数据库系统概论新技术篇

数据库安全

秦 波

中国人民大学信息学院

2017年5月

数据库安全

Contents

目录

数据库安全事件频发

- 2011年，黑客在网上公开了某知名程序员网站的用户数据库，大量明文注册邮箱账号和密码遭到曝光和外泄。随后，多个论坛的网站相继被曝出用户数据遭到泄密。这是中国互联网历史上一次具有深远意义的数据库安全事故。
- 2016年11月底，某金融平台用户数据泄露。所泄露数据内包含用户详尽的个人身份信息、亲友联系方式、甚至包括大量学生的学籍资料。
- 2016年12月初，某电子商务平台用户数据因软件漏洞导致泄露，数据包括用户名、密码、邮箱、QQ号码、电话号码、身份证等多个维度，数量多达数千万条。
- 2016年12月中旬，美国著名互联网门户网站雅虎宣布，该公司发现大规模黑客攻击事件，导致10亿用户账号在2013年8月被盗。这是有史以来最大规模的数据库安全事件。

数据库安全事件频发

- 美国洛杉矶一家医院的计算机系统在2016年初遭到了黑客的入侵。成功入侵之后，黑客便将医院计算机系统中的文件进行了加密，并且向医院索要了三百四十万美金(9000个比特币)来解锁这些数据信息。原因主要是该医院的计算机系统感染了勒索软件，勒索软件通过加密文件锁定了医院的系统，导致医院电脑无法正常工作。医院的管理层因为担心恶意软件继续传播而一度禁止医院员工开启电脑，于是雇员被迫使用纸和笔来进行日常办公，并且用传真机来代替电子邮件。但是在此次事件中，病人没有受到影响，但一些急症病人被转移到了其它医院以接受治疗。根据《洛杉矶时报》的报道，为了尽快恢复计算机的正常工作，医院无奈选择了支付赎金，但医院只支付了40个比特币(约1.7万美元)。截止到2016年12月，总共有十四家医院遭受过勒索软件的侵害。

数据库安全

Contents

目录

1.1 数据库安全需求

数据库安全需求之一：访问控制

确保只有有资格的用户获得访问数据库的权限，其他未被授权的人员无法访问数据。主要通过身份识别和存取控制实现。

数据库安全需求之二：真实性

确保只有有资格的用户获得访问数据库的权限，其他未被授权的人员无法访问数据。主要通过身份识别和存取控制实现。

数据的准确性、可靠性和防止数据被篡改。

数据库安全需求之三：有效性

确保只有有资格的用户获得访问数据库的权限，其他未被授权的人员无法接近数据。主要通过身份识别和存取控制实现。

包含数据的可用性和可生存性：能够阻止非法用户试图对数据库的破坏，并且能够对已经损坏的数据库进行及时的修复。常用的办法有数据加密和数据备份。

数据的准确性、可靠性和防止数据被篡改。

数据库安全需求之四：可审计性

确保只有有资格的用户获得访问数据库的权限，其他未被授权的人员无法接近数据。主要通过身份识别和存取控制实现。

包含数据的可用性和可生存性：能够阻止非法用户试图对数据库的破坏，并且能够对已经损坏的数据库进行及时的修复。常用的办法有数据加密和数据备份。

数据的准确性、可靠性和防止数据被篡改。

保证对数据库的操作进行跟踪记录，以实现对修改和访问数据库的用户进行追踪，事后进行审计、取证，从而方便追查并防止否认对数据库进行的操作。常用办法有审计检测、取证。

1.2 数据库安全策略　之一：身份鉴别

- 定义：确认用户真实身份与其声称的身份是否相符
- 目的：确保合法用户获得数据库的使用权限
- 方法：静态口令鉴别，动态口令鉴别，生物特征鉴别，智能卡鉴别

静态口令鉴别	用户输入口令，与事先存储在数据库中的静态不变的口令进行比较。
动态口令鉴别	口令是动态变化的，即采用一次一密的方法。常用的方式有短信密码与动态令牌。
生物特征鉴别	基于图像处理等技术对生物个体唯一、稳定生物特征如指纹，虹膜，声纹进行鉴别。
智能卡鉴别	智能卡是一种不可复制，具有密码功能的硬件。拥有智能卡就意味着合法的身份。

