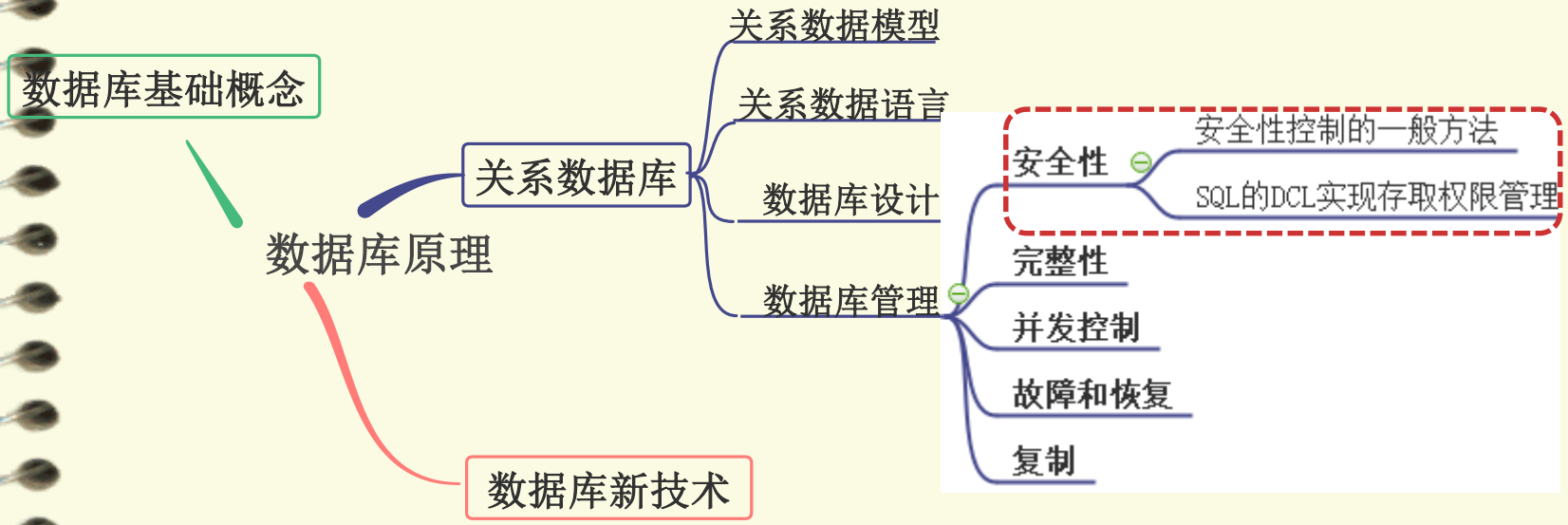
数据库原理

第7章 数据库管理

辽东学院 鲁 琴

本节要点


数据库基础概念
数据库原理
关系数据库
关系数据模型
关系数据语言
数据库设计
数据库管理
安全性
安全性控制的一般方法
SQL的DCL实现存取权限管理
完整性
并发控制
故障和恢复
复制
数据库新技术

1 安全性

问题的提出

- 数据库的一大特点是数据可以共享
- 但数据共享必然带来数据库的安全性问题
- 数据库系统中的数据共享不能是无条件的共享

例：军事秘密、 国家机密、 新产品实验数据、
市场需求分析、市场营销策略、销售计划、
客户档案、 医疗档案、 银行储蓄数据

安全性（续）

- 数据库中数据的共享是在DBMS统一的严格的控制之下的共享，即只允许有合法使用权限的用户访问允许他存取的数据

- 数据库系统的安全保护措施是否有效是数据库系统主要的性能指标之一

安全性（续）

- 什么是数据库的安全性
  - 数据库的安全性是指保护数据库，防止因用户非法使用数据库造成数据泄露、更改或破坏。
- 什么是数据保密
  - 数据保密是指用户合法地访问到机密数据后能否对这些数据保密。
  - 通过制订法律道德准则和政策法规来保证。

