Method and Apparatus for Processing Failure of Cipher Change of Ciphertext in Database

This application claims priority to the Chinese Patent Application No. 201610221942.1 filed on April 11, 2016 and titled "Method and apparatus for processing failure of cipher change of ciphertext data in database," the entire content of which is incorporated herein by reference in the entirety.

Technical field

This application relates to the field of data processing, and in particular, to a method and an apparatus for processing failure of cipher change of ciphertext in database.

Background

The PCI DSS (Payment Card Industry Data Security Standard) has security requirements for all organizations involved with credit card information, including security management, strategies, processes, network architecture, and software design, in order to guarantee as much as possible the security of cardholder transactions. The PCI DSS security standard is considered to be the most authoritative data security measures today, and can ensure the security of sensitive credit card-related information to the highest degree.

Based on the PCI DSS standard, all credit card numbers in the credit card information databases of payment institutions are stored as ciphertext, and the keys used to encrypt card numbers are replaced at least once a year. Therefore, payment institutions must perform a cipher change of the ciphertext data for credit card numbers in their credit card information databases at regular intervals. More specifically, card number plaintext is obtained after the ciphertext data of the card number in each record in the database is decrypted using the old code, and then a new code is used to encrypt the plaintext to obtain new card number ciphertext data. Next, the new ciphertext data is used to replace the ciphertext data in the original record, the key version number of this record is updated to the version number of the new key, and the cipher change time in the record is updated.

In the current technologies, after the cipher change of ciphertext data in a record fails, the identifier of the record and the time of the cipher change failure are output to a failure log. Technicians analyze the failure log and designate one or more retry time frames according to the cipher change time frame of the failed record. For every record with a cipher change time within this designated retry time frame, if the key version number of a record has been updated to a new key version number, the cipher change is not retried; otherwise, the cipher change is reperformed. This failure processing approach requires manual analysis and the designation of retry time frames, and during retries, it is necessary to determine whether a

example, if storing the cipher change error information for multiple database tables, because the primary keys or unique indexes of different tables may be repeated, a combination of the table name and primary key or unique index can be used as the record's identifier. Here, the primary key is one or more fields of a database table, and the primary key value of any given record in this table will be different from the primary key values of the other records. The unique index is a structure for sorting the values of one or more fields in a database table, and the unique index values of different records will be different from each other. The unique index is used for rapidly querying and indexing field values.

The cipher change of ciphertext data in a record may fail for a variety of reasons. Usually, the cause of the failure can be located through hardware or software anomalies at the time of the fault leading to the failure. The cause of the failure can be ascertained by reading logs containing fault and warning information, and the cause of the failure can be recorded in the error information of the record.

In different application scenarios, the cause of a failed cipher change of ciphertext data is highly correlated to the scenario's specific implementation. For example, in the embodiments of this application, if the cipher changes of the ciphertext data and failure processing operates on the same physical device as the database, failure causes may comprise operational faults in the cipher change and failure processing components, database read/write anomalies, etc. In the embodiments of this application, if the cipher changes of the ciphertext data and failure processing operates on a different physical device from the database, in addition to operational faults in the cipher change and failure processing components and database read/write anomalies, failure causes may also comprise communication anomalies between the two physical devices. The embodiments of this application place no limitations on the specific types of failure causes.

Step 120, determining a retry strategy based on the stored failure cause, and employing the retry strategy to reperform the cipher change of the ciphertext data in the record having the identifier.

Some cipher change failures are the result of transient anomalies during the operating process. After the transient anomaly ends, during operation, it is possible to succeed with a cipher change through retries. There may be different recovery conditions required for different transient anomalies. Therefore, retry strategies corresponding to different failure causes can be set, to try to automatically reperform cipher changes for records with cipher change failures, improving the cipher change success rate without requiring manual intervention. Retry strategy can comprise the conditions under which a retry is performed, the

mode by which a retry is performed, the parameters employed in performing a retry, the number of retries performed, etc.

