Research on the Application of Computer Data Encryption Technology in Cloud Security

Zhengying Zhao and Xiangyi Xu

***Abstract*—Computer network is the basis of current enterprise operation and social service operation. Under the network mechanism, high-speed and high-quality operation can further accelerate the gradual development of enterprise and social structure. However, under the diversified and open transmission mode, the network has become the main disaster area where the current security accidents occur. Some hacker attacks and network viruses have brought greater threats to network users. Therefore, this paper mainly takes the practical application of computer data confidentiality technology in cloud security as the main analysis content, and discusses the characteristics of the technology, hoping to have corresponding reference value.**

***Index Terms*—Computer, data confidentiality technology, cloud security.**

I. Introduction

With the advent of the information age, people's daily life and work are inseparable from computers, and they gradually form a deep fit. In particular, 5g technology has been further applied, and some framework constructions such as smart city and smart transportation have been given a new definition by computer networks. In the actual operation of computer network mechanism, because it is open and shared, under the basic principle of information and data transmission, it can provide convenience for people and bring corresponding network security risks, such as network hacker attacks and viruses, so that the relevant data and information of network users face the risk of being stolen by others. For these problems, network information technology personnel are working harder to develop new security protection application technologies to ensure that the computer network system can truly avoid network risks and provide better security services for network end users. The further research and application of the computer network data encryption technology are the basic conditions for the construction of the current network security mechanism. In the face of very complex and redundant data information, the data encryption technology itself has the corresponding work content of the multi line project. When dealing with a lot of data information synchronously, the technology itself has the stability and efficiency, It can lay a solid foundation for the safe operation of the computer network as a whole. Based on this, this paper mainly carries out the following analysis and Research on the application of computer data encryption technology in cloud security, hoping to have corresponding reference significance.

Manuscript received August 31, 2022; revised October 24, 2022.

The authors are with School of Software Engineering, Pingdingshan University, Pingdingshan 467000, Henan, China (e-mail: 790575467@qq.com).

II. Computer Security Challenges and Security Technology System

Under the background of the network age, the original information resource related processing technology is no longer suitable for the rapidly growing data level. The computer mainly relies on the network information technology, through the corresponding technologies such as data mining and correlation analysis, to scientifically process the massive data stored in the distributed storage. Whether for the network environment or storage media, they all belong to different network information systems. Among them, the advent of computers has an asymmetric relationship between defense and attack in the network environment. The original information security protection countermeasures generally focus on "blocking, killing", which is difficult to face the information security challenges of the computer era [1]. Therefore, it is necessary to further accelerate the creation of a multi-level and high-quality computer horizontal and vertical comprehensive defense mechanism. Further strengthening the basic ability of the practical guarantee of computer information security is the way to effectively solve the problems related to computer security.

A. Computer Security Challenges

In the computer environment, the Applied protection risks mainly include the abuse of resources, denial of service provision, unsafe integration modules or API interfaces and web security. Security of virtualized environment: the cloud computing center under cloud computing and virtual technology can provide a more open space for computers, and the resources distributed in the corresponding areas can be integrated and dynamically configured in a short time, and can effectively realize the sharing and co construction of data sets. The actual access of the network has the characteristics of convenience. It can also form a data flow, which can be transformed into the realization of rapid elastic push of resources and personalized services, and provide the main foundation for them. However, the exposure of the platform will promote computers containing massive data and potential value, which is very easy to attract some hackers. Virtualized environment security has become a serious threat to computer security. Mobile access security: byod mobile access security mainly includes identity counterfeiting and information hijacking. Fusion between security and computer: malicious threats to relevant internal staff and data privacy

DOI: 10.7763/IJET.2022.V14.1206

protection.

B. Computer Security Technology System

If the computer passes the security protection, it is mainly used in the deployment of virtualization integrated security equipment in the protection area. It mainly includes DDoS, firewall, IPS and web firewall (WAF). In addition, it is also necessary to deploy a detailed analysis system for vulnerabilities, carry out security assessment and relevant tests for penetration. The actual security problems of the computer virtualization environment mainly need the security of the virtualization firewall top VSP (vgate, ate, TD) and the virtual machine manager, that is, the external firewall. Further, it can effectively optimize the basic performance of the virtualized environment itself, and also carry out the overall migration of security policies.

From top to bottom, mobile access security is mainly divided into three levels: unified access control, data security, threat protection and management of corresponding equipment in the whole life cycle. The unified access control layer passes the identity authentication and corresponding authorization in the terminal access area. It also needs to launch virtual application publishing and virtual desktop, and encrypt through VPN in the network access area. Within the business service area, it needs to be realized through remote locking, data erasure, GPS positioning and other functions. The management of equipment related to the whole life cycle mainly includes the access and deployment of assets, and the final destruction of the whole process. Asset access mainly includes the actual discovery, registration and initialization of assets. Moreover, the asset deployment mainly includes the scientific formulation and configuration of the security baseline. Asset operation mainly includes asset loss reporting, asset locking, password reset, asset location and recovery, and data destruction mainly through remote application unloading, data erasure and other related technologies [2].

