一种模糊级别的多级安全关系数据模型研究*

王六平,鲁建恺,张伟林
(湖南师范大学,湖南 长沙 410081)

摘 要:基于多实例的思想提出了一种新的模糊级别的多级安全模型,将多个仅密级不同的元组合并表示,并用安全模式来表示元组所适用的密级,只要主体的许可级别匹配此安全模式,便可存取此元组。这种模型解决了现有多级安全数据模型中存在的数据冗余度大及隐通道等问题。

关键词:多级安全;多实例;数据模型;合并;安全模式

中图分类号:TP311 **文献标识码**:A **文章编号**:1674-7720(2010)17-0077-04

Study of a fuzzy multilevel security relational data model

WANG Liu Ping, LU Jian Kai, ZHANG Wei Lin
(Hunan Normal University, Changsha 410081, China)

Abstract: In this paper, a new fuzzy multilevel security data model based on polyinstantiation is put forward. By this model, some tuples with different security level are merged into a tuple with a security pattern which matches those tuples' security level, and the user can access the resource if only this resource's security pattern match the user's permits level. This model solves such problems as data redundancy and covert channel.

Key words: multilevel security; polyinstantiation; data model; merge; security pattern

现有的多级安全数据模型都遵循BLP模型[1]中提出的"向下读,向上写"的多级关系的强制访问控制规则,从而确保信息的向上单向流动。然而,在大多数应用中,主体(用户或程序)和客体的敏感度很难严格地划分等级,只存在一些模糊级别。许可级别高的用户未必一定允许查看密级(表示该客体所包含信息的敏感度)低的信息,例如:一个许可级别较高的用户不允许查看另一部门的较低密级的信息。

另外,在一般的多级安全关系数据库中,为了对低许可级的主体隐藏高密级的敏感信息,引入了多实例(Polyinstantiation)和伪元组(Cover Story)的概念,使得真实世界的单个实体在一个多级关系表中会产生多个元组,每个元组对应着不同密级的实例,并为每个字段设置相应的密级附加字段,以记录各数据项的密级信息。当不同实例间的数据差异很大时,这样的设计是合理的。然而,研究表明实际应用时,数据库中敏感数据(即需要对低许可级主体隐藏的数据)所占的比例通常仅仅只有约5%[2],这意味着多实例间的数据差异通常非常小,高密级的元组除个别字段外,绝大部分数据(90%以上)与低密级元组相同[3],造成数据的大量冗余,而且数据定义与操纵规则相当复杂。

为了解决上述问题,本文提出了一种新的模糊级别的多级安全关系数据库模型,采用类似于"同级读,同级写"的原则,既可以防止"高"许可级用户查看或修改"低"密级的信息,造成信息泄漏;又可以防止"低"许可级主体修改"高"密级的数据,形成隐通道,还可以通过多密级共享元组来减少数据冗余。

1 对基于多实例的多级关系的改进

当不同的元组具有相同的主键,却具有不同的密级时,称为多实例。在给定的格中,对每一个许可级都有一个关系实例,代表该许可级的用户眼中的数据版本。例如,对关系模式R而言,实例R_C就是许可级为C的用户所看到的元组的集合。多实例是一个应用多级安全的系统所固有的属性[4-5]。

在SeaView[6]和Jajodia、Sandhu[4-5,7]等人对多级安全数据模型的研究中,对每一个属性定义其相应的密级,并引入了多实例,但由于采用"向下读,向上写"的规

*基金项目:湖南省教育厅资助科研项目(编号:09C406)

则，因此，存在隐匿通道问题。参考文献[8]中引入了主从表，通过在从表中读写伪元组来消除隐通道问题，但按照这些规则进行读写操作后，大部分元组的各属性的密级最终都会与元组的密级相同。因此，本模型直接将各属性的密级属性去掉，只留下元组的密级属性；参考文献[9]直接去掉了属性的密级属性，只留下元组的密级属性TC，但要求为实体的每一种许可级定义一个实例。然而根据前面的分析，实际应用中不同密级实例的大部分属性值可能是相同的，甚至可能只是元组密级属性TC值不同而已，造成大量的冗余数据，而且，当许可级较多时，数据的冗余量将会成倍增长。因此，为了进一步减少冗余，本模型再将所有属性值均相同的多个不同密级的元组合并成一个元组，用一种类似于通配符的数据，即安全模式(Security Pattern)来表示这些密级。强制访问控制就是通过对比主体的许可级别和客体的安全模式是否匹配来确定主体是否能够存取客体。

