

Study on Security Management Strategy of Internet Network Database

Yan-Bo Wang^{1,a}

¹ Library, Xi'an University, Xi'an, Shaanxi, PR. China 710065

^aemail,

Keywords: Internet; Database; Security management; Strategy

Abstract: At present, the advanced Internet technology has penetrated into every corner of people's daily life, which largely promotes the vigorous development of e-commerce and other industries, and also brings many unexpected convenience to human life. While the database is the core of the entire Internet, which is responsible for the storage and management of all the information, so its security is essential. This paper is to briefly introduce the database, analyze the main security problems of the database under the current situation, analyze the various systems of Internet network database security management, and then put forward the pertinent security strategy aiming at contributing to the security of our country database.

Introduction

Since 21st century, many advanced science and technology in our country have made great achievements. Among them, Internet technology and database technology have made great breakthrough. At present, Internet technology has been widely used in various industries and fields and plays an extremely important role. However, the Internet has its advantages and disadvantages, such as the leakage of information and the loss of stored information, therefore, the security of network database is a difficult problem that many technicians have been exploring and trying to overcome.

Brief Introduction to the Database

In this era, the Internet technology is extremely developed. The importance of computer in human work mainly lie in the computer can greatly reduce the workload of the staff, such as dispose information resources, complex calculations, drawing drawings and so on, in which the dispose information resource is the biggest function of the computer, and the database can help the computer to display the information resource processing function. The main components are shown in the figure below.

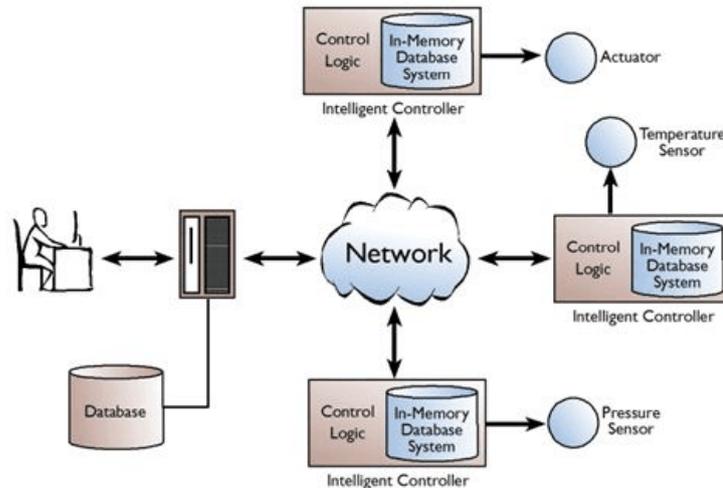


Figure 1: database system

In short, the database is a warehouse that used to store information, and it can organize and manage those information data before storing them into the data according to their data structure, so as to store all the information in different categories in order to convenient for the follow-up operation and search, and to avoid errors. With the continuous progress of computer technology and the popularity of the Internet, there are more and more types of database connect to the Internet, and the database can be adjusted according to user requirements. The previous database can only contain a small amount of data stored in the table. Compared to the past, now the database storage space is greatly increased, which can not only store large amounts of data, but also search and call all data in a short time.

Security Issues of Database

As we all know, all the data stored in the database can be shared, that is, people can simultaneously use, download and store data in the database, because the database has this feature, everyone can enter the database, which may cause data theft and loss, even hacking the database, causing serious safety loophole, then unable to guarantee data integrity and confidentiality.

Security Issues of Data in Database. In order to ensure the integrity of all data, the database set up a check mechanism, which will play its role when a user access to the database and download activities. Because the database has the characteristic of sharing information, which will inevitably result in that many different users simultaneously enter the database and download the same information data. In order to monitor the illegal behaviors of some users, to control and maintain the stored data, and to keep the consistency of the data, the database is usually set up a control mechanism. The database has many influence factors that may come from man-made activities or from the outside world, causing computer failure. On the one hand, it destroys the correctness and completeness of all information data. On the other hand, it interrupts the operation of transaction and brings the user with problems. Therefore, the database is usually equipped with subsystems that can deal with the computer failure, and improve the error state of data, and ensure the consistency of data logic as much as possible, thus greatly reducing the probability of information loss.

Database System Invaded by Illegal Invasion. In general, each database is equipped with a full-time administrator whose job is to maintain the safe operation of the database to clear the potential threats, to timely repair the loopholes, as well as to prevent illegal invasion from some users. Although the inner database has been set up the firewall and other security mechanisms, and

equipped with a full-time administrator to monitor at any time, the security of the overall database system is subject to many external factors, such as network environment, hacker computer technology, and application environment.

