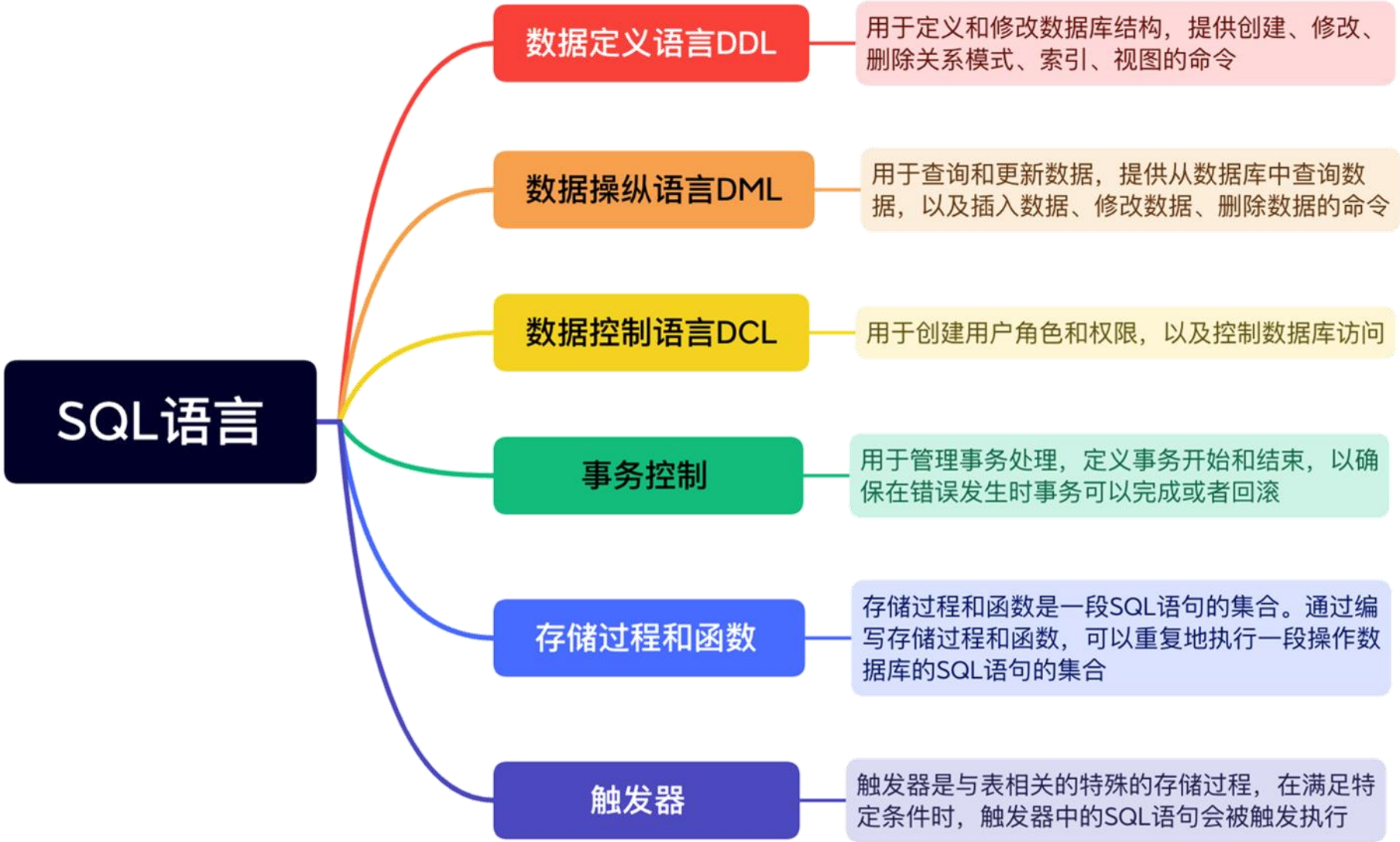
数据库系统概论

计算机与信息学院
人 工 智 能 学 院


SQL语言
数据定义语言DDL
用于定义和修改数据库结构，提供创建、修改、删除关系模式、索引、视图的命令
数据操纵语言DML
用于查询和更新数据，提供从数据库中查询数据，以及插入数据、修改数据、删除数据的命令
数据控制语言DCL
用于创建用户角色和权限，以及控制数据库访问
事务控制
用于管理事务处理，定义事务开始和结束，以确保在错误发生时事务可以完成或者回滚
存储过程和函数
存储过程和函数是一段SQL语句的集合。通过编写存储过程和函数，可以重复地执行一段操作数据库的SQL语句的集合
触发器
触发器是与表相关的特殊的存储过程，在满足特定条件时，触发器中的SQL语句会被触发执行

现状

数据泄露频繁发生

数据泄露、大数据杀熟、倒卖个人信息频发……全国政...

