

改进的 RBAC 模型在电网视频监控平台中的应用

郝小龙

(国网电力科学研究院,江苏 南京 210003)

摘要:针对传统基于角色的访问控制(RBAC)模型在大规模企业应用及复杂业务权限控制中的不足,文中引入了 RULES 和 GROUPS 属性对其进行延伸和拓展,形成了改进的 RBAC 模型。通过 RULES 对数据范围细化,解决了细粒度复杂业务中的权限控制,通过 GROUPS 定义层次结构模型,实现了大规模授权中的分级管理。基于此模型构建了统一视频监控平台权限管理框架,讨论了其功能组成、分级管理授权过程及细粒度权限控制过程,并通过项目验证了其可行性与有效性。

关键词:细粒度;访问控制;基于角色的访问控制;分级授权

中图分类号:TP39

文献标识码:A

文章编号:1673-629X(2014)12-0212-04

doi:10.3969/j.issn.1673-629X.2014.12.050

Application of Improved RBAC Model in Grid Video Monitoring Platform

HAO Xiao-long

(State Grid Electric Power Research Institute, Nanjing 210003, China)

Abstract: To address the drawbacks of traditional RBAC model when it is used in large-scale enterprise application and complex business access control, introduce attributes of RULES and GROUPS to extend and expand, forming the advanced RBAC (Role-Based Access Control) model. RULES can be leveraged to access control of fine-grained complex business by fining the data scope. And GROUPS can be applied to realize the large-scale hierarchical authorization management by defining the hierarchical structure model. The access management structure of SG-UVP is built based on the proposed model. Discuss the function construction, the processes of hierarchical authorization management and access control of the proposed model. The test results demonstrate the feasibility and effectiveness of the proposed method.

Key words: fine-grained; access control; RBAC; hierarchical authorization

0 引言

基于角色的访问控制(RBAC)的概念于1992年由Ferraiolo等人^[1]提出。该方法通过在用户和访问权限之间引入角色概念,实现用户对资源信息的间接访问。经过多年的研究发展,该方法已被广泛使用,它有效地降低了应用授权管理的复杂性,为信息系统的权限管理提供了相对灵活的解决方案。

国内外许多学者都致力于这方面的研究。1996年Sandhu^[2]提出了RBAC96模型。此后,美国国家标准技术研究院(National Institute of Standards and Technology, NIST)提出了RBAC标准及其概念和构架的标准定义^[3-4]。2007年, Ferraiolo等人^[5]整体综合性地对RBAC进行了描述。然而,随着企业信息化管理水平

的提高,其业务应用规模不断扩大、业务关系更为复杂化,传统的RBAC模型暴露出越来越多的不足,这些不足主要体现在权限访问控制时只考虑了业务对象的类别,而没有考虑业务对象的实例,因此无法满足数据级权限管理的需求。用户授权管理只考虑了集中方式,因此无法满足企业用户量大,分级管理的需求。翟征德、吴江栋、李细雨等人^[6-8]提出了细粒度的权限访问控制方法;2010年,龙军等人^[9]提出了自治域概念,形成了基于自治域的RBAC模型;姚寒冰、张沙沙、姚全营等人^[10-12]引入上下文概念对权限进行细化;2012年,李昕昕等人^[13]提出了一种对权限的细化方法,引入了连续与离散范围,形成了RUP(Role—User—Privilege)模型;2013年,许洁、王德鑫等人^[14-15]对多级权

收稿日期:2014-01-10

修回日期:2014-04-15

网络出版时间:2014-10-23

基金项目:国家电网公司项目(2012CETIT-I-7-7, 2013CETIT-II-8-6)

作者简介:郝小龙(1984-),男,山西吕梁人,硕士研究生,工程师,研究方向为电力系统自动化等。

网络出版地址: <http://www.cnki.net/kcms/detail/61.1450.TP.20141023.1047.004.html>

限共享进行了探讨。

以上这些工作在一定程度上为信息系统权限管理提供了新的思路,但是笔者在实际应用开发的过程中发现,这些工作一方面没能对数据权限进行细化分类,使得很难在这些改进的 RBAC 模型上给出一个通用的细粒度权限框架,另一方面对自治的讨论未涉及如何对功能权限与数据权限的分配。针对这一情形,文中提出了一种改进的 RBAC 模型,其主要特点是在传统的 RBAC 模型中引入 RULES 和 GROUPS 属性,通过前者控制权限的细粒度访问,通过后者实现用户权限管理的分级自治。改进后的模型能较好满足大规模企业信息系统中用户授权分散管理,复杂业务中细粒度权限访问控制需求,达到有效控制信息系统中敏感数据的访问的目的。

