·安全技术·　　文章编号：1000-3428(2015)01-0135-04　　文献标识码：A　　中图分类号：TP311

基于角色的多级安全数据库模型

徐沛娟，郑　晶，徐茂敬

（吉林大学计算机科学与技术学院，长春 130012）

摘　要：为提高数据库模型的安全性，同时满足用户对数据的合理化存储要求，对 RBAC 模型与 MLR 模型进行改进，构造一个结合 RBAC 模型与 MLR 模型的综合访问控制模型，使主体通过多级角色间接应用强制访问控制规则来访问客体。实验结果表明，该模型可实现系统中主体对客体的灵活管理，同时具备强制访问控制模型的高安全性。

关键词：数据库安全；多级数据库模型；RBAC 模型；MLR 模型；访问控制模型；操作权限

中文引用格式：徐沛娟，郑　晶，徐茂敬. 基于角色的多级安全数据库模型[J]. 计算机工程，2015，41(1)：135-138.

英文引用格式：Xu Peijuan，Zheng Jing，Xu Maojing. Multi-level Security Database Model Based on Roles[J]. Computer Engineering，2015，41(1)：135-138.

Multi-level Security Database Model Based on Roles

XU Peijuan，ZHENG Jing，XU Maojing

（College of Computer Science and Technology，Jilin University，Changchun 130012，China）

【Abstract】 Lots of multi-level database models with individual advantage have appeared following the development of multi-level database security. People gradually begin to improve optimization of multilevel relation database model，put forward more secure，more manageable database multilevel security model，in order to meet the users' rationalization of data storage and keep the security of data. This paper proposes the idea that combined the RBAC access control model with the MAC mandatory access control model. It makes the system not only have the high security of the mandatory access control model and achieve the flexible management from the subject to object，improves the RBAC model and the MLR model of the MAC mandatory access control model，and combines them to construct an integrated access control model. Combined with the superiority of the two access model，the access control model achieves the subject applies the mandatory access control rules to access object by multilevel roles indirectly. By simulated data，the structure of security access control model based on role of multilevel relation is tested. The experiment proves that the comprehensive access control model has better flexibility，makes the model with the high security of mandatory access control model.

【Key words】 database security；multi-level database model；RBAC model；MLR model；access control model；operation permission

DOI：10.3969/j.issn.1000-3428.2015.01.025

1　概述

由于信息量的激增，计算机逐步被应用到人们的生活中，大量的信息被存储在数据库中。为了确保数据的安全，数据库安全技术逐步被发展起来。确保数据库的安全，不仅要处理好外界因素对数据库造成的破坏，还要处理好数据库内部的访问控制。因此，强制访问控制模型、自主访问控制模型及基于角色的访问控制模型[1]等逐渐被提出。后者的提出弥补了自主访问控制模型与强制访问控制模型[2]在处理主体对客体管理上的不足，但其自身却不具备高安全性。本文通过对强制访问控制模型的研究，了解到强制访问控制模型由于是一种基于格的访问控制模型，主体与客体都附加一个安全等级，系统通过检查主体和客体的相应安全等级来决定一个主体是否可以访问某个客体资源，用户或用户的程序不能加以修改。强制安全访问控制可以避免和防止大多数数据库有意或无意的侵害，

基金项目：吉林省科技发展计划基金资助项目(20090704)。

作者简介：徐沛娟(1959－)，女，副教授、硕士，主研方向：信息安全，数据库技术，数据挖掘；郑　晶、徐茂敬，硕士。

收稿日期：2014-01-16　　**修回日期：**2014-03-07　**E-mail：**xupj@jlu.edu.cn

因此,在数据库管理系统中有很大的应用价值。主体与客体之间的操作主要为读写操作。这种操作在现实管理系统中存在着局限性,为此,本文对RBAC 模型与 MLR 模型进行改进,构造一个结合了 RBAC 模型[3]与 MLR 模型的访问控制模型,以实现主体对客体的灵活管理,同时具备强制访问控制模型的高安全性。

2 RBAC 模型的改进

2.1 RBAC 模型

RBAC 模型[4]即基于角色的访问控制模型。RBAC 模型具有的特点是:主体与客体之间是通过角色进行联系的。在 RBAC 模型中是通过把访问权限赋予给角色[5],管理员再为不同的用户分配角色,用户通过角色获得相应的访问权限。角色作为了访问权限的载体,用户访问数据需要获得相应的角色。一个角色可以被多个用户共享,而一个用户也可以通过获得多个角色来获得多个访问数据库的权限[6]。这种访问关系如图 1 所示。

