ATLANTIS PRESS
Advances in Social Science, Education and Humanities Research (ASSEHR), volume 230
3rd International Conference on Education, Sports, Arts and Management Engineering (ICESAME 2018)

A Brief Analysis of Database Security Policy

Li-jun MA
Baicheng Normal University, 137000, China
mljcjy@163.com

Keywords: database, Security, Network, The age of cloud computing

Abstract. in the network time, the database security problems become issues that people can't ignore, people need to take a series of measures in the security of the database, to ensure the security of data information. This paper expounds the importance and strategy of database security from three aspects: security of database management system, network security and database security of cloud computing era.

Introduction

In today's information society, the development of network technology speeds up the information transmission and processing, cuts down the space-time distance between people, makes communication convenient, but it also puts forward the new challenge of information security. According to statistics, a computer virus invasion occurs every 20 s globally, at the same time, about a quarter firewalls on the Internet were breached, business information stolen events increase at the rate of 260% per month on average, about 70% of the network manager report the loss due to leaking classified information. The problem of information warfare is related to the fundamental security of the country. To solve the security problem of information, we need to understand the strategy of database security in some aspects, and then formulate a series of specific security strategies. This article explore database security controlling strategy from three aspects including the security of the database management system, the security of network database and the database security under the background of cloud computing.

Database management system security

The security of database relies heavily on database management system. At present, most database management systems provide verification mechanism, view mechanism, control authority mechanism and audit mechanism, so that the security of database is guaranteed.

Authentication Mechanism. Set as Windows authentication mode. SQL server safety certification has following two modes: Windows authentication and Windows and SQL server hybrid authentication mode. Windows authentication mode only allows users to log in the server using Windows authentication mode, and using the login account of SQL server is not allowed. This approach limits the connection between Windows users and domain user accounts, thereby protects SQL server from most Internet tools, and the server can benefit from the Windows security enhancement mechanism.

User storage Access Control. Storage access control is the determination, grant and implementation of access rights to the data protected. Different users have different access rights to the database, and the DBMS implements access control according to user's access rights, which is realized through the identification and authentication of users. SQL server permissions system is set up based on users or role set GRANT (awarded) permissions, REVOKE permissions (back), DENY (refuse) permissions, can ensure a specific user specific objects belonging to a specific role permissions, represents that a user or a role has the right to perform certain operations. For example, to grant user U1 with permission to query and modify the student table, and allow him to grant this permission to other users. The authorization statement is as follows:

GRANT SELECT, INSERT ON student TO U1 WITH GRANT OPTION.

View Mechanism. A view is a virtual table of rows and columns, a results data set roots in tables

or other views.

By using different views and granting different permissions to users, different users can see different result sets , data security at the row or column level can be achieved.

For example: to establish “ sno, sname, ssex” information of students with sdept as "computing department" in student (sno, sname ssex, sage, sdept) , the information of other department students is not displayed, and hide the student's sage field information, the view is established as follows:

CREATE VIEW student_computer (sno, sname, ssex) AS SELECT sno, sname, ssex

FROM student WHERE sdept= " computing department ".

Define Stored Procedures. A stored procedure is a set of SQL statements that perform specific functions, which is stored in the database after being compiled, user perform it by specifying names or parameters of the stored procedure. The way to implement the security of a database using stored procedures is to grant users permission to execute the stored procedure without granting permission to modify the table.That is to make users not have permission to access view and tables, then through stored procedures can still make the corresponding data information query, just let users have permissions of that stored procedure. For example: to create a stored procedure of students information of the computing department. The program section is as follows:

CREATE PROCEDURE student

SELECT * FROM student WHERE sdept= " computing department "

The permissions for the stored procedure are then granted to users, and users can query the information when they execute the stored procedure.

Auditing Mechanism. In order that the database can reach a certain level of security, it also needs to provide corresponding support in other areas. A very important security measure is the auditing mechanism, which must be used as a preventive measure for some highly sensitive data. Auditing mechanism is a monitoring measure that tracks and record access to related data. However, using auditing can greatly increase the overhead of the system, so the DBMS usually uses it as an optional feature, providing appropriate operation statements to open or close the audit function flexibly.

Network Database Security Mechanism

The network database is based on the background database, adding the foreground program to provide access control, to complete the information collection of operations such as data storage, querying, through the browser. In the network environment, the main feature of database is the ability to share a large amount of data information while maintaining the integrity and consistency of the data to achieve the minimum redundancy and access control. B/S mode and C/ S mode are two typical network database modes. The C/S mode adopts the three-decker structure of "client - application server - database server", and the B/S mode adopts "browser -Web server - database server" structure. The two patterns have a lot in common: all come down to network, system software, and application software. In order to make a clear concept of the whole security mechanism , in allusion to the characteristics and commonness of the two models, the hierarchical structure model of network database system security mechanism is established. The combination of client/server mode and WWW technology has further evolved into browser server mode B/ S. This model is a combination of database technology and network technology, its structure is expressed as:

Browser, Web server and application server, database server three-decker structure.

