Database Coding Technology and Research of Its Application

Chen li

Department of Computer Science, North China Electric Power University, Hebei Province, China
1520421254@qq.com

Abstract - Database coding technology is the effective way to guarantee the safety of the database information. This essay does some research about the key technology to basic approach and keys of the database coding technology and probe the way to achieving the data coding. Besides, it discusses how to design the data coding system. In addition, it brings about the a concrete model. In the end, it discusses the influence on the original functions of the DBMS after coding the database.

Index Terms - Database encryption technology, Encryption system, Key Management, Design model

1. Introduction

As the important components of the information system, playing a very imperative part in the construction and application of the all system, therefore it is bound to be critical to the insurance of the information system safety. The main reason to cause the unsafe is that the original data is put in the database. If the central information is dealt with the coding, even though some illegal user has the access to the system or plunders the data storage medium. Without the corresponding key to coding, he can not get the information he needs, hence, the safety of the data is guaranteed. Thus database coding means a lot to data safety.

2. Database coding technology

A. the demand for coding database system

The issues the database coding not only includes encryption protection and control unauthorized access during transmission, but also its stored sensitive data is encrypted, so even if the data is leaked, database will not leak. on the other hand, the user can encrypt sensitive information with his own key, even if the DBA can not decrypted, so database coding can meet the demand for encryption on certain occasions. In summary, database encryption requirements are as followings [1]:

1) the adequate strength of the encryption.

2) Fast sped to encrypt / decrypt to minimize the impact on the performance of database access.

3) Storage capacity after stored in the encrypted ciphertext is not increased significantly.

4) Reliable, flexible key management mechanism makes the key u efficient and safe use.

B. encryption level

The database consists of three encryption levels, namely the OS, DBMS kernel layer and the DBMS outer [2].

1) Encryption in the OS layer. The data is first encrypted in memory, then the file system each encrypted memory data is written to the database file, and then decrypted when being read.

2) Encryption in the DBMS kernel layer. Encryption and decryption will be on operation before the data physical access Cryptographic operations, data in memory is written to disk, when the data is read from the disk, decryption will be on operation.

3) In the outer layer of the DBMS encryption. The database encryption system is made independent of the DBMS applications, encryption and decryption operated on the client side is completely transparent to the user operation of the database, The encryption method is shown in Figure 1.

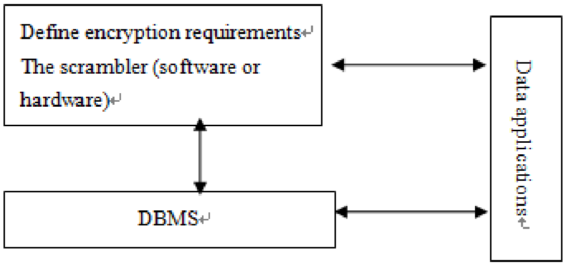
Define encryption requirements↵
The scrambler (software or hardware)↵
DBMS↵
Data applications↵

Fig.1database outer layer encryption

C. encryption granularity

Encryption granularity refers to the minimum unit of data encryption. Encryption granularity of the database can be divided into the database level, table-level, record-level, field-level and item-level. Depending on the application needs, the appropriate encryption granularity can be selected.

1) the database level: the object of encryption is the database. In general, the user gets the access to the database in order to meet the requirements of the records retrieved. If users adopt Database-level encryption, even though they only need to check the small number of records, they also need to decrypt the entire database, which will have a significant impact on system performance. However, for secondary storage to back up the database, you can take this encryption granularity.

2) table-level: the object to be encrypted is the data sheet. Table-level encryption granularity encrypts the important data in the database, which does not restrict the operation of the non-encrypted data table. Compared to database-level encryption, it reduces the decryption and encryption process and improves the system performance. However, when this approach is integrated with the DBMS, DBMS internal core module has to be modified, including modifications to the lexical analyzer, interpreter and query actuator. And the current mainstream commercial DBMS are not open to the source; consequently, it is difficult to integrate them with this approach.