用户非法使用数据库的情况

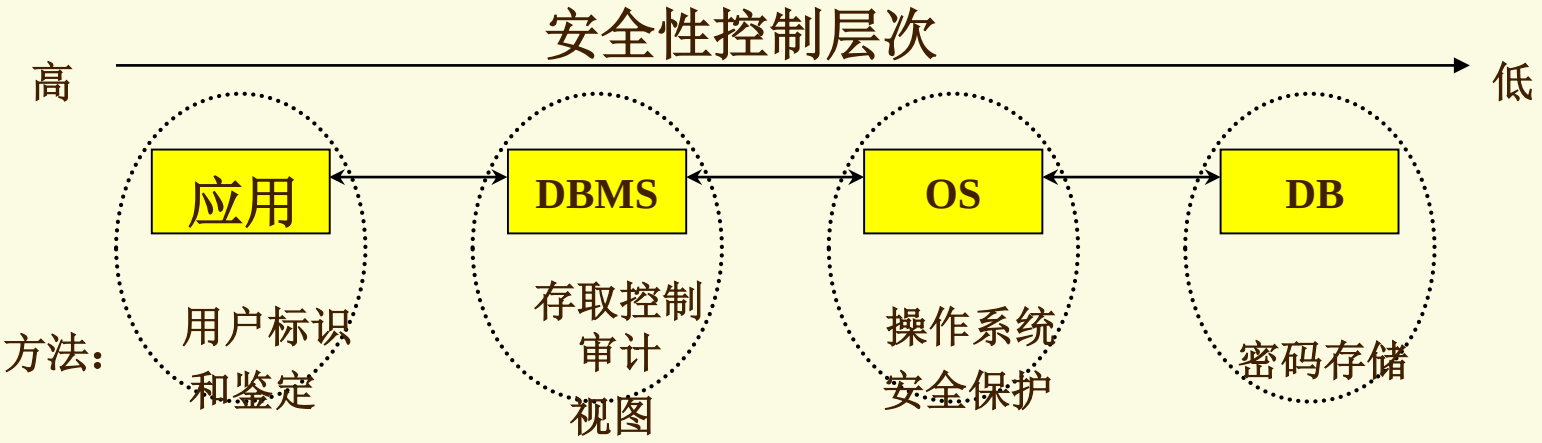
- 用户编写一段合法的程序绕过DBMS及其[illegible]权机[illegible]通过操作系统直接存取、修改或备份[illegible]
- 直接或编写应用程序执行非授权[illegible]
- 通过多次合法查询数据库，从中推导[illegible]据

这些破坏安全性的行为可能是无意的，故意的，恶意的

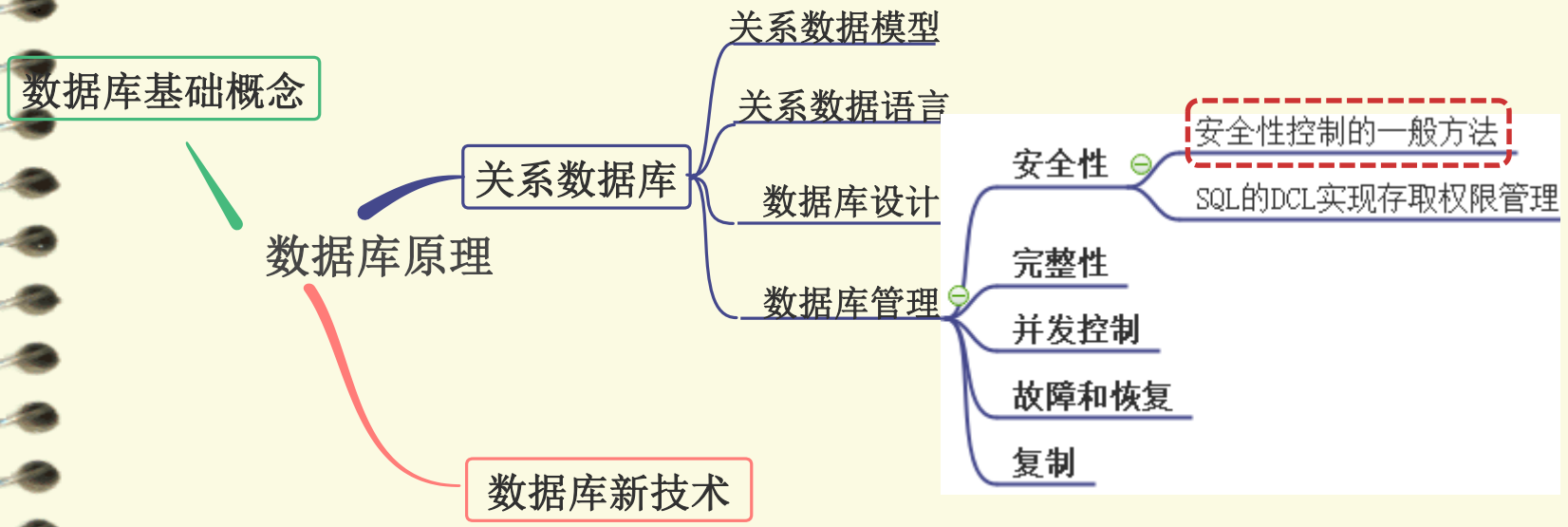
安全性控制

就是要尽可能地杜绝所有可能的数据库非法访问，不管它们是有意的还是无意的。

计算机系统中常用的安全模型



安全性


数据库基础概念
数据库原理
关系数据库
关系数据模型
关系数据语言
数据库设计
数据库管理
安全性
安全性控制的一般方法
SQL的DCL实现存取权限管理
完整性
并发控制
故障和恢复
复制
数据库新技术