As previously described, failure causes vary due to difference in application scenarios and differences in specific implementations. Ideally, retry strategies aimed at specific failure causes will meet the needs of the application scenario and specific implementation. The embodiments of this application place no limitations on the failure causes and retry strategies. A description using several examples is given below.

For example, failure causes usually comprise database state anomalies, and database state anomalies can comprise database inaccessibility, database jitter, and database read/write errors. The duration of self-recoverable database anomalies is usually very brief. Therefore, when the cause of a failed cipher change of ciphertext data is a database state anomaly, the retry strategy can be to immediately reperform the cipher change of the ciphertext data in the record change, for a number of times not exceeding a first predetermined number.

As another example, in one mode of implementation, the cipher change of ciphertext data in a database is performed by a field value access component that is invoked by a cipher change execution component. Here, the field value access component performs operations on the record's field value in which the ciphertext data is located. After the cipher change execution component receives a cipher change task for the ciphertext data of a database record, the cipher change execution component employs pre-set parameters to invoke the field value access component to carry out the cipher change task. The field value access component or cipher change execution component can be an independently running program or application, or can be one part of a program or application. The field value access component and cipher change execution component can run on the same or different physical or logical devices.

In this mode of implementation, state anomalies of the field value access component can be one type of failure cause. State anomalies of the field value access component may comprise operational faults of the field value access component itself and faults when the field value access component is invoked. Fault recovery in a field value access component usually takes a certain amount of time. Therefore the retry strategy can be: after a first predetermined time has elapsed, reperforming the cipher change of the ciphertext data in the record for which the failure cause is a state anomaly of the field value access component, for a number of times not exceeding a second predetermined number. The time of the cipher change failure can be written into the error information of the failed record, in order to determine the time at which a retry can be performed, based on the time of the cipher change

reperformed cipher change fails, the error information's retry number is changed. If the retry number of this error information has reached the maximum number allowed according to the retry strategy, the error information is deleted from the retry processing table, and the error information is written into a failure log.

The parameters required when reperforming the cipher change of ciphertext data in a database record can be written into the error information of a failed record. The specific parameters are determined based on the application scenario. For example, the error information of a failed record can comprise an old key version number and a new key version number. When reperforming the cipher change of ciphertext data in a failed record, based on the determined retry strategy, the original ciphertext data can be decrypted using the key corresponding to the old key version number to obtain plaintext data, and the plaintext data can be encrypted using the key corresponding to the new key version number, yielding new ciphertext data. The new ciphertext data can be used to replace the original ciphertext data in the failed record.

For cipher change failures that are not the result of transient anomalies during operation, it is usually difficult to perform a successful cipher change through retries. For example, if the failure cause is a decryption failure of the record's ciphertext data, this ciphertext data has already been stored in the database, and it is not possible to solve this error through retries. Under these circumstances, an automatic retry is not performed for this record. The record's error information, such as its identifier, can be written into the failure log for manual processing.

In the embodiments of this application, after a cipher change failure for ciphertext data in a database record, the record's failure cause is stored, and a cipher change of the ciphertext data in the failed record is automatically reperformed in accordance with the retry strategy determined by the failure cause. Thus, the success rate of automatic cipher changes is boosted, and the amount of manual work is reduced. In addition, because it is not necessary to process records having completed cipher changes when reperforming cipher changes, the operating efficiency of failure processing is improved.

In an application example of this application, the ciphertext data for credit card numbers in a credit card information database needs to undergo cipher changes at regular intervals. When the cipher change cycle ends, a change task execution system (cipher change execution component) receives a cipher change task and cipher change parameters used for this task, comprising an old key version number and a new key version number. The change task execution system can use the old key version number and new key version number to obtain

failure log.

The change task execution system regularly performs automatic retries for failed records in accordance with the error information stored in the retry processing table. The flow is as shown in FIG. 3.

Step 310, reading the first error information in the retry processing table as the current error information.

Step 320, determining whether the current error information is tagged as unsuccessful; if so, executing Step 330, and if not, proceeding to Step 380.

Step 330, determining whether the failure cause in the current error information is a ciphertext data decryption failure; if so, proceeding to Step 370.