Specification on the Security Mechanism of Each Decker. ***Security Mechanism of Network System***. There are many kinds of security technologies at the network system level, which can be divided into firewall, intrusion detection and cooperative intrusion detection technology.

(1)The firewall is the most widely used protection technology. As the system's first line of defense, its main function is to monitor the access channel between trustable and not trustable networks, to form a protective barrier between the internal and external networks, to intercept illegal access and prevent external internal information from leaking, but it cannot stop illegal operation from within the network.

(2)Intrusion Detection (IDS - Intrusion Detection System) is developed in recent years as a precautionary technology, comprehensively using statistical techniques, rules methods, network communication technology, artificial intelligence, cryptography, reasoning techniques and methods, it is used to monitor that whether or not the signs of abused or invaded of the network and computer System exist. In 1987, Derothy Denning first put forward the idea of intrusion detection, through continuous development and perfection, the IDS system has become an important part of security defense system as standard solution of monitoring and identifying attacking,.

(3)The collaborative intrusion detection technology makes up for the lack of independent intrusion detection system. IDS in collaborative intrusion monitoring system is based on a unified specification, invasive monitoring components automatically exchange information, and through the information exchanging gets the effective invasion monitoring , this can be applied to different network environments.

Security Mechanism of Server Operating System. Operating system is the operation platform of large database system, which provides a certain level of security protection for the database system.

(1)The operating system security policy is used to configure the local computer's security Settings, including password strategy, account locking strategy, audit strategy, IP security policy, user rights assign, recovery agent of enciphered data, and other security options. Concreteness can be reflected in user account, password, access authority, audit and so on.

(2)The security management strategy refers to the methods and strategies adopted by network administrators to implement the security management of the system. The security management strategies for different operating systems and network environments are generally different, and the core mission is to ensure the security of the server and to allocate the rights of all kinds of users.

(3)Data security is mainly embodied in the following aspects: data encryption technology, data backup, security of data storage, security of data transmission, etc.

There are many technologies available, such as Kerberos authentication, IPSec, SSL, TLS, VPN (PPTP, L2TP) and other technologies.

Security Mechanism of Client Application Program. Client application program is an important aspect of network database security. It is characterized by its strong independence and convenient implementation, especially easy to make corresponding changes according to the change of requirements. The client application program can control users' legal login, authentication, and so on, and can directly set data. Strengthen application programs controlling can better guarantee the application system security. In addition, the writing of client application program cab be very flexible, flexible and safe management of clients-side can be achieved. The technology of user identification based on COM+ component application can greatly improve the security control management of clients-side.

Using DBMS Security to Prevent Network Attacks. ***Authentication and Authorization***. Authentication is the process of verifying the identity of the person or application that requests the service in the system; Authorization is the process of granting permission of a database user with an identity mapping that can pass identity authentication, this process limits users' behavior which is allowed to occur within the database. Through the authentication mechanism of SQL Server database, the problem of "who am I " can be solved; Through the authorization mechanism, you can solve the "what I can do" problem. These technologies mainly include user mark and identification, access control and so on.

Backup and Recovery. Through database backup, when the system fails, the administrator can quickly restore the database to its original state to maintain the integrity and consistency of data. Generally speaking, the common methods of database backup include static backup, dynamic backup and logical backup, etc. Database recovery can be done through disk mirroring, database backup files, and database online logs.

The Audit. Auditing is the mechanism of monitoring and recording the various actions that users impose on the database. Through audit, all operations users have done to database can be recorded and put in the audit log automatically, so the database system can use audit tracking information, reappear a series of events that lead to existing status of database, find the person, time, contents,

etc. that is relative with illegal accessing data, so as to pursue the responsibility, at the same time audit can also help to find out loopholes and weaknesses of the system security.

The rapid development of Internet, make the network no longer a simple messenger, but an interactive platform, and the security problem of the database is forever a developing problem, along with the constant improvement of invasion methods, the security technology is also in constant increasing. The security of database can be continually enhanced only if new situations and problems are constantly studied and disposed. Safety precaution is a permanent problem. Only continually improve and perfect the security methods can improve the system's reliability.

