Design of Embedded Network Database Encryption System Based on BS Structure

Qinmin Ma

School of Artificial Intelligence, Shenzhen Polytechnic, Shenzhen, Guangdong, 518055, China

maqinmin@vip.163.com

Keywords: B / S, Embedded, Network Database.

Abstract: With the rapid development of Internet, government, enterprises and individuals will produce a large number of data, most of which will be stored in the database. In particular, governments and enterprises that create state secrets and trade secrets have become an important topic in the field of information security. To ensure the security of database has become a problem that must be faced. Due to the initial sensitivity and aperiodicity of chaos, there is a natural connection between chaos and cipher. The pseudo-random sequence generated by chaos has a good application prospect in the field of information encryption. Based on these related research background, chaos encryption is applied in the field of database information security, a new database cracking scheme is proposed, and a database chaos encryption system based on B / S structure is designed and installed.

1. Introduction

With the rapid development and popularization of the Internet, the government, schools and enterprises have produced a lot of data in the process of work. These data often contain government secrets, trade secrets, intellectual property rights, personal information and other confidential information. Once stolen, the consequences are serious, which will cause huge losses to the economic interests of enterprises. Most of this data is stored in the organization's database. How to protect this data security is an important issue. With the development of the times, the enterprise information security is the database security, and the database security is the key to the enterprise information security. In order to protect the security of the database, it is not enough to rely on the access control permission of the system. The obvious disadvantage of access control is to allow database administrators access. According to relevant information, 80% of enterprise information leakage comes from the person in charge of the system. In addition, some network hackers can also access the data recognized by the system through the corresponding crack technology[1]. At the same time, some database application developers also pose a threat to database security. As the company's confidential information, it is necessary to write corresponding code for developers to deepen the understanding of the whole system. Potential people, at the same time, part of the legal profession may also try to illegally obtain some secret information of the database. Many countries and governments have relevant laws and policies that require relevant companies to ensure the security and confidentiality of customer information. For example, the California Data Privacy Act requires companies to implement appropriate confidentiality procedures to protect California residents. Personal information is secure. In addition, if the company accidentally divulges the customer's personal information, it will bring great damage to the company's reputation. Compared with those database access control, database encryption can provide a more secure and reliable method of database protection[2]. The research on database encryption is necessary. Therefore, database encryption is a good way to protect database security, both from the technical level and from the commercial point of view.

2. Research Status and Development Trend

  DOI: 10.25236/cseem.2020.058

Chaos can be understood from the literal meaning of irregular things[3]. Chaos has the same concept as ancient China. Even with reference to some undifferentiated materials in ancient Greece, there are "three and five calendars" and "Zhuangzi" to explain chaos, but generally speaking, the understanding of chaos is correct. Although the chaos at that time was different from that at present, it was also the beginning of chaos research. Through continuous development of chaotic ciphers, the unique advantages of chaos can be realized continuously. For example, chaos has the advantages of strong confidentiality, large key space and good random performance[4]. However, in practice, it will continue. Chaos will produce short period phenomenon and many other problems. In some cases, their duration will be very short, because each chaotic sequence has no good random performance. This is the reason why the chaotic system responds in a short time. Second, the generation of general chaotic array is produced by the equipment with limited precision. Under the existing general conditions, the accuracy of the equipment used is limited, and the generated sequence is quite different from the theory. Therefore, we can not achieve the chaos sequence we expect, which is the so-called limited precision effect. This is also a big problem of chaos in practical engineering applications. When the accuracy of the system becomes shorter, some shorter duration effects directly reduce the performance of chaotic sequences. Furthermore, the secrecy of the system is affected. The application of chaos to communication security is a big problem.

3. The Development and Research Status of Cryptography

In various fields, only the password field is different. On the contrary, it consists of two branches: interdependence and complementarity. Compared with other information security, the password is designed to prevent it from being obtained by the imaginary enemy to ensure the information. Many security mechanisms are used to restrict access, and then, the recognized users access. They often control the complex process[5]. On the other hand, information encryption also assumes that the enemy can provide relevant information when landing. Complete security, this is the ultimate security. The history of cryptography can be divided into three stages. The first stage is from ancient times to the end of the 19th century. Due to the low level of social development in this era, the production system with low production efficiency can be realized by paper, pen or simple device. The encryption system of this era is called "classical password"[6]. The second stage is from the early 20th century to the late 1950s. During this period, Morse established telegraph communication when he invented telegraph. In order to protect the related information in the communication of telegram, the encrypting device designs the encrypting system which uses the complex machine and the electrical machine to perform the encrypting / decrypting. At the same time, the encryption system generated during this period is called "modern cryptography". The third stage starts from Shannon's epoch-making paper communication theory of secret system in 1949, which proves that the cryptosystem has a solid mathematical foundation [8]. At the same time, the development of microelectronics technology makes the electronic password enter the historical stage. And, especially in the mid-1970s, "modern encryption systems" emerged. The openness of DES encryption algorithm and the introduction of public key thinking promote the vigorous development of modern cryptography.

4. B/S mode

With the rapid development of Internet technology, the existing C / S mode can not meet the new requirements of Internet Interconnection, openness and information sharing[9]. At this time, the newly developed model is B / S model. This mode is mainly composed of client browser, web server, application server and database server. Users of the system developed in B / S mode do not need to install any client software. At present, the corresponding application software upgrade of users is fast and fast. If the traditional development mode is used, the efficiency of round-trip between computers is very low. Use B / S model in development. When updating, the server needs to update and upgrade. Client browser, it's necessary to install. Today's computers are installed in Windows operating system and have their own browser, so it's not necessary to invest too much in

the aspect of development cost. In terms of data security, the original C / s development mode software uses the data transmission characteristics, so in their website application software, the complex number of servers are set in various locations, and data synchronization must be carried out in the server aspect[8]. Database security on the server is known as a problem. When using B / s development mode, the client does not store any business data and database connection information, does not need data synchronization, and ensures the security of database server. This paper introduces the research of database encryption in this subject.

