# Research on Computer Network Security and Cloud Computing Technology Application

[1]Guoquan Liu and [2]Lihe Li,
[1,2]Chongqing Vocational and Technical University of Mechatronics, The Information Center, Bishan, Chongqing, China

***Abstract:*** Research on computer network security and cloud computing technology application is the focus of this study. In the practice of computer network security protection, the application of node encryption technology should be well carried out. In conclusion, in order to effectively safeguard the security of computer networks, the effective use of data encryption technology should be strengthened and applied to different network environments by selecting different data encryption technologies. In order to improve the security of the computing network storage, it is necessary to take effective technical confidentiality measures and this paper gives the novel suggestions that will help to improve the overall performance.

***Keywords:*** *Cloud Computing, Computer Network Security, Network Monitoring, Applications*

## I. INTRODUCTION AND BACKGROUND

Due to its advantages and characteristics, computer technology is widely used in various industries and brings great convenience to people's life, work and study. Among them, network risks threaten the security of computer systems. Generally speaking, the characteristics of big data are reflected in the large data content, more types of the data, and relatively fast data processing speed. In addition, big data has a strong particularity, so we need to carry out network integration when using big data. In the context of the cloud computing era, massive amounts of information can be transmitted over the Internet in the first place, bringing workers the data they need on time, but the confidentiality of the information is also greatly endangered by existing problems within it. Hence, we has listed focuses:

(1) In the process of data transmission, it will follow the inherent program logic to perform calculations, and it can also have a good control effect on each data processing link.

(2) Unlike computer hardware, software system risks have uncontrollable characteristics, and different software systems hide many types of risks and vulnerabilities during operation. In the process of daily use of the computers, in order to meet the diversified needs of the users, software systems are regularly upgraded and updated.

(3) Through the application of cloud computing processing technology, all-round control of data can be realized, and the problem of lack of security in the process of data transmission can also be solved well.

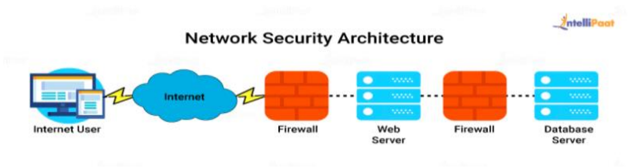

Figure 1. The Computer Network Security Model [12]

In the figure 1, the Computer Network Security Model from the URL [12] is presented. Based on this, in order to effectively safeguard computer network security, the majority of researchers have researched and proposed a series of data encryption techniques for various types of the computer network security problems of the data encryption technology. In the next sections, the details are presented consideing the background.

## II. THE COMPUTER NETWORK SECURITY AND CLOUD COMPUTING TECHNOLOGY APPLICATION

Some computer viruses can even cause great damage to computer networks. For example, today's Internet is full of a large number of the Trojan horse viruses, which often attach to various low-security websites or advertisement pop-up windows. Windows will cause the computer to be infected with a Trojan horse virus that has the following issues.

(1) Computers level of technology has improved, the original weaknesses will be fixed, and old old weaknesses are fixed, new weaknesses will emerge along with them, and it is impossible to It is impossible to avoid the problem completely. Software is always under development, and its weaknesses can only be fixed and repaired. weaknesses can only be repaired and reappear, and the only way to completely solve this problem is to delete the software. The only way to completely solve this problem is to delete the software.

(2) With the increasing development of blockchain technology, the means of hacking have also increased, which has brought a huge impact on technology development, data security, and storage security.

(3) After the computer system is attacked illegally, it will not only cause the leakage of user data information, but also make people's life and property face incalculable loss.

In order to improve the security of the computing network storage, it is necessary to take effective technical confidentiality measures, to give full play to the advantages of cloud computing technology, take traditional technical models as the basis, take effective improvement measures for the problems existing in storage security, and propose effective measures with the technical solution. When the computer and network technology is developed and perfected, the user's calculation function for data transmission is also enhanced, and on the basis of speeding up the information transfer, the information data sharing technology is realized and optimized, which can ensure the security of the computer system and at the same time increase the high confidentiality capability between the user's data and the information system. As the sample, in the figure 2, the Hash Tree Model from Internet is presented.