安全模式定义及其运算规则。

定义1：设 $\Omega=\{C_1, C_2\cdots C_i, \cdots C_n\}$ 表示系统中所有密级的集合构成一个格，其中 C_i 表示某密级，可表示为：$00\cdots0100\cdots0$(即仅第 i 位为1的二进制数)，C_i 与 C_j 可能无严格的级别差。若干密级的集合 $p\subseteq\Omega$，即 $p=\{c_1, c_2, c_3\cdots c_k\}$(其中 $c_i\in\Omega$)，称 p 为某客体的安全模式(Security Pattern)；p 可用 $c_1|c_2|c_3|\cdots|c_k$ 的值表示(其中"|"表示按位"或"运算(下同)，即 n 位二进制数的所有与各 c_i 对应的位置为1，其他位置0)。若某主体许可级别为 c，客体的安全模式为 p，且 $c\in p$，则称 c 与 p 匹配，同时称该主体支配该客体。

定理1：许可级别为 c 的主体支配安全模式为 p 的客体(即 $c\in p$)，当且仅当 $c\&p=c$(其中 & 表示按位"与"运算，下同)。

例如，假设 Ω 代表4个密级的集合，则 C_1, C_2, C_3, C_4 可分别用1000，0100，0010，0001表示；若某安全模式 $p=\{C_1, C_3, C_4\}$，则 $p=C_1|C_3|C_4=1000|0010|0001=1011$；某主体的许可级别 $c=C_3=0010$ 时，$c\in p$，不难验证 $c\&p=c$。反之，若某主体的许可级别为 c，客体的安全模式为 $p=\{C_1, C_3, C_4\}$，且 $c\&p=c$，由于 $p=C_1|C_3|C_6$，显然只有 $c=C_1$ 或 $c=C_2$ 或 $c=C_3$ 时，才有 $c\&p=c$，可见 $c\in p$，即许可级别为 c 的主体支配安全模式为 p 的客体。

因此，一个改进后的多级关系可以定义为：

定义2：设有 $R(A_1, A_2, \cdots, A_n, SP)$，其中，$A_i$ 是定义在域 D_i 上的数据属性，SP表示元组的密级属性，SP的值为安全模式，为所有有权访问该元组的主体所支配。称R为多级关系模式。

可见本模型不仅形式简单，而且由于它保持了标准关系数据库的特点，因此易于在目前常见的DBMS上实现。又由于本模型不同于其他学者提出的模式，不再用属性TC来表示某一个密级别，而是一种称为安全模式的数据来表示多个密级别，只有许可级别与此安全模式匹配的主体才可以访问此元组，类似于"同级读，同级写"的访问控制规则，显然不可能泄漏敏感数据，也不存在隐通道。

2 模型的完整性规则

由于本模型扩展了标准的关系数据模型，引入了元组密级属性，为了保证数据库中数据的完整性和一致性，本模型对标准关系模式的完整性规则进行了增强。

2.1 实体完整性

本模型中，在标准关系模式的基础上增加了表示元组密级的属性SP，标准关系模式的直觉意义上的主键，称外观主键AK(Apparent primary Key)，真正的主键是外观主键加元组密级属性(即 $AK\cup SP$)。

实体完整性：多级关系R的一个实例 r 满足实体完整性，当且仅当，对 r 的所有元组 t，若 $A_i\in AK$ 则 $t[A_i]\neq null$ 且 $t[SP]\neq null$。即假定AK是定义在关系模式R上的外观主键，构成AK的所有属性均不能为空，元组的密级属性SP也不能为空。

2.2 参照完整性

参照完整性：R和S为多级关系，S参照了R，AKr为R的外观主键，FKs为S的外键，许可级别为 c 的主体所支配的R的实例 r_c 和S的实例 s_c 满足参照完整性，对 s_c 的所有元组 t_s，或者 $t_s[FK_s]=null$，或者存在 $t_r\in r_c$ 且 $t_r[AK_r]=t_s[FK_s]$ 和 $t_r[SP]\&t_s[SP]\&c=c$。

任何元组只能参照其他关系(或自身)中存在的元组，且参照及被参照的元组必须受同一许可级别主体支配。

2.3 实例间完整性

实例间完整性反映的是对给定格的所有密级，其对应的各个实例之间的联系和约束。

由于本模型中讨论的是模糊级别的格，采用的是类似于"同级读，同级写"的规则，故不保证一个实体在不同的许可级的关系实例中均可见。如果不可见，则表明本许可级别未被授权存取此实体。但如果实体的两个实例所有属性值均相同时，可用同一个实例来表示，并在此实例的SP属性中将这两个密级合并表示。

