Secure sharing method of network data transmission based on multi-layer encryption technology

Yanrong Jing[1*], Wenqian Zhang[1], Lin Ge[1], Nanfang Li[1], Xiyuan Shang[1] and Yun Ye[1]

[1] Electric Power Research Institute, State Grid Qinghai Electric Power Company, Xining, Qinghai, 810008, China

Absrtact. In order to ensure the effect of network data transmission in scientific research institutions and avoid network information from being attacked and damaged, a secure sharing method of network data transmission based on multi-layer encryption technology is proposed. Combined with multi-layer encryption technology, the network data transmission security protocol is constructed to ensure the security and integrity of the initial file. The network information transmission security evaluation system is further constructed. The network transmission path security of scientific research institutions is tracked, evaluated and tested in real time. The network data transmission security sharing platform is constructed to ensure the safe sharing of massive and complex data Experiments have proved that the security and sharing processing effect of the network data transmission security sharing method based on multi-layer encryption technology are significantly improved compared with the traditional methods, and fully meet the research requirements.

1 Introduction

The network security, host security, identity security and data content security of Electric Power Research Institute are studied. In order to solve the problem of information transmission environment and sharing security of users in scientific research institutions, the security of data transmission and sharing is improved by constructing authentication security protocol to analyze the content of transmitted data. By constructing data security evaluation system, the confidentiality level of information content is divided, and the security transmission scheme is optimized according to the characteristics of network virus and Trojan horse attack[1]. Tracking, monitoring and intercepting illegal intrusion data to avoid stealing data and sensitive information damaging network environment and stealing shared information[2]. By analyzing and filtering the network data flow and operation of the Electric Power Research Institute, the hierarchical structure has good flexibility and scalability, and is easy to be combined with other mature protocols to quickly discover the potential dangerous attacks intercepted and supported, and realize the information security protection of scientific research institutions. Based on this, a secure sharing method of network data transmission based on multi-layer encryption technology is proposed, which can effectively realize the research requirements of effective encryption, accurate authentication and transmission sharing of network data, and realize the encryption protection of shared files.

2 Secure sharing method of network data transmission

2.1 Network data transmission security protocol settings

Based on the network transmission security model of scientific research institutions, this paper uses multi-layer encryption technology to optimize the security of shared data transmission on the cloud platform, laying the foundation for the establishment of data security sharing research methods. In the context of massive cloud storage, a large number of data are mostly transmitted in parallel, which reduces the security of data transmission, so the data characteristics are divided according to the control principle[3]. The original file is processed by multi-layer encryption technology and compared with the initial file keywords after encryption. Symmetric encryption can only be used to encrypt and decrypt data to ensure the confidentiality of the data, and can not be used for digital signature. The private key of the signer is used to encrypt the digest, and then hash the data to generate the digest. The output is transmitted simultaneously with the original file[4-5]. The receiver decrypts the signature digest using the sender's public key to verify whether the signature is correct. If the keywords are the same, then the network data transmission security protocol is effective. Based on this, the information transmission key addition method is optimized.

Further, the physical characteristics of network data transmission code are standardized by multi-layer encryption technology. Based on the transmission mode of

*E-mail: jyrong2531@qh.sgcc.com.cn

network information, the network cloud platform is used to realize the safe transmission of circulating data[6]. As node footnotes, network data transmission has a strong directional transmission ability, which can meet the needs of platform fast storage. However, from a security point of view, the encoded data does not have a solid link bridge organization, which can not effectively resist the spam file attack on the network, and it is easy to cause data damage. As the simplest link bridge node, network data security sharing code can provide connection endpoints for stored data[7]. Adding network data transmission suffixes can improve the stability and security of data itself, and meet the physical characteristics of cloud platform storage data.

