第26卷第3期 上海师范大学学报(自然科学版) Vol. 26, No. 3
1997年9月 J. of Shanghai Teachers Univ. (Natural Sciences) Sep. 1997

商品信息管理系统的安全机制

鲍仁敏

提 要 给出了数据库系统的多种安全机制及其在商品信息管理系统设计中的具体应用.

关键词 商品信息管理系统; 数据库; 安全机制
中图法分类号 TP311.13

0 引 言

商品信息管理系统是管理商业单位在日常的进、销、存业务活动中产生的信息数据,并对这些数据作统计、汇总,进行营业决策的管理信息系统. 在这个含有数据库的系统设计中,必须采用数据库系统提供的安全机制来进行系统设计,以确保系统的数据安全和正确.

1 数据库概念

数据库是由信息实体和这些实体之间的关系组成,这些关系和实体在数据库内以某些物理的方式(记录和指针)表述. 数据库管理系统(DBMS)为用户和其他应用程序提供对数据库的访问,同时也提供事件登录、恢复和数据库组织.

对于数据库管理系统,ANSI/SPARC 研究组提出了3级模式,如图1所示. 在应用一边的

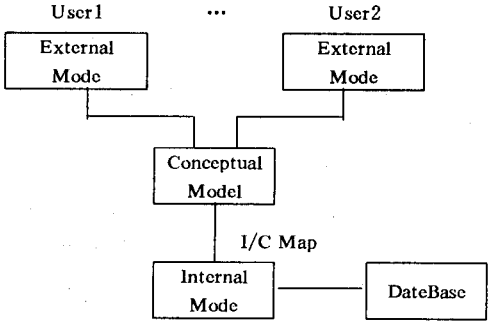

图1 数据库模式

收稿日期:1997-04-04
作者鲍仁敏,女,助理工程师,上海师范大学计算中心,上海,200234

外部模式描述每个用户的数据视图,定义数据模型;在数据库一边,内部模式描述数据如何存储. 这两者之间是定义概念数据模型的概念模式.

2 数据库提供的安全机制

2.1 视图定义和查询修改

为不同的用户定义不同的视图,可以限制各个用户的访问范围. 有些 DBMS 没有视图功能,但是系统可以根据用户的访问限制条件,自动地修改查询条件,使其只能在给定访问范围内查询. 就限制用户访问数据的范围而言,查询修改实际上起了视图的作用,并且其处理比视图简单,易于实现,效率也高.

2.2 存储过程和触发器(Trigger)

一些 DBMS 还提供对存储过程和触发器的支持.

存储过程是 SQL 语句以及流程控制语句的集合,它在生成时被编译存放在数据库中,作为单个数据库对象进行管理. 存储过程的使用对数据的访问与更新提供了特别层次的控制,如果一个用户对数据库过程涉及的表没有直接的访问权限,DBA 可以使用 Grant 语句授权给这个用户执行这个数据库过程的权限,用这种方法,DBA 可以精确地控制一个用户对数据库的操作权限.

触发器是一种特殊类型的存储过程,它在插入、删除或修改特定表中的数据时起作用,无论是录入人员输入数据还是应用程序的作用,它们能够自动响应. 触发器和启动它的语句被当作一个事务(Transaction)处理,事务可以在触发器内回退(Rollback). 这样,可以在触发器中通过适当的 SQL 编程,达到维持不同表中逻辑上相关数据的一致性,保持数据的相关完整性,拒绝或回退那些触发器认为有错误的事务,从而达到安全的目的.

2.3 访问控制(Access Control)

访问控制是对用户访问数据库各种资源(包括基表、视图、各种目录以及实用程序)的权力(包括创建、撤销、查询、增、删、改、执行等)的控制. 这是数据库安全的基本手段. 数据库用户按其访问权力的大小,一般可分为 3 类:一般数据库用户;具有支配部分数据库资源特权的数据库用户;具有 DBA 特权的数据库用户.

