文章编号:1671-4598(2017)05-0184-04 DOI:10.16526/j.cnki.11—4762/tp.2017.05.051 中图分类号:TP309.2 文献标识码:A

基于网络的数据库敏感数据加密模型研究

李自清
(青海民族大学物理与电子信息工程学院,青海 西宁 810007)

摘要:在互联网飞速发展的今天,Web 技术与数据库技术的结合越来越紧密,所以保护数据库的安全成为了信息安全十分重要的一环。在网络环境下,应采用什么样的机制来为用户提供对数据的产生、存储和访问,以及如何有效地保证其中的数据安全性,就成为迫切需要研究的课题。加密技术对数据库中存储的高度敏感机密性数据,起着越来越重要的作用,是防止数据库中的数据在存储和传输中失密的有效手段,所以完全可以用于模型。为了保护互联网中的敏感数据,提出了数据库中敏感数据的加密模型,基于对数据库敏感数据的分析、数据分类,通过加密引擎、密钥管理、失效密钥处理,将用户敏感数据形成密文存储在数据库之中。这样即使是数据库管理员也无法轻易获取用户敏感信息,在因为攻击等问题造成的数据泄露之后也可以减少系统损失,最大限度保证数据库中数据的安全性。实验结果表明该模型可以有效保护数据库中敏感数据安全。

关键词:信息安全;信息过滤;数据分类;密钥管理

Research of Database Sensitive Data Encryption Model Based on Web

Li Ziqing
(School of physics and electronic information engineering, Qinghai University for Nationalities, Xining 810007, China)

Abstract: With the rapid development of Internet, the combination of Web technology and database technology is more and more closely, so the security of database security has become a very important part of information security. In the network environment, what kind of mechanism should be used to provide users with the generation, storage and access to data, and how to effectively ensure the safety of data, it becomes an urgent need to study the issue. High sensitive and confidential data encryption technology in the database storage, plays an increasingly important role, is the effective means to protect confidential data in the database in the storage and transmission, so can be used to model. In order to protect sensitive data in the Internet, put forward the model of encryption of sensitive data in the database, the database analysis, sensitive data classification based on the encryption engine, key management, key processing failure, the user sensitive data stored in the data base in the form of ciphertext. So even the database administrator can not easily obtain sensitive information from the user. After the attack caused the leakage of data it can also reduce the loss of system, ensure the security of data in the database to maximize. The experimental results show that the proposed model can effectively protect the security of sensitive data in database.

Keywords: information security; information filtering; data classification; key management

0 引言

随着互联网的不断发展,它带来的便利深入到我们生活的方方面面,极大地便利了我们的生活。

但是这种便利的背后,也带来了很大的风险:我们的个人信息时时遭受着泄露威胁。现在许多 Web 应用经常使用数据库来对信息进行管理与存储,所以为了保护用户的个人信息,数据库安全就成了当今信息安全十分重要的一环。数据库通常使用身份认证、访问控制、审计跟踪和加密等手段来保证数据安全[1]。其中加密是对数据库中敏感数据的一种特殊处理,即使用一定算法将原来数据库中的敏感数据进行各种代替和变换,使其变为不可识别的格式,这样不知解密方法的人便无法正确识别数据的内容,从而保护了数据库中的敏感数据。

加密算法可分为对称加密算法和非对称加密算法两种,其中较广泛使用的对称加密算法有 1977 年由当时的美国国家标准局,即现在的国家标准与技术协会提出的数据加密标准(DES),和旨在取代 DES,由美国国家标准与技术研究院发布的高级加密标准(AES)[2]。加密算法需要使用密钥,密钥作为加密算法的输入是独立于明文与算法的,因为使用密钥的不同而导致产生的输出密文也会不尽相同,所以我们不需要对加密算法进行保密操作,仅需要对密钥进行保护,就可以达到保护敏感数据的目的。

本文基于以上情况,提出了一种较为安全的数据库敏感数据加密模型,以求最大限度保护数据库中数据的安全。

1 安全风险分析及安全需求说明

1.1 安全风险分析

数据库安全主要指数据库中的信息不会被非法修改或删除,指数据库中的数据保持了完整性、一致性、可用性与保密性等。数据库遭受的威胁主要有:物理威胁,例如水灾、火灾、地震等因素对数据库存储硬件的破坏而造成的数据的破坏与丢失[3];逻辑威胁,例如信息泄露、非法修改等对数据库中数据的人为破坏。

