(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 102855448 B
(45)授权公告日 2016.02.10

(21)申请号 201210284801.6

(22)申请日 2012.08.10

(73)专利权人 深圳市黎明网络系统有限公司
地址 518053 广东省深圳市南山侨香路4060号香年广场A座302-2室
专利权人 深圳市商通信息技术有限公司

(72)发明人 邓一辉 龚智辉

(74)专利代理机构 深圳中一专利商标事务所 44237
代理人 贾振勇

(51)Int.Cl.
G06F 21/62(2013.01)
G06F 17/30(2006.01)

(56)对比文件
US 2002/0129260 A1,2002.09.12,说明书第0013-0037段,图2.
EP 1667396 A1,2006.06.07,全文.
CN 101504668 A,2009.08.12,全文.
CN 101504706 A,2009.08.12,全文.

审查员 张剑峰

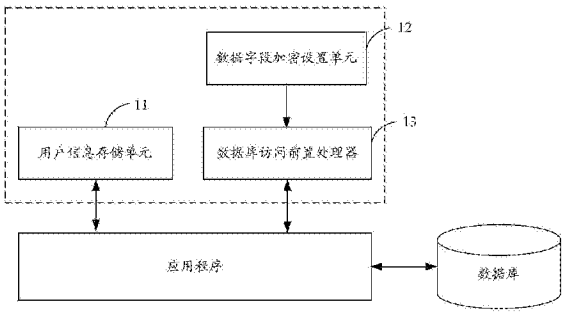
权利要求书1页 说明书5页 附图2页

(54)发明名称

一种字段级数据库加密装置

(57)摘要

本发明适用于信息安全领域,提供了一种字段级数据库加密装置,包括:用户信息存储单元,用于存储经用户公共密钥加密后的数据库加密对称密钥;数据库字段加密设置单元,用于设置数据库中的字段是否加密;以及数据库访问前置处理器,用于根据解密后的数据库加密对称密钥和所述数据库字段加密设置单元中的字段加密设置信息,对数据库访问语句进行加密转换或解密转换。通过本发明实施例,用户可以根据不同加密强度的需要选取数据库系统所支持的不同的对称加密算法,应用程序不需要对数据库进行加密和解密操作,所有的数据加解密操作由数据库系统来完成,可以支持数据项的全文检索功能,原有的数据库访问语句不需要进行变更处理,直接透明使用。



CN 102855448 B

1. 一种字段级数据库加密装置，其特征在于，所述装置包括：

用户信息存储单元，用于存储经用户公共密钥加密后的数据库加密对称密钥；

数据库字段加密设置单元，用于设置数据库中的字段是否加密；以及

数据库访问前置处理器，用于根据解密后的数据库加密对称密钥和所述数据库字段加密设置单元中的字段加密设置信息，对数据库访问语句进行加密转换或解密转换；

其中，所述对数据库访问语句进行加密转换或解密转换，具体为：

根据应用程序的数据库结构化查询语言 SQL 语句的种类对 SQL 语句进行加解密转换处理；

如果 SQL 语句是读语句，则所述数据库访问前置处理器查询数据库字段加密设置单元，查看数据库中哪些字段加密，则利用数据库加密对称密钥 Kdb 将 SQL 语句转换为解密语句，返回应用程序；

如果 SQL 语句是写语句，则所述数据库访问前置处理器查询数据库字段加密设置单元，查看数据库中哪些字段需要加密，则利用数据库加密对称密钥 Kdb 将 SQL 语句转换为加密语句，返回应用程序；

