数据库中密文数据换密失败的处理方法和装置

本申请要求 2016 年 04 月 11 日递交的申请号为 201610221942.1、发明名称为“数据库中密文数据换密失败的处理方法和装置”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本申请涉及数据处理领域，尤其涉及一种数据库中密文数据换密失败的处理方法和装置。

背景技术

PCI DSS（Payment Card Industry Data Security Standard，支付卡行业数据安全标准）对于所有涉及信用卡的信息机构的安全方面作出了要求，其中包括安全管理、策略、过程、网络体系结构、软件设计等，以尽可能全面保障持卡人的交易安全。PCI DSS 安全标准被认为是当前最权威的数据安全保护措施，能够在最大程度上保证与信用卡有关的敏感信息的安全性。

根据 PCI DSS 标准，支付机构的信用卡信息数据库中，所有的信用卡卡号以密文形式存储，并且加密卡号所使用的密钥至少要每年更换一次。因此，支付机构每隔一定时间，都要对信用卡信息数据库中信用卡卡号的密文数据进行换密。具体而言，将数据库中每条记录中卡号的密文数据以旧密码解密后得到卡号明文，再以新密码对明文加密后得到卡号的新密文数据，然后将新密文数据替换原有记录中的密文数据，并将该记录中的密钥版本号更新为新密钥的版本号、更新记录中的换密时间。

现有技术中，当对某条记录中的密文数据换密失败后，将该条记录的标识和换密失败的时间输出到失败日志中。技术人员分析失败日志，按照失败记录所在的换密时间段指定一个或多个重试时间段，对换密时间属于该指定重试时间段的每条记录，如果某条记录的密钥版本号已经更新为新密钥版本号，不再重试，否则重新进行换密。这种失败处理方式需要人工分析和指定重试时间段，并且在重试时还需要对记录是否换密成功做出判断，运行效率较低。

发明内容

有鉴于此，本申请提供一种数据库中密文数据换密失败的处理方法，包括：

当对某条记录的密文数据换密失败时，保存所述记录的错误信息，其中包括所述记录的标识和失败原因；

根据保存的失败原因确定重试策略，采用所述重试策略对具有所述标识的记录中的密文数据重新进行换密。

本申请还提供了一种数据库中密文数据换密失败的处理装置，包括：

错误信息保存单元，用于当对某条记录的密文数据换密失败时，保存所述记录的错误信息，其中包括所述记录的标识和失败原因；

策略及重试单元，用于根据保存的失败原因确定重试策略，采用所述重试策略对具有所述标识的记录中的密文数据重新进行换密。

由以上技术方案可见，本申请的实施例中，在数据库某条记录中的密文数据换密失败后，根据失败原因确定该条记录的重试策略，并按照重试策略自动进行失败记录中密文数据的重新换密，有针对性的重试策略能够极大的提高重新换密的成功率，大大降低了人力工作；同时由于只对失败记录进行重试，提高了失败处理的运行效率。

附图说明

图 1 是本申请实施例中一种数据库中密文数据换密失败的处理方法的流程图；

图 2 是本申请应用示例中替换任务执行系统的换密流程图；

图 3 是本申请应用示例中替换任务执行系统的失败记录重试流程图；

图 4 是本申请实施例所应用的设备的一种硬件结构图；

图 5 是本申请实施例中一种数据库中密文数据换密失败的处理装置的逻辑结构图。

具体实施方式

本申请的实施例提出一种新的数据库中密文数据换密失败的处理方法，保存换密失败的数据库记录的失败原因，按照由失败原因确定的重试策略来自动进行失败记录中密文数据的重新换密，从而不仅在重试时无需处理换密完毕的记录，而且能够极大的提高重试成功的概率，提高了失败处理的执行效率，同时自动执行的重新换密能够减少人工工作，以解决现有技术中存在的问题。

本申请的实施例可以应用在任何具有计算和存储能力的设备上，例如手机、平板电脑、PC（Personal Computer，个人电脑）、笔记本、服务器、虚拟机等设备。本申请实施例应用的设备可以是一个物理或逻辑设备，也可以是由两个或两个以上分担不同职责