2.2 The evaluation system of network data security sharing

In the process of optimizing the network data transmission security sharing method, it is necessary to use the toolbar button to improve the processing method, track and detect and locate the abnormal data processing area, and cancel the sharing processing of dangerous information in time under the dangerous state. In view of the fact that the target point remains unchanged in the process of network data transmission, the reverse search method is used to traverse backward from the point[8]. By keeping the minimum path between the point and the target point and keeping two important values, all nodes in the space can be searched. Through channel allocation, information can be sent from the inside to the outside, and all information nodes in the coverage area can be queried and connected with them. Analysis of all information nodes need to query their coverage respectively before they can be connected. Once connected to a node, there is no need to connect to other nodes, which effectively ensures that the information node has only one parent node and multiple child nodes[9].

Furthermore, based on the multi-layer encryption technology, the quantitative evaluation of network data is carried out, and the evaluation index is standardized, so as to better evaluate the network information transmission security and ensure the data transmission and sharing security of the evaluated object[10]. The evaluation experts design the evaluation scheme according to the application. If p_i is the primary data security evaluation level, i is the data volume, t is the processing time, and z_i is the data commonness The demand factor is used to calculate the safety factor of network data transmission.

$$Q(x)_{\min} = \sum_{i=1}^{n} z_i \left(p_i^{t} x \right) + \delta g(x) \tag{1}$$

Based on the above algorithm, the reference for the selection of network information transmission security trust processing node can be carried out, and the network security can be improved. If the load allows, if two nodes download the same resources, the trust priority is adopted. Select different values according to the super node. In multi-layer encryption environment, the linear range of security complexity of data transmission is the spatial distribution of data to be stored, which is generally affected by the linear coefficient of random parameters of storage nodes in the network. Storage block is an important physical quantity to describe the data of network service cloud platform in network information transmission model. T in the network information transmission model can be expressed as the longest time of network data storage. Based on the above variables, the calculation results of data transmission complexity of random nodes can be expressed as follows:

$$p_u = \mathrm{Re} \int [\frac{\beta_u t}{F_u(2y+q)}] du \tag{2}$$

Where du is the maximum data storage capacity under the network service cloud platform environment, and F_u is the amount of data required for each storage operation on the platform. Based on the physical processes of service architecture, security energy initialization and storage protection positioning, the data storage security of network service cloud platform is studied. Using the above calculation, according to the current evaluation of network information transmission security, the network information security evaluation system is established, the confidentiality, integrity and availability vector of network information security are analyzed, and the ideal evaluation positive and negative standards are determined. By non quantitative processing of evaluation indexes, the linear weighted evaluation model of mobile network information security is completed, which combines qualitative and quantitative evaluation.

2.3 Realization of secure sharing of network data transmission

The network data transmission security sharing framework consists of four levels: data layer, service layer, application layer and management layer. As secure file sharing has the characteristics of universal security application, it has a complete security guarantee system. While ensuring the security of the system, the ease of use and controllability of the system are considered to the maximum extent, thus fully ensuring the availability of the system. It has complete file sharing function and is suitable for insecure windows file sharing. The network service layer based on Visual Studio 2010 is written, which can operate data on the platform, including query, delete, add and modify. The security structure of the data center is based on the multi-layer encryption technology of SDN, which realizes the dynamic control of the data center and calls other resources when the network resources are insufficient.

If s represents the information of the user information resource, n represents the attribute of the network data feature, and m represents the attribute of the data feature, then in the multi-layer encryption environment, if the scheduling parameter of the user information resource is g, the data security Q:

$$Q = \frac{1}{s^n} \prod p_u m \tag{3}$$

According to the different characteristics of network resources in the multi-level encryption technology environment, it is necessary to process the network resources. p_u is the transmission control effect, e is the standard information management parameters, v is the monitoring index, C is the encryption algorithm based on firewall.

$$C=\mathrm{Q}^{e}\sum_{i=1}\sqrt{\frac{1}{\mathrm{v}\left(m-n\right)^{z-1}}} \tag{4}$$

On the basis of this model, a multi-layer encryption network security management system is designed to avoid sending data to the same server during the design, and realize the average distribution of data requests, and ensure the efficient data transmission and processing of internal services through network information transmission and security management. The exchange encryption processing function can simplify the network security management process of multi-layer encryption technology.