1.1 安全性控制的一般方法

(1)用户标识和鉴定

(2)存取控制

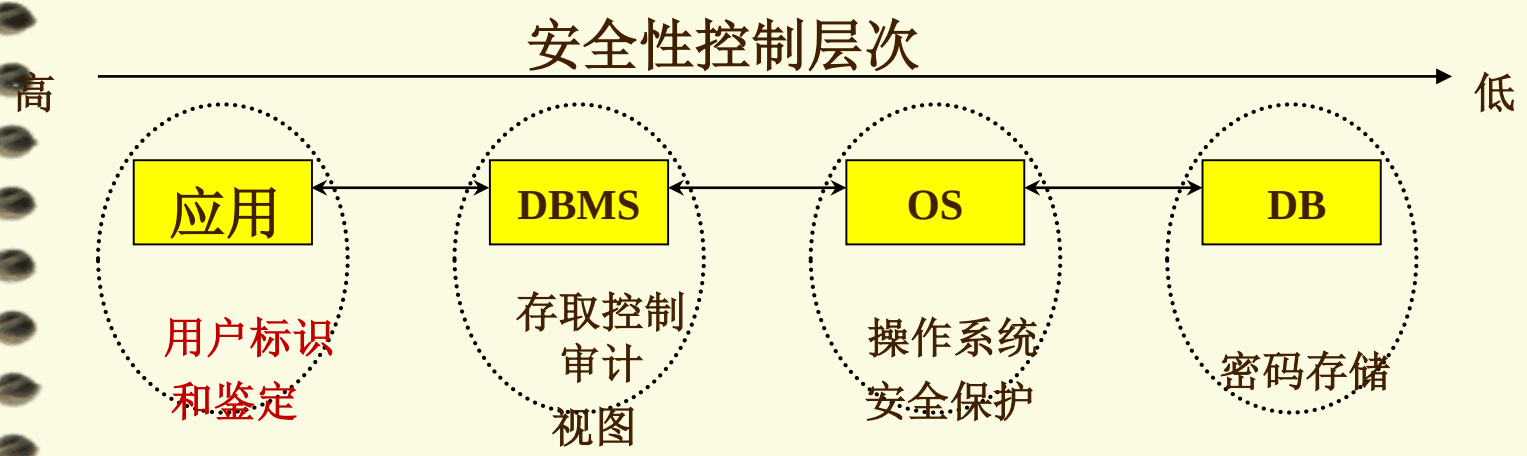
(3)视图

(4)审计

(5)密码存储

（1）用户标识与鉴定

- 用户标识与鉴定（Identification & Authentication）
  - 系统提供的最外层安全保护措施



用户标识与鉴定的基本方法

- 系统提供一定的方式让用户标识自己的名字或身份；
- 系统内部记录着所有合法用户的标识；
- 每次用户要求进入系统时，由系统核对用户提供的身份标识；
- 通过鉴定后才提供机器使用权；
- 用户标识和鉴定可以重复多次。