3) The record-level: the object of encryption is a record in the data table. Record-level encryption granularity encrypts and stores the important record on the data sheet record, unimportant records stored in plain text. Compared with the data sheet encryption granularity, encryption granularity has smaller particle size and good flexibility. However, this method also needs DBMS kernel modifications which is same with table-level encryption.

4) field-level: the encrypted object is a field. Field-level encryption granularity encrypts important fields, such as passwords, ID cards, bank account numbers and other sensitive fields.

5) Data item level: the encrypted object is the value of a field in the record. It is the minimum size of the database encryption. Data item level

D. Encryption Algorithm

The rule which is used to encrypt the plain text is called decryption algorithm, and its inverse process is called the decryption algorithm. Thus the key is the key of the encryption algorithm to encrypt the plaintext process. The encryption algorithm directly affects the security of the database encryption and performance. Therefore, the choice of encryption algorithm of database encryption scheme also appears important. Data encryption includes symmetric encryption and asymmetric encryption and hybrid encryption technology.

1) Symmetric encryption: The feature of symmetric encryption decryption is that the key to decryption can be calculated from the key to decryption, both the sender and receiver using the same key. The symmetric encryption algorithm is disclosed and has a small amount of the calculation and fast encryption and high efficiency, so it is most commonly used encryption technology. Symmetric encryption algorithm mainly includes DES, IDEA and AES . The IDEA encryption is of great strength and faster symmetric encryption algorithm. Symmetric encryption is divided into two types of sequence ciphers and block ciphers in that sequence cipher encryption process is expressly superimposed with a random sequence generated ciphertext and the plaintext characters as a unit-by-bit encryption. And the encryption process of each character has nothing to do with the other part. Block cipher divided plaintext into several groups of fixed length , usually a 64-bit data on the type of group, with a different key for encryption and decryption, the encryption process for each character is not only associated with the key, but also with expressly related to other characters.

2)asymmetric encryption: The asymmetric encryption algorithm uses two both fully paired and completely different key, wherein the encryption key is a public key, i.e. the public key; the user can use the public key to encrypt data and the data can only be decrypted with the corresponding decryption key, the secret Key called the private key. RSA is a public key asymmetric encryption algorithm.

3) Hybrid encryption: Hybrid encryption scheme is IDEA-RSA hybrid encryption scheme. The advantage of this program is that it is the first symmetric key IDEA algorithm to encrypt the data in communication process, but the key in the IDEA algorithm via a public key cryptosystem RSA algorithm to encrypt data transmitted to the recipient finally through the channel.

E. Key Management

The security of the key is the critical part in database encryption technology. Key management of the database is divided into two ways which are centralized key management and multi-level key management. Centralized key management is the establishment of key management center. All keys are stored in the key dictionary, user certified by which can get the key. This method of key management is simple, but there is a big security risk in management of the key dictionary.Multi-level key management is to put key management at different levels, first level key called master key, second level key called working key. The master key role of the secondary key is encrypted generate working key. Working key is used for the database data encryption / decryption.

3. data coding system

A. the basic requirements of the database encryption system

A good database encryption system must meet the following conditions[3]:

1) the field is encrypted. The database encryption / decryption size should be each record field data. Terms of a file or as a unit for encryption, the repeated use of the keys will be formed, thereby reducing the encryption system reliability can not be used due to the additional decryption time is too long. Only recorded field data in units of "one-time pad" encryption / decryption, in order to adapt to the operation of the database, while effective key management, and complete cryptographic operations.

2) Key dynamic management. Complex logical relationships between database objects imply a logical structure which may correspond to multiple physical database objects. Database encryption is not only large, but also organizes and stores more complex work, which needs the key to achieve the dynamic management.

3) Reasonable process the data. Firstly properly handle data types is needed, or DBMS will not meet the encrypted data defined data types and can be refused to load; secondly, the need to deal with the problem of data storage has to be met. Database encryption does not substantially increase the space overhead. Under current conditions, the matching fields in the database relational operators, such as the connection between the table code, index field data, should not be encrypted.

