Research on Education Data Security and Privacy Risk Avoidance Based on Information Security Technology

Yafang Li

Suzhou Chien-Shiung Institute of Technology, Taicang, Jiangsu, 215411, China

Keywords: Information security technicality; Educational data security; Research on privacy risk avoidance

Abstract: With the continuous development of science and technicality and the gradual progress of computer technicality, the world has entered the information age. The use of computers in all parts of the world has become popular, and computer technicality is gradually valued and needed by the masses. It plays an important role in the development of various fields, meets the needs of application and development in various fields, and gives full play to the existing value of information technicality. Computer information security management, strengthening the application of data encryption technicality, can comprehensively consider the actual needs of its application, comprehensively improve the overall work efficiency and quality, and for the continuous development of social economy, information technicality has been used in various fields in China, resulting in frequent network exchanges. In addition, China's continuous improvement of network openness has further increased people's access to information, thus increasing the risk of network information data. It has become a key issue to be solved urgently. The birth and application of data encryption technicality has effectively changed the network information security pattern and greatly improved the network security performance. Under the background of the popularization of computer network, how to protect the information security of computer network has also become a widespread concern of all sectors of society. In the process of computer network information transmission, the application of data encryption technicality can form a strong protection for a large amount of information data in the network environment, avoid data being attacked or destroyed, and ensure the information data security of the masses.

1. Introduction

With the continuous development of science and technicality and the gradual progress of computer technicality, the world has entered the information age. The use of computers in all parts of the world has become popular, and computer technicality is gradually valued and needed by the masses. It plays an important role in the development of various fields, meets the needs of application and development in various fields, and gives full play to the existing value of information technicality. Computer information security management, strengthening the application of data encryption technicality, can comprehensively consider the actual needs of its application, comprehensively improve the overall work efficiency and quality, and for the continuous development of social economy, information technicality has been used in various fields in China, resulting in frequent network exchanges. In addition, China's continuous improvement of network openness has further increased people's access to information, thus increasing the risk of network information data. It has become a key issue to be solved urgently. The birth and application of data encryption technicality has effectively changed the network information security pattern and greatly improved the network security performance. Under the background of the popularization of computer network, how to protect the information security of computer network has also become a widespread concern of all sectors of society. In the process of computer network information transmission, the application of data encryption technicality can form a strong protection for a large amount of information data in the network environment, avoid data being attacked or destroyed, and ensure the information data security of the masses. The characteristics of computer information system include the following three points: openness, sharing and real-time. When operating in e-

commerce, computers are often used for information transmission, so the practical application range of computer networks is also expanding. Although different researchers put forward different strategies and angles to solve the problem, they all think it is necessary to protect learners' personal data and privacy by technical means. The use of data encryption technicality has also solved the problem of information security, and to a great extent, it has ensured the security of the information data of the masses.

2. Computer network information security

2.1 Application value of data encryption technicality in computer network information security

With the application of data encryption technicality in computer network security, a comprehensive analysis of data encryption technicality types and a summary of the characteristics of different data encryption technologies can better design network security and improve the level of network security [1]. In the development of modern society, the computer network is an innovative technical system, and it is in a network-free environment. The computer network security management is adopted as the core, and the data encryption technicality is reasonably applied. According to the data encryption technicality, it mainly includes private key and public key. Key is the simplest data encryption technicality, because the same key needs to be used in the process of encryption and decryption, so it is necessary to strengthen security management. If the firewall and security software can't function, it will inevitably affect the computer hardware and software, which will greatly increase the security risk of computer use. Specifically, it converts information into meaningless ciphertext through encryption key and encryption function, and then restores the ciphertext to original information through decryption key and decryption function when receiving [2]. Symmetric encryption technicality is to send the keys involved in the encryption process and decryption process to the sender's data information and the receiver's data information respectively, so that both the sender and the receiver can know the decryption method of the data information and the contents contained therein [3]. Therefore, our country should constantly study the technicality of data encryption, and constantly try and optimize it in practice, so as to seek a safe application channel in today's computer environment. Since entering the Internet era, especially the mobile Internet era, mobile communication technicality, Internet of Things and Web2.0 technicality have developed rapidly. On the one hand, more and more learning resources are put on the network platform, and learners leave a lot of personal and learning records when using the platform. The technicality cycle of global information security industry is shown in Figure 1.