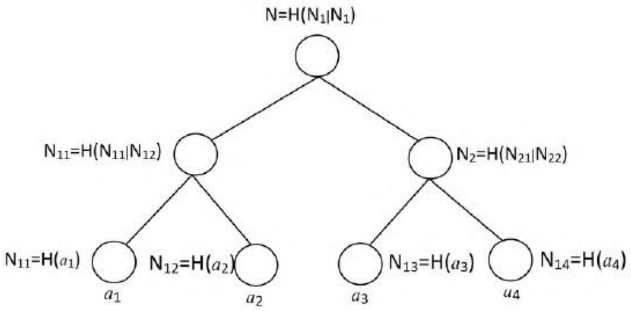

Figure 2. The Hash Tree Model from Internet

The encryption methods complement each other, and the two technologies can be then integrated to improve the efficiency and quality of data transmission and ensure the security of data transmission. Under the cloud computing system, there are still relatively serious security vulnerabilities in the application process of computer data, especially in the process of the data transmission of some large-capacity data at the same network node, which may lead to problems such as data redundancy, which directly affects data security.

Hence, we have the following suggestions.

(1) Analyze and judge the motivation for collecting personal data in the process of use, and combine the memory, processor and related program instructions in the smart terminal device to determine the degree of impact on personal data security as a risk factor and assign a value, and at the same time Use the constructed safety index calculation model to calculate.

(2) In the process of computer operation and use, users need to strictly follow the safety management system, and use the system as a reference to improve the standardization of the operation process.

(3) We should pay more attention to the application of key encryption technology. Key encryption is an encryption service provided to ensure the security of network transmission in an open environment.

(4) Some anti-virus software will infect the computer with viruses during the working process, thus causing varying degrees of damage to the entire computer system. Therefore, when encrypting data, it is necessary to scientifically check relatively confidential data files to see if they are infected with anti-virus software viruses. If so, take effective measures immediately to eliminate the virus.

## CONCLUSION

Research on computer network security and cloud computing technology application is the focus of this study. In the application process of computer network technology, there are still frequent network security problems such as system loopholes. System vulnerabilities may cause buffer overflow problems in the computer, resulting in system commands being affected to a certain extent. Hence, in the paper, the novel suggestions are provided for the task of improving the security, and in the future, the further discussions on the robustness will be verified.

## *References*

[1] Wu, Hsin-Te, and Chun-Wei Tsai. "An intelligent agriculture network security system based on private blockchains." Journal of Communications and Networks 21, no. 5 (2019): 503-508.

[2] Sengupta, Sailik, Ankur Chowdhary, Abdulhakim Sabur, Adel Alshamrani, Dijiang Huang, and Subbarao Kambhampati. "A survey of moving target defenses for network security." IEEE Communications Surveys & Tutorials 22, no. 3 (2020): 1909-1941.

[3] Sundaram, B. Barani, P. Rajkumar, Mrs M. Ananthi, V. Sravan Kumar, Mr Janga Vijaykumar, and P. Karthika. "Network Security Analysis for Signal Strength Based Packet Filitering." In 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS), pp. 1352-1355. IEEE, 2020.

[4] Roshan, Khushnaseeb, and Aasim Zafar. "Deep Learning Approaches for Anomaly and Intrusion Detection in Computer Network: A Review." Cyber Security and Digital Forensics (2022): 551-563.

[5] Lavrov, E. A., A. L. Zolkin, T. G. Aygumov, M. S. Chistyakov, and I. V. Akhmetov. "Analysis of information security issues in corporate computer networks." In IOP Conference Series: Materials Science and Engineering, vol. 1047, no. 1, p. 012117. IOP Publishing, 2021.

[6] Hamza, Ayyoob, Hassan Habibi Gharakheili, and Vijay Sivaraman. "IoT network security: requirements, threats, and countermeasures." arXiv preprint arXiv:2008.09339 (2020).

[7] Silva, João Vitor Valle, Martin Andreoni Lopez, and Diogo MF Mattos. "Attackers are not stealthy: Statistical analysis of the well-known and infamous KDD network security dataset." In 2020 4th Conference on Cloud and Internet of Things (CIoT), pp. 1-8. IEEE, 2020.

[8] Jain, Ankit Kumar, Somya Ranjan Sahoo, and Jyoti Kaubiyal. "Online social networks security and privacy: comprehensive review and analysis." Complex & Intelligent Systems 7, no. 5 (2021): 2157-2177.

[9] Fei, Dingzhou. "Stochastic model for emotion contagion in social networks security based on machine learning." Safety science 118 (2019): 757-762.

[10] Khosravi-Farmad, Masoud, and Abbas Ghaemi-Bafghi. "Bayesian decision network-based security risk management framework." Journal of Network and Systems Management 28, no. 4 (2020): 1794-1819.

[11] Alexei, Lachi Arina. "Network security threats to higher education institutions." In Central and Eastern European eDem and eGov Days, pp. 323-333. 2021.

[12] https://intellipaat.com/blog/what-is-network-security/.