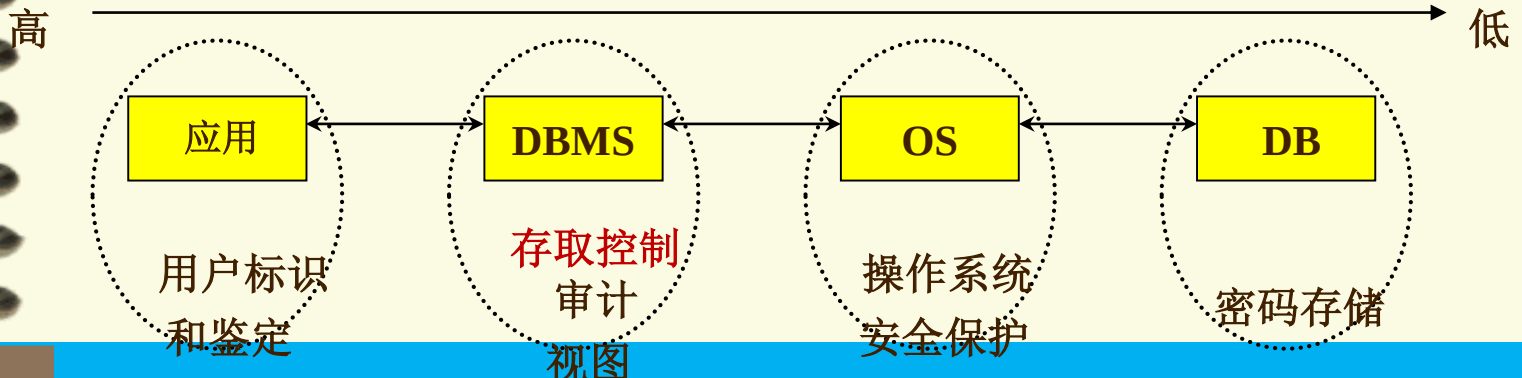
让用户标识自己的名字或身份的方法

- 用户名/口令
  - 简单易行，容易被人窃取
- 每个用户预先约定好一个计算过程或者函数
  - 系统提供一个随机数
  - 用户根据自己预先约定的计算过程或者函数进行计算
  - 系统根据用户计算结果是否正确鉴定用户身份

（2）存取控制

- 存取控制机制的功能
  - 保证用户只能访问其有权存取的数据
- 存取控制机制的组成
  - 定义存取权限
  - 检查存取权限

  用户权限定义和合法权检查机制一起组成了**DBMS的安全子系统**



存取控制机制的组成

- 定义存取权限
  - 在数据库系统中，为了保证用户只能访问他有权存取的数据，必须预先对每个用户定义存取权限。
- 检查存取权限
  - 对于通过鉴定获得访问权的用户（即合法用户），系统根据他的存取权限定义对他的各种操作请求进行控制，确保他只执行合法操作。

定义存取权限

- 存取权限由两个要素组成
  - 数据对象
  - 操作类型
- 定义一个用户可以在哪些数据对象上进行哪些类型的操作
- 在数据库系统中，定义存取权限称为授权（Authorization）
- 授权定义经过编译后存放在数据字典中

关系系统中的存取权限

数据对象		操作类型
模式	模 式	建立、修改、检索
	外模式	建立、修改、检索
	内模式	建立、修改
数据	表	查找、插入、修改、删除
	属性列	查找、插入、修改、删除

一个授权表例子

用户名	数据对象名	允许的操作类型
John	关系student	SELECT
Jack	关系student	ALL
Jack	关系Cource	ALL
Jack	关系SC	SELECT
Jack	列SC.Grade	UPDATE
Mary	列SC.Sno	SELECT
Mary	列SC.Cno	SELECT

检查存取权限

- 对于获得连接权后又进一步发出存取数据库操作的用户
  - DBMS查找数据字典，根据其存取权限对操作的合法性进行检查
  - 若用户的操作请求超出了定义的权限，系统将拒绝执行此操作

授权粒度

- 授权粒度是指可以定义的数据对象的范围
  - 它是衡量授权机制是否灵活的一个重要指标。
  - 授权定义中数据对象的粒度越细，即可以定义的数据对象的范围越小，授权子系统就越灵活。