“当前，随着数据开放流动，网络边界日趋模糊，云计算、ai等新技术给数据安全带来严峻挑战。数据泄露、网络安全事故、数据篡改...

上观新闻 3月6日

威胁猎人发布《2022年数据资产泄露分析报告》

同时，该报告还分享了多个较为典型的数据泄露事件案例，并对其原因以及相关应对思路做了阐述，有着很强的借鉴意义和参考价值。...

安全419 3月6日

防止数据泄露的10个策略

防止数据泄露不仅仅是为了避免诉讼,它也是确保你的企业保护其底线的关键。根据IBM的数据,数据泄露的平均成本增加了2.6%,从2021...

腾讯新闻 3月6日

12306网站用户信息外泄事件 - 百度百科

2014年12月25日上午，漏洞报告平台乌云网出洞报告，危害等级显示为“高”，漏洞类型则是“解，这则关于12306的漏洞报告，危害登记显户资料大量泄漏”，这意味着，这个漏洞将有可

事件背景 漏洞信息 事件经过 乌云报告 官方提醒 更多 >

网易邮箱数据泄漏事件 - 百度百科

乌云漏洞报告平台宣布发现漏洞，此漏洞将导的交易证明数据、邮箱账号、密码、用户密保

网易报告 网易回应

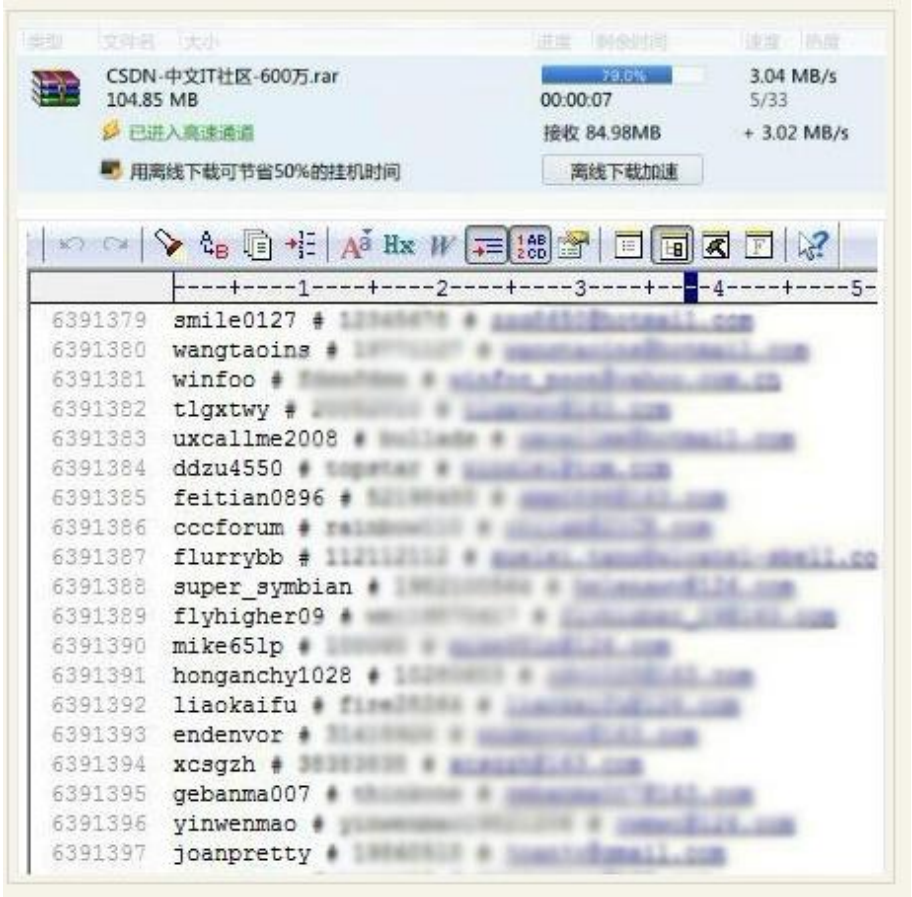
百度百科

京东数据泄露门 - 百度百科

京东数据泄露门是指2016年12月10日晚，京东一个12G的数据包开始在黑市流通，其中包括用户名、密码、邮箱、QQ号、电话号码、身份证等多个维度，数据多达数千万条。事件经过 2016年12月10日晚，据一本财经报道，近期一个12G的数据包开始...