The basic way to realize the security cloud under the computer convergence is to use the security detection and the corresponding computer technologies for fusion, and further realize the access audit of information, the actual discovery of Security Threat Intelligence and the protection of privacy data through the basic capabilities of cloud computing and the main computer processing systems. Security detection and early warning mechanisms are mainly used 7 × 24 monitoring, operation and maintenance, collecting, processing and storing major events, and then carrying out correlation analysis and threat detection analysis, so that the results obtained from the final analysis can be distributed, circulated and disposed in the form of final work orders, knowledge bases and relevant reports by using basic methods such as SMS and email. The main reason for security audit and data privacy protection is to avoid data information leakage caused by improper operation of employees. Further audit and evidence collection of data can be realized by using computer related platforms. The corresponding audit technologies mainly include business access audit, database audit and security operation and maintenance design.

III. Basic Characteristics of Computer Data Encryption Technology

The data encryption technology belongs to the scientific encryption processing for the data information transmitted by the computer network, which is to add secret keys or encryption functions to the specific civilized nodes of the information. The nodes of information inscriptions can be transformed into meaningless close friends. When nodes are displayed, they can show garbled codes or symbols. When users harvest information, they need to use the relevant secret keys and decryption functions to gradually transform the encrypted information into information plaintext, and finally realize the encryption and transmission of information [2]. In this process, the transformation between the ciphertext and the plaintext can be regarded as the actual encryption process of the basic information node. When the plaintext is transformed into the ciphertext, the corresponding decryption algorithm needs to be used to effectively realize it. When confidence encryption is used for transmission, if it is supplied, the attacker can obtain the relevant ciphertext, and cannot obtain the actual plaintext information without obtaining the secret key. Generally speaking, the secret keys at the information transmission end and the receiving end have their own independent characteristics. Only on the basis of having the correct secret keys can the ciphertext information be transformed. This form is also the main guarantee for the operation of the computer network security protection mechanism.

IV. Application Path of Computer Data Encryption Technology in Cloud SECURITY

A. Computer Software Security Application

When the computer network is actually running, it is often realized through software functions. How to browse web pages and application type software, etc. must be effectively realized through relevant network services. In this process, data information transmission will face many security risks. In order to effectively strengthen the overall security within the system, the data encryption technology needs to take the basic operation of users as the core when it is used, and strengthen the overall operation quality of the computer network by creating a relevant information service framework. First, you need to create a correct password framework. For example, when the computer is in public use, you need to set an independent password for some of the specific running software. When non computer users operate the computer, for example, if the software password has inflammatory errors, the software itself cannot be started, This form of manipulation can also fundamentally and effectively solve the risk of information leakage. When the computer equipment is attacked by external viruses, the data encryption technology will also create a protection mechanism, which can help the system to carry out relevant information feedback for the location where the data are supplied. Make the actual operation of the system feedback in time, and make the current operation status of the system

feedback to the specific network operation system. At this time, the system will also give a response, and carry out scientific and timely treatment for the virus. Second, through the data encryption technology and the connection between cloud data paths, it can provide users with the corresponding services of automatic information retrieval, carry out the main check according to the internal relevant data, and carry out effective retrieval for the original data hiding risk in the system, so as to strengthen the overall security of data transmission.

B. LAN Security Application

The continuous development of computer network system will also promote the overall efficiency of social system informatization. At present, many enterprises carry out scientific and comprehensive processing of internal corresponding data and information based on computer network platform during actual operation. The basic operation mode of efficiency and accuracy of computer equipment can greatly enhance their overall development efficiency. Especially in the aspect of enterprise management, we should give corresponding support to the software system, and truly realize the orderly data and information manipulation within the enterprise, which can truly realize the effective information and data manipulation within the enterprise, so as to meet our basic requirements for data and information processing [3]. At present, the actual operation of enterprises is usually based on the actual construction of the LAN. Through the link of the information nodes in the corresponding departments, it can ensure that the data information can be transmitted point-to-point in the LAN. When the data encryption technology is running, it can provide a more secure guarantee for the operation of the enterprise's internal network. For example, when the data information is actually transmitted, the internal router can directly carry out the encryption processing at the nodes for the information, back up the source data information and send it back to the corresponding system of the main control. The relevant departments need to carry out the decryption processing for the files through the secret key. Under this type of data information transmission, the actual processing efficiency and overall quality of the data information can be scientifically improved.