In order to effectively prevent the intrusion and theft of network data by false address, effectively protect the security of network information data, and meet the requirements of network security sharing and updating, the network data transmission processing method is optimized by combining with multi-layer encryption technology, so as to improve the data and sharing effect.

3 Analysis of experimental results

In order to verify the secure sharing method of network data transmission based on multi-layer encryption technology, the 2.4.0 virtual switch is used to realize the underlying switching equipment, which supports path identification and table item release functions. Running on the independent virtual switch provides a control platform for SDN architecture. Mininet is mainly responsible for monitoring network link load and dynamic adjustment table items; mininet is used to design network topology to support network structure and information interaction between optical platforms. In this scheme, program and script language are used to transfer the protocol package to the host and inject the traffic into the backbone network. Taking 60 kinds of services as experimental objects, the network resources are simulated. These services are concentrated between switches 1 and 2, namely the subnet, 168.11.0.0/9 and 168.12.0.0/9, resulting in two link congestion. The platform is developed for Microsoft Visual C + 6.0. With C10 + as the development language, in addition to writing related classes, we also use mfcomfc in VC + 6 + 6.0: Microsoft's basic class. This class library is built on the basis of Windows API. It makes the windows programming process more effective and more in line with the idea of object-oriented. It provides a good interface design environment for vc10+6.0, and also brings a lot of convenience to network programming. Select SQL Server 2000 for database development. It is a fully functional database management system developed by Microsoft on Windows platform. It includes development engine, standard SQL language, extended function, stored procedure, trigger program and so on. In use, it is easy to install and compatible with network platform. In order to ensure the correctness of the test results, the experimental parameters were set uniformly, The details are shown in Table 1 and table 3:

Table 1 Experimental equipment and parameters

Project	Data
Evaluation network	Communication network
Maximum evaluation time	30min
Operating platform	Windows10
Network structure model	Multivariate heterogeneous model
Threat severity parameters	TS

In the mobile network environment, information transmission is further selected to record the security evaluation time of each transmission. Based on the above experimental environment and parameters, further comparative detection of network data transmission security is carried out, and the detection results are recorded, as shown in the Fig. 1.

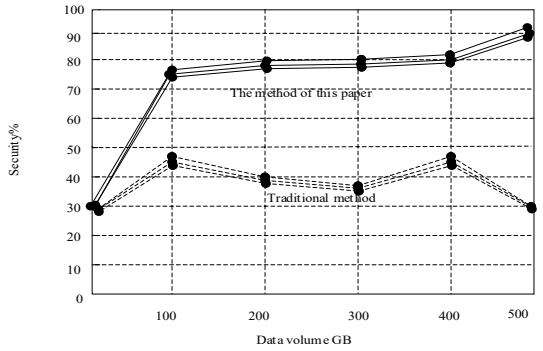

Fig. 1 Comparison test results of network data transmission security

The practicability of the algorithm is verified by detecting the gradient in the information filtering process, and the common effects of the data are further compared, detected and recorded, as shown in the Fig. 2.