如果 SQL 语句是其他的数据库管理语句，则所述数据库访问前置处理器对 SQL 语句保留，不做处理，返回应用程序。

2. 如权利要求 1 所述的字段级数据库加密装置，其特征在于，所述数据库加密对称密钥采用数据库系统所支持的加密算法设置。

3. 如权利要求 1 所述的字段级数据库加密装置，其特征在于，所述装置还包括：

全局加密开关，用于设置数据库是否加密。

4. 如权利要求 1 所述的字段级数据库加密装置，其特征在于，所述用户信息存储单元和数据库字段加密设置单元采用数据表方式。

一种字段级数据库加密装置

技术领域

[0001] 本发明属于信息安全领域，尤其涉及一种字段级数据库加密装置。

背景技术

[0002] 数据库是现代软件系统中数据存储的重要方法，数据库中所存储的数据往往是用户敏感的数据，加密成为保护数据信息不被泄露的重要手段。

[0003] 目前，对于存储在数据库中的数据，根据数据性质的不同往往采用两种不同的加密的方式。

[0004] 一种加密方式是不可逆的加密方式。这种方式对明文数据进行数据散列运算获得数据的特征值，将特征值存储到数据库中，明文数据不存储。由于存储的数据仅仅保存数据的特征值，所以数据是不可还原的，具有比较大的局限性，只能用于一些特殊的数据类型，例如用户密码往往都采用这种方式来进行存储，目的用于验证用户密码的特征值。

[0005] 另外一种加密方式是可逆的加密方式，对明文数据采用加密算法进行加密，并采用相应的解密算法可以将数据解密。这种方式不会有上一种方式的局限，对各种数据都可以进行加密和解密。

[0006] 目前，有各种对称算法和非对称的算法来实现对数据库的加密，但数据加密以后，会给数据库访问的操作带来很多不良影响，包括数据解密的速度、数据字段的检索、数据的搜索、数据的共享访问等。

[0007] 具体而言，存在以下问题：

[0008] 1、性能问题：一般应用中往往采用客户端数据解密的方式，将加密后的数据从数据库取出后进行处理，严重影响数据库访问的性能，在数据记录比较大的情况下，基本不能使用；

[0009] 2、不能进行全文检索：由于数据库存放密文，一般采用将密文取出解密后再进行全文检索，效率比数据库系统直接检索慢，对系统的开销也很大；

[0010] 3、不同的用户不能共享：由于数据采用了用户专用的密钥进行加密，在数据需要共享的场合，则对数据不能加密；

[0011] 4、对字段加密不能设置：对数据库字段的加密与否不能灵活选择，导致数据加密性能问题严重；

[0012] 5、应用系统访问数据库不透明：应用系统需要对数据进行加密和解密的操作，不透明。

发明内容

[0013] 本发明实施例提供一种字段级数据库加密装置，在有效地对数据库数据加密保护的同时，能够保留数据库操作的各种功能。

[0014] 本发明实施例是这样实现的，一种字段级数据库加密装置，所述装置包括：

[0015] 用户信息存储单元，用于存储经用户公共密钥加密后的数据库加密对称密钥；

[0016] 数据库字段加密设置单元，用于设置数据库中的字段是否加密；以及

[0017] 数据库访问前置处理器，用于根据解密后的数据库加密对称密钥和所述数据库字段加密设置单元中的字段加密设置信息，对数据库访问语句进行加密转换或解密转换。

[0018] 通过本发明实施例，用户可以根据不同加密强度的需要选取数据库系统所支持的不同的对称加密算法，应用程序不需要对数据库进行加密和解密操作，所有的数据加解密操作由数据库系统来完成，可以支持数据项的全文检索功能，原有的数据库访问语句不需要进行变更处理，直接透明使用，用户仅仅在数据库操作之前进行数据库访问语句的前置处理。

附图说明

[0019] 图 1 是本发明实施例提供的字段级数据库加密装置的结构图；

[0020] 图 2 是本发明实施例提供的应用程序对数据库进行访问的处理流程图；

[0021] 图 3 是本发明实施例提供的对 SQL 语句进行处理的流程图。

具体实施方式

[0022] 为了使本发明的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本发明进行进一步详细说明。应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

[0023] 在本发明实施例中，采用用户公共密钥对数据库加密对称密钥加密，通过对应用程序的数据库访问语句进行加解密转换，在有效地对数据库数据加密保护的同时，保留数据库操作的各种功能。