Step 340, determining a retry strategy in accordance with the failure cause in the error information, and employing this retry strategy to invoke the card information database maintenance system to reperform the cipher change of the card number ciphertext data in the record having the card index number in the current error information, until the retry is successful or the maximum number of retries allowed according to the retry strategy is reached.

Step 350, determining whether the current error information is a retry success; if so, executing Step 360, and if not, proceeding to Step 370.

Step 360, changing the tag of the current error information in the retry processing table to successful, and proceeding to Step 380.

Step 370, writing the current error information into a failure log, and deleting the current error information from the retry processing table.

Step 380, determining whether there is a next collection of error information in the retry processing table; if so, using the next collection of error information as the current error information and going to Step 320; if not, ending the automatic retry flow.

Corresponding to the implementation of the flows described above, the embodiments of this application also provide an apparatus for processing a failure of a cipher change of ciphertext data in a database. This apparatus can be implemented through software, and it can also be implemented through hardware or a combination of software and hardware. Using software implementation as an example, as a logical apparatus, it is run by having the CPU (Central Processing Unit) of the device in which it is located to read corresponding computer program instructions to internal memory. As for hardware, in addition to the CPU, internal memory, and non-volatile memory shown in FIG. 4, the device in which the apparatus for processing a failure of a cipher change of ciphertext data in a database is located usually also comprises other hardware such as a chip used to perform wireless signal transmission and

reception, and/or other hardware such as a card used for network communications.

FIG. 5 shows the apparatus for processing a failure of a cipher change of ciphertext data in a database provided by the embodiments of this application, comprising an error information storage unit and a strategy and retry unit, wherein: the error information storage unit is configured to store the record's error information when a cipher change of ciphertext data in a record fails, the error information comprising an identifier of the record and a failure cause; the strategy and retry unit is configured to determine a retry strategy based on the stored failure cause, and employ the retry strategy to reperform the cipher change of the ciphertext data in the record having the identifier.

Optionally, the failure cause comprises: a database state anomaly; the strategy and retry unit determining a retry strategy based on the stored failure cause comprises: a retry strategy of immediately reperforming the cipher change of the ciphertext data in the record when the failure cause is the database state anomaly, for a number of times not exceeding a first predetermined number.

In one example, the cipher change of the ciphertext data is performed by a field value access component on the record's field value in which the ciphertext data is located; and the failure cause comprises: a state anomaly of the field value access component; the strategy and retry unit determining a retry strategy based on the stored failure cause comprises: a retry strategy of reperforming the cipher change of the ciphertext data in the record after a first predetermined time has elapsed when the failure cause is the state anomaly of the field value access component, for a number of times not exceeding a second predetermined number.

In this example, during the cipher change of the ciphertext data, the cipher change execution component invokes the field value access component; the failure cause comprises: an execution anomaly of the cipher change execution component; the strategy and retry unit determining a retry strategy based on the stored failure cause comprises: a retry strategy of immediately reperforming the cipher change of the ciphertext data in the record when the failure cause is the execution anomaly of the cipher change execution component, for a number of times not exceeding a third predetermined number.

Optionally, the apparatus also comprises a retry cancellation unit, configured to not reperform the cipher change of the ciphertext data in the record having the identifier when the failure cause is a decryption failure of the ciphertext data in the record.

Optionally, the apparatus also comprises a retry failure unit, configured to write the record's error information into a failure log after the reperformed cipher change of the ciphertext data in the record having the identifier according to the retry strategy fails.

Optionally, the error information storage unit is configured to: when there is a cipher change failure for ciphertext data in a record, add the error information of the record with the cipher change failure to a retry processing table, and tag the error information as unsuccessful; the strategy and retry unit is configured to: when predetermined retry conditions have been met, read the error information tagged as unsuccessful in the retry processing table, determine the retry strategy based on the failure cause in the read error information, employ the determined retry strategy to reperform the cipher change of the ciphertext data for the record having the identifier in the error information, and revise the tag of the error information to successful if the cipher change is successful; otherwise, the error information storage unit is configured to modify a retry number for the error information, and when the retry number reaches a maximum number allowed according to the retry strategy, delete the error information from the retry processing table and write the error information into a failure log.