1.2 数据库安全策略 之二：存取控制

- 定义：对系统内的所有数据规定每个用户对它的操作权限
- 目的：定义并检查用户权限，使数据在合法范围内使用
- 方法：自主访问控制、强制访问控制、角色访问控制

自主存取控制（DAC）	用户对于不同的数据库对象有不同的存取权限，不同的用户对不同对象也有不同权限，允许用户将操作权限传递给其他用户
强制存取控制（MAC）	用户不能更改自己或他人的操作权限，一切操作权限由系统管理员统一分配
角色存取控制（RBAC）	数据权限相同的用户定义为同一角色，系统管理员确定用户角色并分配权限

1.3 数据库安全策略 之三：真实性检测

- 定义：对系统内的所有数据进行数据准确性、可靠性和防篡改等检查
- 目的：防止数据库中存在不正确的数据，防止恶意破坏和非法存取
- 方法：完整性约束，断言，触发器，杂凑运算等

学号	性别	年龄	专业
11001	男	23	计算机
11002	男	21	电子
11003	女	24	生物
11004	男	23	数学
11005	女	22	电子
11006	女	24	通信
11007	男	21	计算机

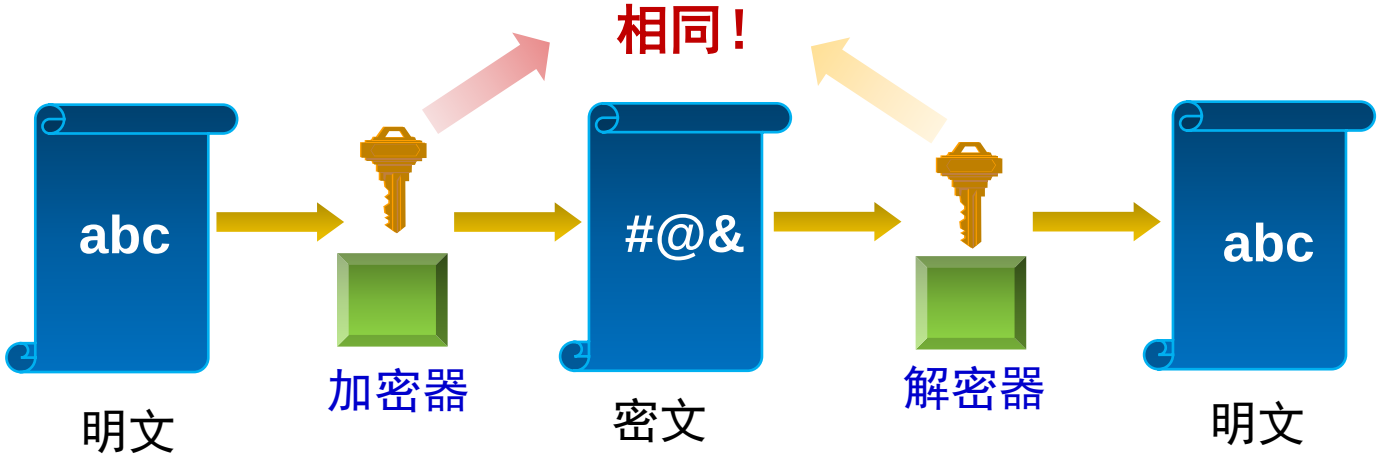
- 新插入的数据为{11003，男，23，计算机}

比较发现，数据库中已经存在学号为11003的同学，插入则造成数据库主码（学号）不唯一，因此拒绝插入该条数据。

1.2 数据库安全策略 之四：数据加密

- 定义：通过算法将明文变换为不可直接识别的密文，合法用户才可解密
- 目的：有效解决数据明文存储引起的泄密风险，防止入侵和越权访问行为
- 方法：私钥加密算法、公钥加密算法