其中逻辑威胁经常带来巨大损失。为了获取数据库中信息,黑客经常利用 web 程序漏洞对数据库进行攻击[4];而且数据泄露也常常发生在内部人员之中,大量相关人员接触敏感数据,导致人员管理问题变得十分困难,因此敏感数据面临的泄露风险也十分巨大。目前对数据库的防护措施主要由防火墙、白名单、协议加密、身份认证、授权管理与审计追踪等方

收稿日期:2016-11-28; **修回日期**:2017-01-05。
基金项目:教育部"春晖计划"合作科研项目(S2015037)。
作者简介:李自清(1975-),男,硕士,讲师,主要从事计算机应用技术方向的研究。

法来保证数据库的安全[5]，但是由于系统中的漏洞、编程人员的疏忽或者内部人员的窃取等问题导致数据库中敏感数据还是时时处在威胁之中。

1.2　安全需求说明

Web 应用面对着各种各样的威胁，大量的用户每天对应用进行大量的访问，大量的数据请求也在不停地发送到相应数据库中，数据库中存储了许多用户与应用的敏感数据，这些数据是不可以被第三方获取的珍贵资料。面对这样的多用户 Web 应用系统，本文提出了一种较为安全的数据库敏感数据加密模型。

（1）因为攻击或者用户的不当操作等原因，数据库经常接收许多非法申请与数据[6]，而且若让应用直接操作数据库，则会有其权限过大的问题，所以为了保护数据库，需要对应用提供接口，用来对用户身份与输入数据库的数据进行一定过滤与验证，这样既可以保护数据库安全，又可以减少不当操作，提高效率。

（2）为了保护数据库中的敏感数据，数据加密是一种十分有力地手段。这种方法可以有效地解决内部人员窃取和泄露的数据安全问题。本系统将数据分为三类：公有数据、敏感数据与私人数据，对不同种类的数据进行不同处理，以提高加密效率。

（3）因为不需对加密算法进行保密处理，密钥的管理变得十分的关键，一旦密钥泄露，其他人就可以根据泄露的密钥解密出加密数据，所以安全地保管密钥对于加密是十分重要的。同时因为密钥也有生命周期[7]，它的更新、存储与销毁都需要进行合理管理，有效的密钥管理可以进一步加强数据库的安全性，保护数据安全。

根据以上需求，本模型通过使用用户数据传输接口对用户的身份与输入的数据进行验证与过滤，设计了一种安全有效的数据库加密引擎，合理的密钥管理模块，保护了数据库中的敏感数据的安全性，增加了数据库的风险抵抗能力。

2　数据库敏感数据加密模型

本文提出了一种针对数据库敏感数据进行加密的加密模型，模型由用户数据传输接口模块、加密引擎模块与密钥管理模块组成，将输入的数据分为三类：公有数据、敏感数据与私人数据，编写数据字典与用户权限表，用以区分数据与密钥的对应关系。

2.1　用户数据传输接口模块

用户或系统提交的数据首先经过用户数据传输模块，此模块提供接口供用户输入数据。本模块首先根据用户权限表对用户的身份与权限进行验证，对合法的用户输入的数据进行正则对比与过滤，保证用户输入的数据有效且正确，例如验证身份证或手机号码的格式、过滤敏感关键字，防止 sql 注入等。将合法的输入交给下一模块——加密引擎模块，若发现用户权限不足或者不合法输入，则返回统一提示，隐藏错误信息，不给出具体描述，防止攻击者利用错误信息猜测数据库结构从而对数据库进行攻击。

2.2　加密引擎模块

根据数据字典与用户权限表中指定的不同类型进行分别处理：公有数据即不需要加密的数据，可以直接存储到数据库中，从而减少加密操作与密钥数量，加快系统处理速度；敏感数据则需要经过加密算法进行加密，保证其不可以被第三方获取；私人数据则使用用户的私人密钥进行加密，保证不同用户间的数据不可以相互查看，保护数据的隐私性。针对三种数据的不同操作既可以保护数据库中数据安全，同时又可增加系统运行效率。