的物理或逻辑设备、相互协同来实现本申请实施例中的各项功能。

本申请的实施例中，数据库中密文数据换密失败的处理方法的流程如图 1 所示。

步骤 110，当对某条记录的密文数据换密失败时，保存该记录的错误信息，其中包括该记录的标识和失败原因。

数据库中，数据通常以表的形式来存储。表的一列称为一个字段，表的一行称为一条记录，每条记录包括一到多个对应于该表的列的字段值。数据以记录为单位保存在数据库的表中，对表中数据的读取、写入、更新等操作通常也针对记录来进行。

本申请的实施例中，数据库的一条记录中可以有一个到多个的字段值是密文数据，不同字段值可以采用相同或不同的密钥，不做限定。如果对某条记录的密文数据换密失败，保存包括该记录的标识和失败原因在内的错误信息。

记录的标识用来在所保存错误信息的范围内唯一确定一条记录。例如，如果保存对一个数据库表换密的错误信息，则记录的标识可以是该数据库表的主键或唯一索引，也可以是主键或唯一索引与其他字段的组合。再如，如果保存对多个数据库表换密的错误信息，由于不同表的主键或唯一索引可能有重复，则可以采用表名与主键或唯一索引的组合作为记录的标识。其中，主键是数据库表中的一个或多个字段，该表中任一条记录的主键值都与其他记录的主键值不同；唯一索引是对数据库表中一个字段或多个字段的值进行排序的一种结构，并且不同记录的唯一索引值互不相同，用来快速查询索引字段的值。

对一条记录中密文数据的换密可能因各种原因而失败。通常可以通过导致失败的故障发生时硬件或软件的异常来定位失败原因，也可以通过读取记载故障、警告等信息的日志来获取失败原因，并且将失败原因记载在该记录的错误信息中。

在不同应用场景中，密文数据换密的失败原因与该场景的具体实现有较大的关联度。例如，如果本申请实施例中密文数据换密及其失败处理、与数据库运行在同一个物理设备上，则失败原因可以包括换密及失败处理功能组件的运行故障、数据库读写异常等；如果本申请实施例中密文数据换密及其失败处理、与数据库运行在不同的物理设备上，则失败原因除换密及失败处理功能组件的运行故障、数据库读写异常外，还可以包括两个物理设备间的通信异常等。本申请的实施例对各种具体的失败原因不做限定。

步骤 120，根据保存的失败原因确定重试策略，采用所述重试策略对具有所述标识的记录中的密文数据重新进行换密。

一些换密失败是由于运行过程中发生的暂时性异常造成的，在之后的运行中当暂时

性异常结束后，可以通过重试而成功换密。不同的暂时性异常所需要的恢复条件可能不同，因此，可以针对不同的失败原因，设置对应的重试策略，来尝试对换密失败的记录自动进行重新换密，以提高在无需人工干预的情况下的换密成功率。重试策略可以包括在什么条件下进行重试、以何种方式进行重试、采用怎样的参数进行重试、进行多少次重试等等。

如前所述，具体的失败原因因应用场景的不同和具体实现的不同而不同，针对具体失败原因而设置的重试策略最好也同样符合应用场景和具体实现的要求，本申请的实施例对失败原因和重试策略均不做限定。以下举几个例子来进行说明。

例如，失败原因通常包括数据库状态异常，数据库状态异常可以包括数据库无法访问、数据库抖动、数据库读写错误等情况，由于可自行恢复的数据库异常持续时间往往很短，因此对密文数据换密的失败原因是数据库状态异常的情形，重试策略可以是立即重新进行该记录中密文数据的换密，并且重新进行换密的次数不超过第一预定次数。

再如，在一种实现方式中，对数据库中密文数据的换密由换密执行功能组件调用字段值访问功能组件来进行，其中，由字段值访问功能组件对记录中密文数据所在的字段值进行操作；换密执行功能组件在接收到对数据库记录中密文数据的换密任务后，采用预设的参数调用字段值访问功能组件来完成换密任务。字段值访问功能组件或换密执行功能组件可以是一个独立运行的程序或应用，也可以是一个程序或应用中的一部分，二者可以运行在同一个或不同的物理或逻辑设备上。