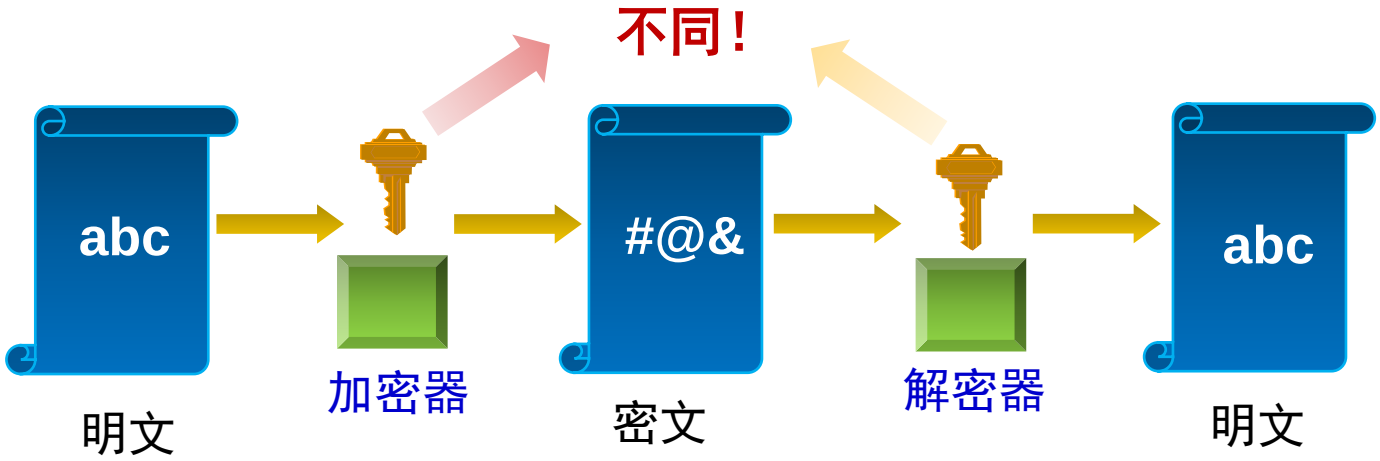
私钥加密：加密和解密的过程中使用相同的密钥，也称单钥加密、对称加密
典型算法：数据加密标准（DES），高级数据加密标准（AES）



1.2 数据库安全策略 之四：数据加密

- 定义：通过算法将明文变换为不可直接识别的密文，合法用户才可解密
- 目的：有效解决数据明文存储引起的泄密风险，防止入侵和越权访问行为
- 方法：私钥加密算法、公钥加密算法

公钥加密：加密和解密的过程中使用不同的密钥，也称双钥加密、非对称加密
典型算法：RSA，ElGamal、椭圆曲线密码算法（ECC）



1.2 数据库安全策略 之四：数据加密

- 定义：通过算法将明文变换为不可直接识别的密文，合法用户才可解密
- 目的：有效解决数据明文存储引起的泄密风险，防止入侵和越权访问行为
- 方法：私钥加密算法、公钥加密算法

数据库级加密	对数据库中的所有表格、视图、索引等都要执行数据加密。易实现，密钥管理简单，但查询效率较低。适合移动存储设备的机密数据加密
表级加密	对数据库中的每一个表格使用专门的函数来进行加密，效率略低，灵活度提高
记录级加密	对数据库中每一条记录使用专门的函数来进行加密，比表级加密有更高的灵活性、查询性能更好。但对单个字段查询需要对整条记录解密。
字段级加密	对表格中的某一个或者几个字段进行加密，适用性和灵活性高，适合频繁查询操作，但字段采用同一密钥加密，攻击者可对比明文获取密文信息。
数据项级加密	对数据库中记录的每个字段采用不同密钥进行加密。安全强度高，抗攻击。但在密钥的管理使用、定期更新方面较复杂。

1.2 数据库安全策略 之四：数据加密

- 定义：通过算法将明文变换为不可直接识别的密文，合法用户才可解密
- 目的：有效解决数据明文存储引起的泄密风险，防止入侵和越权访问行为
- 方法：私钥加密算法、公钥加密算法

