数据库的安全性是指保护数据库以防止不合法的使用造成的数据泄露，更改或破坏。

DBMS对数据库的安全保护方功能是通过四方面实现的，即安全性控制、完整性控制、并发性控制和数据库恢复。

<https://blog.csdn.net/u011589338/article/details/78986703>

方法一、数据库数据加密

数据加密可以有效防止数据库信息失密性的有效手段。通常加密的方法有替换、置换、混合加密等。虽然通过密钥的保护是数据库加密技术的重要手段，但如果采用同种的密钥来管理所有数据的话，对于一些不法用户可以采用暴力破解的方法进行攻击。

但通过不同版本的密钥对不同的数据信息进行加密处理的话，可以大大提高数据库数据的安全强度。这种方式主要的表现形式是在解密时必须对应匹配的密钥版本，加密时就尽量的挑选最新技术的版本。

方法二、强制存取控制

为了保证数据库系统的安全性，通常采取的是强制存取检测方式，它是保证数据库系统安全的重要的一环。强制存取控制是通过对每一个数据进行严格的分配不同的密级，例如政府，信息部门。在强制存取控制中，DBMS所管理的全部实体被分为主体和客体两大类。主体是系统中的活动实体，它不仅包括DBMS 被管理的实际用户，也包括代表用户的各进程。

客体是系统中的被动实体，是受主体操纵的，包括文件、基表、索引、视图等等。对于主体和客体，DBMS 为它们每个实例(值)指派一个敏感度标记。主客体各自被赋予相应的安全级，主体的安全级反映主体的可信度，而客体的安全级反映客体所含信息的敏感程度。对于病毒和恶意软件的攻击可以通过强制存取控制策略进行防范。但强制存取控制并不能从根本上避免攻击的问题，但可以有从较高安全性级别程序向较低安全性级别程序进行信息传递。

方法三、审计日志

审计是将用户操作数据库的所有记录存储在审计日志(Audit Log)中，它对将来出现问题时可以方便调查和分析有重要的作用。对于系统出现问题，可以很快得找出非法存取数据的时间、内容以及相关的人。从软件工程的角度上看，目前通过存取控制、数据加密的方式对数据进行保护是不够的。因此，作为重要的补充手段，审计方式是安全的数据库系统不可缺少的一部分，也是数据库系统的最后一道重要的安全防线。

6 评论