[0024] 图 1 示出了本发明实施例提供的字段级数据库加密装置的结构，为了便于描述和理解，仅示出了与本发明实施例相关的部分。

[0025] 用户信息存储单元 11 存储经用户公共密钥 Kup 加密的数据库加密对称密钥 Kdb。

[0026] 在本发明实施例中，利用数据库加密对称密钥 Kdb 对数据库中的字段加密，数据库加密对称密钥由数据库管理员或应用管理员统一设置，其他人员不能修改。

[0027] 本发明实施例中，可以采用高级加密标准（Advanced Encryption Standard，AES）加密算法等数据库系统所支持的加密算法设置数据库加密对称密钥 Kdb，系统管理员可以通过 Web 界面设置一串密码作为密钥。

[0028] 系统管理员设置数据库加密对称密钥 Kdb 时，使用各个用户的公共密钥 Kup 对数据库加密对称密钥 Kdb 加密，存储到用户信息存储单元 11 中。

[0029] 应用程序在使用数据库加密对称密钥 Kdb 时，利用用户的私钥 Kus 将加密后的数据库加密对称密钥 Kdb 解密，就可以获得数据库加密对称密钥 Kdb，然后可以进行后续的数据库字段的加解密操作。

[0030] 每个数据库由若干个数据表组成，每个数据表由若干个数据字段组成。数据库字段加密设置单元 12 用于设置数据库中的字段是否加密。字段的加密设置由系统管理员完成，可以通过前端界面设置。

[0031] 在本发明实施例中，在每个数据库中建立一个数据库字段加密设置单元，设置相应数据库的字段是否加密。

[0032] 数据库访问前置处理器 13 根据解密后的数据库加密对称密钥 Kdb 和数据库字段加密设置单元 12 中的数据库字段加密设置信息对数据库访问语句进行加密转换或解密转换。

[0033] 图 2 示出了应用程序对数据库进行访问的处理流程，详述如下：

[0034] 在步骤 S201 中，使用用户私钥 Kus 解密出数据库加密对称密钥 Kdb；

[0035] 在步骤 S202 中，调用数据访问前置处理器；

[0036] 在本发明实施例中，应用程序在调用数据访问前置处理器 13 时，将解密后的数据库加密对称密钥 Kdb 传递给数据访问前置处理器 13；

[0037] 在步骤 S203 中，使用数据访问前置处理器 13 处理后的数据库访问语句访问数据库，进行相应的操作。

[0038] 本发明实施例中的数据库一般为数据库管理系统(Data Base Management System，DBMS)，可以采用 MySQL，应用程序采用超级文本预处理语言(Hypertext Preprocessor，PHP)，用户端通过浏览器访问，数据库访问一般采用数据库结构化查询语言(Structured Query Language，SQL)。

[0039] 在本发明实施例中，数据库访问前置处理器 13 是一个通用的 SQL 处理程序，根据数据库字段加密设置单元 12 所设置的数据库字段加密设置信息将 SQL 语句进行预处理，形成满足加密和解密需要的 SQL 语句。

[0040] 为了提高处理性能，数据库访问前置处理器 13 通过 C++ 实现。

[0041] 当用户访问数据库中的数据时，应用程序通过用户的登录信息获取用户私钥 Kus，使用用户私钥 Kus 将用户信息存储单元 11 中保存的利用用户公开密钥 Kup 加密后的数据库加密对称密钥 Kdb 进行解密，获得数据库加密对称密钥 Kdb 的明文。

[0042] 应用程序对于每个 SQL 语句，调用数据库访问前置处理器 13，将数据库加密对称密钥 Kdb 的明文传递给数据库访问前置处理器 13，数据库访问前置处理器 13 根据据库加密对称密钥 Kdb 的明文和数据库字段加密设置信息，对 SQL 语句进行加解密处理，向应用程序返回处理后的 SQL 语句，应用程序根据处理后的 SQL 语句对数据库进行访问。