- 数据库级加密
- 表级加密
- 记录级加密
- 字段级加密
- 数据项级加密

根据实际情况适当选择加密方法！

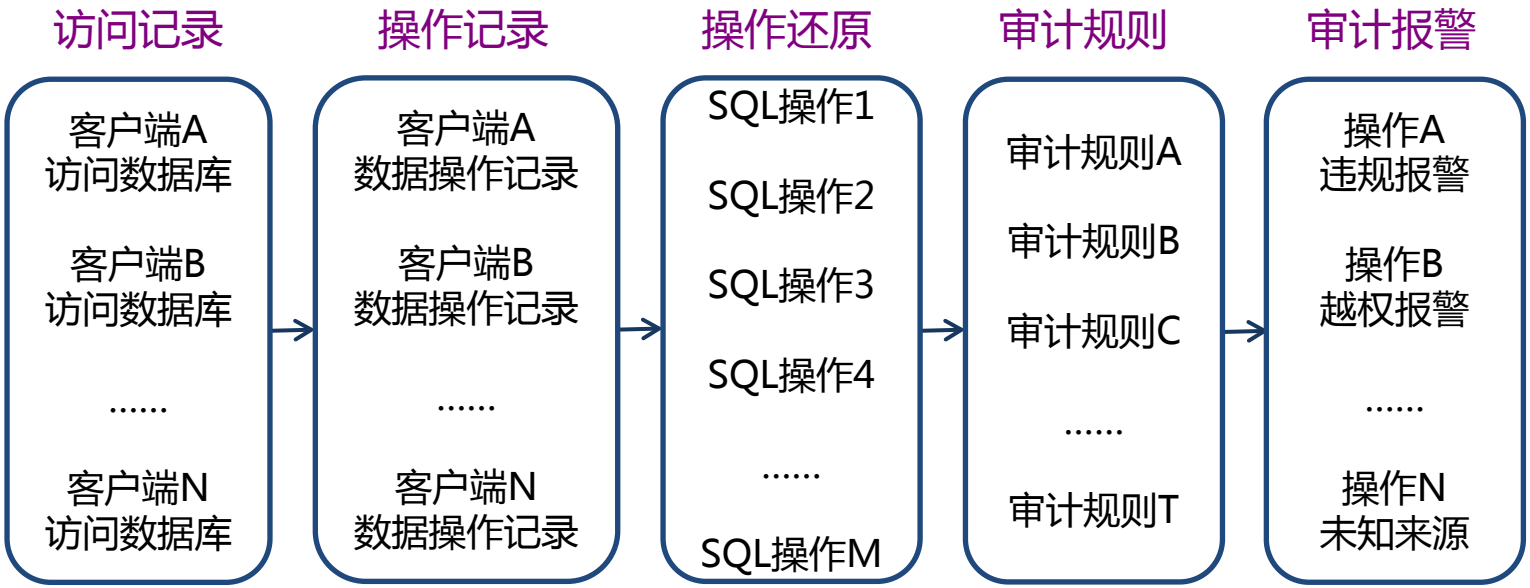
1.2 数据库安全策略 之五：数据备份

- 定义：将数据库中的数据复制到其它存储介质上的过程
- 目的：防止系统出现操作失误或系统故障导致数据丢失
- 方法：全备份，增量备份，差分备份

全备份	按备份周期对整个系统所有的数据进行备份。
增量备份	每次只备份相比于上一次备份后修改过的内容。
差分备份	每次只备份相比于上一次全备份后修改过的内容。

1.2 数据库安全策略 之六：审计检测

- 定义：启用专用的审计日志（Audit Log），记录用户对数据库的操作
- 目的：通过审计日志追踪操作信息，找出非法存取数据的恶意用户
- 方法：本地审计、安全信息和事件管理、数据库活动监控、专门审计平台