实例间完整性：对R的任意实例 r，及 $\forall t_1\in r, t_2\in r$，若 $t_1[U]=t_2[U]$(其中U表示所有属性)，则可将 t_2 删除，并将 t_1 和 t_2 的SP属性合并，即 $t_1[SP]=t_1[SP]|t_2[SP]$。

此规则并不要求严格满足，亦即各属性值相同仅SP值不同的元组不一定强制合并，只是合并可减少数据冗余。

2.4 多实例完整性

多实例完整性：对 $\forall c\in\Omega$ 和 $\forall ak\in AK$，许可级别为 c 的主体所支配的R的实例 r_c 中，不存在 $t\in r_c$ 和 $s\in r_c$，$t\neq s$，$t[AK]=s[AK]$。

此规则要求对于任意许可级别 c 和任意实体，多级关系R中至多存在一个实例 t 受许可级别为 c 的用户

支配。

在一个关系中可能有多个实例具有相同的 AK 值，但主体在任何密级最多只能接受 1 个 AK 值的实例。对某个特定许可级的关系，其所有元组的密级均受此许可级 c 支配，而且是其支配的元组的唯一代表，而密级属性的存在对用户是透明的，因此在用户眼中，仍是 $AK \rightarrow A_i(A_i \notin AK)$，保持了标准关系模型中的函数依赖特性。为了禁止一个实体在同一密级中的多实例存在，首先要求多级关系中的主键为 AK ∪ SP，然后再通过读写规则加以控制。

3 读写规则

3.1 读规则

在本模型中，不是为每一密级创建 1 个元组，而可能是多密级别共享 1 个元组。每个密级别对应的关系实例的元组为多级关系中可由此许可级主体支配的元组组成。因此本模型中读规则为：用户在其有效的读范围内，读取元组安全模式 SP 值与主体许可级匹配的元组。如果某 AK 值对应的所有元组中所有 SP 值都与主体许可级不匹配，表明此实体的所有信息均对此主体隐藏了。

例 1：假设某情报机构使用 MLS 数据库记录职员的信息。假定系统中密级分为四级分别是 a、b、c、d(分别用 1000，0100，0010，0001 表示)。系统中存在 2 个多级关系：职员关系 Empl 与部门关系 Dept，外观主键分别为 EName 和 DName，元组如表 1、表 2 所示(其中 SP 部分的字段对用户是透明的，下同)。

表 1 Empl

EName	DName	SP
王平	机要	1000
王平	后勤	0010
刘欢	管理	1100
刘欢	后勤	0011

表 2 Dept

DName	Addr	SP
机要	1-101	1000
机要	2-102	0001
管理	3-201	1100
后勤	4-101	1111

根据上面的读规则，许可级别为的 a，b，c，d 的用户看到两表的关系实例如表 3~表 8 所示。

a 级用户视图：

表 3 Empl(a 级)

EName	DName	SP
王平	机要	1000
刘欢	管理	1100

表 4 Dept(a 级)

DName	Addr	SP
机要	1-101	1000
管理	3-201	1100
后勤	4-101	1111

b 级用户视图：

表 5 Empl(b 级)

EName	DName	SP
刘欢	管理	1100

表 6 Dept(b 级)

DName	Addr	SP
管理	3-201	1100
后勤	4-101	1111

c 级用户视图(略)。

d 级用户视图：

表 7 Empl(d 级)

EName	DName	SP
刘欢	后勤	0011

表 8 Dept(d 级)

DName	Addr	SP
机要	2-102	0001
后勤	4-101	1111

不同级别的用户，Empl 引用的 DName 都是 Dept 中存在的 DName，而且是受同许可级的主体支配。可见，不同用户视图都满足参照完整性。同样本例中多级安全数据库满足前述的其他各项完整性约束规则。

3.2 插入操作

情形 1：对单个多级关系的插入操作。

(1)检查多级关系的用户视图中是否存在与待插入的外观主键值相同的元组，如果存在则插入失败；否则按步骤(2)进行；

(2)检查多级关系中是否存在各数据项与待插入元组各数据项相同的元组，如果存在则将此元组的 SP 值 sp 用 $sp\&c$ 代替(c 代表执行插入操作的用户的许可级)，插入完成；否则继续下面的步骤。

(3)插入此元组，并将该元组的密级属性置为用户的许可级。

例 2：许可级为 b 的用户执行以下插入语句：insert into Dept values('机要','1-101')，插入后的效果如表 9 所示。

表 9 Dept(例 2)