2.4 数据加密

前面介绍的数据库安全措施,都是防止从数据库系统窃取保密数据. 但是数据以可读的形式存储在介质上(例如磁盘、磁带等),还常常通过通信线路进行传输. 一些计算机内行,完全可以攻击进入系统,或从介质中导出数据,或通过从通信线路窃听的方法获得数据,使数据库系统无法控制.

为了解决这种泄密问题,除控制非法访问外,还必须对数据进行加密保护. 然而对数据库进行加密处理后,在存入时必须加密,在查询时必须解密,开销很大,降低了数据库性能. 只有对那些保密要求特别高的数据,才值得采用此方法.

2.5 完整性控制

一般数据库系统提供根据语义的完整性检验. DBMS 中一般提供了以下几种完整性控制手段:

①在SQL语句的语义分析过程中,检查输入数据的数据类型和长度与数据库中的定义是否相配.

②通过在建表语句中指定某个域为not null来实现该域的"不允许空值",使在输入时在该域必须输入数据.

③在某个或某些域上,定义一些关于数据的规则或值域范围,确保输入数据的相互关系符合设计者的要求.

④指定某个域(主键或Idendity列)或某些域的组合(主键)为表中唯一,可以防止输入重复的数据.

2.6 封锁机制

大多数的DBMS都提供一种封锁机制实现并发控制. 封锁是一种防止在进程之间发生破坏性相互影响的机制,避免其他用户影响活动事务正在使用的数据,确保数据更新正确或正确地改动基础数据结构.

数据库系统一般提供两种类型的锁:共享锁和排他锁.

对数据更新操作(INSERT、UPDATE和DELETE),一般使用排他锁. 当一个排他锁被设置时,其他事务则不能对被加锁的数据库对象获得任何种类的锁,也不能访问该对象,直到当前事务结束后该锁被释放为止.

对非更新操作,如SELECT,一般使用共享锁. 如果对表和数据使用了共享锁,其他事务也可获得共享锁,即使当前事务没有完成. 然而,除非所有的共享锁被释放,任何事务均不能获得排他锁,即多个事务可以同时读取表和数据但都不能进行更新操作.

3 商品信息管理系统采用数据库的安全机制

由于商品信息管理系统管理的数据量大、变化大、要求较高的安全性和正确性,在商品信息管理系统软件的设计中,采用了数据库提供的视图、触发器、数据加密、完整性控制等安全机制.

3.1 视图定义

根据商业单位中岗位级别(如经理、统计员、营业员)为重要的数据基表建立若干视图,为不同级别用户提供不同密级的数据;又如:要限制商场中各个柜台查询、修改本柜台的数据情况,可为它们分别定义只包含本柜台数据的视图;再如:对某些统计人员,只能让其了解统计数据,而不能让他们了解个别数据,可以为他们定义个只包含统计数据的视图.

3.2 触发器

禁止在非工作时间内开单,即禁止在非工作时间内对Sales表进行插入、修改,提高了每天统计的进、锁、存数据的安全性和正确性.

```
creat trigger stop-trigger
on sales
for insert /* It could be update */
as
if detepart(hour,getdate())<8 or datepart(hour,getdate())>17
begin
```

```
rollback trasaction
print "We do not allow modifying with sales when it is not working time"
end
```

3.3 数据加密

对统计后得到的总销售额、总进货额、毛利等重要数据进行加密存放,在具有特定权力的人进行查询、打印时,才给予解密,取得真正的数据.

参 考 文 献

1 莫瑞·加瑟著,吴亚非等译. 计算机安全的技术与方法. 北京:电子工业出版社,1992

2 王化文,张德向. 计算机安全保密原理与技术. 北京:科学出版社,1993

3 陶浦洲,李强. Sybase 数据库技术大全. 北京:科学出版社,1995

4 Ernstl leiss. Principles of Data Security. Plenum Publishing Corporation, 1982

5 Philip E Fites, Martin P J, Kratz. Control and Security of Computer Information Systems. Computer Sicence Press, Inc, 1989

Security Mechanism of the Commerical Information Management System

Bao Renming

(Computer centre)

Abstract Serveral security mechanisms of datebade system are given. They are applied in the desigin of commercial information management systems.

Key words commercial information management system; database; security mechanism