DOI:10.16208/j.issn1000-7024.2009.01.054

• 信息安全 •

信息系统访问控制的层次模型

吴开超[1,2]， 沈志宏[1]， 周园春[1]， 阎保平[1]

(1. 中国科学院 计算机网络信息中心，北京 100190；2. 中国科学院研究生院，北京 100049)

摘 要：信息系统访问控制用以在不同层次上要保护不同类型的客体对象。按照客体类型及其层次关系将访问控制逻辑分层处理，在不同层次上采取与客体特点相符的访问控制技术，从而形成一种访问控制的层次模型。在功能模块级采取基于角色的访问控制，而在数据对象级采用基于规则的实现方式。分层结构将复杂的访问控制分解为若干个在不同层次上易于处理的问题，降低了问题复杂性，并使得各层之间互相独立，灵活性好，易于实现、维护和扩展。

关键词：访问控制；层次模型；RBAC；信息系统；细粒度访问控制

中图法分类号：TP393.08 **文献标识码**：A **文章编号**：1000-7024 (2009) 01-0022-03

Hierarchy model of access control in information system

WU Kai-chao[1,2], SHEN Zhi-hong[1], ZHOU Yuan-chun[1], YAN Bao-ping[1]

(1. Computer Network Information Center, Chinese Academy of Sciences, Beijing 100190, China;
2. Graduate University, Chinese Academy of Sciences, Beijing 100049, China)

Abstract: Access control of information system can protect various objects at different levels. The logic of access control is hierarchically implemented based on the object types and their relationships, different access control techniques are applied at different levels. Role-based access control is applied at module-level, and rule-based implementation is used at object-level. The hierarchical architecture can decompose the complex access control into various easy-to-solve small pieces. Thus it decreases the complexity, and makes different layers be independent with each other, and it also brings great flexibility and simplicity to implement, maintain and scale.

Key words: access control; hierarchy model; RBAC; information system; fine-grained access control

0 引 言

由于互联网所具有的开放性及共享性，使得信息系统的安全问题日益受到重视。而访问控制技术是信息系统安全防范和保护的主要技术，在保证合法用户访问合理资源的前提下，限制非授权用户访问系统资源以及合法用户对系统资源的非法使用。因此访问控制是保证信息系统安全最重要的核心策略之一[1]。根据访问控制策略类型的差异，早期的安全策略模型大致可以分为自主访问控制(discretionary access control，DAC)和强制访问控制(mandatory access control，MAC)两大类[2]。自主访问控制策略是一种通用访问控制策略，该策略决定用户能否访问客体对象的依据是在系统中是否存在明确的授权。每个对象都有且仅以一个属主，对象属主有权制定该对象的保护策略，有选择地与其他用户共享。强制访问控制将所有的权限都归于系统集中管理，而不是让普通用户进行访问授权的管理，保证信息的流动始终处于系统的控制之下。强制访问控制主要使用于军队、政府机要部门等安全保护需求比较严格的环境[2]。

20 世纪 90 年代初期，访问控制领域中传统的自主访问控制和强制访问控制的划分受到挑战，研究者提出了若干策略中立型的策略和模型，其中最有影响力的是基于角色的访问控制模型(role-based access control，RBAC)[3-5]。在 RBAC 模型中，用户对客体的访问权限取决于用户在组织中的角色，拥有某个角色的用户自动拥有该角色所具有的权限。RBAC 模型因其出色的管理特性和多策略支持能力得到了极大的关注，当前大量访问控制的研究工作也都是在 RBAC 的基础上进行的。20 世纪 90 年代中后期，多安全策略支持的研究取得了很大进展，在信息系统中单一的访问控制策略模型已经无法满足多样化的安全需求。信息系统的安全涉及到不同层次上的访问客体对象，包括系统、系统模块、数据对象、存储对象等，按照客体对象的层次关系建立信息系统访问控制的层次模型，针对不同客体对象的不同特点，采取不同的访问控制策略，这样可以更好地满足各类安全需求，尤其在数据的细粒度访问控制需求方面[6-8]。