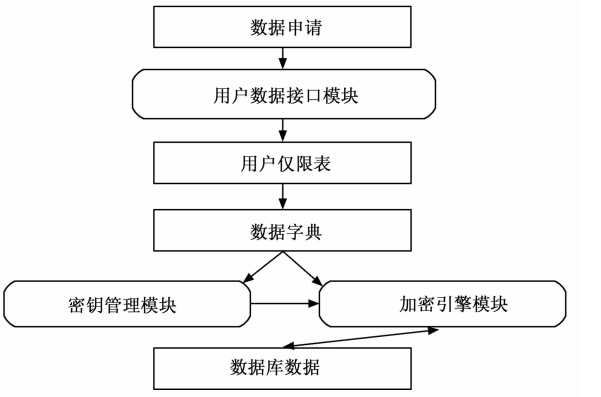

图 1　数据库敏感数据加密模型

2.3　密钥管理模块

因为数据分为三类，其中需要加密的两类数据会产生许多密钥，本模块根据数据字典与用户权限表来确定与管理每个加密数据所使用的加密密钥，使用二级密钥管理的方式来管理每个密钥。因为密钥也存在生命周期，对它的生成、更新、存储与销毁的不同生命周期需要进行有效的管理，以确保密钥的安全性和有效性。敏感数据根据数据字典与用户权限表来查找密钥进行加密，这些密钥称为数据密钥，而数据密钥则使用根密钥进行加密后存储；私人密钥则分成两部分，一部分由用户保存，另一部分同样使用根密钥加密后存储在数据库中，从而达到保护数据库中数据安全的目的。

3　数据库敏感数据加密模型详细设计

3.1　用户数据传输接口模块

本模块针对用户输入提供统一接口，首先验证用户身份与权限，再对输入数据进行过滤，返回统一提示信息。在本模块中首先根据用户权限表对用户身份与权限进行验证，验证合法后再根据业务流程对输入进行统一验证，查看是否符合系统要求，之后再对符合要求的输入进行关键字比对，例如包含 update、delete 等关键字[8]的输入不被允许通过，防止 sql 注入的发生。只有通过过滤的数据才会提交给下一模块进行处理，如果用户身份不合法或者输入数据没有通过验证，则对用户进行统一信息反馈，防止数据库错误提示的泄露，从而保护数据库中信息的安全。

3.2　加密引擎模块

通过检验的数据将被交给加密引擎模块分类进行加密，之后再将密文数据存入数据库中。下面首先介绍本模型使用的算法：

3.2.1　AES 加密算法

AES 加密算法属于对称加密算法，对称加密算法根据对明文的加密方式不同可分为分组密码与流密码[9]，AES 加密算法就属于分组密码，它的输入输出都按 128 比特来进行分组，在使用循环结构迭代加密，使用字节替换、行移位、列混

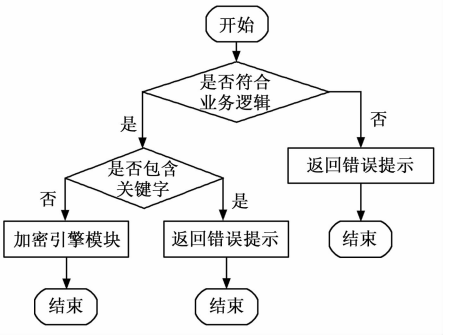

图 2 用户数据过滤工作流程

合和轮密钥加来达到加密的效果。加密输入的密钥会经过密钥扩展模块被扩展成为 128 比特、192 比特或者 256 比特再进行加密运算。

若用 X 代表加密前输入的明文，Y 代表加密后输出的密文，加密操作可表示为：$Y=A_{k_{r+2}}\otimes R\otimes S\otimes(A_{k_j}\otimes C\otimes R\otimes S)\ r\otimes A_{k_{j1}}(X)$。

其中：A 为轮密码加运算，k 为此轮的子密码，因为总共进行 $r+2$ 轮，所以子密码有 $K1$、$K2$、……、$K(r+2)$ 共 $r+2$ 个。S、R、C 分别指字节替换、行移位与列混合运算，中间共重复 r 次，最后再进行一次字节替换、行移位与第 $r+2$ 个子密码进行轮密码加运算即可产生加密后的密文。

3.2.2 加密引擎模型

数据库数据可表示为集合 $D=\{d_1、d_2、……、d_n\}$[10]，本文将数据分为三类：公有数据、敏感数据和私人数据，他们经过用户数据传输接口模块过滤后传到加密引擎模块进行不同加密处理，敏感数据使用数据密钥 $K=\{k_1、k_2、……、k_n\}$，私人数据使用私人密钥，私人密钥是每个用户私有的，可表示为集合 $U=\{u_1、u_2、……、u_n\}$。