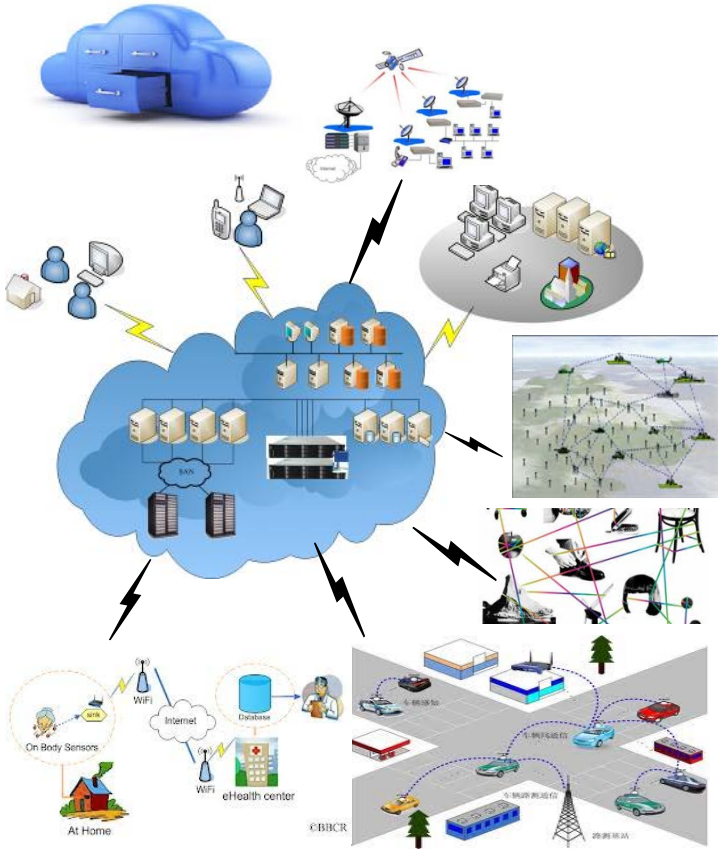
1.3 当前数据库安全挑战

云平台：大数据存储与计算服务

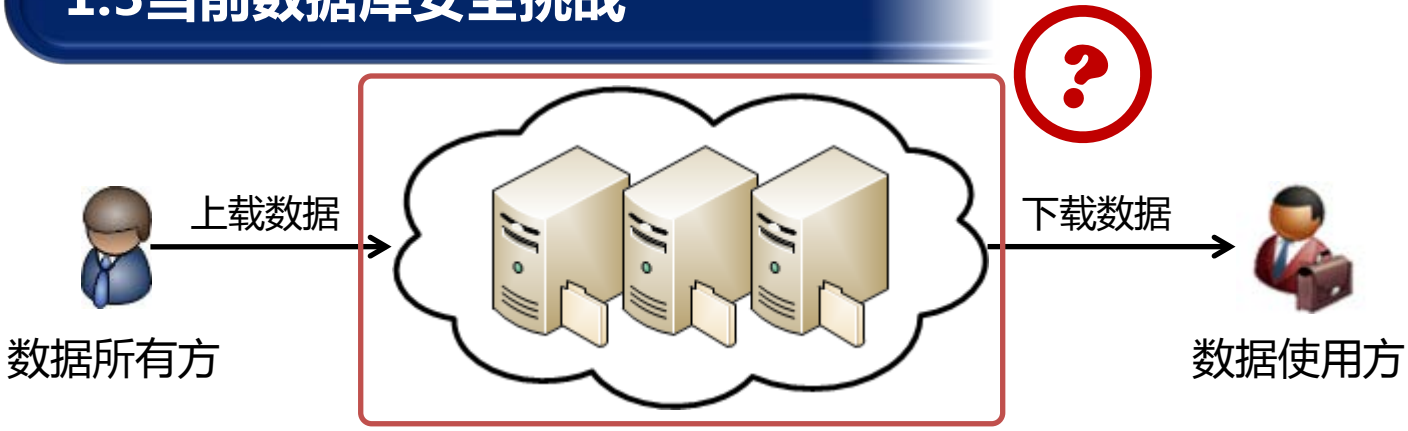
- 由云服务运行商提供服务
- 按需请求存储与计算资源
- 节省数据存储与处理成本
- 无需专业存储与处理能力
- 随时随地获取与处理数据