1 访问控制层次模型

用户访问信息系统的过程实际上就是主体(用户)访问客

收稿日期：2008-01-10 E-mail：wkc@sdb.cnic.cn

基金项目：国家 863 高技术研究发展计划基金项目(2004AA104240)；中国科学院信息化建设专项基金项目(INF105-SDB)。

作者简介：吴开超(1970－)，男，江苏建湖人，博士研究生，高级工程师，研究方向为信息安全、科学数据集成； 沈志宏(1977－)，男，安徽东至人，硕士，高级工程师，研究方向为信息安全、科学数据管理； 周园春(1975－)，男，江西余江人，博士，助理研究员，研究方向为数据挖掘、信息安全； 阎保平(1950－)，女，山东青岛人，博士后，研究员，博士生导师，研究方向为大规模科学数据共享。

体(信息系统中的数据)的过程，而访问控制是对用户访问数据的过程所施加的限制性控制。信息系统可分为若干个功能模块，在每个功能模块中都会访问到不同类型的数据资源，数据资源在应用层以应用对象的形式存在，每个数据对象在具体实现时可能以某种形式存储在关系数据库或其它系统中。图1是信息系统结构示意图，描述了信息系统中不同层次客体对象之间的基本关系。

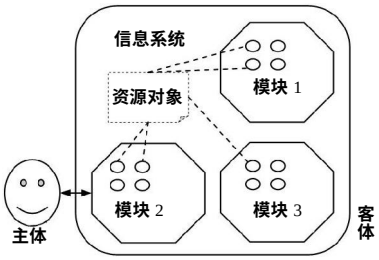

图 1 信息系统结构

从数据访问的过程来分析，用户访问信息系统的过程可以看成是用户主体通过信息系统、相关功能模块来访问系统中数据资源的过程。整个访问过程中主要涉及用户主体以及信息系统、功能模块、数据对象、存储对象等客体对象，用户访问操作中所涉及的5类对象之间形成串行的信息传递路径，如图2左侧所示。

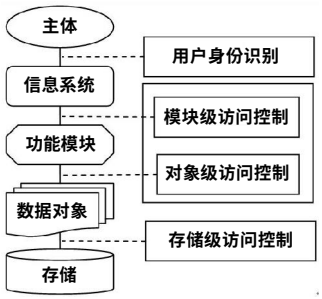

图 2 访问控制层次模型

信息系统访问控制就是要在信息传递路径中加上限制性的控制条件，以限制对资源的访问。在信息访问的传输路径上设置访问控制点，按照客体类型分层，形成如图2右侧的分层访问控制。

采用分层结构主要有以下优点：

(1)各层之间互相独立，整个访问控制的效果是各层的组合；

(2)按照客体对象的粒度从粗到细，各层之间具有严格的先后次序，从而达到对访问过程的逐级保护；

(3)具有较好的灵活性和适应性，各层结构上分离，可采用各自最合适的技术来实现；

(4)易于实现和维护，能促使访问控制逻辑的规范化。

按照客体类型不同，图2所示信息系统访问控制可分为如下4层：

(1)用户身份识别：是一种施加在用户主体与系统接口上的访问控制形式，其含义是无论针对何种资源做何种操作，首先要识别用户身份，以确认主体是受控的，只有通过认证的用户才能使用系统功能。从访问控制的角度来说，用户认证可以看成是一种最粗粒度的访问控制形式。用户身份识别可以有多种不同方式，可以基于用户名/密码，也可以基于数字证书或基于生物特征识别等。

(2)模块级访问控制：是施加在功能模块接口上的访问控制，只有获得模块授权的主体才能够访问该应用系统模块，这种访问控制形式称为模块级访问控制(也叫功能级访问控制或应用级访问控制)。从权限管理的角度来说，主体获得的权限是模块级权限(也叫操作权限或功能权限)。

(3)对象级访问控制：是直接施加在特定数据资源对象实例上的访问控制，主体访问资源对象时需要取得对应对象的授权，这种访问控制形式是对象级访问控制。应用对象是应用逻辑中的数据对象，比如文档管理系统中的文档，网站内容管理系统中的网站栏目、新闻，在线商店中的目录、商品等。从权限管理的角度来说，对象级访问控制所对应的权限也称为资源权限(也叫数据权限)。

(4)存储级访问控制：是由负责资源存储的数据库管理系统来实施的访问控制，也称为存储级访问控制。针对最常见的关系数据库存储来说，存储对象包括数据库、数据表、数据字段等，应用对象最终需要映射为存储形式，在关系数据库中，存储级访问控制通过关系数据库管理系统自身的访问控制机制来实现。