数据对象粒度

- 关系数据库中授权的数据对象粒度
  - 数据库
  - 表
  - 属性列
  - 行
- 能否提供与数据值有关的授权反映了授权子系统精巧程度

关系系统中的存取权限

定义方法（书3.3节,P110）

- **GRANT** 授权
- **REVOKE** 回收权限

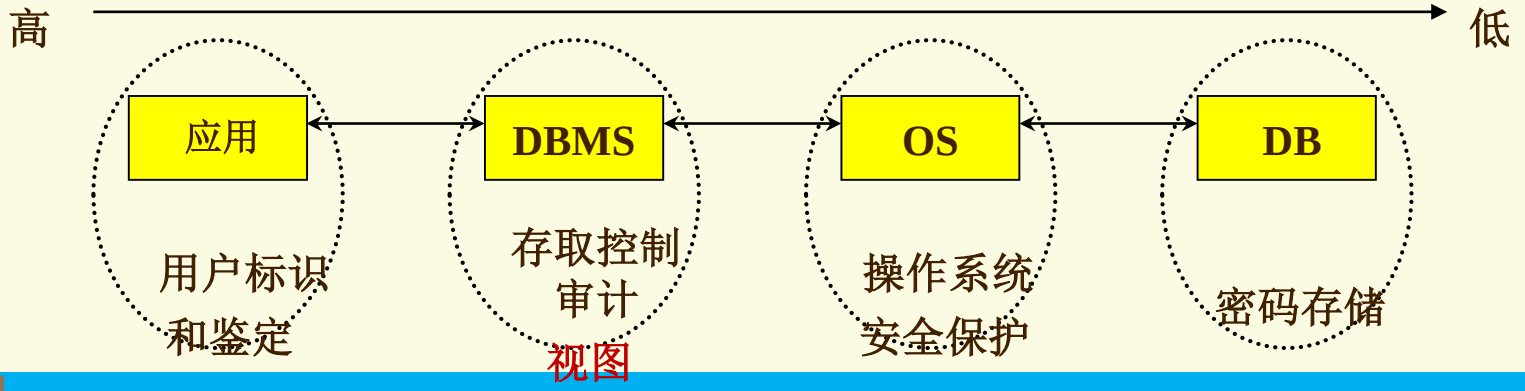
DBMS实现存取控制的过程

- 用户或DBA把授权决定告知系统，这是由SQL的GRANT和REVOKE语句来完成的
- DBMS把授权的结果存入数据字典
- 当用户提出操作请求时，DBMS根据授权情况进行检查，以决定是否执行操作请求

(3) 定义视图

视图机制把要保密的数据对无权存取这些数据的用户隐藏起来，从而自动地对数据提供一定程度的安全保护。

视图机制更主要的功能在于提供数据独立性，其安全保护功能不太精细，往往远不能达到应用系统的要求。



定义视图（续）

在实际应用中通常是视图机制与授权机制配合使用，首先用视图机制屏蔽掉一部分保密数据，然后在视图上面再进一步定义存取权限。

- 这时视图机制实际上间接实现了支持存取谓词的用户权限定义

定义视图（续）

例：王平只能检索计算机系学生的信息

先建立计算机系学生的视图CS_Student

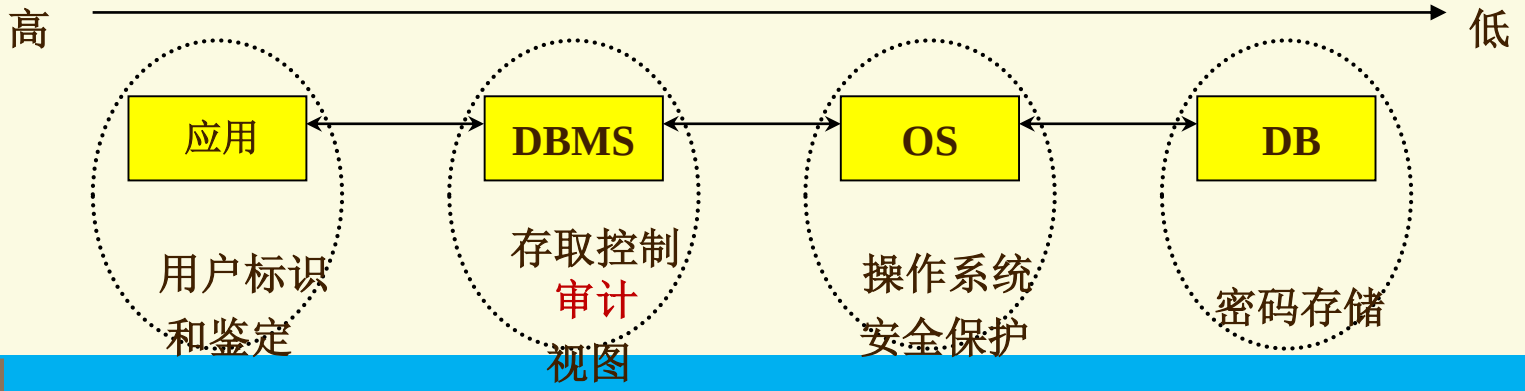
```
CREATE VIEW CS_Student
        AS
        SELECT Sno,Sname,Ssex,Sdept,Sage
        FROM   Student
        WHERE  Sdept='CS';
```