(1) 公有数据。

可以被所有人获取的数据，即不需要加密的数据，它在此模块直接交给数据库进行储存。

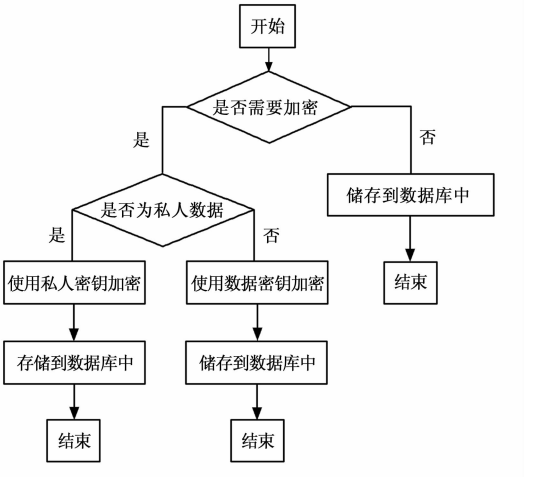

图 3 加密引擎模型

(2) 敏感数据。

即针对系统内部用户可以共享，但对非系统用户需要保密的数据，它不需要针对不同用户进行分别加密，只需要防御系统外部人员，所以本系统根据数据字典的设定，使用数据密钥来对数据进行加密。加密的粒度选择直接决定了数据库的安全性与密钥的数量，加密粒度越细安全性则越高，同时密钥数量也会越多[11]，虽然一次一密可以保证理论上加密不可破解，但会产生数量庞大的密钥，增加管理难度，所以合适的粒度选择也是个十分关键的问题。本系统不设定统一的加密粒度，具体情况根据数据字典的预先设定动态加密，这样可以根据不同数据的使用频率与危险等级等标准来设定不同加密粒度，在加强保护数据安全的情况下，尽量减少密钥数量，减少密钥管理难度。

操作敏感数据时首先根据申请加密的字段名称去密钥管理模块查询此敏感数据所对应密钥，然后使用 AES 加密算法进行加密，即将明文 X 加密处理后产生密文 Y，表示为 $Y=AES(D,K)$，之后再将密文 Y 储存在数据库中。

(3) 私人数据。

这类数据是用户自己的私人信息，除了自己不想被其他人获取的信息，即只有用户自己可以查看自己的信息，其他用户的信息对其是保密的。私人数据同样使用 AES 加密算法与私人密钥进行加密处理，产生密文 Y 并存储起来。加密时首先根据数据字典与用户权限表查询用户的私人密钥，它是由用户口令与系统随机生成的字符串拼接而成，用户口令由用户自己设置与保管，随机生成的字符串则由根密钥加密后储存在数据库中。使用时用户输入口令，与数据库中保存的随机字符串解密后拼接成私人密钥。过程可以描述为：$Y=AES(D,U)$，其中：U=用户口令+随机字符串。

3.3 密钥管理模块

本模型采用二级密钥管理的方式，使用数据字典与用户权限表管理数据与密钥关系，储存在数据库中的密钥会使用根密钥进行相应加密后储存，保证管理员也无法获取密钥，从而保护了数据的安全。

表 1 数据字典结构

属性	是否可以为空	说明
字段	否	加密字段名称
所属表格	否	字段所说表格
所属类型	否	数据所属三类中的哪一类的说明
约束	是	是否根据条件划分更仔细加密粒度
密钥	否	储存的数据密钥或者私人密钥所属用户
有效期	是	密钥有效期到期时间
备注	是	其他备注信息

3.3.1 密钥的查找与生成

在加密引擎模块，每当需要对敏感数据进行加密时，首先都需要查询加密所需使用的密钥。在操作敏感数据时，根据提交申请的数据名称，首先去数据字典查找相应数据密钥，使用根密钥解密数据密钥后再对敏感数据进行加解密操作。

私人密钥是在用户注册时，由用户自己设定的口令与系统随机生成的字符串拼接而成的，用户口令由用户自己保存，而随机字符串则由系统自动生成后用根密钥加密后存储在用户权限表中。操作私人数据时根据数据字典与用户权限表查找用户自己的私人密钥，用根密钥解密后再对数据进行加解密操作。