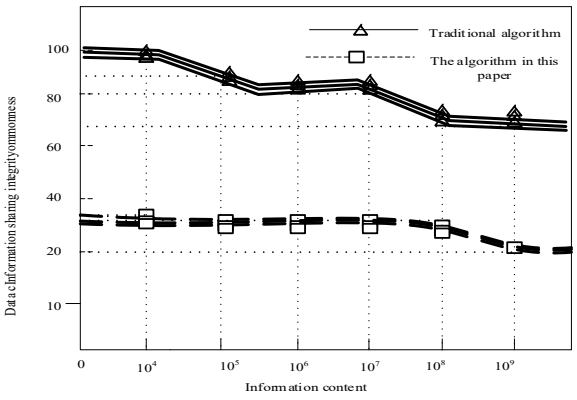

Fig. 2 Information sharing integrity test results

After analyzing the detection results in the Fig. 6 and

the Fig. 7, it is not difficult to find that, compared with the traditional methods, the network data transmission security sharing method based on multi-layer encryption technology proposed in this paper can realize the safe transmission of massive data more quickly and accurately, and better ensure the integrity of data transmission and sharing, effectively intercept dangerous data and ensure the number According to the transmission and sharing effect, it fully meets the research requirements.

4 Conclusion

Data transmission security control is an important guarantee to reduce network consumption and realize data security transmission. In the process of data transmission, wireless network transmission data has a high bit error rate and is prone to data packet loss. The energy loss of network nodes will lead to data transmission path failure, resulting in the imbalance of channel bandwidth allocation. Based on this, multi-layer encryption technology is used to optimize different network data transmission application methods, and information transmission encryption technology is used to optimize the design of network data transmission sharing link. In order to better ensure the security of mass data transmission in complex network environment, and reasonable research requirements for data sharing, this paper proposes a network data transmission security sharing method based on multi-layer encryption technology. By setting encryption protocol for the transmission data, the evaluation index system of data commonness is constructed, so as to better ensure the security and effectiveness of data transmission.

Acknowledgments

The study was supported by “Science and Technology Project of China Railway Corporation, China (Grant No. 1341324011)”.

References

1. Tiwari D, Gangadharan G R. (2018) SecCloudSharing: Secure data sharing in public cloud using ciphertext-policy attribute-based proxy re-encryption with revocation[J]. International journal of communication systems, 31(5):1-28.
2. Zhang Y , Lu Y , Huang X , et al. (2020) Blockchain Empowered Asynchronous Federated Learning for Secure Data Sharing in Internet of Vehicles[J]. IEEE Transactions on Vehicular Technology, 6(99):1-8.
3. Chen W , Chen Y , Chen X , et al. (2020) Toward Secure Data Sharing for the IoV: A Quality-Driven Incentive Mechanism With On-Chain and Off-Chain Guarantees[J]. IEEE Internet of Things Journal, 7(3):1625-1640.
4. Huang Q , Yue W , He Y , et al. (2019) Secure Identity-Based Data Sharing and Profile Matching for Mobile Healthcare Social Networks in Cloud Computing[J]. IEEE Access, 6(2):36584-36594.
5. Kang J , Yu R , Huang X , et al. (2019) Blockchain for Secure and Efficient Data Sharing in Vehicular Edge Computing and Networks[J]. IEEE Internet of Things Journal, 6(3):4660-4670.
6. Wang Z , Chen F , Qiu W , et al. (2018) A two layer chaotic encryption scheme of secure image transmission for DCT precoded OFDM-VLC transmission[J]. Optics Communications, 410(5):94-101.
7. Fan K , Pan Q , Zhang K , et al. (2020) A Secure and Verifiable Data Sharing Scheme Based on Blockchain in Vehicular Social Networks[J]. IEEE Transactions on Vehicular Technology, 69(6):5826-5835.
8. Melkumov M A , Mikhailov V , Hegai A M , et al. (2018) E-band data transmission over 80 km of non-zero dispersion fibre link using bismuth-doped fibre amplifier[J]. Electronics Letters, 53(25):1661-1663.
9. Dabos G , Manolis A , Papaioannou S , et al. (2018) CMOS plasmonics in WDM data transmission: 200 Gb/s (8×25Gb/s) transmission over aluminum plasmonic waveguides[J]. Optics Express, 26(10):12469-12472.
10. Ledentsov N N , Shchukin V A , Kalosha V P , et al. (2018) Anti–waveguiding vertical–cavity surface–emitting laser at 850 nm: From concept to advances in high–speed data transmission[J]. Optics Express, 26(1):445-451.