# 【论文】加密技术及其在数据库加密中的应用

摘要：数据库系统作为信息系统的核心，其安全直接影响信息系统的安全。本文简要介绍了加密技术的概念及主要方法，针对数据库系统的特点和安全问题提出数据库系统加密的策略，并对数据库系统加密的相关技术进行了阐述。最后讨论了数据库加密技术存在的局限性。

关键字：加密技术 数据库系统 安全

1、引言

随着因特网的普及和计算机技术的飞速发展，各行各业的信息化程度得到了显著的提高。信息系统已经成为企业、金融机构、政府及国防等部门现代化的重要标志。如何保证现代信息系统的安全是计算机领域面临的一大挑战。数据库系统作为信息的聚集体是信息系统的核心，其安全性对整个信息系统来说至关重要，数据库加密技术成为保障数据库系统安全的基石。

2、加密技术

加密技术主要是为了能够有效地保护数据的安全性，下面简单介绍加密技术的概念及主要算法。

2、1加密的概念

数据加密的基本过程就是对原来为明文的文件多数据按某种算法进行处理，使其成为不可读的一段代码，通常称为“密文”，使其只能在输入相应的密钥之后才恩能够显示出本来内容，通过这样的途径来达到保护数据不被非法人窃取、阅读的目的。该过程的逆过程为解密，即将该编码信息转化成为其原来数据的过程。

2、2数据加密的原理

数据加密就是把数据信息即明文转换为不可辨识的形式即密文的过程，目的是使不应了解该数据信息的人不能够知道和识别。将密文转变为明文的过程(如图1所示)就是解密。加密和解密过程形成加密系统，明文与密文统称为报文。任何加密系统通常都包括如下4个部分：

(1)需要加密的报文，也称为明文P。

(2)加密以后形成的报文，也称为密文Y。

(3)加密(解密)算法E(D)。

(4)用于加密和解密的钥匙，称为密钥K。

加密过程可描述为：在发送端利用加密算法E和加密密钥Ke对明文P进行加密，得到密文Y=EKe(P)。密文Y被传送到接收端后应进行解密。解密过程可描述为：接收端利用解密算法D和解密密钥Kd对密文Y进行解密，将密文恢复为明文P=DKd(Y)。在密码学中，把设计密码的技术称为密码编码．把破译密码的技术称为密码分析。密码编码和密码分析合起来称为密码学。在加密系统中，算法是相对稳定的。为了加密数据的安全性，应经常改变密钥。

图1 数据加密模型

2、3加密的两种主要算法

加密技术通常通常分为两大类：“对称式”和“非对称式”。

对称式加密就是加密和解密使用同一个密钥，通常称之为“Session Key”。这种加密技术目前被广泛采用，如美国政府所采用的DES加密标准就是一种典型的“对称式”加密法，它的Session Key长度为56Bits。

非对称式加密就是加密和解密所使用的不是同一个密钥，通常有两个密钥，称为“公钥”和“私钥”，她们两个必须配对使用，否则不能打开加密文件。这里的“公钥”是指可以对外公布的，“私钥”则不能，只能由持有人一个人知道。它的优越性就在这里，因为对称式的加密方法如果是在网络上传输加密文件及很难把密钥告诉对方，不管用什么方法都有可能被窃听到。而非对称式的加密方法有两个密钥，且其中的“公钥”是可以公开的，也就不怕别人知道，收件人解密时只要用自己的私钥就可以，这样就很好的避免了密钥的传输安全性问题。

3、加密技术在数据库加密的应用

加密技术的应用是多方面的，例如电子商务、VPN、数据库系统等，下面主要介绍加密技术在数据库加密中的应用。

3、1数据库加密的特点

数据库是大量、持久、结构化数据的集合，数据的存储、管理和使用都有自身特点，不适合像一般文件存储加密那样对整个文件加密。与传统的数据加密技术相比，数据库存储加密系统有自身的特点和要求。构建数据库有两种基本方式：硬件平台是通用计算机系统，即数据库专用计算机，数据库直接构建在磁盘上；软件平台是通用的操作系统。数据库存储加密的主要目的是按照用户的要求将敏感数据加密存储，防止非法用户采用其他手段获取数据，同时保证合法用户通过数据加密系统仍然能够正常访问数据。因此，数据库存储加密系统的开发原则应该是：安全，高效，保持数据库特点。

