Research of Database Encryption Technology and Its Application

Rui Wang

Liaoning Jianzhu Vocational College, Liaoyang, Liaoning, 111000

Abstract

With the continuous improvement of the national level of information technology, especially the rapid development of Internet technology, IT database system is more and more widely. However, the database system data storage and extensive sharing of features, making the database system security issues become very prominent. At present, only through the database management system's own security mechanism is also difficult to completely solve their security challenges. So the database encryption technology research has a considerable practical significance, it will modern cryptography principles applied to the database system, and further improve the database security system, effectively guarding the DBMS super administrator privileges too high risk, can be effective Against the invaders in the application layer of the attack, so as to ensure the safe operation of information systems.

Keywords: Data Base, Encryption Technology, Application Study

1 Introduction

With the extensive application of computer in all fields of society, the database management system of information system bears the sacred mission of storing and processing a large amount of important information. Attacks on information systems include frequent attacks on database systems, theft, tampering and destruction of information in databases, computer viruses, Trojan horses and other attacks on the database system are seriously endangering the security of information systems. Therefore, in order to adapt to the requirements of modern society, to ensure the government, finance and national defense and other vital information security, as a centralized storage and management of large amounts of data and for many users to share the database system, its security becomes Particularly important. Database management system (DBMS) is an important part of the information system, its main function is to organize and manage the data information, and provide convenient retrieval and use. Database management system security is to store the data stored in the database information security, so that due to man-made and natural causes of leakage, destruction and unavailability of the risk. The security of the database management system should not only consider the safe operation protection of the database management system, but also the protection of the data information stored, transmitted and processed in the database management system. Because the attack and the threat may be aimed at the database management system movement, may also be regarding the database management system in the storage, transmission and processing data information confidentiality, the integrity and the usability, therefore to the database management system security protection, The need for safe operation from the system and information security to consider the two aspects of comprehensive. As an effective means of information security, encrypted storage of data information has become an important line of defense for database security, and how to overcome the problems of dense database management and record query difficulties has become the most important design database encryption system. Is also the subject of this paper.

2 Data encryption technology in database

Encryption system architecture is complex and more closely linked, without affecting the accuracy of data under the premise of ensuring data security, authenticity and integrity, the need to start from the overall system, and the traditional encryption technology for data security Different needs, the implementation should be used in different ways. Traditional encryption technology consists of file-based database encryption technology, record-based database encryption technology, sub-key encryption technology, field-based database encryption technology and secret homomorphic technology. File-based database encryption technology, mainly to the database information as a whole system, the use of encryption algorithms for encryption, to ensure the authenticity and integrity of data information at the same time, but also a good guarantee of information security. However, this method has many shortcomings, such as data storage and modification procedures complicated, cumbersome information to read, making information security there are some hidden dangers. Record-based database encryption technology is the main characteristic of its data information closed. In general, the encrypted data information is an independent and integrated whole, therefore, it has a high security, has been widely used. Sub-key encryption technology has the advantages of other encryption methods do not have, it can be a single data encryption and decryption to solve the problems of the record, but also caused the encryption and decryption of the cumbersome work. Based on the field of database encryption technology, the basic content is recorded in different fields to form the basic encryption unit encryption means. It not only has a smaller encryption granularity, but also can be a single data encryption, with good adaptability and flexibility. The secret homomorphic technique is different from other encryption methods. It can operate on the ciphertext database, which has certain advantages.

With the development of information technology, encryption technology has gradually become an important means to protect the security and integrity of data information, but for now, the traditional encryption technology still has some shortcomings, so for numerical data preservation order encryption technology gradually Get people's attention, and slowly applied to various fields. Similar to the traditional encryption technology, this encryption technology is from the encryption system architecture, but directly applied to the encrypted data, do not decrypt the operands. At present, OPEC is a more common numerical data preservation order of the encryption scheme, which in the data information query and processing with high security and accuracy, but also timely processing and updating of data, In the practical application has certain advantages. In contrast, this encryption technology for data security and confidentiality of information is very important, but also has good encryption and decryption speed, to solve the other several encryption technology problems. However, this encryption technology has some limitations, can not fully apply the secret homomorphic technology, while key management also has some shortcomings, so the application of this encryption technology to a variety of factors to carry out.