事件经过 官方回应 背景信息

- 2011年12月，CSDN（中国软件开发者联盟）数据泄露，黑客在网上公开了CSDN用户数据库，高达600多万个明文的注册邮箱账号和密码外泄；



➢数据泄露的原因：

Web应用程序存在漏洞（SQL注入攻击、XSS跨站脚本攻击、CSF跨站请求伪造攻击….）——软件安全

数据库存储：明文存储关键信息

【公告】致CSDN会员的公开道歉信

2011-12-21 20:41 | 185044次阅读 | 来源：CSDN【已有1275条评论】发表评论
关键词：csdn | 作者：CSDN | 收藏这篇资讯

尊敬的CSDN会员：

我们非常抱歉，近日发生了CSDN用户数据库泄露事件，您的用户密码可能被公开。我们恳切地请您修改CSDN相关密码，如果您在其他网站也使用同一密码。请一定同时修改相关网站的密码。

再次向您致以深深的歉意！

关于CSDN网站用户帐号被泄露的声明：

CSDN网站早期使用过明文密码，使用明文是因为和一个第三方chat程序
程序员始终未对此进行处理。一直到2009年4月当时的程序员修改了密码
码。

但部分老的明文密码未被清理，2010年8月底，对帐号数据库全部明文密
且我们升级改造了CSDN帐号管理功能，使用了强加密算法，解决了CSD
题。

小米论坛数据泄露

username	password	email	ip
[redacted]	201e4a5117cf97f1ba83984c68a611d2:109027	[redacted]34163@bbs_ml_as_uid.xiaomi.com	hidden
[redacted]shengmi	bee886a8f78ec7b0e540e31446696f90:e05807	[redacted]309045@bbs_ml_as_uid.xiaomi.com	124.193.221.166
[redacted]4	baeffb479c4711447d5a4bf704a9b623:ac1f38	[redacted]0076@bbs_ml_as_uid.xiaomi.com	124.193.221.166
[redacted]z	c9eb7cc483672a5dddd9ac9510ffafca:2ec61c	[redacted]0089@bbs_ml_as_uid.xiaomi.com	72.52.124.158
[redacted]milan	875154143d09041f8690085b918bb677:23cdd9	[redacted]0028@bbs_ml_as_uid.xiaomi.com	114.246.64.34
[redacted]dexter	1a6330d387e5e38bfe2a01b6b670dccc:8ae148	[redacted]ndexter@163.com	123.123.4.61
[redacted]er	405a074509e8b7207489ae1ba06ae506:b67683	[redacted]0055@bbs_ml_as_uid.xiaomi.com	222.130.129.169
[redacted]留	4e4d49914f42e6c86c719059a3d6c000:2a4870	[redacted]0037@bbs_ml_as_uid.xiaomi.com	124.193.221.166
[redacted]e	f9d0b93c57fd38b133d654327f8b43e1:fe986e	[redacted]fe329@hotmail.com	124.193.221.166
[redacted]长	c58dc8e45e5b8045bd956e7ea300dcbb:db2f13	[redacted]0004@bbs_ml_as_uid.xiaomi.com	124.193.221.166
[redacted]la	d16ed15da31fcc8787ac93cb98b4ff73:9899fb	[redacted]0002@bbs_ml_as_uid.xiaomi.com	124.193.221.166
[redacted]tail	79dfd747835baa18686542597fe07899:cbb226	[redacted]0108@bbs_ml_as_uid.xiaomi.com	218.121.97.148
[redacted]	ecf5aa7a91b89b745af03a8ed7f50984:49a092	[redacted]4117@bbs_ml_as_uid.xiaomi.com	124.193.221.166

DBMS安全性控制

➢DBMS安全性控制方法有哪些?

保护数据库中的数据，防止不合法的使用，造成数据泄露、篡改和破坏

1. 身份认证:
2. 访问控制
3. 审计
4. 视图
5. 加密

DBMS安全性控制

- DBMS安全性控制方法有哪些?