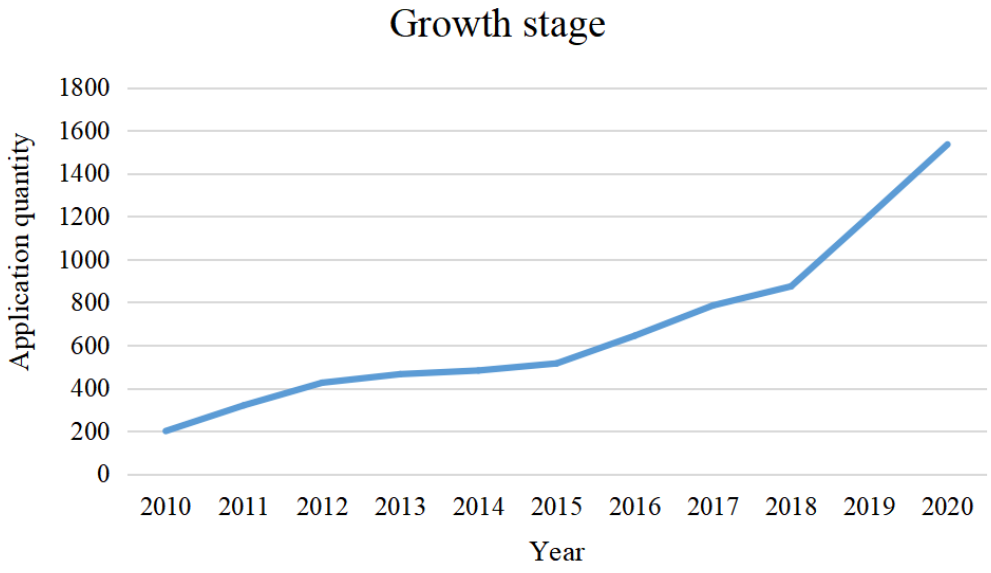

Figure 1 Global information security industry technicality cycle

2.2 Different categories of data encryption technicality

When using data encryption technicality to protect network information data, the most basic key algorithm is the use of symmetric key and asymmetric key. Through the analysis of computer network information security management system, various processing methods can be innovated, and the processing methods can be reasonably selected according to the actual requirements, so that the data encryption technicality can provide a good guarantee for computer network information security. Because there are differences between encryption key and decryption key, disclosing one of them can still ensure the security of data files, thus highlighting the superiority of public key algorithm [4]. Especially when the network data is deliberately attacked, it will bring great losses and serious consequences to the owners of information data. Node encryption technicality, centering on the nodes of the computer system, forms an information security area, and the data information is presented in the form of ciphertext, which can improve the security level of computer data. This technicality is highly similar to the basic link encryption technicality in the process of decryption and encryption, but the related information does not appear on the node in the process of node encryption, so it can re-encrypt the information transmitted to the node. Therefore, computer users need to be careful not to trust and ignore in the mail sending and receiving system, and the attack of network viruses can be avoided without opening this mail virus. Asymmetric key, contrary to symmetric key, means that different keys need to be used in the process of encrypting and decrypting network information data [5]. The hierarchical system of information system security technicality is shown in Figure 2.

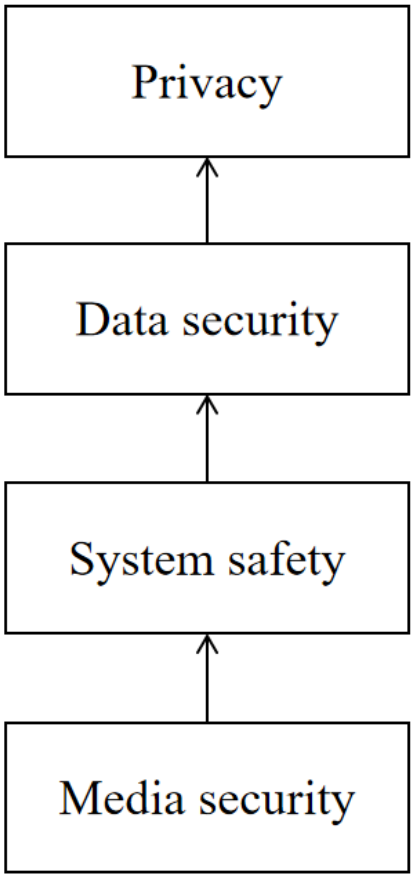

Figure 2 Educational information system security technicality hierarchy

3. The threat of the network

3.1 Link technicality in data encryption technicality

Link technicality in data encryption technicality is a technical way to encrypt and protect data

information in transmission by using computer network lines. Application in computer database. At present, China has entered the era of big data, with abundant network resources, and computers are the four important media for storing network information and data. The application of data encryption in e-commerce is particularly important. Enterprises providing operating platforms and communication services must ensure the information security of enterprises and individual users according to network security protocols [6]. Simply put, after criminals steal private information in the computer field, the computer system can't judge whether its own security has been violated, so it won't give a security reminder. Digital signature technicality is combined with the application of encryption algorithm to prevent information from being tampered by other external factors in the process of transmission, use and storage, thus ensuring the information security of computer users in the e-commerce environment. When an illegal data visitor who does not have the correct decryption key requests to execute the instruction, the data encryption technicality will automatically refuse to execute the access request, which will reduce or avoid the problem of network information data being changed and leaked [7]. With the development of link encryption technicality, it has gradually become the main technical form of data encryption. Now the link encryption technicality can design two independent links to implement secondary encryption protection for information data, so as to enhance the data encryption effect [8]. If it exists in the shared pool of network resources, it will invade the computer system through the network, resulting in the loss, damage and leakage of computer information, which seriously threatens the security of computer network information.