1 NIST RBAC 标准模型

经过多年的发展,RBAC 模型已经衍生出多种新模型,文中提出的模型是基于 NIST RBAC 模型^[4-5]进行扩展构建。NIST RBAC 模型由四种模型组件组成,包括 Core RBAC、静态职责分离(Static Separation of Duty Relations)模型和动态职责分离(Dynamic Separation of Duty Relations)模型。其中 Core RBAC 定义了 RBAC 最小的元素集合,它包括五个基本要素和五种关系,如图 1 所示(图中单箭头表示一对多分配关系,双箭头表示多对多分配关系)。

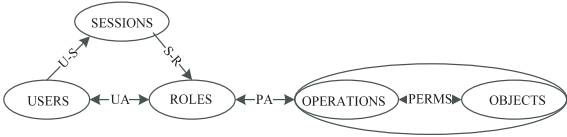


图 1 Core RBAC 模型图

- 现对其作简要说明如下:
- (1)USERS,是访问系统中的数据或资源的主体集合,是对数据对象进行操作的主体。
 - (2)ROLES,是具有一组访问权限集合的抽象实体,划分同一类用户的职责。
 - (3)SESSIONS,是用户某一时刻与系统进行的交互。用户和会话是一对多的关系,一个用户可关联一个或多个会话。
 - (4)OBJECTS,系统中数据或资源对象的集合。
 - (5)OPERATIONS,对系统中的数据和资源进行操作的集合。
 - (6)UA,User Assignment 表示 USERS 和 ROLES 多对多的映射关系,一个 USER 可以分派一个或者多个 ROLE,同时一个 ROLE 能被一个或者多个 USER 拥有。
 - (7)PA,Permission Assignment 表示 PERMISSIONS

和 ROLES 多对多的映射关系,一个 PERMISSION 可以被分派给一个或者多个 ROLE,同样一个 ROLE 可以拥有多个 PERMISSION。

(8)U-S,表示 USERS 和 SESSINS 的一对多分派关系,一个 USER 可以产生多个 SESSION,而一个 SESSION 只允许一个 USER 参与。

(9)S-R,表示 SESSIONS 和 ROLES 一对多的映射关系。

(10) PERMS,表示 PERMISSIONS 集合,也表示 OBJECTS 和 OPERATIONS 多对多的映射关系。

传统的基于 RBAC 模型的访问控制的核心是以 ROLES 为媒介实现给 USERS 赋予对 OBJECTS 执行 OPERATIONS 的权限,一定程度上简化了权限管理。但在实际应用中该权限模型只涉及功能权限,难以满足很多常用的数据级权限管理的需求,且无法满足复杂组织结构或特定应用系统中分级管理的需求,具体表现在:

(1)传统的 RBAC 模型只定义了对象上的功能权限,未定义功能权限具体可应用的数据范围,即数据权限,因此无法实现精细化授权,如无法实现某用户只能查看自己单位权属的设备。

(2)传统的 RBAC 模型未涉及对大量用户及其授权如何进行有效管理。因此在未作扩展的情况下无法满足在大型企业信息系统或特定应用系统中,系统权限授权管理分级管理的需求。

2 细粒度改进后的 RBAC 模型

2.1 改进 RBAC 模型定义

传统的 RBAC 采用 OPERATIONS 和 OBJECTS 这两个属性来定义 PERMS,且未定义用户及其授权管理。改进 RBAC 模型通过引入了规则(RULES)属性,结合 OPERATIONS 和 OBJECTS,可以在模型中清晰地体现出功能权限和数据权限的区别。通过引入 GROUP 属性,结合 USERS 和 PERMS,可以实现用户与授权的分级管理。