DName	Addr	SP
机要	1-101	1100
机要	2-102	0001
管理	3-201	1100
后勤	4-101	1111

情形 2：若是对有外键的多级关系进行插入操作，还要满足参照的完整性。亦即先检查被参照关系的用户视图中是否存在相应 AK=fk(fk 表示待插入元组的外键值)，若存在，则直接按情形 1 完成插入操作；否则，插入失败。

例 3：许可级为 b 的用户执行以下插入语句：insert into Empl values('王平','机要')，由于在 Dept 的 b 用户视图中不存在 AK='机要'的元组，故插入失败。但 d 级用户却可以成功执行此插入操作，成功操作后结果如表 10、表 11 所示。

表 10 Empl(例 3)

EName	DName	SP
王平	机要	1001
王平	后勤	0010
刘欢	管理	1100
刘欢	后勤	0011

表 11 Dept(例 3)

DName	Addr	SP
机要	1-101	1000
机要	2-102	0001
管理	3-201	1100
后勤	4-101	1111

3.3 更新操作

由于在本模型中，将多个不同的密级元组合并成 1 个元组，因此，1 个元组可能代表多个密级的实例，一个许可级主体的更新操作不应该影响其他许可级的视图。

(1)检查待更新的元组的 SP 值是否为某单个密级(即二进制数只有一位为 1，下同)，若是，则表明此次更

新不会影响其他许可级的视图,因此可按标准关系模型的更新操作进行;否则,按以下步骤。

(2)先将此元组的SP值*sp*更新为*sp*&~*c*(*c*表示执行更新操作的主体的许可级,下同),再按"插入操作"插入新元组,新元组各项为待更新的元组的新值。

例4:许可级为b的用户欲执行命令:update dept set addr='4-201' where DName='管理',根据表6可见,元组{管理,3-201,1100}代表了a、b密级的实例。为了不影响a的实例,先将此元组的SP从1100更新为1000,再执行插入操作:insert into dept values('管理','4-201')。

3.4 删除操作

在本模型中,1个元组可能代表多个密级的元组,故删除规则应按下面的步骤进行:

(1)检查待删除元组的SP值是否为某单个密级,若是,则可按标准关系模型的删除操作进行。否则,按以下步骤。

(2)先将此元组的SP值*sp*更新为*sp*&~*c*(*c*表示执行删除操作的主体的许可级)。

本模型继承了多实例的概念,并作了改进。如果多个实例仅仅只有元组的密级属性不同,则直接将这些实例用1个元组表示,其SP值为这些密级属性的并集,由于实际应用中敏感数据很少,故这种规则在应用中是合理的,从而大大减少了数据的冗余。

本文提出的多级关系数据模型中使用类似"同级读,同级写"的规则,任何许可级的用户都无法看到其他密级的元组(除非与此许可级用户共享该元组),同时,也无法修改其他密级的元组(即使与此许可级用户共享元组,修改也不会影响其他许可级的用户视图),既避免了隐通道,又防止了敏感数据的泄漏。

参考文献

[1] BELL D E, LAPADULA L J P. Secure computer system: Unified exposition and multics interpretation [R]. Tech Rep MTR-2997, MITRE Corp, Bedford, MA, 1975.

[2] SANDHU R, CHEN F. The multilevel relational (MLR) data model [J]. Transactions on Information and System Security, 1998:1(1):93-132.

[3] 冯朝阳,岳丽华,翟小栋,等.一种紧凑的多级安全关系数据模型[J].计算机工程与应用,2005(4):170-174.

[4] JAJODIA S, SANDHU R, SIBLEY E. Update semantics for multilevel relations[J]. In Proceedings of the 6th Annual Computer Security Applications Conference. 1990 (10):103-112.

[5] JAJODIA S, SANDHU R. Polyinstantiation integrity in multilevel relations[C]. IEEE Symposium on Security and Privacy, 1990.

[6] DENNING D E, LUNT T F. The seaview security model [C]. IEEE Symposium on Security and Privacy, 1998.

[7] JAJODIA S, SANDHU R, LUNT T F. A new polyins-tantiation integrity constraint for multilevel relations [C]. IEEE Work-shop on Computer Security Foundations, 1990.

[8] 武立福,毛宇光.一种改进的多级安全关系数据模型[J].计算机应用,2003,23(7):103-108.

[9] 冯玉才,张勇.多实例的多级安全关系数据库数据模型研究[J].小型微型计算机系统,2003,24(3):452-455.

(收稿日期:2010-03-05)

作者简介:

王六平,1972年生,讲师,硕士,主要研究方向:数据库,信息安全。

鲁建恺,1963年生,工程师,主要研究方向:数据库应用。