Optionally, the error information also comprises: an old key version number and a new key version number; the strategy and retry unit employing the retry strategy to reperform the cipher change of the ciphertext data for the record having the identifier comprises: employing the retry strategy, and reperforming the cipher change of the ciphertext data in the record having the identifier based on a key corresponding to the old key version number and another key corresponding to the new key version number.

Optionally, the ciphertext data comprises: ciphertext data for a credit card number.

The preceding is merely preferred embodiments of this application and does not limit this application. All modifications, equivalent substitutions, and improvements made within the spirit and principles of this application shall fall within the scope of protection of this application.

In one typical configuration, the computation equipment comprises one or more processors (CPUs), input/output interfaces, network interfaces, and internal memory.

The internal memory may comprise the forms of volatile memory on computer-readable media, random access memory (RAM), and/or non-volatile RAM, such as read-only memory (ROM) or flash RAM. Internal memory is an example of computer-readable media.

Computer-readable media may include permanent, nonpermanent, mobile, and immobile media, which can achieve information storage through any method or technology. The information may be computer-readable instructions, data structures, program modules, or other data. Examples of computer storage media include, but are not limited to, Phase-change RAM (PRAM), Static RAM (SRAM), Dynamic RAM (DRAM), other types of Random Access Memory (RAM), Read-Only Memory (ROM), Electrically Erasable Programmable

Claims

1. A method for processing a failure of a cipher change of ciphertext data in a database, comprising:

storing a record's error information when a cipher change of ciphertext data in the record fails, the error information comprising an identifier of the record and a failure cause; and

determining a retry strategy based on the stored failure cause, and employing the retry strategy to reperform the cipher change of the ciphertext data in the record having the identifier.

2. The method according to Claim 1, wherein: the failure cause comprises: a database state anomaly; and the determining a retry strategy based on the stored failure cause comprises: a retry strategy of immediately reperforming the cipher change of the ciphertext data in the record when the failure cause is the database state anomaly, for a number of times not exceeding a first predetermined number.

3. The method according to Claim 1, wherein: the cipher change of the ciphertext data is performed by a field value access component on the record's field value in which the ciphertext data is located; and the failure cause comprises: a state anomaly of the field value access component; and

the determining a retry strategy based on the stored failure cause comprises: a retry strategy of reperforming the cipher change of the ciphertext data in the record after a first predetermined time has elapsed when the failure cause is the state anomaly of the field value access component, for a number of times not exceeding a second predetermined number.

4. The method according to Claim 3, wherein: the cipher change of the ciphertext data is performed by the field value access component invoked by a cipher change execution component; the failure cause comprises: an execution anomaly of the cipher change execution component; and

the determining a retry strategy based on the stored failure cause comprises: a retry strategy of immediately reperforming the cipher change of the ciphertext data in the record when the failure cause is the execution anomaly of the cipher change execution component, for a number of times not exceeding a third predetermined number.

5. The method according to Claim 1, further comprising: not reperforming the cipher change of the ciphertext data in the record having the identifier when the failure cause is a decryption failure of the ciphertext data in the record.

6. The method according to Claim 1, further comprising: after the reperformed cipher change of the ciphertext data in the record having the identifier according to the retry strategy fails, writing the record's error information into a failure log.

7. The method according to Claim 1, wherein the storing a record's error information comprises: adding the error information of the record with the cipher change failure to a retry processing table, and tagging the error information as unsuccessful; and

the determining a retry strategy based on the stored failure cause, and employing the retry strategy to reperform the cipher change of the ciphertext data in the record having the identifier, comprises: when predetermined retry conditions have been met, reading the error information tagged as unsuccessful in the retry processing table, determining the retry strategy based on the failure cause in the read error information, employing the determined retry strategy to reperform the cipher change of the ciphertext data for the record having the identifier in the error information, and revising the tagging of the error information to successful if the cipher change is successful; if the cipher change is unsuccessful, modifying a retry number for the error information, and when the retry number reaches a maximum number allowed according to the retry strategy, deleting the error information from the retry processing table and writing the error information into a failure log.