上述4种访问控制形式中，用户身份识别属于传统的用户认证范畴，主要是确认用户身份，通常由单独的用户认证系统来实现；而存储级访问控制主要由数据管理系统来实施，与应用系统模块相对独立，而且存储级访问控制通常只能实现部分访问控制逻辑，对访问控制逻辑的支持受限。从访问控制的角度来说，信息系统访问控制主要考虑模块级访问控制以及对象级访问控制。

2 模块级访问控制

模块级访问控制是施加在信息系统功能模块上的访问控制，是一种粗粒度访问控制形式，其对应的访问客体是系统的功能模块，其访问控制过程对应于用户主体访问系统功能模块的限制性操作。功能模块在不同类型系统中有不同的表示形式，一般应用系统中可能是子系统，在客户端应用中可能表现为系统菜单项，在Web应用系统中则可能对应于子目录等。

通常情况下，信息系统在建设完成后，其所包含的功能模块以及每个功能模块所对应的访问权限也就已经确定。模块级访问控制的访问客体在系统交付后就不会发生变化，相对应的功能级权限也已确定，因此，可以通过权限组合的方式在功能权限的基础上定义角色，通过角色来简化系统的权限管理，这种情况下采用RBAC实现模块级访问控制最为合适。

基于角色的访问控制RBAC最早由Ferraiolo、Kuhn等最早比较系统地提出[5]，基本思想是通过角色将主体和客体在逻辑上加以分离，访问控制被分成两个部分，即用户与角色的关联、角色与访问权限的关联，使访问控制更加灵活，便于管理。Ferraiolo和Sandhu等对RBAC模型进行了形式化定义，形成了比较完善的RBAC模型框架。目前，美国国家标准与技术学会(NIST)制定的RBAC模型标准已被采纳为美国国家标准ANSI INCITS 359-2004。RBAC核心模型包含5个基本的静态集合：用户集(users)、角色集(roles)、客体集(objects)、操作集(ope-

rators)、和权限集(perms),以及运行过程中动态维护的集合—会话集(sessions),这些集合称为 RBAC 组件,如图 3 所示。

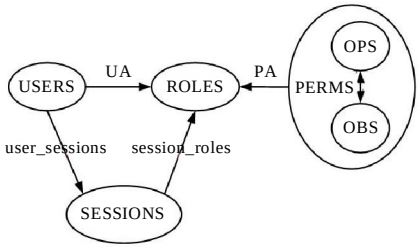

图 3 RBAC 核心模型

角色是RBAC模型的中心,它是用户与权限的桥梁,从图中可以看出,通过用户分配(UA)和权限分配(PA)使得用户去权限关联起来。其中:

(1) 用户分配(UA):UA⊆USERS× ROLES。UA 是一个多对多的关系,记录了系统为用户所分配的角色,或称用户所拥有的角色。如果把用户 u 分配给角色 r,则 UA = UA∪(u, r)。

(2) 权限分配(PA):PA⊆PERMS× ROLES。PA 是一个多对多的关系,记录了系统为角色所分配的权限。如果把权限 p 分配给角色 r,则 PA = PA∪(p, r)。

在信息系统部署后,功能模块及相关权限关系就已经确定,若采取 RBAC 的访问控制形式,则可以功能模块为基础,通过权限分配关系 PA 定义相应的功能角色 ROLES。这样,权限授予过程中只需要通过用户分配UA建立角色集ROLES与用户集 USERS 之间的关联,通常情况下角色的数量远小于权限的数量,因此,对于模块级访问控制,采用基于角色的授权能够简化管理,并且更加灵活。

3 对象级访问控制

对象级访问控制是在应用程序的数据对象上所施加的访问控制机制,是一种所谓的细粒度访问控制形式,其访问控制过程对应于用户(主体)访问数据对象(客体)的限制性操作。对象级访问控制通常与系统应用逻辑的联系非常紧密,目前大多是通过直接嵌入到应用逻辑中加以实现。

与模块级访问控制不同,数据层上数据对象通常是在系统交付运行后才逐步建立的,在系统运行过程中数据对象的数量以及每个数据对象的属性都可能发生变化,具有较高的动态性;数据层安全需求相对更加复杂,数据对象的访问控制需要建立在对数据对象的全面理解的基础上,从关系模型角度来看,有所谓的行级控制 (row-level) 和列级控制 (column-level),并且数据对象数量很多,不可能将每个数据对象作为独立客体来描述。