[0043] 如图 3 所示，数据库访问前置处理器 13 根据应用程序的 SQL 语句的种类对 SQL 语句进行加解密转换处理：

[0044] 如果 SQL 语句是读语句，则数据库访问前置处理器 13 查询数据库字段加密设置单元 12，查看数据库中哪些字段加密，则利用数据库加密对称密钥 Kdb 将 SQL 语句转换为解密语句，返回应用程序；

[0045] 如果 SQL 语句是写语句，则数据库访问前置处理器 13 查询数据库字段加密设置单元 12，查看数据库中哪些字段需要加密，则利用数据库加密对称密钥 Kdb 将 SQL 语句转换为加密语句，返回应用程序；

[0046] 如果 SQL 语句是其他的数据库管理语句，则数据库访问前置处理器 13 对 SQL 语句保留，不做处理，返回应用程序。

[0047] 以下通过示例具体说明，假设某用户数据库有一个用户信息存储单元 11，用户名为 bizapp_users，该数据库的字段加密设置信息如下表所示：

[0048]

序号	字段名	数据类型	长度	是否加密
1	id	Int		否
2	name	Varchar	50	是
3	password	Varchar	100	是
4	email	Varchar	200	否

[0049] 数据库访问前置处理器 13 判断应用程序的 SQL 语句的种类：

[0050] 1. 如果为 Select 查询类的 SQL 语句，其对数据库是一个读取的操作，则将该 SQL 语句转换为解密语句：

[0051] 例 如，Select name,mobilephone,email,address FROM bizapp_users WHERE name= ‘thomas’;

[0052] 数据库访问前置处理器 13 通过查询数据库字段加密设置单元 12，假如得到字段“name”和“password”是加密的，数据库加密对称密钥 Kdb 为‘dbpassword’，则将该 SQL 语句转换为：

[0053] SELECT AES_decrypt(name, ‘dbpassword’),AES_decrypt(mobilephone, ‘dbpassword’),AES_decrypt(UNHEX(email), ‘dbpassword’),address

[0054] FROM bizapp_users;

[0055] WHERE AES_decrypt(UNHEX(name), ‘dbpassword’)= ‘thomas’;

[0056] 2. 如果是 Insert 操作的 SQL 语句，则数据库访问前置处理器 13 将该 SQL 语句转换为加密的 SQL 语句：

[0057] 例如，INSERT INTO`bizapp_users`

[0058] SET ‘name’ = ‘thomas’, ‘password’ = ‘123456a’, ‘email’ = ‘gzh@liming.com’;

[0059] 该语句是一个插入记录的语句，对数据库中的数据进行写操作，则将需要加密的字段进行加密处理。如果加密设置与上例 SELECT 时的相同，则该 SQL 语句应该转换为：

[0060] INSERT

[0061] INTO`bizapp_users`

[0062] SET

[0063] `id`=’0’,

[0064] `name`=HEX(AES_ENCRYPT(’thomas’,’dbpassword’)),

[0065] `password`=HEX(AES_ENCRYPT(’123456a’,’dbpassword’)),

[0066] `email`=’gzh@liming.com’;

[0067] 3. 如果是 UPDATE 语句，假设为：

[0068] UPDATE`bizapp_users`SET

[0069] `name`=’martin’,

[0070] `password`=’123456a’,

[0071] `email`=’martin@liming.com’

[0072] WHERE

[0073] `name`=' jason';

[0074] 上述 SQL 语句为有条件的 UPDATE 语句，WHERE 后的表达式是一个读取的过程，使用解密函数，而其他语句是更新数据到数据库中，使用加密函数。所以，数据库访问前置处理器 13 将该语句转换为：

[0075] UPDATE`bizapp_users`SET

[0076] `name`=HEX(AES_ENCRYPT('martin','dbpassword')),

[0077] `password`=HEX(AES_ENCRYPT('123456a','dbpassword')),

[0078] `email`='martin@liming.com'

[0079] WHERE

[0080] AES_DECRYPT(UNHEX(`name`),'dbpassword')=' jason';