The Security Management System of Internet Network Database

An Internet system often contains many databases of varying sizes, and each database can be divided into different levels. Therefore, the security of Internet network database not only means that the existence of the associated database security, but also to ensure the security of a database that contains more level functions. The security management system of network database can be divided into two main aspects of the outer layer and the core layer, of which the former one can be divided into two parts, one is the network system, and another one is the computer operating system. While the latter one is the database itself. The following part will analyze the security management strategy respectively base one these aspects.

The Security Management Strategy of Internet Network Database

First of all, we need to consider the security of the database from the outer layer, because the threat of the outer layer is mainly come from the virus. Therefore, it is necessary to strengthen security technology, and use the methods of prevention, killing and management to solve it as well as to ensure that the two parts of outer layer keep away from the violations of virus. Second, the security of the database needs to be considered from the core layer, which is to ensure the security of the database itself, and use different ways to protect the database from other outer factors, and keep them confidential. The principle is shown as below:

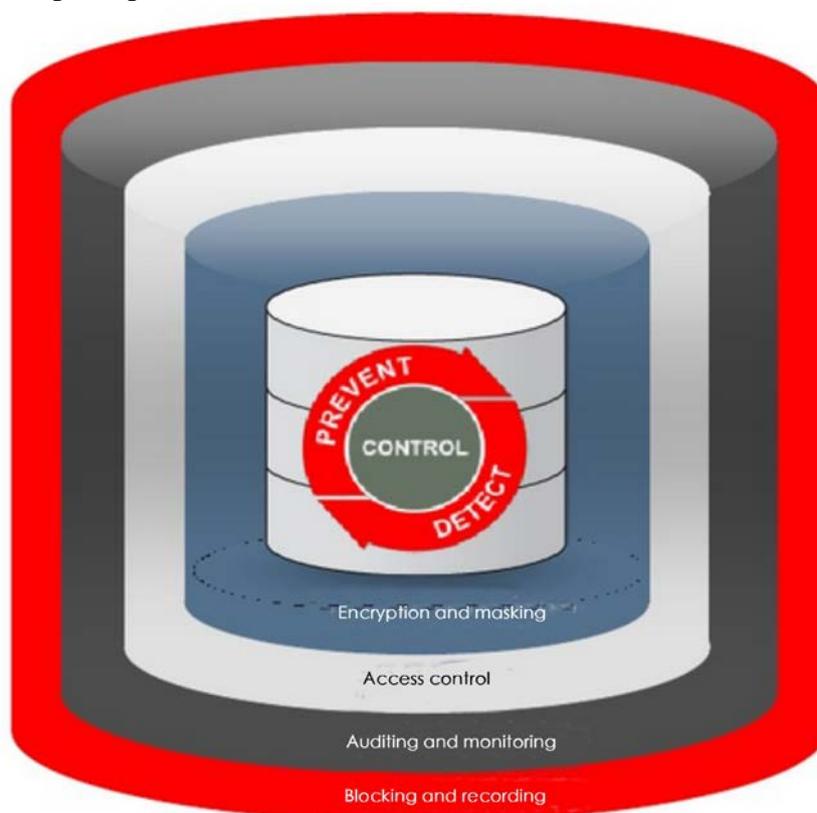


Figure 2: the schematic diagram for database safety protection

Strengthen the Security Technology of Network System. At present, the Internet technology and network technology has been expanded massively, which promote the rapid development of all

walks of life, and have changed people's lives dramatically. Its application is very broad, especially favored by the e-commerce industry, so network security and manageability are extremely important. As a part of the network system, the database is of great significance in the storage and organization of information resources, which can help the network system play its major role to some extent. However, the security of database is more vulnerable to threats when it is connected to the network and builds up inter connection. For example, some users may tamper and steal the information on the Internet. Some users may suffer from viruses like trap doors, Trojans and other foreign invasion under the open network environment, resulting in incomplete information, and even cause leakage for some confidential information. However, the network system is the first protection layer for the security of the network database, which has the effect of resisting on the virus invasion. Therefore, we should pay attention to strengthen the security technology of network system. While there are many types of security systems for the network technology, such as firewalls, intrusion detection, etc. The administrators should always pay attention to whether the firewall is an active mode, and the computer system is needed to be processed with intrusion detection regularly in order to prevent hacker intrusion. To achieve this, it is necessary to establish a virtual private network for the database, and network access security, so as to make the information transmission channel more secure. At the same time, the technical researcher should increase their research and development efforts to enhance the network security technology as much as possible, and to resist the external virus from the outer layer, thus to maintain the security of network boundaries. For example, a well-known bank on the east coast of the United States is using the database firewall to accurate protection of the database. As the amount of transactions in the bank could be up billions of dollars every day, in order to monitor and protect critical databases, to avoid the loss of important data and PII exposure and prevent unauthorized access to the database, the bank adopts Oracle Database Firewall for real-time protection to the database, monitoring all transactions, as well as preventing malicious behavior of illegal user, so as to ensure the normal operation of the bank's business.

