配和权限端分配两个步骤,但不需要同时完成两个步骤的分配操作。与基本RBAC模型相比,用户端的用户角色分配细分为用户角色分配和岗位角色分配两种方式,岗位角色分配本质上仍是用户角色分配;权限端的角色权限分配细分为角色权限分配和角色权限组分配两种方式,角色权限组分配本质上仍是角色权限分配。

RBAC-OMSNA模型中的否定授权也分为用户端分配和权限端分配两个步骤,同样不需要同时完成两个步骤的分配操作。通过配置岗位黑名单或用户黑名单,建立用户和角色的否定授权策略;通过配置权限组黑名单或权限黑名单,建立角色和权限的否定授权策略。在用户端进行肯定或否定授权,在权限端并不需要对应地进行肯定或否定授权,在用户端和权限端只需要根据权限配置目标按需进行肯定或否定授权操作即可。

RBAC-OMSNA模型通过两阶段验证完成权限控制,只有同时满足肯定授权和否定授权的权限验证才能执行相应访问策略。当进行权限验证时,首先根据用户所拥有的肯定授权策略判断是否允许用户执行权限规定的业务操作。如果不允许,则权限控制流程直接结束;如果允许,则进入否定授权策略验证阶段,存在针对该项业务操作的否定授权,则权限控制流程结束。只有拥有肯定授权策略,并且不存在否定授权策略时才能在信息系统中执行对应的业务操作。

2.3 权限获取过程

RBAC-OMSNA模型获取权限按照以下步骤进行,如图2所示。

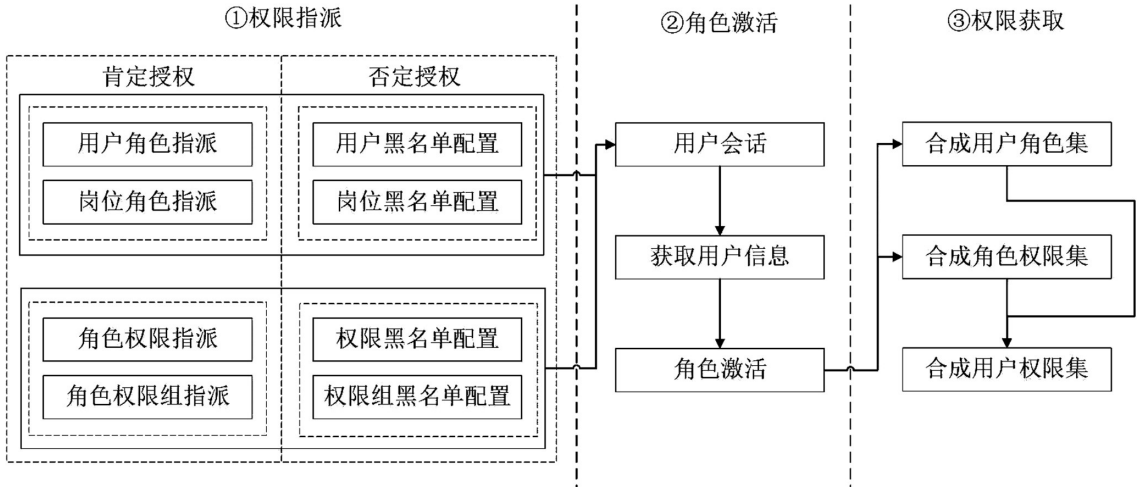

图2 权限获取过程

步骤1 权限指派。根据权限配置场景需要进行肯定授权和否定授权。其中肯定授权包括用户角色指派、岗位角色指派、角色权限指派和角色权限组指派;否定授权包括用户黑名单配置、岗位黑名单配置、权限黑名单配置和权限组黑名单配置。

步骤2 角色激活。根据用户登录信息创建用户会话,获取用户信息,激活用户全部角色。

步骤3 权限获取。根据角色用户端的配置信息,包括用户角色指派、岗位角色指派、用户黑名单配置和岗位黑名单配置信息合成用户角色集;根据角色权限端的配置信息,包括角色权限指派、角色权限组指派、权限黑名单配置和权限组黑名单配置信息合成角色权限集;根据用户角色集和角色权限集合成用户权限集。

2.4　模型分析

RBAC-OMSNA模型授权过程主要具有以下特点:

(1)权限分配的高效性。模型不仅可以将用户分配给角色,而且可以将岗位分配给角色;不仅可以将权限分配给角色,而且可以将权限组分配给角色。通过岗位和权限组可以在用户端和权限端实现组合化、批量化的授权操作,提高模型权限分配效率。

(2)权限分配的安全性。模型通过引入否定授权,并且采用否定授权优先策略可以有效地阻止用户非授权访问,增强模型访问控制策略的安全性。

(3)权限分配的灵活性。模型可以按需进行肯定授权或否定授权;模型用户端肯定授权可以按需进行用户角色指派或者岗位角色指派;模型用户端否定授权可以按需进行用户黑名单配置或者岗位黑名单配置;模型权限端肯定授权可以按需进行角色权限指派或者角色权限组指派;模型权限端否定授权可以按需进行权限黑名单配置或者权限组黑名单配置;模型可以按需进行用户端配置或者权限端配置。模型的按需权限分配使得模型授权过程具有极大的灵活性和适应性。

(4)权限分配的动态性。模型支持面向不同应用场景灵活选择不同用户属性,进而基于用户属性及其规则表达式动态决定用户和角色的分配关系,不仅使得模型以角色为中心的访问控制方法进一步得到优化和完善,而且使得模型可以支持实时、动态的授权管理,增强模型的动态访问控制能力。

3　角色查询

RBAC-OMSNA模型不仅可以将用户指派给角色,还可以将岗位指派给角色;不仅可以为角色分配权限,还可以为角色分配权限组;不仅可以进行肯定授权,还可以进行否定授权。相比RBAC模型,其提供了更为精细和灵活的权限控制,同时也对角色管理提出了更高的要求。

RBAC-OMSNA模型对角色的依赖程度依然较高,在面对大量用户、角色、权限及其之间复杂的关系时,为提高该访问控制模型在实际应用中的实效性和灵活性,从信息系统功能设计与实现的角度出发,提出了一种针对RBAC-OMSNA模型的辅助角色定义和授权的角色查询方法。

该方法包括正向的角色查询和逆向的用户查询以及权限查询。其中角色查询指通过角色名称或角色编码查询为该角色指派的用户端的用户和岗位以及为该角色指派的权限端的权限和权限组。用户和岗位同时包括否定授权的黑名单用户和黑名单岗位,权限和权限组同时包括否定授权的黑名单权限和黑名单权限组。用户查询指通过用户姓名查询为该用户指派的所有角色及角色对应的权限,为用户指派的角色同时包括通过岗位指派的角色、通过用户黑名单配置指派的角色和通过岗位黑名单配置指派的角色。角色对应的权限包括指派给该角色的所有肯定授权的权限和权限组以及否定授权的黑名单权限和黑名单权限组。权限查询指通过权限名称或权限组名称查询为该权限或权限组指派的所有角色及角色对应的用户和岗位。为权限或权限组指派的角色同时包括通过权限黑名单配置指派的角色和通过权限组黑名单配置指派的角色。角色对应的用户和岗位包括指派给该角色的所有肯定授权的用户和岗位以及否定授权的黑名单用户和黑名单岗位。

角色的定义、修改和删除常常隐含在基于角色的访问控制模型中,角色的查询,尤其是以用户为视角的角色查询却常常被忽视。但在实际应用场景中,角色查询往往是系统管理员进行角色定义、修改和删除的必要支撑,可以使授权过程更加准确、高效和安全。这里的角色定义一般指创建角色并为角色分配用户和权限。角色修改指修改角色自身的属性信息,如角色名称、角色描述等,也包括修改基于角色的肯定授权和否定授权。而角色删除指取消用户和角色、岗位和角色、黑名单用户和角色、黑名单岗位和角色、角色和权限、角色和权限组、角色和黑名单权限以及角色和黑名单权限组之间的映射关系并删除角色本身,在删除角色前应判断该角色已取消所有用户端和权限端的指派关系。以角色查询结果为基础,通过角色修改,可以在某种程度上减少创建角色的数量;同样,以角色查询结果为基础,通过角色修改和删除,甚至可以直接减少角色数量。