3、1、1快速随机存取

虽然数据库中的数据最终是以文件形式存储在物理介质上，却不能将整个数据作为一个文件来加密。一般情况下，文件是作为一个整体来使用的。传统的文件存储加密从头至尾顺序执行，访问加密文件时再从头至尾进行解密。而数据库操作最小单位是一个数据元素，该元素是数据库文件中随机的一段；同时，数据库文件较为庞大，如果每次访问数据库都一次全文加/解密，则执行速度很慢，以致数据库实际不可用。因此数据库加密必须解决对数据库文件快速随机存取问题和最小操作粒度的数据加/解密问题。

为了快速的查询、更新数据，数据库管理系统通常有一系列快速随机存取的方法，这些方法的实现基于存储数据的模型和描述应用数据的元数据。关系数据库中，组织存储数据的模型就是系统表。系统表是保证数据库管理系统正常工作的数据信息。

关系数据库所使用的关系语言是高度的非过程化的，用户不必请求数据库管理员为其建立特殊的存取路径，存取路径的选择是由DBMS自动完成的。这是关系数据库的主要优点之一。因此，在关系数据库存储加密系统中，沿用数据库管理系统对存储数据的定位和维护功能，是实现快速随机存取数据库文件的一个好办法。

3、1、2存储容量

数据库存储数据量大、存储时间长，这给敌方破译加密数据带来一定的有利条件。因此，数据库存储加密必须采用高强度的算法，同时要保证密钥定期更换。由于数据存储量大，应尽量避免加密造成的数据长度增加，防止数据库存储容量大幅度膨胀。

3、1、3一次一密

数据库中的数据是结构化的。因此，必须保证加密后的数据仍然是结构化的。同时，由于数据库中数据的结构化存储，同一字段的数据类型(长度、值域)和逻辑含义相同，这便于破译者分析密文数据结构，获得大量相同密文，从而利用统计规律获得明文。数据数存储加密也应采取“一次一密”。因此，这里的“一次一密”与传输加密的一次一密不同，是指每个加密单位采用不同的密钥。对于实现最小操作粒度的加密来说，就是一个数据元素一个密钥。保证即使明文中同段值重复出现，对应的密文也各不相同。

3、2数据库加密的方法

3、2、1加密粒度的选择

数据库加密的粒度一直是一个令人困扰的问题。一般来讲，数据库加密的粒度可以有三种：表、记录和数据项。

(1)表级加密：表级加密是在表一级进行加密，加密解密的对象是整个表。这种加密方法完全是照搬操作系统中文件的加密方法，用于数据库的加密显然是不合适的。

(2)记录级加密：记录级加密是在表一级上进行，即记录加密方法。它将数据库中的记录看成操作对象，统一作加密解密处理。这种方法比第一种能更好地保证数据的安全，使用时较为方便，但其灵活性不高。

3、2、2加密算法的选择

密码算法在早期有序列算法，移位算法等。当前，加密技术通常通常分为两大类：“对称式”和“非对称式”。如DES就是一种对称密钥算法，而RSA是一种公开密钥算法。选择合适的加密算法是很重要的，其加密强度应能满足系统安全需要，但要考虑加密结果是否符合数据约束条件，存储会不会造成额外负担；对加密速度的要求则是不应该对系统性能产生明显影响，响应时间越短越好。同时，对应用系统的用户来说，数据库加解密过程应该是透明的，不能影响合法用户的正常操作。数据库加密要求加密效率要尽可能的高，以DES算法为代表的对称密钥加密算法则是简单高效，适合进行数据库加密，不过由于DES密钥长度过短，随着计算机运算能力的增强和密码分析技术的发展，DES将会由AES替代。而以RSA算法为代表的公开密钥加密算法加密强度较高，但算法复杂，效率较低，但由于它的非对称加密的特点，可以用它来对AES加密的密钥进行加密保护，这样用户只要保证自己的私钥安全，在保证加密信息安全性的同时，大大简化了加密数据库的密钥管理。