在视图上进一步定义存取权限

```
GRANT  SELECT
 ON  TABLE CS_Student
 TO 王平 ;
```

(4) 审计

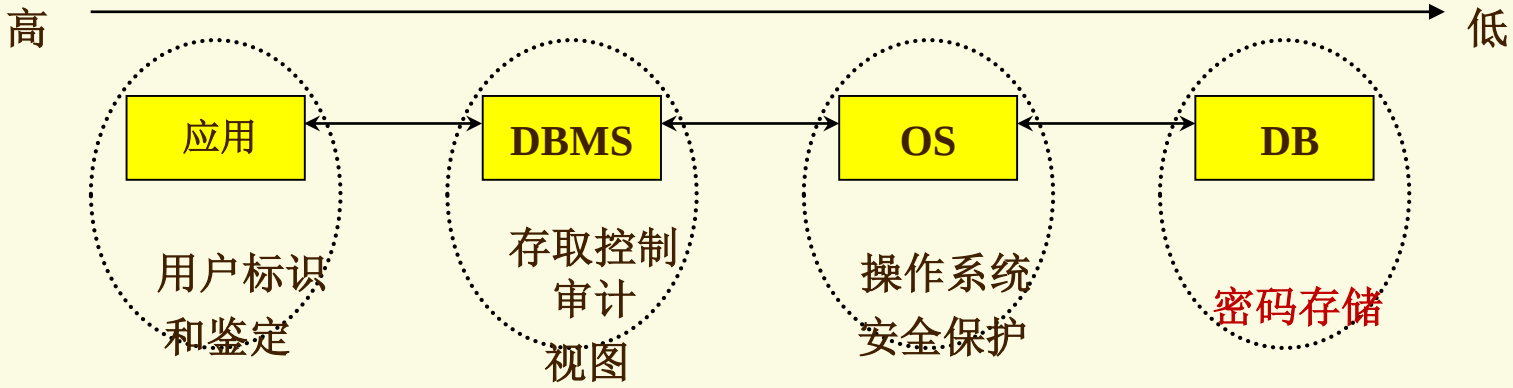
- 审计功能启用一个专用的审计日志（Audit Log），系统自动将用户对数据库的所有操作记录在上面
- DBA可以利用审计日志中的追踪信息，重现导致数据库现有状况的一系列事件，以找出非法存取数据的人
- C2以上安全级别的DBMS必须具有审计功能



审计功能

- 审计很费时间和空间，所以DBMS往往都将其作为可选特征
- DBA可以根据应用对安全性的要求，灵活地打开或关闭审计功能
- 用户识别和鉴定、存取控制、视图等安全性措施均为强制性机制，将用户操作限制在规定的安全范围内
- 审计技术是预防手段，监测可能的不合法行为
- 由于任何系统的安全性措施都不可能是完美无缺的，蓄意盗窃、破坏数据的人总是想方设法打破控制
- 所以，当数据相当敏感，或者对数据的处理极为重要时，就必须使用审计技术

（5）数据加密



数据加密

数据加密

- 防止数据库中数据在存储和传输中失密的有效手段

加密的基本思想

- 根据一定的算法将原始数据（明文，**Plain text**）变换为不可直接识别的格式（密文，**Cipher text**）
- 不知道解密算法的人无法获知数据的内容