这种实现方式中，可以将字段值访问功能组件状态异常作为失败原因中的一种。字段值访问功能组件状态异常可能包括字段值访问功能组件本身运行故障、对字段值访问功能组件的调用发生故障等情形。由于字段值访问功能组件的故障恢复通常需要一定时间，因此重试策略可以是：在间隔第一预定时间后重新进行失败原因为字段值访问功能组件状态异常的记录中密文数据的换密，并且重新进行换密的次数不超过第二预定次数。可以在失败记录的错误信息中写入换密失败的时间，以便根据换密失败的时间和第一预定时间来确定可以进行重试的时间。

在上述实现方式中，换密执行功能组件状态异常也可以作为失败原因中的一种。换密执行功能组件状态异常可能包括换密执行功能组件本身运行故障、通信故障等情形。当失败原因为换密执行功能组件执行异常时，重试策略可以是：立即重新进行记录中密文数据的换密，并且重新进行换密的次数不超过第三预定次数。

在上述几个例子中，第一预定次数、第二预定次数和/或第三预定次数的合适值与实

际应用场景的实现和当前业务运营情形相关，可以先根据经验设定某个值，然后根据系统的运行情况、重试成功的比例等因素来对设定值进行调整。如果应用场景的硬件或软件、或者业务负载、业务流程等影响系统运行的因素有变化时，还可以重复上述调整过程，以得到合适的第一预定次数、第二预定次数和/或第三预定次数的值。

可以预置失败原因与针对该失败原因的重试策略的对应关系，根据某条记录的失败原因即可查找到对应的重试策略，并采用该重试策略来对该记录重新进行换密。如果按照某条记录的重试策略对该记录的重新换密仍然以失败告终，可以将该记录的错误信息写入失败日志，供人工分析、干预或做其他处理。

在一种实现方式中，可以采用专门的重试功能组件来进行失败记录的重新换密。重试功能组件的运行逻辑可以根据实际应用场景的需要来实现，一个例子中，可以维护一张重试处理表，当某条记录中的密文数据换密失败时，将该记录的错误信息添加到重试处理表中，并标记为未成功。重试功能组件在满足预定重试条件时，读取重试处理表中标记为未成功的错误信息，取得该错误信息中的记录标识和失败原因；按照由该失败原因决定的重试策略，重试功能组件对具有该标识的数据库中记录的密文数据重新进行换密。如果重新进行的换密成功，则修改该错误信息的标记为成功；如果重新进行的换密失败，则更改该错误信息的重试次数；如果该错误信息的重试次数达到该重试策略允许的最大次数，删除重试处理表中的该错误信息并将该错误信息写入失败日志。

可以在失败记录的错误信息中写入对数据库记录中的密文数据重新进行换密时所需的参数，具体的参数根据实际应用场景的实现来确定。例如，失败记录的错误信息中可以包括旧密钥版本号和新密钥版本号，在对失败记录中的密文数据重新进行换密时，可以根据所确定的重试策略，重新根据旧密钥版本号对应的密钥来解密原密文数据得到明文数据，根据新密钥版本号对应的密钥加密明文数据得到新的密文数据，并以新的密文数据替换该失败记录中的原密文数据。

对并非由运行中暂时性异常导致的换密失败，则通常难以通过重试来成功换密。例如，如果失败原因是记录中密文数据解密失败，该密文数据已经存储于数据库中，无法通过重试来解决这一错误；在这种情况下，不对该记录进行自动重试，可以将该记录的标识等错误信息写入失败日志中，留待人工处理。

可见，本申请的实施例中，在数据库某条记录中密文数据换密失败后，保存该记录的失败原因，按照由失败原因确定的重试策略来自动进行失败记录中密文数据的重新换密，极大的提高了自动换密的成功率，减少了人工工作；并且由于在重新换密时无需处