总的来说,对象级访问控制过程具有以下特点:①数据对象在系统运行过程中动态产生,并且会不断地变化;②系统中数据对象数量通常比功能模块数量多得多;③数据对象访问控制的要求比较精细,一般可通过主客体的属性关系来描述。以上特点决定了数据对象的访问控制不适于采用类似于 RBAC 的聚合模型来实现,只能考虑采取间接的方式来实现。规则引擎是一种由推理引擎发展而来、嵌入在系统中的组件,可实现将访问控制决策从系统代码中分离出来,并使用预定义的语义描述来编写访问授权的决策。规则引擎接受访问控制请求的输入,并解释访问控制规则,并根据规则做出访问控制的决策。规则引擎通过定义规则来描述主客体安全属性的之间的关系,并可通过规则组合描述更复杂的逻辑关系。

规则引擎可以通过(S,O,R)组成的三元组来描述,其中S是由主体类组成的集合,O是由客体类(数据对象类)组成的集合,R 是规则组成的集合。规则集中每条规则由二元组组成<rexp, action>,rexp 是规则表达式,描述该条规则的主客体属性之间的关系,rexp=expr(Si,Oi),Si 是主体类的安全属性,Oi 是客体类的安全属性,rexp 还可以通过 NOT、AND、OR 进行扩展;action 为动作集,表示匹配该规则后主体能对客体执行的授权操作。

比如,在网站内容管理系统中,需要实现以下访问控制策略:网站编辑能修改/删除自己创建的文章;网站主编可以审核发布下属所编辑的、尚未发布的文章。则可以定义如下规则引擎:

S={普通用户类 User,系统进程类 Process,…}

O={网站 Site,栏目 Channel,文章 Thread,…}

R={<(Thread.作者=User.uid),[删除,修改]>,<(Thread.作者.主编=User.uid) AND (Thread.status<> '已发布'),[审核]>,…}

可以看出,访问控制规则引擎能够较好地分离出业务逻辑和访问控制逻辑,并且能灵活地适应技术需求的变化,能在运行时动态地管理和修改从而提供软件系统的柔性和适应性。另外访问控制规则能够灵活地描述系统的需求,是一种适应数据对象访问控制的解决方案。

4 模型应用

基于以上信息系统访问控制的层次模型,开发了原型系统,在信息系统功能模块、应用对象层面上实现访问控制。原型系统基于Java技术实现。图 4 是科学数据库系统平台软件结构图。

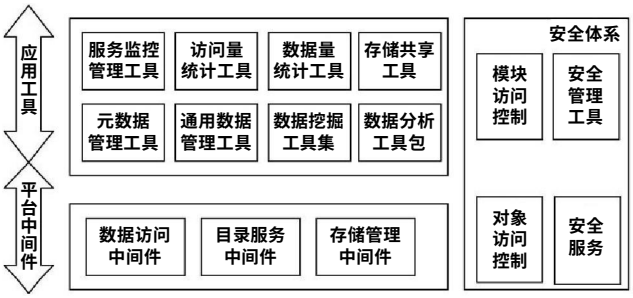

图 4 科学数据库系统平台软件结构

目前,上述原型系统已集成到作为科学数据库平台安全体系中,并在中国科学院科学数据库服务系统中部分站点上得以部署,对于限制合法用户非法使用科学数据,尤其是在防止恶意下载上取得了较好的应用效果。

5 结束语

信息系统的访问控制是应用逻辑的重要组成部分。访问控制机制,尤其是细粒度访问控制大多是通过嵌入到应用逻辑中实现的。本文通过对信息系统资源访问过程的分析,按照访问客体类型及其层次关系提出了访问控制的层次模型,

(下转第 50 页)

4 算法分析

从算法的实现可看出,与传统算法相比,该算法的优点为:

(1) 每个节点只利用自己的连接权值信息,不用知道其它所有节点的所有连接状况;

(2)每个节点独立运行分簇算法,这一过程不用同步,极大地加快了算法收敛速度;

(3) 采用局部到整体的分布式算法,构建过程中的各种信息通告依靠局部最小代价生成树传递,进行了有效的数据融合,减少每个节点的连通信息在整个网络中传播;