保护数据库中的数据，防止不合法的使用，造成数据泄露、篡改和破坏

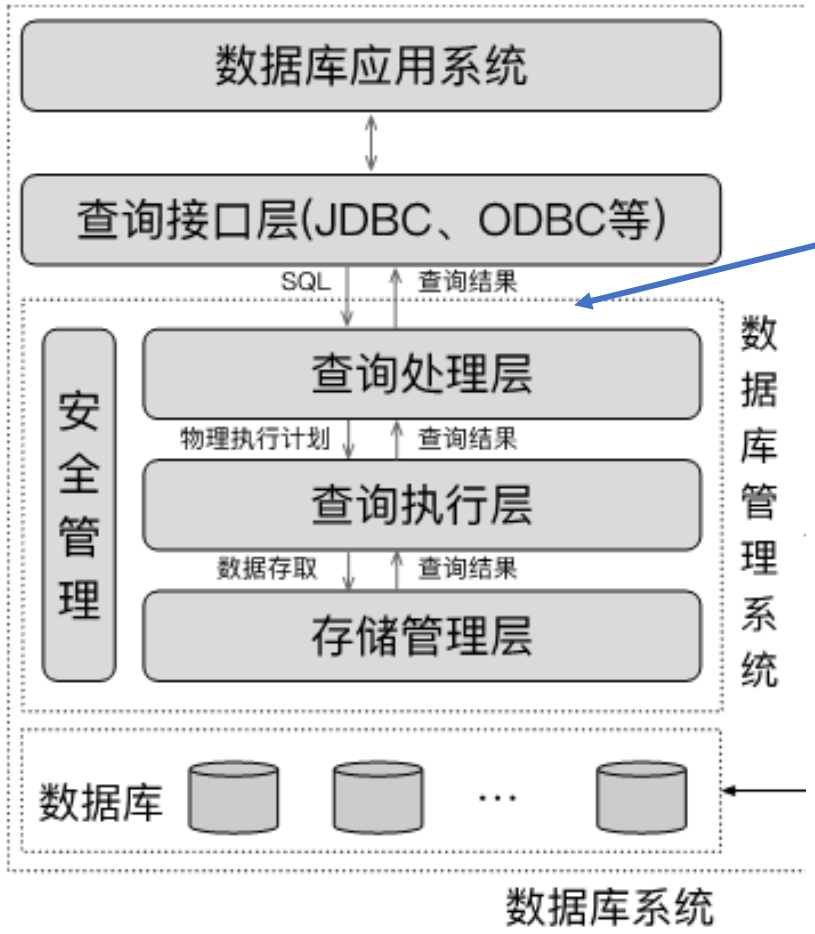
1. 身份认证：证明你是谁?

用户名/password

生物认证

身份证：数字证书

- **1）身份认证**



SQL客户端工具

SQLserver：SQL Server Management Studio

MySQL：Navicat

Oracle： Navicat 、SQLPlus

OpenGauss：gsql、DataStudio

GaussDB：DAS、gsql、 Navicat

- **1）身份认证**

本地登录：username/password (user：数据库的用户)

远程登录：SHA256/MD5、SSL（安全套接字协议）

```
import psycopg2
#创建连接对象
conn=psycopg2.connect(database="postgres",user=" python_user",password="
python_user@123",host="数据库实例的公网 IP",port=8000)
cur=conn.cursor() #创建指针对象


# 创建表
cur.execute("CREATE TABLE student(id integer,name varchar,sex varchar);")
```

hid_kwzi_eyfxf4gt63

• 2）访问控制

——根据用户的身份，控制用户对数据库中数据的访问权限

- ✓ 主体：提出请求或要求的实体（用户/进程//设备……）
- ✓ 客体：接收主体访问的被动实体（文件/程序/数据库对象……）
- ✓ 控制策略：定义了主体对客体的动作行为，以及客体对主体的条件约束

主体（用户）

- 超级管理员（sys/root/sa/….）
- 数据库拥有者：可以创建DB，成DB owner
- 普通用户
- 安全管理员
- 审计管理员

……

客体

- **数据库对象（？）**
- **不同的数据库对象，对其执行的操作也不同**

数据库对象：指在数据库、Schema、表等数据库对象上执行的操作

对象类型	对象	操作类型
数据库和模式	数据库和模式	CREATE
	基本表	CREATE TABLE，ALTER TABLE
	视图	CREATE VIEW
	索引	CREATE INDEX
数据	基本表和视图	SELECT，INSERT，UPDATE，DELETE，REFERENCES，ALL PRIVILEGES
	属性列	SELECT，INSERT，UPDATE， REFERENCES，ALL PRIVILEGES

授权和撤权

- Grant

```
GRANT <权限>[,<权限>]...
    [ON <关系名> <视图名>]
    TO <用户>[,<用户>]...
    [WITH GRANT OPTION];
```