3.3.2 密钥的更新与销毁

密钥也有生命周期，其存在的时间越长，所遭受的泄露风险也就越大，而且 Web 应用每时每刻都有许多用户进行访问

与操作，数据量通常十分庞大。针对这个特性，本系统对不同密钥设定不同有效期，通过数据字典设定的密钥有效期定时对已有的密钥进行扫描更新，从而确保密钥的安全性。因为本模型是将密钥分为数据密钥、根密钥与私人密钥的二级密钥管理方式，根据密钥的种类不同，更新分为以下几种情况：

（1）数据密钥。

敏感数据使用数据密钥进行加密，根据数据字典的设置，其中会存在多个密钥，这些密钥使用根密钥加密后存储在数据库中，使用时再解密取出。所以根据数据字典中设定的不同有效期，定期对不同等级的密钥进行扫描更新，更新时将此密钥相关的数据一次性取出解密，再使用新密钥进行加密存储，新密钥使用根密钥加密后，替换旧密钥存储在数据库中，以供下次使用。

（2）私人密钥。

为了保护私人数据的安全性，需要使用私人密钥对其进行加密，为了保证加密的安全性，需要密钥保证一定长度，但是用户一般无法记住一个太长的口令，所以本系统将用户自己设定的一个口令与系统自动生成的随机字符串拼接形成私人密钥，这样既保证了密钥的长度，同时也没有增加用户的使用难度。随机生成的字符串也由根密钥进行加密后存储在用户权限表中，在用户更新自己的口令的时候，系统也会自动更新随机字符串，然后根据数据字典与用户权限表对此用户的私人数据进行一次性更新，储存根密钥加密后的随机字符串，替换私人密钥存储在数据库中的部分，即一次性更换用户私人密钥。

（3）根密钥。

因为数据密钥与私人密钥的一部分都是由根密钥进行加密后存储的，这样即使管理员也无法获得真正的密钥，从而保护的数据的安全。但是这样根密钥的储存就变得十分关键了，一旦根密钥泄露，则其他密钥的加密也就失去了作用，数据就会暴露在危险之中。所以根密钥需要定时进行更新，因为根密钥加密的对象也是密钥，数据量相对于数据库库中的数据少很多，所以根密钥更新时可使用一次性更新的方式，即同时取出所有密钥进行解密，使用新根密钥加密更新的操作。

3.3.3　密钥的存储

密钥生成与更新后，都需要存储起来以供之后使用。但一旦处理不好使密钥泄露则可造成灾难性的后果，这相当于数据库中的数据加密失去了意义，得到密钥的黑客只要得到敏感数据，就可以对其进行解密操作，得到具体信息，用户重要的信息就会泄露。为了防止这种事情的发生，我们需要对密钥进行严密的管理，防止密钥泄露。

本系统使用的数据密钥与私人密钥存储的部分都使用根密钥进行过加密，可以直接储存在数据库中而保证不泄露，所以根密钥的保存就至关重要了，为了防止攻击者获得根密钥，它可以储存在物理令牌中，由专人保管，防止泄露。

4　数据库敏感数据加密模型评测

4.1　可行性分析

本系统为了保护数据库安全设计了一个针对敏感数据的加密模型，通过用户数据接口模块、加密引擎模块与密钥管理模块共同作用保护了数据库中的数据安全。

首先用户数据接口模块针对用户身份合法性与输入的数据进行了过滤，即保证了业务上的数据完整性与可用性，又减少了 sql 注入的风险，保护了数据库中的数据安全。

加密引擎模块首先将数据分为三类，公有数据不需加密，极大减少了系统开销，增加了系统运行速度；敏感数据需要根据数据字典进行加密，从而在庞大的系统数据中减少使用的密钥数量，减少系统开销，同时避免黑客攻击或内部人员对数据的窃取；私人数据需要使用用户口令与系统生成的随机字符串拼接的私人密钥进行加密，使用数据字典与用户权限表来对应密钥与数据的关系，从而保证仅用户本人才可以看见数据内容。

密钥管理模块使用二级密钥管理的方式，提供对密钥的查询与生成、更新与销魂和存储操作，根据数据字典中设置的不同有效期定时扫描，对密钥进行一次性更新，替换失效旧密钥。这些密钥管理方式共同保护了密钥的安全，使得加密更加安全可靠。