图 2 中给出了改进 RBAC 模型的结构图及在传统 RBAC 模型上新增的元素和关系定义。

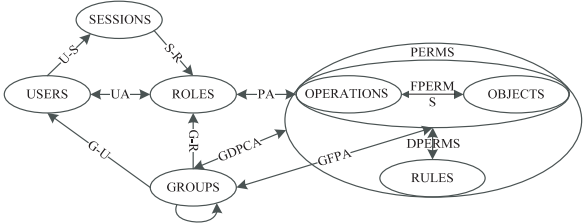


图 2 改进 RBAC 模型图

- 现对其作简要说明如下:
- (1)RULES,是对计算机系统的数据和资源对象

的集合 (OBJECTS) 具体记录范围的描述,如描述自己单位权属的设备的记录规则。施加在同一 OBJECT 上的不同 RULE 采用或逻辑运算关系。

(2) FPERMS, 表示功能权限 (Function Permission) 的集合, 与传统 RBAC 模型中 PERMS 等价。

(3) DPERMS, 表示数据权限 (Data Permission) 的集合, 是 FPERMS 与 RULES 的多对多的分配关系。

(4) PERMS, 表示功能权限与数据权限的集合。

(5) GROUPS, 表示组织或分组层次结构, 每个 GROUP 可以有一个或多个子 GROUP, 每个 GROUP 可以是一个分级管理单元, 当该 GROUP 为分级管理单元时, 认为该 GROUP 是自治的, 自治组通过在 GROUPS 上附加属性 Autonomy 进行区分。

(6) G-U, 表示 GROUPS 和 USERS 间的一对多分配关系, 即一个 USER 只能属于一个 GROUP, 通过在其分配关系上引入 isGroupAdmin 属性区分用户是否为 GROUP 的自治管理员。

(7) G-R, 表示 GROUP 和 ROLE 间的一对多分配关系, 通过该关系, 自治组的管理员可以根据需要维护自治组的 ROLES 集合。

(8) GFPA, Group Function Permission Assignment 表示自治 GROUP 所拥有的所有权限的集合, 自治管理员只可以对其管理范围内的用户授权该集合中的权限。GFPA 由上级自治管理员进行分配。

(9) GDPCA, Group Data Permission Constraints Assignment 表示施加在 GROUP 上的数据约束, 限制了 GROUP 所能有功能权限的数据范围。约束具有继承性, 即所有子 GROUP 都会继承父 GROUP 的约束。

采用该改进 RBAC 模型后, 可以较好地满足上面提到的分级管理及细粒度数据权限控制的需求。分级管理可通过如下过程实现:

(1) 确定自治 GROUP。

(2) 通过 GFPA 为自治 GROUP 分配权限。通过 GDPCA 为自治 GROUP 分配规则约束。

(3) 自治 GROUP 管理员建立需要的 RULES、DPERMS、ROLES、子 GROUPS 及 USERS。

(4) 通过 UA 和 PA 分配管辖自治组及所有子组用户的权限。

细粒度数据权限控制过程如下:

(1) 确定 OBJECT 的 FPERMS。

(2) 确定某 FPERM 对 OBJECT 可操作的 RULES。

(3) 将某 FPERM 与 RULES 关联形成 DPERMS。

(4) 通过 UA 和 PA, 将 FPERMS 和 DPERMS 授予用户。

(5) 权限验证过程中, 用户的 PERMS 由步骤 (4) 与所有父组的 GDPCA 组成。

2.2 分级分组自治结构

根据 2.1 节可知, 分级权限管理的核心是引入了自治 GROUP 概念, 自治 GROUP 类似于国家的自治区概念, 自治 GROUP 拥有其管辖范围内用户权限管理的自主权, 又有一定的约束。其结构如图 3 所示。

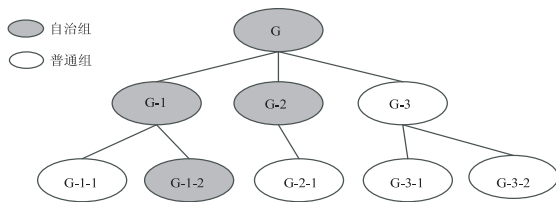


图 3 分级自治结构图

在该自治结构中, 组是用户的集合, 组层次间存在父子继承关系。分组自治 GROUP 可逐级向下推进, 如 G 可确定 G-1 与 G-2 为自治子 GROUP, G-1 可确定 G-1-2 为自治子 GROUP, 普通 GROUP 由最邻近的自治 GROUP 负责用户与授权管理。自治 GROUP 通过图 2 中 UA、PA 进行授权管理, 但其有 GFPA、GDPCA 的约束限制, 即其所能授予的所有 FPERMS 来源于 GFPA 授权的结果集, 所有 DPERMS 来源于所有父 GROUP 及自身 GDPCA 的结果集。这样在保障自治的同时, 约束了所有子 GROUP 的权限。同时如果父 GROUP 通过 GFPA 与 GDPCA 进行权限回收时, 应用于所有子 GROUP。