GRANT SELECT
ON TABLE Student
TO U1;

GRANT ALL PRIVILIGES
ON TABLE Student, Course
TO U2,U3;

授权和撤权

- Grant

```
GRANT <权限>[,<权限>]...
    [ON <关系名> <视图名>]
    TO <用户>[,<用户>]...
    [WITH GRANT OPTION];
```

GRANT UPDATE(Sno), SELECT

ON TABLE Student

TO U4;

GRANT INSERT

ON TABLE SC

TO U5

WITH GRANT OPTION;

授权和撤权

- Revoke

```
REVOKE  <权限>[,<权限>]...
[ON <关系名> <视图名>]
FROM <用户>[,<用户>]... [CASCADE | RESTRICT];
```

REVOKE UPDATE(Sno)

ON TABLE Student

FROM U4;

REVOKE INSERT

ON TABLE SC

FROM U5 CASCADE ;

授权和撤权

- Revoke

```
REVOKE  <权限>[,<权限>]...
[ON <关系名> <视图名>]
FROM <用户>[,<用户>]... [CASCADE | RESTRICT];
```

REVOKE UPDATE(Sno)

ON TABLE Student

FROM U4;

REVOKE INSERT

ON TABLE SC

FROM U5 CASCADE ;

- **授权/撤权（主体对客体的访问权限）**

1）谁有授权/撤权的权限？

2）如何存储主体对客体的访问权限？

- **授权/撤权（主体对客体的访问权限）**

1）谁有授权/撤权的权限?

主体（用户）

- 超级管理员（sys/root/sa/….）
- 数据库拥有者
- 普通用户
- 安全管理员
- 审计管理员

……

- **授权/撤权（主体对客体的访问权限）**

2）如何存储主体对客体的访问权限？

访问控制权限表

授权用户名	被授权用户名	数据库对象名	允许的操作类型	能否转授权
DBA	U1	关系Student	SELECT	不能
DBA	U2	关系Student	ALL	不能
DBA	U2	关系Course	ALL	不能
DBA	U3	关系Student	ALL	不能
DBA	U3	关系Course	ALL	不能
DBA	U4	关系Student	SELECT	不能

- **授权/撤权（主体对客体的访问权限）**

创建USER

CREATE USER <username> [WITH]

[SUPERUSER|**CREATEDB**]

|PASSWORD 'password';

- 例：创建用户、创建数据库、授权

●首先以超级用户system(初始用户)登录，然后创建system2

```
CREATE USER system2
WITH SUPERUSER
PASSWORD '123456';
```

●以超级用户system登录，创建用户U1，U2

```
CREATE USER U1
WITH CREATEDB
PASSWORD ‘123456

CREATE USER U2
PASSWORD ‘123456
```