(4) 这种分簇机制,有效利用了多层分族有利于网络的稳定、最小代价生成树有利于基于内容的数据融合[2]的特点。可以作为基于内容的网络架构基础,构建以数据为中心的多汇聚节点的无线传感网络。

(5)分簇完成后,簇成员节点不用维护路由信息,只用选择最小权值边节点作为自己的下一跳节点即可。分簇算法已得到一个以最上一层簇首为根节点的 MST,发布的数据沿着此方向进行传递,并按照数据类型选择融合算法[3]。以此 MST 为基础,由各层簇首节点来负责为每个汇聚节点保存一个以汇聚节点为根节点的数据传播路径,订阅[2]的数据以此路径方向传递。

该算法的不足在于:不满足前提假设的网络(如节点不稳定的网络),需按照情况对算法作进一步的修正。

5 结束语

本文采用一种新的方法来实现多层分簇,该算法利用 MST 的性质,从局部到整体,一层一层地构造一个基于 MST 的多层分簇网络来。该算法让每个节点独立运行分簇算法,不用同步,极大的加快了分簇的收敛速度,在分簇过程中,利用局部 MST 来传递权值信息,实现数据的融合,减少节点洪泛权值信息的资源消耗。这一分簇网络,将有利用以数据为中心的网络的数据融合,易于数据的订阅与发布。与以前的多层分簇网络不同的是,本文的方法在网络分簇前,节点不用洪泛权值信息,分簇不用同步,实验表明有较快的收敛速度。

参考文献:

[1] Holger Karl, Andreas Willig. Protocols and Architectures for wireless sensor networks[M].邱天爽,译.北京:电子工业出版社, 2007:289.

[2] Carzaniga A,Wolf A L.Content-based Networding: A new communication infrastructure[C]. Scottsdale,AZ: Proceedings of the NSF Workshop on an Infrastructrue for Mobile and Wireless Systems,2001.

[3] Th Eugster P,Felber P A,Guerraoui R, et al.The many faces of publish/subscribe[J].ACM Computing Surveys(CSUR), 2003, 35(2):114-113.

[4] 孙利民,李建中,陈渝,等.无线传感器网络[M].北京:清华大学出版社,2005.

[5] Gupta G,Younis M.Fault-tolerant clustering of wireless sensor networks[J]. Wireless Communications and Networking,2003,3: 1579-1584.

[6] 崔莉,鞠海玲,苗勇,等.无线传感器网络研究进展[J].计算机研究与发展,2005,42(1):163-174.

[7] Karp B,Kung H.GPSR: Greedy perimeter stateless routing for wireless networks[C]. Proc of the 6th Annual Int'l Conf on Mobile Computing and Networking. Boston: ACM Press, 2000: 243-254.

[8] 唐勇,周明天,张欣.无线传感器网络路由协议研究进展[J].软件学报,2006,17(3):410-421.

[9] Niculescu D,Nath B.Trajectory based forwarding and its applications[C]. Proc of the 9th Annual Int'l Conf on Mobile Computing and Networking. San Diego: ACM Press,2003:260-272.

(上接第 24 页)

并对模块级访问控制、对象级访问控制进行了较为深入的分析。层次模型使得各层之间是互相独立,具有较好的灵活性,并易于实现和维护,能更好地满足系统的安全需求。

参考文献:

[1] 张敏,徐震,冯登国.数据库安全[M].北京:科学出版社,2005.

[2] DoD 5200.28-STD, National computer security center department defense trusted computer system evaluation criteria[S].

[3] David F Ferraiolo, Richard Kuhn D, Ramaswamy Chandramouli. Role-based access control [M].2nd ed. Artech House Inc, 2007.

[4] Elisa Bertino, Ravi Sandhu. Database security-concepts, approaches, and challenges[J]. IEEE Trans Dependable Secure Comput, 2005,2(1):2-19.

[5] ANSI INCITS 359-2004, American national standard for information technology-role based access control[S].

[6] Barkley J F, Cincotta A V. Implementation of role/group permission association using object access type[P]. U. S. Patent 6,202,066, 2002.

[7] Boebert W,Kain R.A practical alternative to hierarchical integrity policies[C]. Proceedings of the 8th National Computer Security Conference, 1985.

[8] 周功业,易佳,陈进才.基于角色访问控制的对象存储安全认证机制[J].计算机工程与设计,2008,28(24):5847-5849.