4 结语

RBAC-OMSNA模型采用递进式和组合化方法对RBAC模型进行多维度的整体性优化。通过优化用户端和权限端的授权机制,提高了角色和权限的管理效率;通过将用户属性及其规则表达式融入模型中,实现了以非指派的方式进行用户角色授权;在完成RBAC模型用户端和权限端优化之后,通过引入否定授权策略,并将否定授权策略在用户端和权限端分别具象化为不同的表现形式,实现了模型细粒度和多样化的授权操作;在优化用户端和权限端并实施否定授权策略的基础上,新增全面灵活的角色查询功能,不仅降低了角色管理复杂度,而且减少了授权操作的随意性和盲目性。同时,如需在不同应用场景中面对不同访问控制需求实施RBAC-OMSNA模型,只需对该模型的不同优化内容进行适应性裁剪和调整,即可完成该模型的敏捷应用。后续该模型的进一步优化方向主要为实现角色权限或角色权限组的动态分配。

参考文献:

[1] 余波,台宪青,马治杰. 云计算环境下基于属性和信任的RBAC模型研究[J]. 计算机工程与应用,2020,56(09):84-92.
[2] 房梁,殷丽华,郭云川,等. 基于属性的访问控制关键技术研究综述[J]. 计算机学报,2017,40(07):1680-1694.
[3] 周超,任志宇. 结合属性与角色的访问控制模型综述[J]. 小型微型计算机系统,2018,39(04):782-785.
[4] 张焕国. 信息安全工程师教程[M]. 北京:清华大学出版社,2016.
[5] 李峰. 基于角色的参数化访问控制模型[J]. 新疆师范大学学报(自然科学版),2023,42(01):1-5.
[6] 袁学斌,李文萍,刘生成,等. RBAC中角色挖掘算法研究[J]. 通信技术,2020,53(08):1994-2001.
[7] 熊厚仁,陈性元,费晓飞,等. 基于属性和RBAC的混合扩展访问控制模型[J]. 计算机应用研究,2016,33(07):2162-2168.
[8] 王静宇,张伟. 结合属性和RBAC的访问控制模型及算法研究[J]. 小型微型计算机系统,2022,43(07):1523-1527.
[9] 张世龙,沈玉利. 一种 RBAC模型中实现否定授权的方法[J]. 计算机应用与软件,2009,26(05):65-67.
[10] 刘月琴,朱艳琴,陈玉春. 支持否定授权的基于子角色的授权代理模型[J]. 计算机应用与软件,2008,25(11):80-82.
[11] 李佳,徐向阳. 角色管理自动化的访问控制[J]. 计算机工程,2007,33(05):120-122.
[12] 顾春华,高远,田秀霞. 安全性优化的RBAC访问控制模型[J]. 信息网络安全,2017,(05):74-79.
[13] 何萍. 针对数据平台的细粒度访问控制方法研究[D]. 西安:西安理工大学,2020.
[14] 彭友,李怀明,王延章. 电子政务系统中基于组织的访问控制方法和模型[J]. 系统管理学报,2014,23(04):481-488.
[15] 王涛,王延章. 一种基于岗位和角色的访问控制模型研究[J]. 计算机应用研究,2009,26(03):1084-1085.
[16] 唐金鹏,李玲琳,杨路明. 面向用户属性的RBAC模型[J]. 计算机工程与设计,2010,31(10):2184-2186.

A RBAC Optimization Model Supporting Negative Authorization

LI Feng

(*Technology Center, Hubei Sanjiang Space Hongfeng Control Limited Company, Xiaogan, Hubei, 432000, China*)

Abstract: Aiming at the shortcomings of the Role Based Access Control (RBAC) model in authorization management, in this paper, a RBAC optimization model supporting negative authorization is constructed, which is a multidimensional holistic optimization of the RBAC model. Firstly, a combination approach is adopted to optimize the user side and the authorization side of the RBAC model, respectively, which simplifies the process of assigning roles and authorizations. Secondly, the dynamic access control capability of the model is enhanced by incorporating the user attributes and their rule expressions into the RBAC model. Thirdly, the negative authorization strategy is introduced into the model, and the practice approach of negative authorization strategy is clarified, the flexibility and security of access control are improved. Finally, a role query method is proposed based on this optimization model to support role an authorization management. Meanwhile, a formal description of the optimization model is given, and its authorization and permission verification and permission acquisition processes are analyzed and elaborated in detail.

Keywords: Role; RBAC; Negative authorization; Access control; Optimization; RBAC-OMSNA