Application of Data Encryption Technology in Electric Power Informationization

Cai Yingkai, Zhang Ye, Cao Shilong, Mu Rong

State Grid Liao Ning Marketing Service Center Caiyingkai Zhangye Caoshilong Murong, Shenyang, 110000, China

Abstract. A large amount of data information will be generated during the construction and operation of the power system, and once these data are leaked, it will undoubtedly threaten the information security of power users, which will bring avoidable economic losses to power companies and users. Therefore, many electric power companies are paying more and more attention to data security, and data encryption technology solves this problem well. And this article has launched a detailed analysis on the application of data encryption technology in the construction of electric power information. At the same time, it has carried out an in-depth discussion with the practical application of the two-layer encryption method in the informationization of electric power enterprises. I hope the research results of this article It can provide a certain reference for the information security management of the power system.

Keywords: power informationization; data encryption; application

1 Introduction

With the development and progress of social science and technology, the level of power informatization is constantly improving, but with it, the threats to data security are also increasing. Illegal behaviors such as data tampering, theft, and loss have impaired the power information system. The normal operation of power plants has had a serious impact. Therefore, data security work plays a major role in the entire development process of power companies. In 2014, State Grid Corporation successively launched handheld power APP software in many provinces, users can use the software to recharge electricity bills, emergency power transmission, fault repair, power query, check power outage notices and many other services. During the promotion period, many shops that provide users' electricity binding services appeared on Taobao. In the process of binding, a large number of users' personal information was obtained, which led to the leakage of personal information of many users and brought users A huge economic loss. Therefore, in the process of power grid information construction, data leakage prevention work needs to be done well. To avoid leakage of data and information. Encryption technology is one of the most practical and simple methods, which can effectively ensure the communication security of power system information, and is widely used in power information systems.

2 Overview of Electric Power Information System

Electric power informatization can improve the production efficiency of power enterprises, but at the same time some potential network security risks are also accompanied by it, so certain measures need to be taken to ensure the safety of the system. First of all, standardization and effective management of network identity credentials is the prerequisite for the construction of a network trusted system. With the help of identity federation technology and unified identity management, network access can be well controlled. In addition, during the operation of the electric power information system, it is necessary to carry out regular guarantee evaluations in order to be able to timely discover the existing and safety risks and omissions in the electric power information system. Figure 1 shows the specific flow chart of the network information system and other insurance evaluation.

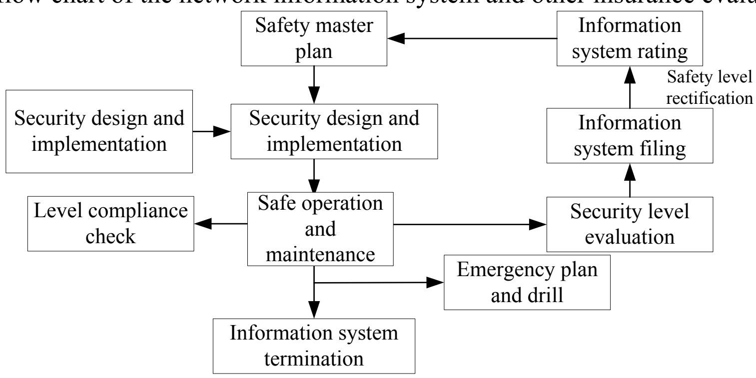

Figure 1. Equal assurance evaluation of network information system

In view of the regular and regular evaluation of the power information system, when some content in the system cannot meet the security protection conditions, adjustments should be made in time, through the strengthening of network access control, and the installation of isolation devices and firewalls and other hardware devices. The programs and services that have an impact on security in the software system are closed to increase the security level of the information system.

3 Analysis of Data Security Requirements and Importance of Power Information System

3.1 Analysis of Data Security Requirements of Electric Power Information System

With the development of science and information technology, the current electric power information system is becoming more and more intelligent and automated, but many information vulnerabilities and data leakage problems have also followed and become a thorny problem. In the process of informatization of power information system, the main requirements for data security are as follows: First, to ensure the integrity of the data, all the statistics and information in the power information system should be complete, and ensure that no matter what accident occurs Data will not be destroyed; the information that should be encrypted includes upstream and downstream data, management data and economic data.