所以本系统可以有效保护数据库中数据的机密性、完整性与可用性，同时兼顾系统开销，减少密钥数量，从而减少密钥管理难度，是种安全的数据库敏感数据加密模型。

4.2　实验

4.2.1　实验环境

本文涉及的加密模型主要使用了 AES 加密算法，将数据分为三类分别进行了处理，使用二级密钥管理的方式，既保证了敏感数据的安全性，同时也兼顾了系统的开销。

因为 Web 应用经常会一次性取出几条数据进行各种处理，其中可能包含多个字段数据。而且要是单纯使用 AES 加密算法对 Web 应用进行加密，要保证加密的安全性，使数据内容不会轻易泄露，一次一密是非常保险的方式。本模型根据数据库特性，使用 java 语言及相应方法库模拟了单纯使用 AES 加密算法一次一密的加密数据方式与使用本模型加密数据的方式，用以对比对数据库中数据进行加密所用时间与模型效率。具体环境参数如下。

表 2　数据库敏感数据加密模型实验环境

环境	参数
主机参数	Windows7、64 位操作系统、8G 内存
编程环境	JDK 1.6.0_13
编程工具	MyEclipse10.7
编程语言	Java

分别取出数据库中某张表的 30 条与 60 条数据，每条数据 3 个字段，即总共 90 个与 180 个数据项，设定每个数据项都需要进行加密。同时设定有 2 个用户，数据字典预先设定的信息如下。

表 3　实验数据字典设定

字段	所属表格	所属类型	约束	有效期
字段 1	表 1	敏感数据	UserId＝1	2016.12.01
字段 1	表 1	敏感数据	UserId＝2	2016.12.01
字段 2	表 1	私人数据	UserId＝1	
字段 3	表 1	私人数据	UserId＝2	

4.2.2　实验结果

使用 AES 加密算法采用一次一密的方式加密所有数据项，再使用本模型根据以上数据字典对数据分类进行加密，记录每次的加密运行时间，多次运行汇总出了如表 4 所示。

（下转第 191 页）

相对误差率逐渐增大，预测精度逐渐降低。通过该实验结果可知该预测算法对于短期的航天器遥测数据的预测是有效的。由于该预测算法所采用的预测模型属于线性模型，而卫星主母线电压参数具有非线性的特点，所以该预测算法对于短期内遥测数据预测的拟合度较高，而对于长期的预测精度较低。

6　结论

通过上述分析表明，上述算法对航天器遥测数据在未来短时期内的发展趋势的预测是有效的。由于航天器长期运行在复杂的空间环境中，遥测数据不仅会受到外部空间环境的影响，同时也会受到自身工作环境等内在因素的干扰，从而导致一些遥测数据具有强烈的非平稳变化趋势。对于非线性的遥测参数，该算法的拟合度较低，参数的估计精度还有待进一步提高。今后的研究中可以结合 BP 网络算法等方法对该算法不断优化，提高该方法对于遥测数据长期的预测精度。

参考文献：

[1] 孙　健. 在轨航天器遥测数据在线预测系统分析与设计 [D]. 北京：北京邮电大学，2013.

[2] 闫　坤. 基于时间序列模型的分析预测算法的设计与实现 [D]. 北京：北京邮电大学，2008 (5).

[3] 肇　刚，李言俊. 基于时间序列数据挖掘的航天器故障诊断方法 [J]. 飞行器测控学报，2010 (3)：1－5.

[4] 张金玉，张　炜. 装备只能故障诊断与预测 [M]. 北京：国防工业出版社，2013.

[5] 罗凤曼，时间序列预测模型及其算法研究 [D]. 成都：四川大学，2006.

[6] 王咪咪，时间序列 ARMA 模型的贝叶斯分析 [J]. 科技信息，2011：568.