8. The method according to any one of Claims 1 through 7, wherein the error information also comprises: an old key version number and a new key version number; and

the employing the retry strategy to reperform a cipher change of the ciphertext data in the record having the identifier comprises: employing the retry strategy, and reperforming the cipher change of the ciphertext data in the record having the identifier based on a key corresponding to the old key version number and another key corresponding to the new key version number.

9. The method according to Claim 1, wherein the ciphertext data comprises: ciphertext data for a credit card number.

10. An apparatus for processing a failure of a cipher change of ciphertext data in a database, the apparatus comprising:

an error information storage unit, configured to store a record's error information when a cipher change of ciphertext data in the record fails, the error information comprising an identifier of the record and a failure cause; and

a strategy and retry unit, configured to determine a retry strategy based on the stored failure cause, and employ the retry strategy to reperform the cipher change of the ciphertext data in the record having the identifier.

11. The apparatus according to Claim 10, wherein the failure cause comprises: a database state anomaly; and

the strategy and retry unit determining a retry strategy based on the stored failure cause comprises: a retry strategy of immediately reperforming the cipher change of the ciphertext data in the record when the failure cause is the database state anomaly, for a number of times not exceeding a first predetermined number.

12. The apparatus according to Claim 10, wherein: the cipher change of the ciphertext data is performed by a field value access component on the record's field value in which the ciphertext data is located; and the failure cause comprises: a state anomaly of the field value access component; and

the strategy and retry unit determining a retry strategy based on the stored failure cause comprising: a retry strategy of reperforming the cipher change of the ciphertext data in the record after a first predetermined time has elapsed when the failure cause is the state anomaly of the field value access component, for a number of times not exceeding a second predetermined number.

13. The apparatus according to Claim 12, wherein: the cipher change of the ciphertext data is performed by the field value access component invoked by a cipher change execution component; the failure cause comprises: an execution anomaly of the cipher change execution component; and

the strategy and retry unit determining a retry strategy based on the stored failure cause comprising: a retry strategy of immediately reperforming the cipher change of the ciphertext data in the record when the failure cause is the execution anomaly of the cipher change execution component, for a number of times not exceeding a third predetermined number.

14. The apparatus according to Claim 10, wherein the apparatus also comprises: a retry cancellation unit, configured to not reperform the cipher change of the ciphertext data in the record having the identifier when the failure cause is a decryption failure of the ciphertext data in the record.

15. The apparatus according to Claim 10, wherein the apparatus also comprises: a retry failure unit, configured to write the record's error information into a failure log after the reperformed cipher change of the ciphertext data in the record having the identifier according to the retry strategy fails.

16. The apparatus according to Claim 10, wherein the error information storage unit is configured to: when there is a cipher change failure for ciphertext data in a record, add the error information of the record with the cipher change failure to a retry processing table, and tag the error information as unsuccessful; and

the strategy and retry unit is configured to: when predetermined retry conditions have been met, read the error information tagged as unsuccessful in the retry processing table, determine the retry strategy based on the failure cause in the read error information, employ the determined retry strategy to reperform the cipher change of the ciphertext data for the record having the identifier in the error information, and revise the tagging of the error information to successful if the cipher change is successful; if the cipher change is unsuccessful, the error information storage unit is configured to modify a retry number for the error information, and when the retry number reaches a maximum number allowed according to the retry strategy, delete the error information from the retry processing table and write the error information into a failure log.

17. The apparatus according to any one of Claims 10 through 16, wherein the error information also comprises: an old key version number and a new key version number; and

the strategy and retry unit employing a retry strategy to reperform the cipher change of the ciphertext data in the record having the identifier, comprising: employing the retry strategy, and reperforming the cipher change of the ciphertext data in the record having the identifier based on a key corresponding to the old key version number and another key corresponding to the new key version number.

18. The apparatus according to Claim 10, wherein the ciphertext data comprises: ciphertext data for a credit card number.