(1) Encryption of uploaded data

In the power information system, the data uploaded in real time are mainly important remote signaling, remote measurement and corresponding information about the sequence of recorded events. The data information of these systems can be used to determine whether the grid is running in a stable working state. For example, the real-time working status of the power grid can be analyzed by recording information in the corresponding order. In addition, the fundamental basis for the system to make decisions and dispatching also depends on this information. Therefore, encrypting the uploaded data is very practical.

(2) Downstream data encryption requirements

The real-time downlink data of the power information system includes information such as remote control, remote control and system protection devices, and setting value data corresponding to automatic devices. The main function of the downlink data affects the final operating state of the system equipment. Therefore, it is very directly related to the operation of the entire grid, which not only requires practicality but also pays attention to safety.

(3) Manage data encryption needs

Management data is mainly for the management of information system data. For example, power outage management plans, grid load management, etc., management data requires high confidentiality, and management data needs to strictly implement confidentiality requirements and value. As long as these requirements are met, different encryption methods can be used.

(4) Economic data encryption needs

Economic data mainly refers to information on resource operation quotations, grid load management, and outage management plans in the entire power market. Economic data is an important part of the data flow of power system materials. Such data will directly affect the balance of capital flow and the overall Electricity resources in the electricity market, so this type of data requires extremely high confidentiality. Therefore, it is necessary to do the access authority work first, which requires the relevant system administrators to pay attention to the management of confidentiality, and multi-level verification and verification should be carried out during the visit to avoid non-internal personnel pretending to be staff members to invade the power information system. The second is storage security, which requires data managers to back up and store all data and information, and there will be no impact on the entire system due to data loss. The last is network security, which is the most critical requirement. Every aspect of the power information system must take security management and protection measures to ensure that the entire system can withstand network virus intrusion and malicious network attacks, thereby fundamentally ensuring the entire operating system And the safety of power companies.

3.2 Analysis of Importance of Data Security in Electric Power Information System

Since the reform and opening up, my country's economy has developed rapidly, and electricity consumption has expanded year by year. At the same time, coupled with the strong support of national policies, the power industry has gradually become the focus of people's lives. With the rapid development of the Internet and science and technology, electric power companies are gradually moving in the direction of automation and intelligence. However, the information security of the power system is decreasing. Some key confidence and core data are leaked or even stolen. These emerging security issues are threatening the safe operation of the entire data information system. Therefore, the data protection of the power information system is particularly important.

4 Data Encryption Technology in Electric Power Informationization

Encrypt the data transmitted by the network channel of the power information system, so that the security of data transmission can be effectively improved. The specific encryption principle of information data is shown in Figure 2. The process of converting plain text into cipher text through encryption is called information data encryption, and the encryption process uses an encryption algorithm, which is mainly to encrypt the string in the process of transmitting data. After the data is delivered to the destination, it is necessary to take decryption operations on the data information, so that the real usable data can be restored. While encrypting and transmitting data at the source end, an authentication certificate is required, and decrypting the transmitted data at the destination end also requires an authentication certificate.

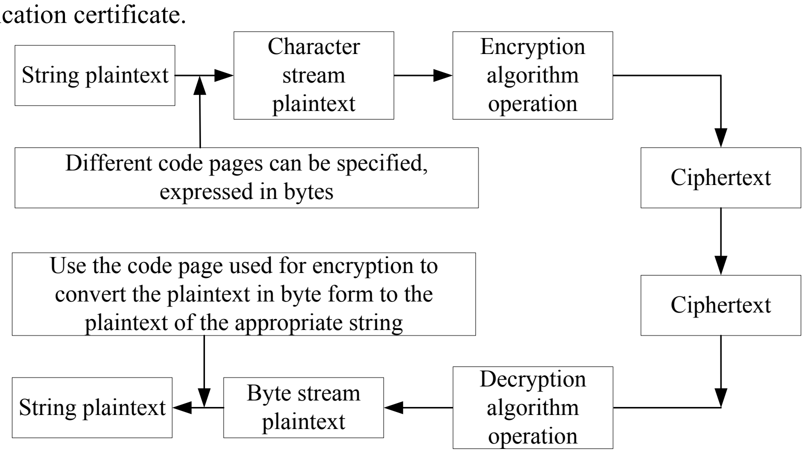

Figure 2. Data Encryption Technology in Electric Power Informationization

5 Application of database multi-layer encryption

The above is a detailed description of the necessity of data encryption and the encryption principle in power informationization. The following uses a management information system of a power company as an example to discuss the realization of a database multi-layer encryption system. The composition of the application system is a standard three-tier architecture with a certain number of sub-function modules. Among these sub-modules, there is a sub-module that needs to be encrypted. However, considering the need for further data calculations, encryption is not adopted on the client side. Instead, the access control has been strengthened, and login must be done through PKI/Ca certificate. To this end, an encryption method at the application layer and the database layer is adopted. Finally, the data stored in the database table is encrypted twice.