[0081] 4. 如果是其他的操作，则数据库访问前置处理器 13 判断 SQL 语句中是否存在加密的字段，如果没有则直接向应用程序返回原来的语句，如果存在加密的字段，则分析加密的字段在 SQL 语句中是读取还是写入。如果是读取，则对字段名进行解密转换，如果是写入，则对字段内容进行加密操作。

[0082] 如下表所示：

[0083]

操作	原 SQL 语句	转换后的 SQL 语句
读取	'Fieldname'	AES_DECRYPT(UNHEX('Fieldname'),'dbpassword')
写入	'Fieldname'='value'	'Fieldname'=HEX(AES_ENCRYPT('value', 'dbpassword'))

[0084] 本发明实施例通过修改底层类实现，对应用程序不需要进行任何修改，直接使用原来的代码进行调用即可。

[0085] 作为本发明的一个实施例，还可以设置全局加密开关，用于设置数据库是否加密。当设置数据库为加密时，查询所有的数据字段加密设置单元，对所有加密字段的数据进行加解密处理。

[0086] 在本发明实施例中，用户信息存储单元 11 和数据库字段加密设置单元 12 采用数据表方式。

[0087] 通过本发明实施例，用户可以根据不同加密强度的需要选取数据库系统所支持的不同的对称加密算法，应用程序不需要对数据库进行加密和解密操作，所有的数据加解密操作由数据库系统来完成，可以支持数据项的全文检索功能，原有的数据库访问语句不需要进行变更处理，直接透明使用，用户仅仅在数据库操作之前进行数据库访问语句的前置处理。

[0088] 以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内所作的任何修改、等同替换和改进等，均应包含在本发明的保护范围之内。