(上接第 187 页)

表 4　运行时耗对比

加密方式	30 条数据运行时耗/s	60 条数据运行时耗/s
AES 加密算法	0.393	0.502
本模型敏感数据加密	0.189	0.247
本模型私人数据加密	0.212	0.266
本模型整体加密时间	0.401	0.513

针对以上表格，可以看出 AES 加密算法与本模型的数据加密总时耗接近，虽然 AES 加密算法需要在加密每个数据项时产生新的密钥并存储，但是本模型则需要查找相应密钥并返回，所以在加密时间本模型总加密时间会多一点。其中敏感数据只需要查询数据字典来确定密钥，所以所需时间相对短一点；而私人数据则需要同时查询数据字典与用户权限表两张表，所以会更耗时一些，但是因为总体加密时间不会增加太多，所以系统效率的降低在可接受范围内。

单纯使用 AES 加密算法一次一密的加密方式产生了 90 个与 180 个密钥，而本系统不受数据量的影响只有 4 个密钥，远远小于单纯使用 AES 加密算法一次一密加密的密钥数量，在密钥管理方面节省了大量空间与时间。

本模型中敏感数据根据数据字典动态选用加密粒度，不仅可以减少密钥数量，减轻密钥管理的负担，因为密钥的读取的时耗也是常数级的，也不会大量增加系统运行时间。私人数据部分由用户自己保管，减少了密钥泄露的可能性，从而保证私人数据不会被第三者获知，保护其隐私性。三类数据与二级密钥管理的方式大大提高了数据库的安全性，在系统耗时增加可以接受的情况下，节省了查询时间与存储空间。

4.3　模型评测

本系统开销较小，相对于单纯使用 AES 加密算法一次一密加密的方式时耗增加不多，密钥管理更加方便，可以更好地对数据库中敏感数据进行保护。用户数据接口模块也降低了应用的所承受的压力，将一部分数据过滤交由后台处理，对 sql 注入进行了一定过滤。数据分类方式大大减少系统开销，对私人密钥分割的方式也增加了私人数据的安全性，而根据数据字典动态选取加密粒度的方式不仅增加了安全性，也减轻了密钥管理的复杂度，在保证数据安全性的前提下，减轻了系统负担，增加了可行性。密钥管理模块的的二级密钥管理方式，对储存在数据库中的密钥进行加密，同时将根密钥储存在物理令牌中，保护了密钥的安全，从而保证数据库敏感数据的安全性。

但是为了保证加密效果，数据字典的预先设定十分重要，所以需要事先设定一个考虑全面的数据字典，这是对数据库设计者的一个挑战。

5　结论

本文提出了针对敏感数据的数据加密模型，该模型使用了用户数据接口、加密引擎与密钥管理模块来对数据进行分类处理，根据数据字典与用户权限表确定数据与密钥的对应关系，采取根据数据字典动态选择加密粒度加密的方式，使用二级密钥管理的方式，对密钥采用定时扫描，一次性更新的方式，解决了敏感数据的加密与密钥管理问题，实验数据表明本模型的时耗增加是可接受的，密钥管理则便利许多，节省许多存储密钥的空间，数据库的安全性也得到了保证，保护了数据库中的敏感数据的安全。

参考文献：

[1] 胡　敏. Web 系统下提高 MySQL 数据库安全性的研究与实现 [D]. 北京：北京邮电大学，2015.

[2] 张金辉. AES 加密算法分析及其在信息安全中的应用 [J]. 信息网络安全，2011，05 (5)：31－33.

[3] 李卫平，张天伍. 数据库加密模型设计探讨 [J]. 煤炭技术，2012，31 (6)：217－218.

[4] 吴翰清. 白帽子讲 Web 安全 [M]. 北京：电子工业出版社，2014.

[5] 成晓利. Web 应用 SQL 注入漏洞测试系统的研究与实现 [D]. 成都：西南交通大学，2013.

[6] 李绍武. 试析计算机网络数据库存在的安全威胁和应对措施 [J]. 通讯世界，2014，18 (09)：32－33.

[7] 吴开均. 数据库加密系统的设计与实现 [D]. 成都：电子科技大学，2014.

[8] 常红梅. 基于存储过程的数据库安全性实践初论 [J]. 网络安全技术与应用，2015，4 (4)：112－112.

[9] 盖玉莲. 加密技术在数据库安全中应用研究 [J]. 计算机科学研究，2009，12 (51)：81－84.

[10] Fonseca J，Seixas N，Vieira M，et al. Analysis of Field Data on Web Security Vulnerabilities [J]. IEEE Transactions on Dependable & Secure Computing，2014，11 (2)：89－100.

[11] Fonseca J，Vieira M，Madeira H. Evaluation of Web Security Mechanisms using Vulnerability and Attack Injection [J]. IEEE Transactions on Dependable & Secure Computing，2014，11 (5)：440－453.