云发展：市场规模爆发式增长

- 2013年，我国云计算市场规模达到1174.12亿元
- 2015年，我国云计算上下游产值规模超过3500亿元



1.3当前数据库安全挑战

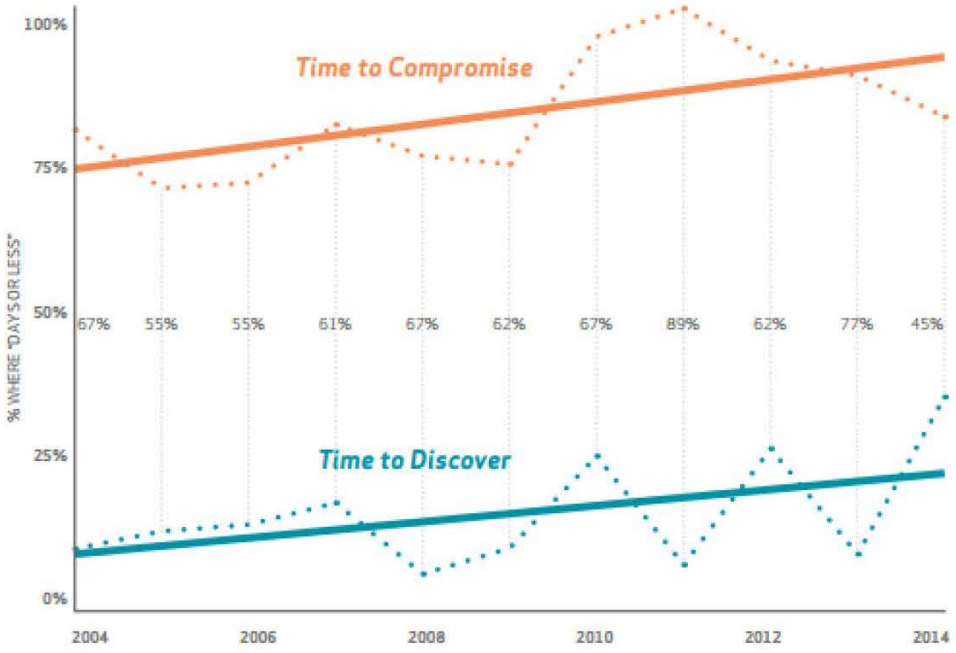


云数据存储平台数据安全与隐私风险

- **个人风险**：云平台中存储了海量敏感数据，包括用户姓名、身份证号、家庭住址、学历情况、收入情况、社会关系、乃至实时动态信息等。这些信息的泄露将为用户带来安全风险，甚至人身安全风险。
- **商业风险**：中小型企业委托云平台存储和处理商业信息，减轻数据管理负担。敏感商业信息一旦泄露，将对企业造成无法估量的损失。
- **国家风险**：境外势力若获得大量国家公民的敏感信息，极易通过数据分析和数据挖掘技术推测国家战略情报，为国家发展带来战略损失。

1.3 当前数据库安全挑战

针对云平台的攻击中，60%的攻击可在数分钟内窃取云平台中的数据信息



60%

IN 60% OF CASES, ATTACKERS ARE ABLE TO COMPROMISE AN ORGANIZATION WITHIN MINUTES.

数据来源： Verizon Data Breach 2015 report

1.3 当前数据库安全挑战

云存储安全需求	◘ 数据细粒度访问控制需求 用户应可指定数据的访问控制政策，满足安全数据共享 ◘ 数据安全第三方检索需求 在不解密的前提下，用户应允许第三方对数据进行检索 ◘ 数据安全第三方发布需求 用户授权下允许进行数据分析，发布数据保护用户隐私
解决方案	高级数据库安全技术
支撑技术	◘ 加密数据细粒度访问控制 属性加密、谓词加密、函数加密 ◘ 加密数据查询 保序加密、同态加密、可搜索加密 ◘ 隐私保护（统计）数据发布 K-匿名性、L-多样性、差分隐私



谢　谢！