加密方法

替换方法

- 使用密钥（Encryption Key）将明文中的每一个字符转换为密文中的一个字符

置换方法

- 将明文的字符按不同的顺序重新排列
- 这两种方法结合能提供相当高的安全程度

例：美国1977年制定的官方加密标准：数据加密标准（Data Encryption Standard，简称DES）

数据加密（续）

DBMS中的数据加密

- 有些数据库产品提供了数据加密例行程序
- 有些数据库产品本身未提供加密程序，但提供了接口

数据加密功能通常也作为可选特征，允许用户自由选择

- 数据加密与解密是比较费时的操作
- 数据加密与解密程序会占用大量系统资源
- 应该只对高度机密的数据加密

安全控制的一般方法小结

（1）用户标识和鉴定

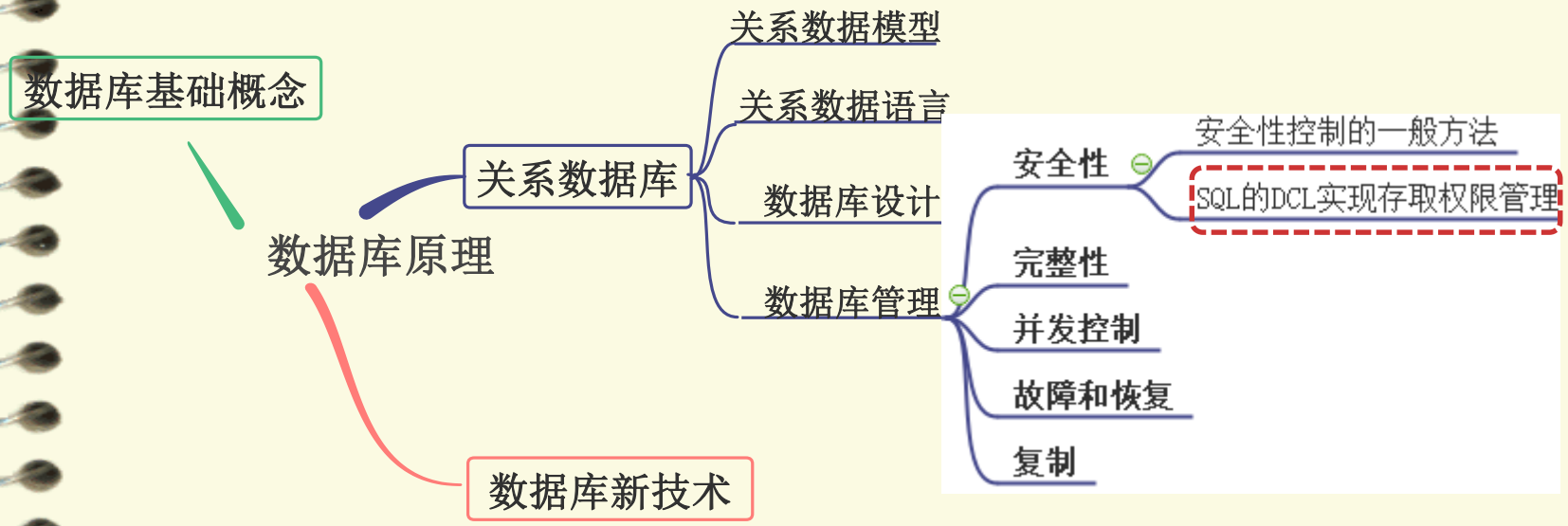
（2）存取控制

（3）视图

（4）审计

（5）密码存储

安全性


数据库基础概念
数据库原理
数据库新技术
关系数据库
关系数据模型
关系数据语言
数据库设计
数据库管理
安全性
安全性控制的一般方法
SQL的DCL实现存取权限管理
完整性
并发控制
故障和恢复
复制

1.2 SQL的DCL实现存取权限管理

不同的用户对不同的数据应具有何种操作权力，是由DBA和表的建立者（即表的属主）根据具体情况决定的

SQL语言则为DBA和表的属主定义与回收这种权力提供了手段

SQL的DCL

- 授 权
- 回收权力

(1) SQL的授权功能

GRANT语句的一般格式：

GRANT <权限>[,<权限>]...

[ON <对象类型> <对象名>]

TO <用户>[,<用户>]...

[WITH GRANT OPTION];

功能：将对指定操作对象的指定操作权限授予指定的用户。

① 操作权限

对象	对象类型	操 作 权 限
属性列	TABLE	SELECT, INSERT, UPDATE DELETE, ALL PRIVILEGES
视图	TABLE	SELECT, INSERT, UPDATE DELETE, ALL PRIVILEGES
基本表	TABLE	SELECT, INSERT, UPDATE DELETE ALTER, INDEX, ALL PRIVILEGES
数据库	DATABASE	CREATETAB

② 用户的权限

数据库的建立表（CREATETAB）的权限属于DBA，可由DBA授予普通用户，普通用户拥有此权限后可以建立基本表。

基本表或视图的属主拥有对该表或视图的一切操作权限。

③ 接受权限的用户

一个或多个具体用户

PUBLIC（全体用户）

④ WITH GRANT OPTION子句

如果指定了WITH GRANT OPTION子句，则获得某种权限的用户还可以把这种权限再授予别的用户。

如果没有指定WITH GRANT OPTION子句，则获得某种权限的用户只能使用该权限，但不能传播该权限

例题

一次向一个用户授权

例1 把查询Student表权限授给用户U1

```
GRANT   SELECT
    ON   TABLE   Student
    TO   U1;
```

例题（续）

一次向多个用户授权

例2 把对Student表和Course表的全部权限授予用户U2和U3

```
GRANT ALL PRIVILEGES
      ON TABLE Student, Course
      TO U2, U3;
```

例题（续）

一次向多个用户授权

例3 把对表SC的查询权限授予所有用户

```
GRANT SELECT
      ON TABLE SC
      TO PUBLIC;
```

例题（续）

例4 把查询Student表和修改学生姓名的权限授给用户U4

```
GRANT UPDATE(Sname), SELECT
    ON TABLE Student
    TO U4;
```

一次可以完成对基本表、视图和属性列这些不同对象的授权

例题（续）

一次传播多个同类对象的权限

例5 把对表SC的INSERT权限授予U5用户，并允许他再将此权限授予其他用户

```
GRANT INSERT
      ON TABLE SC
      TO U5
      WITH GRANT OPTION;
```

传播权限

执行例5后，U5不仅拥有了对表SC的INSERT权限，还可以传播此权限：

```
GRANT INSERT ON TABLE SC TO U6
        WITH GRANT OPTION;
```

同样，U6还可以将此权限授予U7：

```
GRANT INSERT ON TABLE SC TO U7;
```

但U7不能再传播此权限。

例题（续）

例6 DBA把在数据库S_C中建立表的权限授予用户U8

```
GRANT CREATETAB
    ON DATABASE S_C
    TO U8;
```

授予关于DATABASE的权限必须与授予关于TABLE的权限分开

（2）SQL收回权限的功能

REVOKE语句的一般格式为：

REVOKE <权限>[,<权限>]...