3、2、3数据类型的转换

数据库中的数据是以结构化方式存储的，各种类型的数据有其特定的格式、长度、值域。如果要将加密后的数据仍然存储在原来的表(简称明表)中，则必须保证加密后数据的格式、长度、值域都仍然保持不变。这样的要求对于加密算法来说是难以达到的。于是我们将各种类型的数据以统一的格式加密，并存储在一张表(简称密文表)中，对数据进行查询和更新操作时，再将密文表中所操作的各字段数据根据加密字典“属性信息表”中相应的类型进行转换。

3、2、4密钥的管理

数据库具有高度共享的特点，数据库中数据信息长期存储，反复加密解密，相应地密钥也需要长期存储，宜采用共享密钥机制。数据库加密的主要目的在于防止非法用户通过非法途径获得明文数据，而仍要保证任何合法用户可以通过合法渠道获得解密数据。所以，密钥共享机制一方面要求加密算法的绝对保密和一定的强度，另一方面则要求密钥的共享是一定范围和程度的，不是任何人都可以无条件地获得密钥。

1、 密钥管理体制应该具备的特性

首先，密钥难以被窃取。

其次，一定条件下窃取了密钥也是没有用的，密钥的使用范围和时间有一定的限制。 再者，密钥的分配和更换过程对用户透明，用户不一定要亲自掌管密钥。

2、 密钥管理方式

层次化的密钥管理方式，用于数据加密的工作密钥需要动态产生：工作密钥由上层的加密密钥进行保护，最上层的密钥称为主密钥，是整个管理系统的核心；多层密钥体制大大加强了密码系统的可靠性，因为用得最多的工作密钥时时更换，而高层密钥的数量有限，使得破译的难度大大提升。

3、3 数据库加密的局限性

数据库加密技术在保证安全性的同时，也给数据库系统的可用性带来一些影响

3、3、1系统运行效率受到影响

加密技术带来的主要问题之一是影响效率。为了减少这种影响，一般对加密的范围做一些约束，如不加密索引字段和关系运算的比较字段等。

3、3、2对数据的SQL语言及SQL函数受到制约

SQL语言中的Group by、Order by及Having子句分别完成分组和排序等操作，如果这些子句的操作对象是加密数据，那么解密后的明文数据将失去原语句的分组和排序作用。另外，DBMS扩展的SQL内部函数一股也不能直接作用于密文数据。

3、3、3难以实现对数据完整性约束的定义

数据库一般都定义了关系数据之间的完整性约束，如主／外键约束及值域的定义等。数据一旦加密，DBMS将难以实现这些约束。

3、3、4密文数据容易成为攻击目标

加密技术把有意义的明文转换为看上去没有实际意义的密文信息，但密文的随机性同时也暴露了消息的重要性，容易引起攻击者的注意和破坏，从而造成了一种新的不安全性。加密技术往往需要和其他非加密安全机制相结合，以提高数据库系统的整体安全性。

4、总结

随着计算机技术的飞速发展，数据库的应用十分广泛，深入到各个领域，越来越多的资源与信息被放入数据库供大家使用，但随之而来产生了数据的安全问题。数据库系统作为信息的聚集体，是计算机信息系统的核心部件，其安全性至关重要。关系到企业兴衰、国家安全。因此，如何有效地保证数据库系统的安全，实现数据的保密性、完整性和有效性，已经成为人们探索研究的重要课题之一。目前除了数据库的安全性以外，最有效的方式就是对数据库内的数据进行加密储存。这样即使有非法入侵者能进入到数据库窃取到密文数据，由于解密技术相对复杂，他们也不能轻易得到其明文资料，因此能在很大程度上保护数据的安全，可以说数据加密是数据安全的最后一道防线，也是最后可用的安全手段。数据库加密技术作为一种对数据进行安全保护的有效手段，将起到越来越重要的作用。

参考文献

1、 吴晓春 《加密技术概念、加密方法以及应用详解》 中国科技信息2006.3 17-18

2、 林斯 《数据库加密策略及相关技术研究》 科技创新导报 2009 34

3、 陈云 《数据库加密系统相关技术研究》 硅谷

4、 周碧英 张鹏 《数据库加密技术的实现与加密方法》 内肛科技 2008.2 119

5、 陈铁英 陈华 刘瑜 《基于三层次的数据库加密应用系统》 华中科技大学学报（自然科

学版）2005.7 41-46