2.3 RULES 结构

根据 2.1 节可知, 细粒度数据权限控制是通过引入 RULES 实现, 它是对计算机系统的数据和资源对象的集合 (OBJECTS) 具体记录范围的描述。通常依据 OBJECT 的特点, 其数据子集合可通过其属性的特点分为离散型、连续型和层次型, 如设备资产 OBJECT 有如下设备类型、投运时间、所属单位, 其设备类型属性为离散型、投运时间属性为连续型、所属单位为层次型属性。因此一个 RULE 可以通过该三种类似属性组合进行描述。下面分别说明:

(1) 离散型范围: 表示 OBJECT 的某类型或具体某个或几个实例, 如可以表示设备类型为一次设备、设备厂商为海康或设备编号以 AR 开始的数据范围。离散型范围形式上可以表达为其属性 $A=a$ 、 $A \text{ IN } [a_1, a_2]$ 及 $A \text{ LIKE } a$ 。

(2) 连续型范围: 表示某范围内的 OBJECT, 如设备投运日期在 2008 年以后的所有数据。连续型范围形式上可表达为其属性 $A>a$ 、 $A<a$ 、 $A\geq a$ 或 $A\leq a$ 。

(3) 层次型范围: 表示某一或多个层次的 OBJECT, 如设备资产归属单位为江苏省电力公司的所有数据。层次型范围形式上表示为 $A \text{ CHILD_OF } a$ 或 $A \text{ CHILDS_OF } a$, 前者表示直接子数据, 后者表示其下所有子数据, 即包含所有子层次的数据。

通过组合离散型、连续型及层次型范围形成 RULE,可以灵活描述 OBJECTS 记录的范围,达到细粒度划分数据及控制的目的。

3 改进 RBAC 模型在电网统一视频监控平台中的应用

3.1 整体结构

改进 RBAC 模型在电网统一视频监控平台中实现功能框架结构如图 4 所示,包含组管理、用户管理、角色管理、对象管理、权限管理、授权管理,其中组管理又包含自治组及自治组管理员管理、权限管理包括功能权限管理和数据权限管理,授权管理包括用户角色授权、角色权限授权及组权限授权。

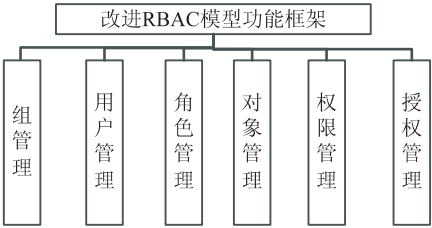


图 4 改进 RBAC 功能框架图

组管理、用户管理、角色管理、对象管理是基本数据的维护,权限管理根据已有的对象建立功能权限和数据权限,授权管理是自治组管理员可根据应用实际需求为角色分配相应的功能权限和数据权限,再将角色赋予相应的用户,或将功能权限与数据约束授予子自治组,从而完成授权过程。这一过程包括扩展 RBAC 模型中针对 USERS 的 UA 和 PA 过程及针对 GROUPS 的 GFPA 和 GDFCA 过程。

3.2 平台分级授权过程

电网统一视频监控平台的资源主要为视频监控设备,需要控制的内容包括设备资源的可访问性、视频调阅、云镜控制等,分级授权按照国家电网公司总部、各网省公司进行组织,总部对其直属调度的视频资源自己进行权限控制,各网省公司的视频设备由各网省自己控制,其分组自治如图 5 所示。