[ON <对象类型> <对象名>]

FROM <用户>[,<用户>]...;

功能：从指定用户那里收回对指定对象的指定权限

例题

例7 把用户U4修改学生姓名的权限收回

```
REVOKE UPDATE(Sname)
    ON TABLE Student
    FROM U4;
```

例题（续）

例8 收回所有用户对表SC的查询权限

```
REVOKE SELECT
    ON TABLE SC
    FROM PUBLIC;
```

例题（续）

例9 把用户U5对SC表的INSERT权限收回

```
REVOKE INSERT
    ON TABLE SC
    FROM U5;
```

系统将收回直接或间接从U5处获得的对SC表的INSERT权限

DCL小结

SQL提供了非常灵活的授权机制

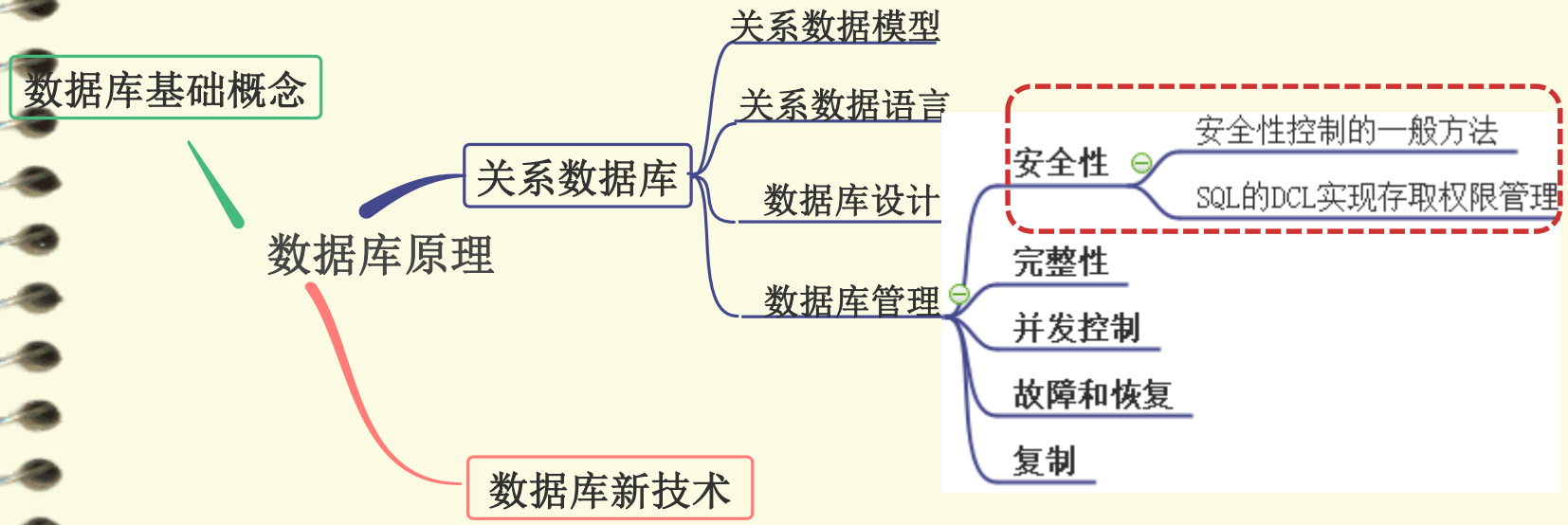
用户对自己建立的基本表和视图拥有全部的操作权限，并且可以用GRANT语句把其中某些权限授予其他用户

被授权的用户如果有“继续授权”的许可，还可以把获得的权限再授予其他用户

DBA拥有对数据库中所有对象的所有权限，并可以根据应用的需要将不同的权限授予不同的用户

所有授予出去的权力在必要时又都可以用REVOKE语句收回

本节小结


数据库基础概念
数据库原理
关系数据库
关系数据模型
关系数据语言
数据库设计
数据库管理
安全性
安全性控制的一般方法
SQL的DCL实现存取权限管理
完整性
并发控制
故障和恢复
复制
数据库新技术