Research on Application of Data Encryption Technology in Computer Network Security Based on Multivariate Large Data Platform

Jinyong Liu

Guangdong University of Science and Technology, No. 99 Xihu Road, Nancheng District, Dongguan City, 523083, Guangdong Province, China

email: 10823856@qq.com

Keywords: Network Security; Data Encryption; Internet

Abstract: Computer network application has become one of the main platforms for enterprises and individuals to process information and data. In the Internet database, users can establish private and exclusive network storage space to save personal files and information. Although the era of big data adds luster to people's life and work, the problem of network security also comes quietly. Data utilization technology has made a breakthrough change, and network security issues have naturally become the focus of attention. Failure of the network security system will not only cause the computer system to be paralyzed, but also affect the normal operation of the entire system. This paper deeply studies data encryption technology to ensure the security and effectiveness of network information. The data encryption technology has been systematically sorted out, in order to bring new ways to the development of computer network information security management.

1. Introduction

In the era of big data, the trend of network development in the world has been pushed into a new situation by means of massive data. While big data brings great convenience to the whole world, the problem of network security has become increasingly prominent [1]. With the rapid development of Internet of Things and cloud computing, the amount of information in the Internet has also increased rapidly, and human beings have really entered the era of big data [2]. Data encrypted need to be transformed by decryption function or key. If the decryption function or key is not obtained, the data reading will be scrambled or unable to open. The big data computer network brings many conveniences to the public, and it also has hidden dangers that will harm the public interest [3]. Due to the complexity and high-end nature of the confidentiality process, both encryption and decryption take a while, and the user needs to have some patience to wait. A deeper understanding of the security status of computer networks with a positive attitude is a prerequisite for ensuring the steady development of computer networks [4]. If computer Internet security cannot be guaranteed, it will cause immeasurable losses to the country and the entire industry.

The era of big data has brought convenience to all network users, and the personal information security of network users has become a focus of attention in the era of data [5]. Failure of the network security system will not only cause the computer system to be paralyzed, but also affect the normal operation of the entire system. To properly keep the key, you can keep the data information safe. This kind of data encryption method is popular in network data management, which plays an important role in ensuring the security of the entire network [6]. In computer network security, the storage and transmission of information are encrypted. Ensuring the privatization and exclusiveness of network users'information and data and improving the confidentiality of information and data is one of the important contents of modern computer network security [7]. Big data belongs to a new era of rapid increase in information and efficient use of data. The application of data encryption technology can improve the reliability and security of computer network, and has very important practical significance for the future development of computer network.

  DOI: 10.25236/mmmce.2019.081

2. Influencing Factors of Computer Network Information Security in Big Data Era

In the context of big data, many related emerging industries, such as e-commerce and Internet of Things finance, have been derived. The original data encryption technology is still effective because the data type of the encryption management is relatively simple and the amount of encrypted data is small. However, for the present and future, it is impossible to effectively encrypt big data and multiple types of data by using traditional encryption technology. With the advent of the era of big data, the volume of data has suddenly increased, and the use of methods has become more efficient and diversified. The information transmission of the computer is mainly carried out by external network equipment, and only through the professional external equipment computer can the various corners of the world be connected. Once the computer system itself has a vulnerability, there will be errors in the software [8]. The process of network data transport requires continuous encryption between network nodes through multiple network nodes. Then the degree of data protection is continuously enhanced to achieve the strict management of data until the data file reaches the receiving end.

As a user, they want their private information not to be stolen on the network. Many useful information can be obtained by scanning the port of the target computer. Data cleaning is carried out from the analysis of abnormal node training data and extracted parameters, and then data generalization is carried out to determine the possibility of the data being sampled and detected appearing in the model. Figure 1 shows how big data reshapes the structure of Internet information security supervision.

Fig.1. Big data reshapes the structure of Internet information security supervision

Because of the openness of the computer information network itself, it is widely used in all walks of life and generates data that can obtain huge profits. The data extracted by data sampling has certain pertinence, criticality and sensitivity. When encrypting this part of data, the amount of data extracted is small and has certain directivity. The advent of the era of big data has brought a new space for the development of computer network technology, which adds luster to people's lives, but also strengthens the virus's infection ability invisibly. Although computer network equipment has been equipped with corresponding protective equipment at the time of installation, protective equipment is not a panacea [9]. The exchange and sharing of data information in the computer is very frequent. The software and hardware of the computer may have security risks, which have a serious impact on the security of the data. After setting the network access right, if the operator wants to access certain websites or some computers and some software systems, the account needs to be authorized by the administrator, otherwise there will be no permission to access.

3. Solutions to Network Information Security Problems in the Background of Big Data Era

3.1. Strengthening the Development and Management of Information Security Technology

In the era of big data, more and more high-value secret data are transmitted through the network, and once the computer security system has problems, it is very likely to cause the leakage of information and data. If a computer is invaded by a virus, there must be risks in its future operation.

Once the virus spreads, it will surely bring an indelible disaster to computer programs and files. After entering the era of big data, hackers' attacking methods are gradually changing. The hacker's attack way is a little more concealed than before, and the damage consequences caused by it are even worse. The transmission process of volume is based on specific nodes, so it is difficult to achieve full coverage of information at both ends. Affected by a variety of subjective or objective factors, the problem of computer system security vulnerabilities has occurred from time to time, which has increased the risk of network security. Security and security technology can also be used to control and encrypt information keywords, thus playing an effective role in protection.