Database Security in the Era of Cloud Computing

So-called cloud computing is a kind of virtualized technology, using this technique, users do not need to understand the basic mechanism of its operation, users can be directly connected to the cloud computing services and related services ones need through networks, this can effectively improve the utilization of computer network resources, at the same time also can effectively realize network resource sharing, can effectively save the cost of the related hardware resources.

However, with the convenience of cloud computing, the security of the database becomes a problem that people cannot ignore, people need to take a series of measures in terms of the information security.

Database Security Issues and Challenges in the Context of Cloud Computing. The cloud, private cloud, hybrid cloud, and community cloud are the main components of the cloud deployment model in the context of cloud computing. The related security issues (examples of relational databases) are summarized in the following aspects.

(1)High concurrency, slow reading and writing. The related problem appears mostly in a state when the data reach relevant scales, relational database has a more complex system logic, so the deadlock phenomenon happens frequently, and then, affect system’s reading and writing speed, for example, for Web2.0 the website needs creating in time related dynamic pages, and then providing relevant dynamic information in accordance with the users’ personalized needs of relevant networks.

(2)The support capacity is limited. Similar to social networking sites like Facebook, Twitter, a large number of users’ information is produced every day, the amount of information can even reach hundreds of millions of the dynamic information each month, the efficiency of information processing process is hard, or even intolerable to meet the needs of users for a relational database to query data in billions of forms.

(3)Poor expansibility. It is difficult to effectively horizontally extend for the database under the framework based on WEB technology, when users and visits of related application reach a certain number, it’s hard for relational database to extend the hardware and software, and then, can not fully meet the extension and load capacity of relevant data. It is difficult to upgrade and extend the database system for many websites that need to provide uninterrupted service to users.

(4)The cost of system construction and operation is high. The cost price of establishing an enterprise database is higher, and the cost is rising with the increasing scale of database, the high construction costs and maintenance costs make it very difficult to meet the requirements of relevant applications to the database, it is a bottleneck in the development of a relational database.

The Corresponding Strategy of Database Security in Cloud Computing Environment. The security of database mainly includes two aspects: first, the security of the computer system. On the other hand, it refers to the security of the database system. We propose the following three security strategies:

(1)Establish data-centric security systems. The relevant data in cloud computing is usually in the corresponding Shared environment, so the developers of the data should strictly regulate the right to use and use scope of the information data.

(2)Improve the corresponding authentication and management system. In the process of cloud computing, it is necessary to perfect the corresponding identity management system and beautifully deal with the problems of private and key identity attribute. Cloud computing systems should be

user-centered, appropriately inspect the context of the user identity information, under the premise of fully ensured data security the whole system should respectively restrain or relax the corresponding limiting condition, and then effectively meet the needs of users. At the same time, it is necessary to further study the scheme of identity management system, which can be fully integrated with the existing identity management system of enterprises, so as to effectively enhance the security of the cloud environment.

(3)Adopting authentication of double security mechanism and effectively controlling corresponding access through access control list also can prevent hackers to destroy the system database. The authentication methods commonly used in the actual process are: password authentication, certificate authentication and biometric authentication. Currently, passwords authentication are used more often, but the security is unsatisfactory.

Summary

The database security problems have always been a horrible dream of database application system designers and users, database data lost and invasion by illegal users make the database application system designers and users physically and mentally exhausted. To realize database security it is necessary to increase awareness and improve the use and management technical level under the influence of factors of technique, legislation and administration, so make the safety of database achieve a more ideal standard. This paper analyzes the security mechanism of database from different aspects of database application, and provides certain reference value for the security of data in database.

References

[1] Li-jun MA. The Integrity Rules and Constraints of Database[J].2011 International Conference on Electronic & Mechanical Engineering and Information Technology (EMEIT 2011), 2011.08 pp3796-3799.

[2] WANG Shan. Rang. Introduction to database systems [M]. Advanced education publishing house. 2016

[3] Hui Yuan , Lei Zheng , Xiangli Peng. Security Workflow Model for Database Storage [J]. 2nd International Conference on Computer Engineering, Information Science & Application Technology (ICCIA 2017).

[4] Umarani Jayaraman. Use of geometric features of principal components for indexing a biometric database[J]. Umarani Jayaraman, Surya Prakash, Phalguni Gupta. Mathematical and Computer Modelling. 2013(1-2)

[5]LIU Xiao-ling, LIU Zheng. The Analysis and Discussion of Computer Database Security Management [J]. Journal of Shandong polytechnic university 2013.2

[6] Li-jun MA Analysis of the relationship between the relational database, data warehouse and data mining 2012 International Conference on Electronic & Mechanical Engineering and Information Technology (EMEIT 2012), 2012.08