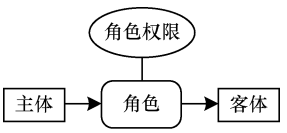

图 1 角色在主体与客体间的关系

2.2 改进的 RBAC 模型

从图 1 中可以看出,在 RBAC 模型中角色是主体与客体之间相互联系的桥梁。本文设计综合模型的目的是用 RBAC 模型实现强制访问控制,但是在用 RBAC 模型实现强制访问控制时,用户只能通过角色来获得相应的安全等级与操作权限。实际上具有相同的操作权限用户具有的安全等级不一定相同,这样用户对数据库的操作就产生了局限性。

为了解决这种局限性,使用户既能具备同样的操作权限却可以持有不同的安全等级,相同的安全等级上的用户也可以具备不同的操作权限。本文通过应用内部角色[7]与多级角色来实现对 RBAC 模型的改进。内部角色是由某一安全等级下的操作权限构成。这些操作权限主要有查询权限、插入权限、删除权限、更新权限等。而这些权限主要是由一些 SQL 语句组成。多级角色是名称与内部角色集合的组成。内部角色与多级角色是一对多的关系,即特定安全等级下的内部角色有且只有一个。但是这个内部角色可以赋给多个多级角色。这样就把主体与客体之间的角色拆分成两部分即内部角色与多级角色,来实现模型的改进。

3 MLR 模型的改进

3.1 MLR 模型

MLR 模型不仅提出了数据借用完整性[8]与 UPLEVEL 语句,而且同时对多实例完整性与引用完整性语句进行了修改。相比于其他关系模型,其为多级关系提供的安全标签是元素级的。

MLR 模型的定义[9]如下:

定义 1 一个多级关系表示为 $R(A1,C1,\cdots,Ai,Ci,\cdots,An,Cn,TC)$。其中,$Ci$ 表示的为对应的属性 Ai 的安全等级;TC 表示的为对应的元组的安全级别。

定义 2 一个多级关系实例是一些形如 $(a1,c1,\cdots,an,cn,tc)$ 的不相同的元组的集合,其中,ci 不可以为空,i 是 1 ~ n 之间的某个值,其被表示为 $r(A1,C1,\cdots,Ai,Ci,\cdots,An,Cn,TC)$,$TC$ 是该元组中属性安全等级的最小上界[10]。

定义 3 多级关系集合组成一个多级数据库,在同一时刻所有关系实例的集合,表示的为一个数据库的状态[11]。

MLR 模型的数据解释如下:

(1)主体只可以接受或者可见低于或者等于其本身安全级别的数据。

(2)任一等级主体所接受的数据是由其本身的数据与通过 uplevel 借用来的数据组成的,借用的数据会随着原有的主体变化而变。

下面通过一个 MLR 模型的例子,理解下面元组的含义,如表 1 所示。

表 1 学生成绩表 1

StudentName	TestScore	Attendence	*TC*
Tom U	80 S	20 U	TS
Tom U	80 S	18 S	S
Tom U	70 U	20 U	U

从表 1 中可以看出,表中有 3 种安全等级分别为 U,S,TS 的 3 种不同的主体的不同观点。S 级主体可能认为其相较于 U 级主体更可信。但是 TS 级主体的 attendance 的数据值是从 U 级主体借用的。表明 TS 级主体更相信 U 级主体。TS 级主体和 S 级主体都相信 Tom 的 U 级主体存在,说明 3 种主体讨论的为同一人。TS 级主体在数据属性上既可以选择相信 U 级主体也可以选择相信 S 级主体。通常含有相同主键值 $A1$ 与相同主键安全级 $C1$ 的多实例元组在现实生活中可能指代的是同一实体。

3.2 改进的 MLR 模型

本文通过一个例子来说明 MLR 模型的缺点,并围绕这个缺点对 MLR 模型进行改进,如表 2 所示。

表 2　学生成绩表 2

StudentName	TestScore	Attendence	*TC*
Tom S	80 S	20 S	S
Tom U	75 U	Null S	TS
Tom U	75 U	18 U	U

从表 2 中可以看出,存在(Tom S)和(Tom U)2 种实体,这 2 个实体分别是由 S 级与 U 级用户创建。*TC* 值为 TS 的数据值是由 TS 用户创建的。从 MLR 的数据解释(1)来看,U 级用户只能看到自己等级的数据,而 TS 级用户则可以看到 U 级,S 级以及 TS 级的数据。TS 级用户的 TestScore 数据值则是从 U 级用户借用而来的,所以当 U 级用户想要删除或者更新其数据时,TS 级用户的数据也会同时被删除与更新,这就是 MLR 模型的其中一个缺点。而对于 TS 级的 attendance 数据值,TS 用户想要从 S 级主体借用,但是 S 级主体对于(Tom U)并没有自己的数据,致使 TS 级用户的 attendance 值为 Null。这就表明S 级主体不接受(Tom U)这个主体,现实中这是非常不合理的,此即为 MLR 模型的第 2 个缺点与不足。