3.2 Educational data security and privacy protection based on information security technicality

The goal of educational data security and privacy protection is through information security technologies such as access control, attack prevention, data encryption and privacy protection. One of the classic algorithms is RSA, which can resist all the known attack modes, and RSA is also the most commonly used encryption algorithm [9]. Relevant technicians should use online encryption technicality and node encryption technicality scientifically and reasonably, and technicians should encrypt the lines in data transmission to ensure the security of data information. However, it should be noted that in the use of computer database, different servers should be designed and encrypted to ensure the difference of decryption keys, so as to further achieve the accuracy of data field records and the effectiveness of data backup. In the end-to-end encryption technicality, the beginning and end of information data transmission are open in the network environment, which is easy to become the target of network attacks [10]. Therefore, in the transmission of computer network information, we should pay attention to the selection of encryption technicality, so as to achieve the best data encryption effect. Differentiate network consulting security from network equipment according to security requirements. In order to reliably transmit integrity data, it is necessary to ensure the security of network equipment and avoid human factors affecting network equipment. Usually, it is the application of link encryption, and the information data is encrypted twice, so that some illegal points can't get the real data of the information data, no matter some simple input paths or basic output paths. With a reasonable firewall system, it can intercept the computer in time when there is a security abnormality, further ensuring the security and stability of the database and the security of users' information and data.

4. Conclusions

At present, people make more frequent use of computer technicality, which improves the convenience of people's life, but also brings security risks. To sum up, this paper mainly analyzes the use of data encryption technicality in computer network information security. The application of computer Internet technicality can improve the overall work efficiency and quality, but it brings advantages, while there are certain security risks. In order to improve the security of users' network information, data encryption should be applied to it, and the ability of computer network security protection should be improved by automatically encrypting and transmitting user data. In the

computer network information transmission, the data encryption technicality is used to construct the security of the data information, which forms an effective security defense against the illegal access of the information data. At the same time, in the era of big data in China, the combination of computer network information security and data encryption technicality can better meet the development needs of network information development in China. Therefore, according to the existing data encryption methods, we should conduct in-depth research and exploration, and combine with the actual security requirements at this stage, and rationally apply various data encryption methods, so as to effectively promote the actual utility of computer networks in information security.

References

[1] Liu Mengjun, Jiang Yuwei, Cao Shuzhen, et al. Application analysis of information security technicality in education data security and privacy [J]. China Audio-visual Education, 2019(6):8.

[2] Wang Yunwu, Wang Tengteng, Li Xueting, et al. The influence of data security and privacy protection on teaching and learning in the intelligent age-the interpretation and mirror of "information security" edition and "teaching and learning" edition of Horizon Report 2021 [J]. china medical education technicality, 2021, 35(4):8.

[3] Fang Yujie. Research on the Core Technology and Risk of Internet of Things Information Security [J]. Think Tank Times, 2019(11):2.

[4] He Wenhai, Xin Jiajia. Problems existing in network information security and research on data encryption technicality [J]. Information Security and Technology, 2019, 010(001):24-26.

[5] Gu Haisheng, Feng Mei, Li Qing. Research on security risk and technicality of intelligent optical network identification-comment on multicast routing and security technicality of intelligent optical network [J]. People's Changjiang, 2022, 53(4):1.

[6] Chen Yingchun. Analysis and Research on Data Security Technology in Big Data Application [J]. Jiangsu Science and Technology Information, 2022, 39(4):3.

[7] Zou Jiabin. Research on data encryption technicality in computer network information security [J]. China High-tech, 2022(2):2.

[8] Zhang Ming. Public security computer information security risks and prevention [J]. Digital Technology and Application, 2022, 40(4):3.

[9] Zhang Yuanyuan. On the protection of personal privacy data in digital society-based on the value orientation of technicality towards goodness [J]. Research on Socialism with Chinese Characteristics, 2022(1):8.

[10] Yao Xiangzhen, Zhang Xiao, Hao Chunliang, et al. Research on Automobile Data Security Policy and Standardization [J]. China Information Security, 2022(3):4.