The following will analyze the specific encryption application process.

(1) Implementation of application layer encryption

On the application server side, with the help of programming integrated encryption algorithm, it is sent to the data storage library in ciphertext form, which is called the first layer encryption.

(2) Database encryption deployment

The deployment of dual-machine database servers through database security middleware is also called the second-layer encryption. The main scheme is summarized as follows: For the operation of the database, you can use Oracle RAC dual-node, and 0mcle database is installed on the shared disk array cabinet. The two database instances run on two hosts respectively. This implementation scheme mainly achieves a synchronized operation mode with the two computers through the redundancy design of the database security management system. The encryption operation and decryption operation of the database security management system are mainly completed by means of an agent program installed on the database. The security management server can provide the local node to temporarily store logs, policies, keys, etc.

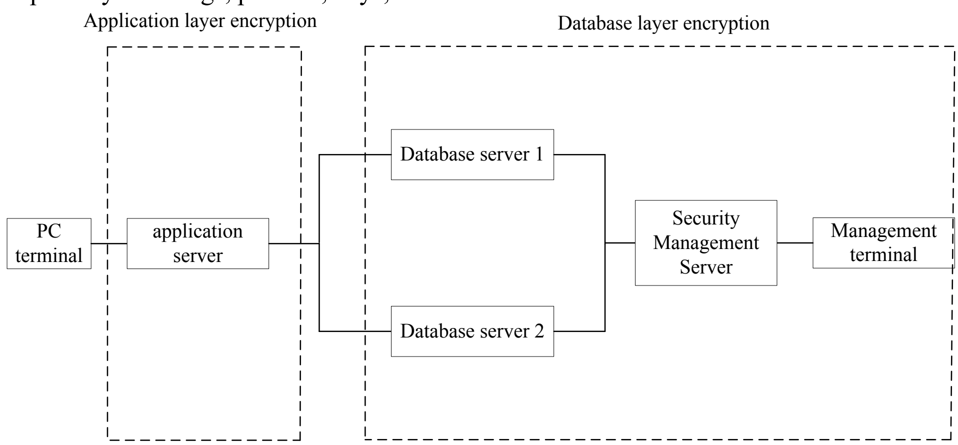

Figure 3. Double-layer encryption diagram

(3) Security scheme

(a) The IP access address is restricted to the application server.

(b) Restrict database access users to application server JDBC users, and other users are not allowed to access it. Even users with DBA authority can only see the ciphertext.

(c) Turn on the audit function and record all visits.

After the above deployment. Unrelated personnel other than database administrators and system administrators cannot see the plaintext. At the same time, if you access through a server other than the application server, even if you get the account and password of an authorized user, you cannot see the plain text. Even if hackers steal the data in the database, it is difficult to obtain the real information, and data security is greatly improved.

6 Conclusion

In this article, a detailed analysis of data encryption technology in power informatization is carried out, and the necessity of data encryption in power informatization and the specific principles of data encryption are introduced. Two-layer encryption is taken as an example to analyze the application of encryption technology in detail. In general, the encryption of real-time data in the power information system is a safe and economical technology, and the use of encryption technology can effectively ensure the communication and data security of the power enterprise information system. But how to encrypt, which layer of encryption, and how to be safe are always issues worthy of in-depth discussion. Specific to the text, according to the actual situation, a two-layer encryption method is adopted, which is a way worth trying for data encryption.

References

1. Luo Jun; Research on dynamic key generation algorithm in database encryption [J],

Computer and Modernization. 2017(12): 26

2. Gu Chunhui. Discussion on the security technology of power information system based on cloud computing[J]. Electronic Technology and Software Engineering, 2014(9):27.
3. Jia Xiang. The application of cloud computing in the construction of electric power information [J]. Digital Communication World 2017 (7): 06-207.
4. Guo Bohua, Li Lei, Zhang Yanwu. Application of Data Encryption Technology in Computer Network Security [J]. Science and Technology Information, 2018(4): 31 -33.