理已经换密完毕的记录，提高了失败处理的运行效率。

在本申请的一个应用示例中，信用卡信息数据库中信用卡卡号的密文数据，每隔一定时间需要进行换密。当换密周期到时，替换任务执行系统（换密执行功能组件）接收到换密任务和用于本次任务的换密参数，其中包括旧密钥版本号和新密钥版本号。替换任务执行系统可以利用旧密钥版本号和新密钥版本号获取到旧密钥和新密钥。

信用卡信息数据库中每条记录对应一张信用卡，其字段包括卡索引号、卡号密文数据、加密卡号的密钥版本号。其中，卡索引号用来唯一代表信用卡信息数据库中的一张信用卡，在本应用示例中以卡索引号来作为记录的标识。

替换任务执行系统通过调用卡信息数据库维护系统（字段值访问功能组件）来访问信用卡信息数据库，进行其中每条记录的卡号密文数据的换密，其流程如图 2 所示。

步骤 210，以信用卡信息数据库中的第一条记录作为当前记录。

步骤 220，调用卡信息数据库维护系统来进行当前记录的换密。

步骤 230，判断当前记录的换密是否成功，如果失败，执行步骤 240；如果成功，转步骤 250。

步骤 240，将当前记录的卡索引号、失败原因、换密执行时间、旧密钥版本号和新密钥版本号作为错误信息，写入重试处理表中，并将重试处理表中的该条错误信息标记为未成功。

步骤 250，判断是否信用卡信息数据库中有下一条记录，如果有，以下一条记录为当前记录，转步骤 220；如果没有，换密流程结束。

换密的失败原因包括以下四种：

第一种：卡信息数据库维护系统状态异常；对应的重试策略为：在换密执行时间 1 小时后重试，最多允许 5 次重试；

第二种：信用卡信息数据库状态异常；对应的重试策略为：立即重试，最多允许 2 次重试；

第三种：替换任务执行系统状态异常；对应的重试策略为：立即重试，最多允许 2 次重试；

第四种：密文数据解密失败，即无法以旧密钥将记录中的卡号密文数据解密为符合卡号数据格式的明文数据；不进行自动重试，将本条错误信息输出到失败日志中。

替换任务执行系统定时按照重试处理表中保存的错误信息进行失败记录的自动重试，其流程如图 3 所示。

步骤 310，读取重试处理表中的第一条错误信息作为当前错误信息。

步骤 320，判断当前错误信息的标记是否为未成功，如果是，执行步骤 330；否则转步骤 380。

步骤 330，判断当前错误信息中的失败原因是否为密文数据解密失败，如果是，转步骤 370。

步骤 340，按照错误信息中的失败原因确定重试策略，采用该重试策略调用卡信息数据库维护系统进行具有当前错误信息中卡索引号的记录中卡号密文数据的重新换密，直到重试成功或者达到该重试策略最多允许的重试次数。

步骤 350，判断当前错误信息是否重试成功，如果是，执行步骤 360；否则转步骤 370。

步骤 360，将重试处理表中当前错误信息的标记修改为成功，转步骤 380。

步骤 370，将当前错误信息写入失败日志中，删除重试处理表中的当前错误信息。

步骤 380，判断重试处理表中是否有下一条错误信息，如果有，以下一条错误信息作为当前错误信息，转步骤 320；如果没有，自动重试的流程结束。

与上述流程实现对应，本申请的实施例还提供了一种数据库中密文数据换密失败的处理装置。该装置可以通过软件实现，也可以通过硬件或者软硬件结合的方式实现。以软件实现为例，作为逻辑意义上的装置，是通过所在设备的 CPU（Central Process Unit，中央处理器）将对应的计算机程序指令读取到内存中运行形成的。从硬件层面而言，除了图 4 所示的 CPU、内存以及非易失性存储器之外，数据库中密文数据换密失败的处理装置所在的设备通常还包括用于进行无线信号收发的芯片等其他硬件，和/或用于实现网络通信功能的板卡等其他硬件。