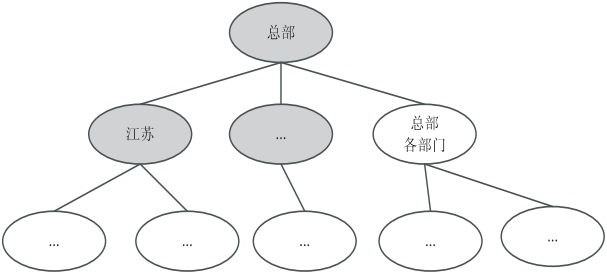


图 5 平台分级自治图

平台首先设定江苏等网省公司为自治组,然后为每个自治组分配管理员,将所有功能权限都授予各自自治组,并授予各网省只能查看权属自己单位的视频监

控设备的数据约束权限,这样各网省只能授予其管辖范围内用户操作自己权属设备的权限,保障了授权可管理性。各网省目前并未再设置下级自治组,但随着设备规模的增加,可进一步设置地市一级自治组,实现权限的分级授权。在分级自治组确定后,各自治组管理员可以对其管理的 USER 通过 UA 和 PA 过程进行用户授权管理,通过 GFPA 和 GDFCA 过程进行子自治组授权管理。通过该分级授权过程极大地方便了权限的管理,满足了业务控制的需要。

3.3 平台权限控制过程

权限控制是在授权完成后对用户访问系统功能有效性的验证,保障了只有授权用户才能对特定资源进行特定操作。电网统一视频监控平台权限控制流程如图 6 所示。

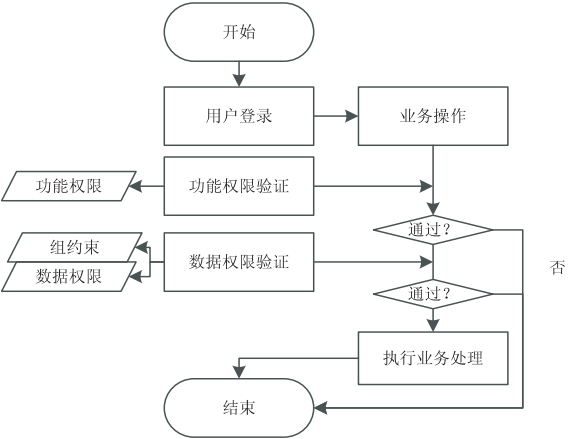


图 6 平台权限控制流程图

权限控制流程在响应一项业务操作时,通过两阶段完成权限的验证。首先根据用户所拥有的功能权限集合判断用户是否可进行该业务操作,如果没有则直接结束,如果有再进入数据权限验证阶段,数据权限来源于用户自身的数据权限集及施加在用户所属组及父组上的所有约束。只有两阶段验证通过后会真正执行业务处理。在权限验证中,为了提高其效率,平台采用了两种方式,一是缓存组、用户及其权限数据,这样可以极大提高权限访问效率,二是为了提高数据权限的运算速度,对层次型范围进行了特殊处理将其转化为离散型范围,即引入 LEVEL 字段,如 L-1 表示二级, L-1-1 表示三级,这样要获取所有上级或下级资源时,只需通过 LIKE 运算即可实现。

4 结束语

文中探讨了 RBAC 模型的改进及其在电网统一视频监控平台中的应用,通过引入自治 GROUP 和 RULES 的概念来扩充传统的 RBAC 模型,将传统的集中式授权模型扩展为分级自治模型,将权限区分为功

系统建设和集成问题。这个课题本身是较复杂的,因为后方油库信息化涉及到的信息系统较多,已有的系统和数据是宝贵信息资源,不可能全部推倒重建,因此,运用合适的系统集成方法和技术,最大限度对已有异构系统进行集成,成为当前系统集成的有效途径和重要手段。文中阐述的系统集成思路和方法已在部分后方油库中实施,取得了巨大的军事经济效益,对其他后方油库信息系统建设和集成具有很高的参考价值。

参考文献:

- [1] 秦瑞胜,霍文武,唐 锐. 对后方油库信息化建设的几点思考[J]. 后勤学院学报,2013,126(1):62-63.
- [2] 杨晓婕,崔相谦. 海军油库信息化建设问题思考[J]. 海军后勤学报,2012(3):35-36.
- [3] 张利敏. 后方油库信息化建设对策探讨[J]. 仓储管理与技术,2012(6):19-20.
- [4] 王晓娟,罗正军,邱广华. 省域道路运输管理系统集成应用研究[J]. 计算机技术与发展,2013,23(5):163-166.
- [5] 沈安慰,郭基联,王卓健. 基于 B/S 结构的航空维修保障训练系统[J]. 计算机应用与软件,2013,30(2):253-255.
- [6] 吕 雪,凌 捷. 基于 J2EE 架构的信息安全应急预案管理系统研究与实现[J]. 计算机工程与设计,2013,34(4):

1197-1201.