Strengthen the Operating System Security Technology. Operating system is an important part of the computer system, which can not only provide users with the opportunity to communicate with the computer, but also provide a running platform for database system, to a certain extent, play a protective role. In the current situation, the operating system security technology is mainly divided into three aspects, namely, security strategy, security management strategy and data security, of which the former one is mainly focus on the computer itself to set the security, such as IP address security management strategy, password strategy, etc. The users can set a password for them or lock their account, set up a permission for foreign users, in order to protect the computer from being operated by other person, as well as to recover the enciphered data and ensure the authenticity and confidentiality of the data.

System Security Strategy. The strategy is developed from six different perspectives. First, to set permission for all users who can manage the database, because different databases have different daily tasks, which require different numbers of administrators, but the database has no permission setting for the administrator user. So there are some special users can manage the phenomenon of the database, resulting in potential security threats, we must develop some strategies against this phenomenon, and pick out the trustworthy administrator; Second, all users who can access to the database are needed to be identified, which required the users to input themselves identity information by operating system before entering database, and the system will process their information, so as to ensure the legitimacy of operation by each user and avoid the occurrence of

illegal activities; Third, to strengthen the security of the operating system, the administrator has the permission to create or delete files in order to facilitate the management of the administrator, by doing this, it can ensure that the operating can be correctly modified when necessary, and to maintain the security of the operating system; Fourth, to strengthen the security measures of users, in general, the ordinary users are needed to be identified the information when enter the database system. Each user has a corresponding account and password. However, we need to figure out the security strategies for those end-users, for example, the management can divide all users into groups, and give each group a corresponding role, and finally manage the users' permissions according to their role; Fifth, to strengthen the security measures of administrator, due to the server and the user are connected through the network. The manager has connection to the database through the operating system, and the system should protect the security of the two connections, and govern the permissions of the managers by roles; Sixth, the security strategy for application developer, in order to facilitate the processes and follow-up management of program development, the permission of developers and administrators should be clearly divided, and to authorize the development of application.

Encrypting the Database. The information and data in the database are stored and managed in the form of file, and the user downloads the data in the form of file, which makes it possible for some illegal users to invade the database, causing the stored information being tampered and incomplete. And usually, the users are not easy to discover, so the files of database management system must be encrypted to reduce the possibility of the file for being stolen and tampered. The encryption of the database can be divided into three levels, namely, the operating system layer, inner nuclear layer and outer layer of the database management system. For the operating system layer, it cannot identify which file contains the data relationship, resulting in the key cannot be generated, not to mention the use and management of the key. Therefore, it is almost impossible to encrypt the operating system layer; for the inner nuclear layer, the encryption work must be completed ahead of schedule, that is, before all the data has been physically accessed. This approach more effectively ensures the security of information. For the outer layer, the system may be considered as an outer instrument, and then automatically processing the encryption according to the specific requirements. For example, Cornell University carries out the Enterprise Manager to monitor the entire school database and server, and encrypts all sensitive data by using Data Masking Pack, in order to ensure that teachers and students can access to the operating system and academic systems under entire distributed IT environment, so as to service teachers and students.

Conclusion

The well-developed Internet in the network causes the proliferation of information, as well as the abuse of network technology, which brings a threat to network security. As the core of the Internet system, the database plays an important role in the storage and management of data. Although many improvement measures have been done for the security of the database, the database still has potential safety hazards, which requires continuous exploration by the developers and continuous research and development by the related technicians to further ensure the safety of the network database.

Reference

- [1] Liu Cunyan. The measures of safety management in Internet network database [J] Computer

CD - ROM Software and Application, 2013,01: 92-97.

- [2] Cai Wei. Managing Strategy and network safety analysis in the era of “Internet” Information Security and Technology, 2015,09:8-11.
- [3] Zhang Yumei. Research on Security Management Technology of Computer Database in Internet. Journal of Mudanjiang University, 2016,08:134-136.