图 5 所示为本申请实施例提供的一种数据库中密文数据换密失败的处理装置，包括错误信息保存单元和策略及重试单元，其中：错误信息保存单元用于当对某条记录的密文数据换密失败时，保存所述记录的错误信息，其中包括所述记录的标识和失败原因；策略及重试单元用于根据保存的失败原因确定重试策略，采用所述重试策略对具有所述标识的记录中的密文数据重新进行换密。

可选的，所述失败原因包括：数据库状态异常；所述策略及重试单元根据保存的失败原因确定重试策略，包括：当失败原因为数据库状态异常时，重试策略为立即重新进行所述记录中密文数据的换密，并且重新进行换密的次数不超过第一预定次数。

一个例子中，所述密文数据换密中由字段值访问功能组件对记录中密文数据所在的

字段值进行操作；所述失败原因包括：字段值访问功能组件状态异常；所述策略及重试单元根据保存的失败原因确定重试策略，包括：当失败原因为字段值访问功能组件状态异常时，重试策略为在间隔第一预定时间后重新进行所述记录中密文数据的换密，并且重新进行换密的次数不超过第二预定次数。

上述例子中，所述密文数据换密中由换密执行功能组件对字段值访问功能组件进行调用；所述失败原因包括：换密执行功能组件执行异常；所述策略及重试单元根据保存的失败原因确定重试策略，包括：当失败原因为换密执行功能组件执行异常时，重试策略为立即重新进行所述记录中密文数据的换密，并且重新进行换密的次数不超过第三预定次数。

可选的，所述装置还包括重试取消单元，用于当失败原因为记录中密文数据解密失败时，不对具有所述标识的记录中的密文数据重新进行换密。

可选的，所述装置还包括重试失败单元，用于在采用重试策略对具有所述标识的记录中密文数据的重新换密失败后，将所述记录的错误信息写入失败日志。

可选的，所述错误信息保存单元具体用于：当对某条记录中密文数据换密失败时，将换密失败的记录的错误信息添加到重试处理表中，并标记为未成功；所述策略及重试单元具体用于：在满足预定重试条件时，读取重试处理表中标记为未成功的错误信息，根据其中的失败原因确定重试策略，采用所确定的重试策略对具有错误信息中标识的记录重新进行密文数据换密，如果换密成功则将所述错误信息的标记修改为成功；否则更改所述错误信息的重试次数，当重试次数达到所述重试策略允许的最大次数时，删除重试处理表中的所述错误信息并将所述错误信息写入失败日志。

可选的，所述错误信息中还包括：旧密钥版本号和新密钥版本号；所述策略及重试单元采用重试策略对具有所述标识的记录中的密文数据重新进行换密，包括：采用所述重试策略，重新根据旧密钥版本号对应的密钥和新密钥版本号对应的密钥对具有所述标识的记录中的密文数据进行换密。

可选的，所述密文数据包括：信用卡卡号密文数据。

以上所述仅为本申请的较佳实施例而已，并不用以限制本申请，凡在本申请的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本申请保护的范围之内。

在一个典型的配置中，计算设备包括一个或多个处理器（CPU）、输入/输出接口、网络接口和内存。

内存可能包括计算机可读介质中的非永久性存储器，随机存取存储器 （RAM）和/

或非易失性内存等形式，如只读存储器（ROM）或闪存（flash RAM）。内存是计算机可读介质的示例。

计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存（PRAM）、静态随机存取存储器（SRAM）、动态随机存取存储器（DRAM）、其他类型的随机存取存储器（RAM）、只读存储器（ROM）、电可擦除可编程只读存储器 （EEPROM）、快闪记忆体或其他内存技术、只读光盘只读存储器（CD-ROM）、数字多功能光盘（DVD）或其他光学存储、磁盒式磁带，磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质，可用于存储可以被计算设备访问的信息。按照本文中的界定，计算机可读介质不包括暂存电脑可读媒体（transitory media），如调制的数据信号和载波。

还需要说明的是，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。

本领域技术人员应明白，本申请的实施例可提供为方法、系统或计算机程序产品。因此，本申请可采用完全硬件实施例、完全软件实施例或结合软件和硬件方面的实施例的形式。而且，本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。