- [7] 韩 光,杨晋生,崔 博. 基于 PDA 的大坝混凝土施工信息数据采集系统的设计与实现[J]. 计算机应用与软件,2013,30(7):62-65.
- [8] Dennis A, Wixom B H, Roth R M. System analysis & design [M]. 3rd ed. [s.l.]: John Wiley & Sons Inc, 2006.
- [9] Sahay B S, Ranjan J. Real time business intelligence in supply chain analytics [J]. Information Management and Computer Security, 2008, 16(1):28-48.
- [10] 王 超,倪志伟,刘 晓,等. 基于构件式 workflow 框架的电力 GIS 系统集成研究[J]. 计算机技术与发展,2008,18(6):206-209.
- [11] 刘晓娇,詹永照. 基于 J2EE 的异地社会保障信息系统框架模型[J]. 计算机技术与发展,2013,23(7):194-197.
- [12] Moore W, Allen O, Bracht R, et al. Managing information access to an enterprise information system using J2EE and services oriented architecture [M]. USA: International Business Machines Corporation, 2005.
- [13] Li Kangtong, Miao Fang. Study on e-commerce system architecture based on MVC model and J2EE platform[J]. Journal of Communication and Computer, 2008, 5(2):46-50.
- [14] 程建军. 基于 Ajax 技术的研究生教育管理系统设计与实现[J]. 计算机技术与发展,2008,18(12):207-209.

(上接第 215 页)

能权限和数据权限,形成了改进 RBAC 模型,并将其与视频平台很好集成。通过实践证明,该权限模型能实现数据的细粒度控制及权限的分级自治,提高权限管理的有效性效率。目前,该模型未涉及权限的转授及一个 USER 属于多个 GROUP 等情形,尚需进一步的研究。

参考文献:

- [1] Ferraiolo D F, Kuhn D R. Role-based access controls [C]// Proc of 15th NIST-NCSC. [s.l.]: [s.n.], 1992:554-563.
- [2] Sandhu R S. Role-based access control models [J]. IEEE Computer, 1996, 29(2):38-47.
- [3] International Committee for Information Technology Standards (INCITS). Information technology - role based access control [S]. 2004.
- [4] Ferraiolo D F, Sandhu R S, Gavrila S I, et al. Proposed NIST standard for role-based access control [J]. ACM Transactions on Information and System Security, 2001, 4(3):224-274.
- [5] Ferraiolo D F, Kuhn R. Role-based access controls [M]. 2nd ed. United States: Artech House, 2007.
- [6] 翟征德,冯登国,徐 震. 细粒度的基于信任度的可控委托授权模型[J]. 软件学报,2007,18(8):2002-2015.

- [7] 吴江栋,李伟华,安喜锋. 基于 RBAC 的细粒度访问控制方法[J]. 计算机工程,2008,34(20):52-54.
- [8] 李细雨,韩建民,于 娟,等. 基于粒逻辑的扩展 RBAC 模型[J]. 浙江师范大学学报:自然科学版,2009,32(3):303-307.
- [9] 龙 军,曾小仁,张祖平. 基于自治域的 RBAC 访问控制模型[J]. 山东大学学报:工学版,2010,44(3):137-142.
- [10] 姚寒冰,胡和平,李瑞轩. 上下文感知的动态访问控制[J]. 计算机工程与科学,2007,29(5):1-3.
- [11] 张沙沙,姜 华,谢圣献,等. 基于上下文感知的 RBAC 动态访问控制研究[J]. 计算机安全,2009(8):5-8.
- [12] 姚全营,姚淑珍,黄 河,等. 基于上下文感知和用户组的访问控制模型[J]. 北京航空航天大学学报,2011,37(7):901-906.
- [13] 李听听,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.
- [14] 许 洁,葛家宏,牛光辉,等. 一种 RBAC 的改进方案在文件共享系统中的实现[J]. 计算机技术与发展,2013,23(9):123-127.
- [15] 王德鑫,张茂军,王 炜,等. 基于 X-RBAC 模型的访问控制方法研究与实践[J]. 计算机工程与科学,2008,30(6):22-25.