本文总结 MLR 模型上述 2 个缺点如下:

(1)高等级用户借用的低等级用户的数据会伴随着低等级用户的删除更新等操作传递给高等级用户[12]。

(2)如果低等级元组没有自己的数据。当高等级从低等级借用数据时,高等级借用不到相应的数据而使其数据值置空。

本文针对上述 2 个缺点,对 MLR 模型进行改进。首先,提出将元组中的属性设置成主键属性与非主键属性,然后对这两类属性进行分开对待的思想。元组中主键属性的存在与非主键属性的存在所表示的意义是不同的。元组中的主键属性说明的是这个元组描述的实体是客观存在的,元组改变实体并不会随着进行改变。而非主键属性表示的是这条元组描述的实体的特征。当高等级用户与低等级用户之间存在通过 Uplevel 借用来的数据时,主键属性上的数据借用,高等级元组借用的数据保持原状,不会随着低等级用户对元组的操作而改变;非主键上数据的借用,则会相应发生变化。

如果高等级用户向低等级用户借用数据,无论低等级元组在该属性上是否有自己的数据值,高等级元组都会把低等级元组在该属性值上的数据作为自己要借用的数据,这就解决了 MLR 模型的第 2 个缺点。问题解决的原因在于高等级用户对低等级用户的信任。

4　综合访问控制模型的构建

结合改进之后的 MLR 模型与 RBAC 模型,本文构造一个既具备 MLR 模型的高安全性又具备 RBAC 模型的高灵活性的综合访问控制模型。

在新形成的访问控制模型中,不仅改进了 MLR 模型的漏洞,引进的基于角色的机制,使数据库安全的管理更加简化便捷。通过内部角色与多级角色的使用,使系统在进行增添,删除等处理数据的操作得以简化。基于角色的多级关系安全访问控制模型的构造,使访问控制模型的应用得以提高。这个综合访问控制模型的构造如图 2 所示。

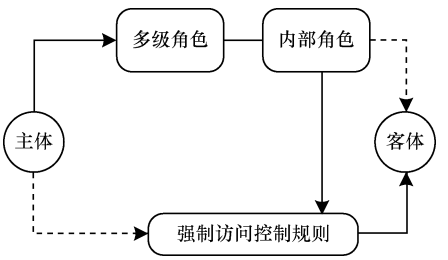

图 2　多级安全访问控制模型架构

首先,主体要根据其用户的名称被赋予相应的多级角色名称。多级角色又是内部角色的集合。内部角色又可以细化为某个客体表的一种 SQL 语言的操作,例如查询,插入,删除等操作。所以主体获得多级角色之后,再根据这个多级角色的名称获得相应的内部角色。一旦获得相应的内部角色,内部角色为其分配其具有的相应的操作权限。这样主体就通过多级角色,内部角色获得访问数据库中数据的权限。但是一旦获得内部角色的相应权限之后,用户对客体表中的任何操作都要遵循改进的 MLR 强制访问控制模型的访问规则。只有符合 MLR 访问控制系统的访问控制规则才可以对客体表中的数据进行操作。如果不符合,系统将会拒绝其对客体进行操作。由图可以看出与传统的强制访问控制模型相比,在获得权限方面没有传统的直接。在强制访问控制方面是通过多级角色与内部角色进行控制的。但是此综合模型更加的容易管理。

5　模型的实现与测试

该访问控制模型的实现类似于把其看成一个子系统嵌入在用户与数据库之间。可以把这个子系统看成是一个可信过滤器。用户向这个子系统提供信息请求。符合访问控制系统条件的用户,可以对数据库进行访问。不符合条件的用户被过滤掉,不能访问数据库,从而保障数据库的安全。这样即可实现基于角色的多级安全强制访问控制系统。系统的整体架构如图 3 所示。