4.1. Overall System Structure

According to the research in the previous section, all database encryption systems can be designed according to some of the above research objectives[9]. The system designed in this paper is divided into three parts: database application layer, database encryption service layer and back-end data.

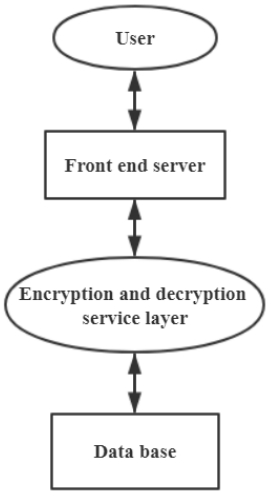

Figure 1 Database encryption process

In the database application layer, this article is based on the B / S architecture, so the application layer is the user's browser. When the client software installation is added, it can greatly promote the use of the system and improve the commonality of the system. Database encryption server layer is the core component of the whole system. Be responsible for the encryption and decryption of the whole database. The overall performance of the system is reflected in this layer. In this draft, including the design and installation of encryption algorithm, the generation and management of key, and the interaction with other layers, this layer is the center of the research[10]. The back-end database layer mainly includes all kinds of databases needed to design the system. In order to provide encryption services to the database, this paper installed encryption separately outside the database system, and adopted modular design. The functions of each functional module are independent of each other. At the same time, the control center of the database encryption system calls each module evenly. The system module is mainly composed of user login module, database encryption, decryption control center module, key management and front-end server.

4.2. Key Replacement

In order to enhance the security of database encryption system and improve the difficulty of system decryption, we must determine the service life of the key according to the strength of the encryption algorithm designed by the system, and exchange the key regularly. When exchanging keys, decrypt all encrypted data in the database and encrypt them with new keys. At the same time, the previously used key must be completely discarded or placed in a safe storage environment. In key exchange, the use of database is temporarily stopped. Because the amount of data stored in the database will increase, it will be very difficult to exchange keys frequently. In this system, due to the multi-level key management method, the data key is encrypted and saved through the user

public key. When the user changes the password, the secret key of the user is decoded first. Re encrypt the user's secret key with the new user password. This increases the security of the system to a certain extent, so the key exchange of the whole system is updated every few years.

5. Conclusion

In this chapter, based on the B / S architecture of the database chaotic cryptosystem design, the corresponding B / S mode is proposed to expand, the introduction of modules to encapsulate the whole system response suggestions, according to the design of each module, analysis and discussion. This paper proposes the solution corresponding to the generation of data encryption key and the corresponding research related to the storage and management of key. A scheme of secondary key management combining AES and RSA encryption algorithm is proposed. The key problems of permutation are studied.

References

[1] Reinharz, Vladimir., Soulé, Antoine., Westhof, Eric. Mining for recurrent long-range interactions in RNA structures reveals embedded hierarchies in network families. Nucleic Acids Research, vol. 8, no. 8, 2018.

[2] L. LuAnn, Minich., Victoria, L., Pemberton, Lara S. Shekerdemian. The Pediatric Heart Network Scholar Award programme: a unique mentored award embedded within a multicentre network. Cardiology in the Young, vol. 28, no. 6, pp. 1-8, 2018.

[3] Rawat, D. B., Bajracharya, C., Grant, S. nROAR: Near Real-Time Opportunistic Spectrum Access and Management in Cloud-Based Database-Driven Cognitive Radio Networks. IEEE Transactions on Network & Service Management, 2017.

[4] Yin, Bincan., Xin, Shichao., Zhang, Han. Building Asian Tumor-patients Prognostic Model with Bayesian Network and SEER Database——Case Study of Non-Small Cell Lung Cancer. Data Analysis & Knowledge Discovery, 2017.

[5] Sihang, Qiu., Bin, Chen., Rongxiao Wang, Estimating contaminant source in chemical industry park using UAV-based monitoring platform, artificial neural network and atmospheric dispersion simulation. Rsc Advances, no. 7, 2017.

[6] Dr. Salwa Mohammad, Dr. Basma Kamal Ramadan, Dr. Mona Schaalan Schaalan. Mitigation of Azathioprine-induced Testicular Atrophy by Taurine; An Impact on Inflammation, Oxidative Perturbations and Apoptosis. Canadian Journal of Physiology & Pharmacology, no. 96, 2018.

[7] Herron, J., Hutchinson, R., Lecky, F., et al. The impact of age on major orthopaedic trauma: an analysis of the United Kingdom Trauma Audit Research Network database, vol. 99-B, no. 12, pp. 1677, 2017.

[8] A. Majumdar., D. Roccarina., D. Thorburn. Management of people with early or very early stage hepatocellular carcinoma: an attempted network meta-analysis. Cochrane Database Syst Rev, vol. 66, no. 1, pp. S214, 2017.

[9] Matej, Usaj., Yizhao, Tan., Wen, Wang., TheCellMap.org: A Web-Accessible Database for Visualizing and Mining the Global Yeast Genetic Interaction Network. G3 Genesgenetics, vol. 7, no. 5, pp. g3.117.040220, 2017.

[10] Rosa, Lombardi., Simona, Onali., Douglas, Thorburn. Pharmacological interventions for non-alcohol related fatty liver disease (NAFLD): An attempted network meta-analysis. Cochrane Database of Systematic Reviews, vol. 3, no. 3, pp. CD011640, 2017.