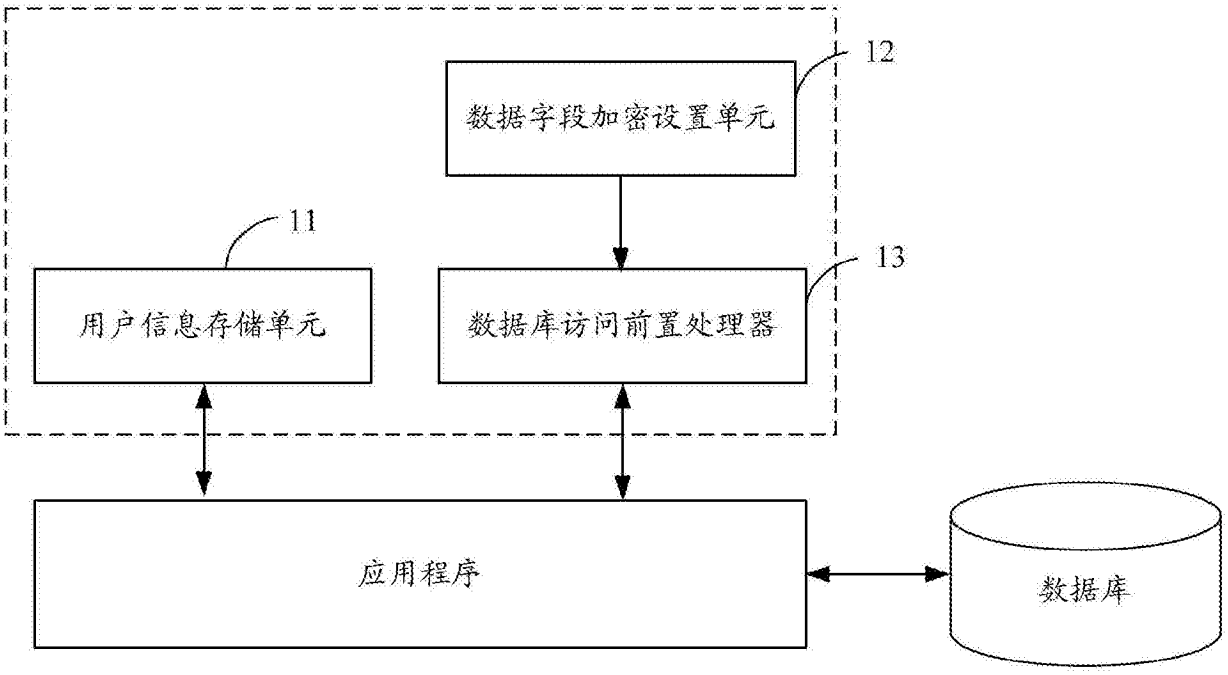

12
数据字段加密设置单元
11
用户信息存储单元
13
数据库访问前置处理器
应用程序
数据库

图 1

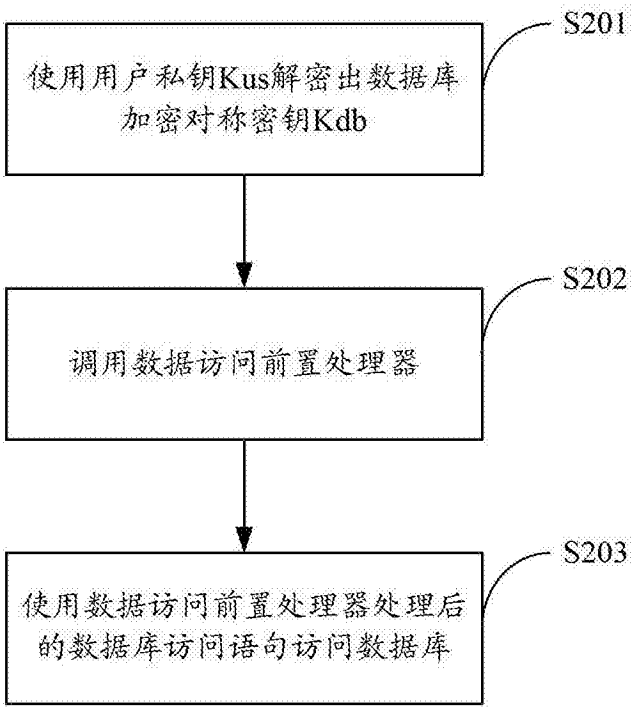

S201
使用用户私钥Kus解密出数据库加密对称密钥Kdb
S202
调用数据访问前置处理器
S203
使用数据访问前置处理器处理后的数据库访问语句访问数据库

图 2

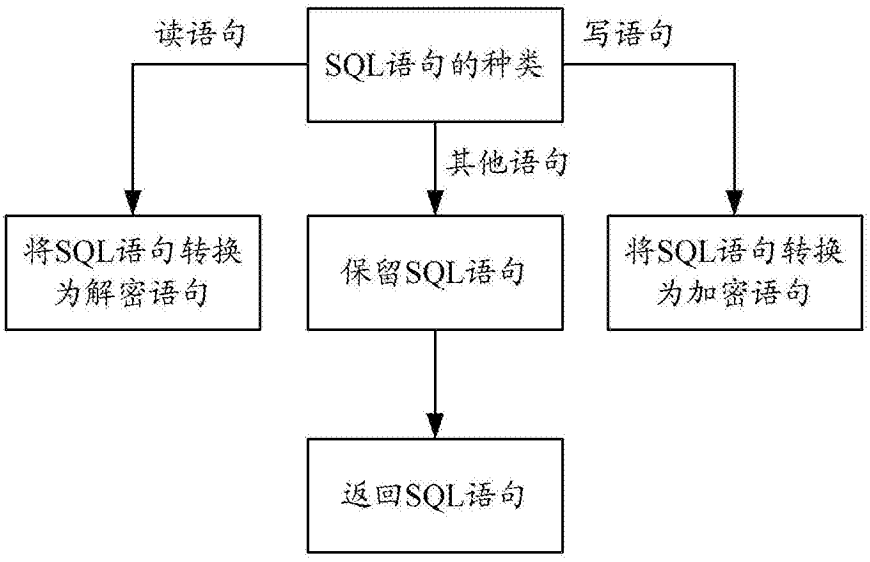

读语句
SQL语句的种类
写语句
其他语句
将SQL语句转换为解密语句
保留SQL语句
将SQL语句转换为加密语句
返回SQL语句

图 3