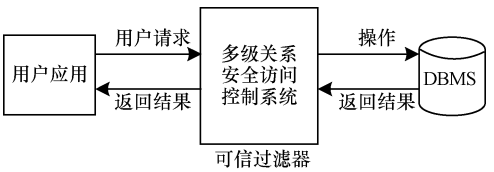

图 3 多级关系安全访问控制系统架构

本文以公司中的职工福利来模拟多组数据。下面在 MyEclipse 平台下,使用 Java 连接 Mysql 数据库进行编译测试。在数据库中要创建的数据主要有职工名字、职工的职务,与之关联的数据表等信息。而本文进行强制访问控制的客体表,即是所创建的数据表。

首先要创建一个客体表,本文以职工的薪酬为例,创建员工工资表,其次创建的是访问测试表。由于多级角色是内部角色的集合,因此在构造测试表时,要先构造内部角色。其次把创建好的客体表分配给内部角色,然后把操作的安全等级以及对客体表的操作权限等信息也进行分配。之后创建出符合系统要求的多级角色,将内部角色合理的组合好分配给多级角色,最后通过多级角色来创建用户进行测试。表中的多级角色与内部角色分别用 MRole 与 NRole 表示,用户访问测试表与员工工资表如表 3 和表 4 所示。

表 3 用户访问操作测试表

User	MRole	NRole	Object-table	operation	class
Dave	会计	Wage_select_0	wage	Select	U
		Wage_insert_0	wage	Insert	U
		Wage_delete_0	wage	Delete	U
Tom	工程师	Wage_select_1	wage	Select	S
		Wage_insert_1	wage	Insert	S
Bob	审计员	Wage_update_2	wage	Update	TS
		Wage_insert_2	wage	Insert	TS
		Wage_select_2	wage	Select	TS

表 4 员工工资表

职工名	年薪	福利	安全等级
王明 U	50 000.00 U	10 000.00 U	U
王明 U	60 000.00 S	10 000.00 U	S
王明 U	60 000.00 S	10 000.00 U	TS
李红 S	70 000.00 S	20 000.00 S	S
李红 S	85 000.00 S	20 000.00 S	TS
张丽 S	90 000.00 TS	30 000.00 TS	TS

可以看出,不同的用户的多级角色是不同的,不同的多级角色含有不同的内部角色,每个用户的访问权限都是不同的。例如,表 3 中的用户 Tom 想要对 Wage 表进行更新操作,但是其不具备这种操作权限,他的操作权限只有查询和插入,所以当其对客体表进行更新操作时,系统会拒绝他的操作。

在其他操作中,系统允许执行的 Dave 用户对 Wage 表的 insert 操作,因为用户 Dave 具有插入操作的权限。但是系统只会允许 Dave 插入的元组的安全级别都是公开的。例如,如果 Dave 执行插入语句那么在员工工资表中 Dave 插入的数据年薪与福利以及元组的属性都是公开的。可见,同样 Bob 与 Tom 也具备相同的插入权限。但是 Bob 与 Tom 执行这样的插入语句,系统允许插入的元组的安全等级为机密与秘密。从这些操作中可以看出,虽然这 3 个用户具备相同的操作类型,但是他们的安全等级不同,所以插入的元组也不同。这就符合了改进后 RBAC 模型的设计思想。

从表 3 中可以看出,低等级用户具有更新的操作权限,高等级从低等级借用数据,当低等级数据进行更新操作的时候,系统会对高等级用户的数据执行相应的操作。例如用户 Dave 执行更新语句把职工名称为王明的元组的福利属性值全部变为4 000.00,系统则会将等级为秘密和绝密的元组的福利的值相应的更新为4 000.00,因为秘密元组与绝密元组的福利值都是借用于等级为 U 的元组。但是如果 Dave 执行删除语句时,删除名字为王明的元组时,秘密元组与绝密元组不会因为公开元组的删除而消失,删除的只是公开元组的数据。这就是改进后的 MLR 模型想要达到的目的。消除了原有的 MLR 模型的漏洞,提高了其安全性。通过测试表明,对 MLR 模型的改进使访问控制的安全性得以提高,使数据不会丢失。用户所访问的数据更真实、准确。而改进后的 RBAC 模型使用户的权限管理更加的灵活,提高了对数据表的操作速度。综合的访问控制模型的构建结合了改进后两个模型的所有优点,此访问模型的构造使系统更完善、安全、灵活。

6 结束语

MLR 特有的数据借用思想使其能够联系高等级元组与低等级元组,因此,本文分别对 MLR 和 RBAC 模型进行改进,增添了内部角色与多级角色的概念,结合 2 种改进后的模型提出综合访问控制模型的概念,即基于角色的多级安全强制访问控制模型。测试结果表明,本文模型比原有的强制访问控制系统更灵活,操作更便捷。消除访问控制模型的隐蔽通道是下一步研究的重点。

(下转第 157 页)