●以U1用户登录，创建数据库U1DB

CREATE DATABASE U1DB

U1：U1DB的owner

U1：可以在U1DB数据库上创建Schema、Table、View

可以对U2进行授权和撤权

Grant/Revoke

- ✓用户对不同的数据对象有不同的存取权限
- ✓不同的用户对同一对象也有不同的权限
- ✓用户还可将其拥有的存取权限转授给其他用户

——自主访问控制（Discretionary Access Control， DAC）

- 自主访问控制DAC：灵活、安全级别较低（C2）
- 强制访问控制MAC（Mandatory Access Control）：安全级别较高（B1）

——1985年美国国防部正式颁布《可信计算机系统评估准则》（简称TCSEC）

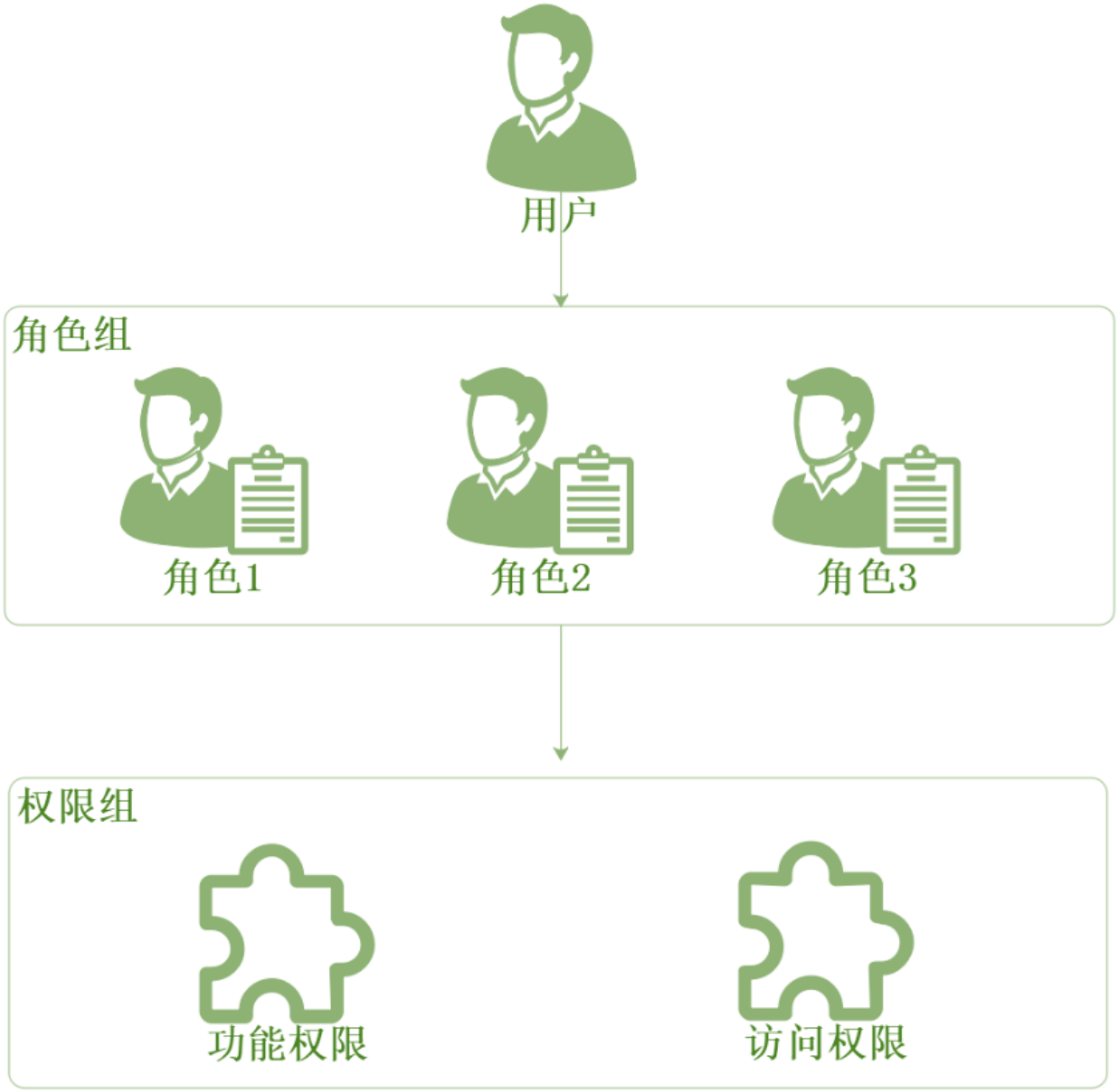
——计算机安全从高到低分为：A、B、C、D四类八个级别）

MAC：

主体：许可证级别

客体： 密级

- **角色（role）**
  - DAC：用户/数据库对象较多的情况下
  - 角色：
    - ✓角色是权限的集合
    - ✓可以为一组具有相同权限的用户创建-
    - ✓简化授权的过程



1）创建角色

CREATE ROLE <角色名>

2）给角色授权

GRANT <权限>[,<权限>]…

ON <对象类型>对象名

TO <角色>[,<角色>]…

3）撤回角色的权限

REVOKE <权限>[,<权限>]…

ON <对象类型> <对象名>

FROM <角色>[,<角色>]…

4）将角色的权限分配给用户或其他角色

GRANT <角色1>[,<角色2>]…

TO <角色3>[,<用户1>]…

[WITH ADMIN OPTION]

GRANT R1

TO U1,U2,U3;

5）将用户从角色中撤回

REVOKE <角色1>[,<角色2>]…

FROM <用户1>[,<角色3>]…

REVOKE R1

FROM U1,U2,U3;