3 Research on application of database encryption technology

Because of the particularity of data information, data information often involves many aspects, for people's normal life and social stability have a certain influence. Therefore, in the database encryption, it is to take full account of the security of data information. At the same time, due to the read and view of data information permissions, for those who are not authorized to strictly prohibit the user to view and read, so key management is particularly important. For the database, the data read and query data is the focus of the database system and difficult. In general, the database encryption, due to encryption algorithms, data information has been inconvenient to query, thus reducing the encrypted data query rate of the database. In order to ensure the efficiency of data query, we should give enough attention to the query of data in database. For the efficiency of data query requirements, we have to choose the appropriate encryption algorithm and decryption algorithm to meet the efficiency of data query needs.

Database data security not only embodies the integrity of the data, but also should ensure the accuracy of the data. Therefore, in the database information data encryption and decryption process, to ensure that the data in the database is not unauthorized users to modify. At present, because of the database encryption and decryption process loopholes, so the accuracy of data information is sometimes difficult to be guaranteed, the data and information security posed a huge threat. Therefore, in the database data encryption, pay attention to data theft, limit the rights of administrators to a certain extent, to ensure the accuracy of data and security information.

4 The problem in database encryption

In order to make the database security can be effectively improved, the application of encryption technology is of great significance. However, the application of database encryption technology there are some problems in the process of data encryption, may be due to improper handling of the database security does not rise instead of falling. And cause some adverse effects. Therefore, in the process of database encryption, the following questions should be fully considered and analyzed.

Traditional access control in the database provides users with a mechanism to achieve effective control of user access to data through the creation of the user and the authorization of the corresponding user to enable control to be achieved. The user only has access to the appropriate permissions, be able to carry out the relevant data operations. In the field of database security, the application of this mechanism can effectively improve the security, at this stage is basically all commercial DBM S are used in this mechanism can make illegal access to the database users be effectively avoided. Access control is divided into two categories: autonomous access control and mandatory access control. For autonomous access, the user access control of information is mainly based on user authentication and access control rules on the basis of the system, each access object requires the user to give access. For example, if a user needs access to a database resource, the system first checks the resource ownership of that user, allowing access to the request. Access control model is the most classic access to the rectangular model, access to the model and so on. For mandatory access control, the system assigns different security tags to the subject and the object, and performs the access authorization by comparing the subject and the object security tag to determine whether they match. Mandatory access control of the most classic model Bell-LaPaedula model, role-based access control model and so on. For a system, autonomous access control and mandatory access control can coexist, there is no conflict in the inspection system access process, first of all to check the M AC, and then check the DAC, if both are passed, then visit Can be allowed.

In the process of encrypting data, should be different for different data, there are dynamic data and static data, which is because they are using different encryption methods. Compared with the dynamic data encryption, the research on static data encryption still needs to be improved, and the relative research is lacking. In the database, the data structure is very high, and has a strong sharing, so the data stored in the database encryption, these features must be fully considered, and choose a reasonable encryption algorithm, encryption and encryption the way. First of all, in the choice of encryption algorithm, encryption and decryption must be made on the high speed requirements, should ensure that encryption and decryption process will not seriously affect the performance of the system. Second, the flexibility of encryption granularity is also analyzed and considered. The user's needs as the basis, select the appropriate encryption method, and also with the current phase of the D BM S combination, select the appropriate encryption. As the core of encryption algorithm, the choice of encryption algorithm is very important for the security and performance of database encryption. A good encryption algorithm must ensure that the generated ciphertext has a balanced frequency, with random and no rules of the code and a longer period, so as to avoid attackers by analyzing the ciphertext frequency and recoding to obtain confidential data. According to the structure of the database hierarchy, the database encryption can be divided into specific database-level, table level, record level, field level and data item level. In the choice of encryption granularity process, the corresponding application requirements must be adequately analyzed and considered.

5 Conclusion

At present, in order to ensure database information security, we need database encryption technology support, the purpose is to ensure that the data in the database based on the security of information, to avoid unauthorized disclosure of the problem. Database encryption technology as an effective measure to protect the data, in the future development will certainly be a broader application space.

References

[1] Yu Ting. Application of database encryption technology in enterprise information management. Silicon Valley, 9(3), pp. 16–18, 2013.

[2] Li Chu. Database-based security protection. Computer Learning, 1(8), pp. 23–28, 2009.

[3] Wei Huicai. Database encryption technology overview. Occupation, 12(2), pp. 72–77, 2007.

[4] Wang Yanhong. Design and Implementation of a Database Encryption System. Journal of Huangshi Institute of Technology, 3(6), pp. 16–19, 2007.

[5] Yang Chao. Database encryption technology features and application analysis. Silicon Valley, 3(5), pp. 42–43, 2005.