C. E-commerce Security Application

The actual construction of e-commerce platform indicates a new economic development pattern. Based on the network platform, the exchange of funds and goods can be realized more quickly, and the overall consumption of social resource costs can be saved to a great extent. However, when the e-commerce platform is actually running, it will also face some loopholes, which will cause the user's own information to be stolen, and will also make both sides of the transaction subject to economic threats, and will also bring more obstacles to the actual development of our platform. The further application of data encryption technology can create a data-based security management framework for users and enterprises. When users develop their operational knowledge at a certain stage, the software system will automatically send out protocol requests. Computer data encryption technology can create corresponding encryption nodes for the data transmission end, ensuring that the data information actually transmitted by the user end has always been in a relatively safe environment, Moreover, the identity authentication module and transaction password module inside the system platform can provide more scientific protection means for the basic process of the overall transaction, so that users can carry out more secure operations in the e-commerce platform.

D. Application of Data Encryption Technology in VPN

VPN is a virtual private network. This virtual private network will generally be used in international enterprises. These enterprises will establish their own private LAN, but it will also bring some security problems in the use of LAN when it is convenient to use. Because of the rapid development of science and technology, network security needs to be paid attention to. Relevant personnel need to transmit various data to the network, encrypt them through the Internet router, and then transmit the information data. When the information is transmitted to the router, it will be decrypted. This can effectively avoid information theft, It can also enable users to see the information data they need to use [4].

E. Application of Data Encryption Technology in Data

Data audit of big data platform. By using a variety of conditional correlation audit related analysis countermeasures, we can further achieve a more intuitive display of big data logs. The data adopts computer data encryption technology [5], and the other party will use the same decryption secret key, which can ensure the usefulness and integrity of the information as a whole when there is no leakage between both parties. The common algorithm has a basic algorithm for binary metadata source encryption, which divides the information into 64 and arranges them into different groups. Through the decryption secret key with a length of 56, the encrypted data can be generated finally. Then, the parity check code is used to expand the overall verification, and then each group is grouped and rearranged to expand the basic process of mutation and operation. Finally, the encrypted data source will be generated [6]. For the scientific processing that each group takes up the next 19 steps, the output of each step belongs to the input of the next step. Only by reversing the initial replacement can the whole process of encryption be truly completed. This form of data encryption process can really ensure the overall security of data transmission, and then ensure the overall security of data transmission.

F. Desensitization for Computer Big Data Platform

Data desensitization related technologies are actually the basic capabilities that hive, HbAS and other technologies in Hadoop components can provide for data desensitization. During data flow, security desensitization related countermeasures are configured according to the basic characteristics of syntax [7], and matching identification related processing is carried out for the actual request access statements in the traffic, which needs to be in the basic forms of shielding, encryption, hiding or auditing. First, according to different sensitive data and basic requirements, different

sensitive data desensitization calculation models are configured [8]. Secondly, it can realize the practical algorithm of dynamically adding and deleting desensitization. Third, fine-grained sensitive data is protected. The corresponding management personnel configure users to use specific database actual performance and column time desensitization algorithm, which can ensure desensitization without affecting the actual experience of users [9].

V. Conclusion

To sum up, the application of computer data encryption technology can create a more secure protection mechanism for the computer network, carry out scientific encryption processing for the actual transmission path and transmission nodes of data information, and further improve the security of the overall transmission process of data information. When the information is intercepted during the actual transmission, it can still be in a secure state under the encrypted state, Thus, the corresponding risks of information theft and tampering can be avoided, and the security can be ensured for the information transmission and reception during the actual use of the computer.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

Zhengying Zhao and Xiangyi Xu wrote the paper; all authors had approved the final version.

References

[1] J. Yang and X. Li, "On the application of data encryption technology in computer network security," *Information System Engineering*, vol. 5, pp. 52-55, 2022.
[2] Y. N. Zhou and J. D. Pan, "Application of data encryption technology in computer network security," *Network Security Technology and Application*, vol. 5, pp. 37-38, 2022.
[3] Z. K. Wu, "Application of data encryption technology in computer network communication security," *Changjiang Information and Communication*, vol. 35, no. 4, pp. 142-144, 2022.
[4] L. Duan, L. Zhu, Y. Y. Yue, C. Y. Zhao, and Z. L. Lv, "Research on the application of data encryption technology in computer network security," *China New Communications*, vol. 24, no. 5, pp. 121-123, 2022.
[5] Y. D. Ren and R. J. Cao, "Application analysis of data encryption technology in computer network security," *Information Recording Materials*, vol. 5, pp. 10-12, 2020.
[6] J. R. Mu, "Research on data encryption technology in computer network information security," *Small and Medium-Sized Enterprise Management and Technology*, vol. 1, pp. 188-189, 2018.
[7] Z. L. Zheng, "Analysis on the application of data encryption technology in computer network security," *Network Security Technology and Application*, vol. 1, pp. 94-95, 2015.
[8] S. J. Wu, "Research on the application of data encryption technology in computer network security," *Computer Knowledge and Technology*, vol. 10, no. 36, pp. 8633-8634, 2014.
[9] L. H. Liu, "Application of data encryption technology in computer network communication security," *Digital Technology and Application*, vol. 40, no. 2, pp. 216-218, 2022.