If the Internet's protective measures are not in place, it is vulnerable to hackers and causes huge losses to users and Internet operators. In order to implement decision-making at the decision-making level, a management layer that manages day-to-day work and an executive maintenance layer that is responsible for implementing security plans and decisions are required. The security organization includes the organizational decision layer, the management control layer, and the execution maintenance layer as shown in Figure 2.

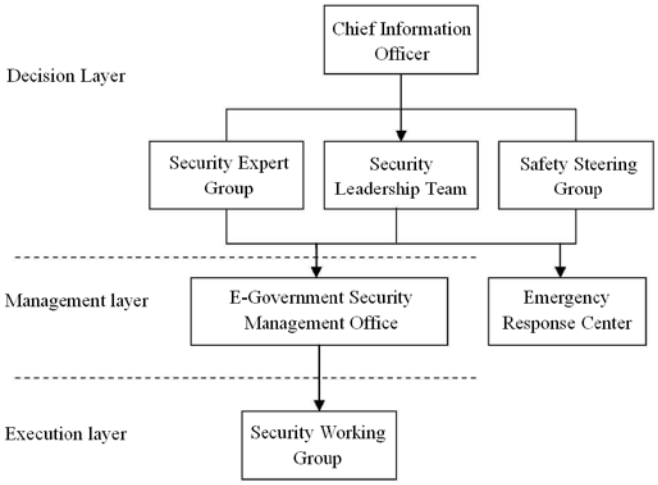

Fig.2. Hierarchical Information Security Organization

3.2. Effective Use of Security Systems such as Firewalls

When a computer transmits information over the Internet, it needs to be completed by a computer user through specific operations. However, many computer operators do not have professional computer technology knowledge, and computer operators have a strong subjective consciousness during the operation. In the era of big data, the virus is updated more quickly. Therefore, during the application of this anti-virus software, users must regularly update the virus database to effectively protect the mainstream viruses on the market [10]. We should make full use of security software such as firewalls to resist virus attacks and carry out regular virus detection and killing on computers. Driven by the interests of information and data itself, hacking has become more and more rampant in recent years. Therefore, in order to ensure the security of computer network system, it is urgent to strengthen the integration of information and data processing, and establish a scientific data system and preventive measures. With the changing types of network data and the increasing number of network data, the original text data encryption technology has been difficult to meet the actual needs.

4. Conclusions

Nowadays, with the rapid development of computer industry and the whole people entering the era of big data, information security is closely related to everybody's daily life. Whether it is the confidentiality, controllability and integrity of information in network applications, or the prevention and control of security vulnerabilities, computer networks are designed to create a network environment that can safeguard public information rights and interests. Through database automatic operation and maintenance management, it is possible to monitor various indicators of the database, discover abnormal information in real time, and issue alarm information. In order to ensure the

security of computer information, from hackers and viruses, it is necessary to use a variety of means and methods, and also requires users to enhance their awareness of information security protection. We should pay more attention to and develop data encryption technology to protect the security of computer network information in the big data environment.

References

[1] Wang G, Yu J, Xie Q. Security Analysis of a Single Sign-On Mechanism for Distributed Computer Networks. IEEE Transactions on Industrial Informatics, 2013, 9(1):294-302.

[2] Shukla P, Khare A, Rizvi M, et al. Applied Cryptography Using Chaos Function for Fast Digital Logic-Based Systems in Ubiquitous Computing. Entropy, 2015, 17(3):1387-1410.

[3] Kawai Y, Kunihiro N. Secret handshake scheme with request-based-revealing. Computers & Mathematics with Applications, 2013, 65(5):786-798.

[4] Obert J, Pivkina I, Huang H, et al. Proactively applied encryption in multipath networks. Computers & Security, 2016, 58(C):106-124.

[5] Kumar M, Verma S, Lata K. Secure data aggregation in wireless sensor networks using homomorphic encryption. International Journal of Electronics, 2015, 102(4):690-702.

[6] Xing L, Dexin C, Chunyan L, et al. Secure Data Aggregation with Fully Homomorphic Encryption in Large-Scale Wireless Sensor Networks. Sensors, 2015, 15(7):15952-15973.

[7] Haihua L, Xinpeng Z, Hang C, et al. Secure and Efficient Image Retrieval over Encrypted Cloud Data. Security and Communication Networks, 2018, 2018:1-14.

[8] Ma C, Li J, Ouyang W. Lattice-Based Identity-Based Homomorphic Conditional Proxy Re-Encryption for Secure Big Data Computing in Cloud Environment. International Journal of Foundations of Computer Science, 2017, 28(06):645-660.

[9] Hasan M Z, Mahdi M S R, Mohammed N. Secure Count Query on Encrypted Genomic Data. Journal of Biomedical Informatics, 2017, 22(2):71-82.

[10] Wang Y, Li R. FPGA based unified architecture for public key and private key cryptosystems. Frontiers of Computer Science, 2013, 7(3):307-316.