保护数据库中的数据，防止不合法的使用，造成数据泄露、篡改和破坏

1. 身份认证
2. 访问控制
3. 审计
4. 视图
5. 加密

• 3）审计

——启用一个专用的审计日志（Audit Log）

把用户对数据库的所有操作自动记录放入审计日志

监控数据库中的各种行为，找出非法存取数据的人、时间和内容

. AUDIT语句：设置审计功能

. NOAUDIT语句：取消审计功能

• 4）视图

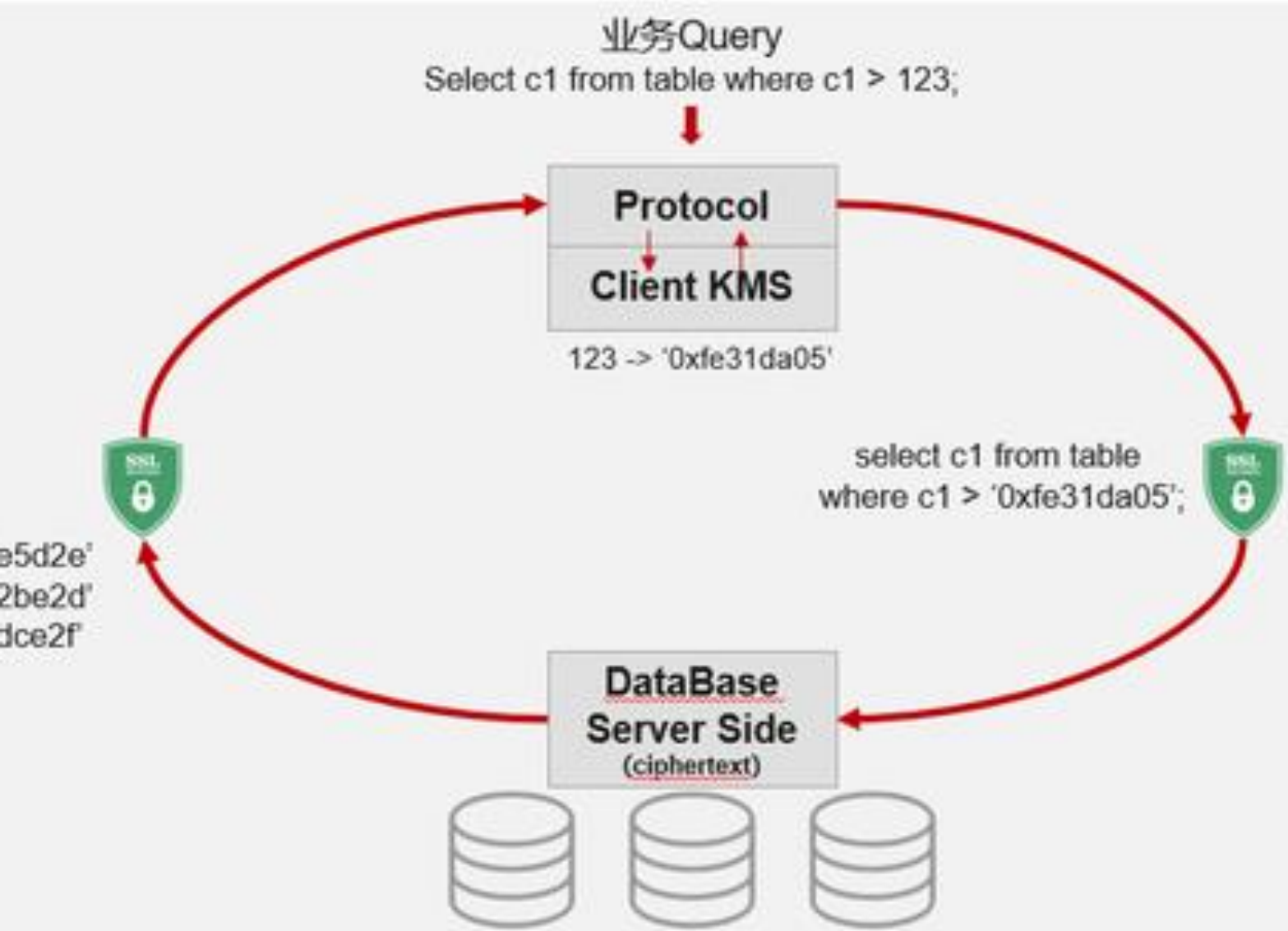
——提供一定的安全性：局部的逻辑结构，隐藏部分属性

对于Student表，U1和U2只能访问“计算机专业的学生”，U1只能查询，U2具有对“计算机专业”学生的所有操作权限

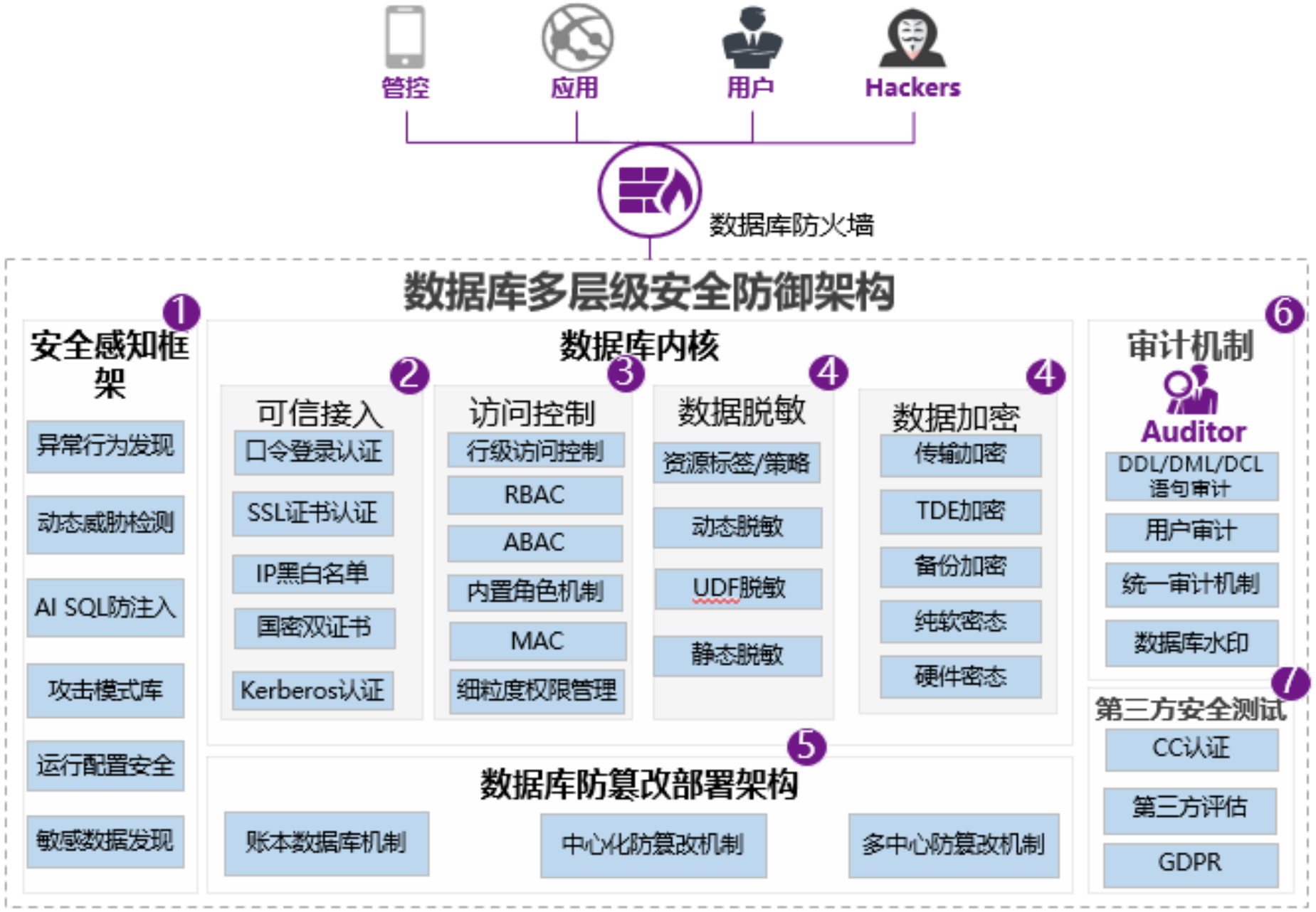
1）创建“计算机专业”学生视图V1

2）将视图V1的select权限授予U1

3）将视图V1的所有操作权限授予U2



id	c1 (plaintext)	c1 (ciphertext)
C10001	256	0xad6e5d2e
C10002	157	0x5892be2d
C10003	97	0x124f4ed2
C10004	685	0x784dce2f
C10005	58	0x324f4ed2



1. 攻不破
2. 进不来
3. 拿不走
4. 看不懂
5. 改不了
6. 赖不掉
7. 信得过

6．对下列两个关系模式：学生（学号．姓名，年龄，性别，家庭住址，班级号）班级（班级号，班级名，班主任，班长）使用 GRANT 语句完成下列授权功能：

（1）授予用户 U1 对两个表的所有权限，并可给其他用户授权。

（2）授予用户 U2 对学生表具有查看权限，对家庭住址具有更新权限。

（3）将对班级表查看权限授予所有用户。

（4）将对学生表的查询、更新权限授予角色 R1。

（5）将角色 R1 授予用户 U1，并且 U1 可继续授权给其他角色。