4) Does not affect the operation of the legitimate user. The time of affecting the data encryption system operation response should be as short as possible. At this stage, the average delay time should not exceed 1/10 second. Moreover, for legitimate users of the database, data entry, modification and retrieval operation should be transparent to the data and need not consider the plus / decryption.

B. database encryption system structure

Database encryption system is designed into two functionally independent main parts[4], an encryption dictionary management program, the other a database plus / decryption engine, the architecture shown in Figure 2.

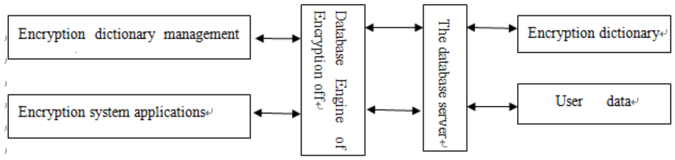
Encryption dictionary management
Encryption system applications
Database Engine of Encryption off
The database server
Encryption dictionary
User data

Fig.2 system architecture of Database Encryption

In the drawing, database encryption system records the concrete encryption needs of users to the database information. Encryption dictionary is the basic information of database encryption system. Process of the encryption dictionary mainly meets the needs of encryption. It is based on add / decryption engine database table encryption, de-dense and data conversion functions by database. At the same time, it can be used as the special users to utilize the plus / off Password engine. Plus / off Password engine is the critical role in database system, which completes the encryption / decryption process in the background and is transparent to the application development and operations staff.

4. Database encryption system limitations and database.

The database encryption cipher algorithm of the system encrypts the sensitive data in a high intensity and uses secondary key system to protect table key. his design can effectively prevent the attack from the operating system and DBMS[5]. However, the DBMS must be able to identify some of the data in order to complete the management and use of the database file, so you must have certain restrictions on the encryption system. In addition, the database encryption system will inevitably have some impact on DBMS.

A. Database encryption system limitations

1) The index field can not be encrypted. Database index field generally aims at rapid query, so index field needs to be built up and be used in maintenance in plaintext, or or they will lose the role of the index.

2) The connection between the code field in the table can not be encrypted. In the database, there exits the close connection among the database table, which is completed by the outer code. If the code is encrypted , the connection calculation between tables can not be performed.

3) The relational operators compare the field can not be encrypted. DBMS data in the complete relational operators, such as participation and poor selection and connection operations generally have to go through the screening of conditions, which must be plain text, or the DBMS will not be able to compare.

B. database encryption system DBMS

Data encryption is expressly complex cryptographic operations, which can not find the internal relationship between the plaintext and ciphertext and between the ciphertext and key. In other word, encrypted data can stand from the operating system and database management systems attacks. However, the sensitive data in the form of ciphertext stored in database can not to some degree use the database management system[6].

The database management system is relatively complete database data encryption, however, some of the features of the database management system will not be able to be used directly.

(1) Loss of ciphertext data grouping, sorting and classification functions
(2) Can Not be achieved on the definition of data constraints.
(3) Internal function in the SQL language will be useless in encrypting the data.
(4) The connection between the code field in the table can notbe encrypted.

5. Conclusion

The database encryption technology is an effective way to achieve the security of database information. This article discusses the basic database encryption key techniques as well as a database system design which should be adopted according to different requirements in practical applications. From the speed of encryption operation , increased storage space and the efficiency of database management system, to evaluate the encryption means performance, which id the only way to have a safe, efficient database encryption technology to ensure the security of the database system. Database encryption technology as an effective means of a data security protected will play an increasingly important role.

References

[1] Li Ping. Database encryption technology, Xinzhou Teachers University, 2010, 26 (5): 43-45.
[2] The Han Likai. Database encryption technology research and application, Journal of Xi'an University of Arts and Sciences: Natural Science Edition, 2011, 14 (4): 67-69.
[3] Zheng-fei database encryption technology and its application, Fudan University PhD thesis, 2005:16 of-19.
[4] Zhulu Hua, Chen Rongliang Database Encryption System, Computer Engineering, 2002, 28 (8): 81-63.
[5] Zou Bin laying the design of the database encryption system, Journal of Southeast University, 2005:1-3.
[6] Into the Miao of Database encryption technology Technology, 2010, 29:87.