

Big Data Technology and Computer Network Security Application Research

¹Guoquan Liu and ²Lihe Li,

^{1,2}Chongqing Vocational and Technical University of Mechatronics, The Information Center, Bishan, Chongqing, China

Abstract: Big data technology and computer network security application research is the main focus of this study. In network security situational awareness, effective assessment and prediction of security situation is one of the key steps. At present, there are many technical researches on network security situation awareness and prediction. Furthermore, the computer network security application research is then studied. Through the in-depth analysis, the model is then demonstrated for the referring.

Keywords: Big Data, Technology Model, Computer Network Security, Application Research

I. INTRODUCTION

The application of information technology must follow the principle of consistency, mainly involving the security technology in the network environment, and try to achieve the same effect as the network. If the security technology is not compatible with the network, the function of the security technology will be lost, and the information technology cannot play its due role while after functioning, different data and files are found in the network, losing security. In the figure 1, the information security model is defined.

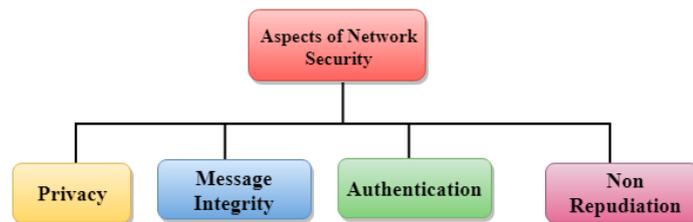


Figure 1. The Information Security Concern Model
(<https://www.javatpoint.com/computer-network-security>)

There are many factors that cause network security problems, and the most common one for ordinary people is human factors. Human factors include two aspects, one is that the user's own security awareness is not enough, ignoring the importance of computer network security. The other is a malicious attack from someone else that causes problems with your computer. Before evaluating the network security situation, it is necessary to establish an evaluation index system first. When constructing an evaluation index system, it is usually necessary to follow several basic principles such as systematicness, approximation, hierarchy and ease of operation.

For the analysis, specifically: first, through the calculation of the subjective and objective weights, the combined weights of the various indicators listed in the previous index system are obtained, and then the processed data are converted into trust degrees, and finally the index data are calculated according to

the combined weights and trust degrees trust in the network. The challenges are then considered as the follows.

The main reason for virus intrusion is that the compiler of the program or file did not repair the code that was damaged when the computer was running in time, so that the wrong code caused damage to the entire system through infinite self-replication. A virus will not use a single individual as the main medium to then cause damage to data information, it will use all electronic carriers as attachment objects, spread destructive factors in a wide area, and then destroy important data and files.

The importance of the computer network security is undeniable. If computer network information security is not taken seriously in daily management, criminals will use it to carry out harmful actions that may damage the interests of the country and the people as well as further protecting computer network information has become a national priority. important task at the level, good work protecting computer network information.

To ensure the safety of personal data, users should regularly protect their computers from viruses. When using a computer, you should install anti-virus software, and then perform anti-virus operations to then repair the loopholes in the network system, and at the same time prevent viruses to make the network system more secure.

II. THE PROPOSED METHODOLOGY

In the development of computer networks, companies and financial institutions of all walks of life have introduced Internet technology. It not only contributes to their economic growth, but also greatly improves the efficiency of the local corporate governance. But cyberattacks and intrusions are getting more sophisticated. In modern society, the Internet, as an indispensable tool, is of great significance to the production and operation of society. Nowadays, network security technology is widely used, of course, many problems will be encountered in normal use.

Usually, the information security of the computer network is more complex and contains more content. In the era of high-speed information exchange, network information security is particularly important. Then, we give the following suggestions. (1) Enterprises need to update the system regularly, further strengthen the computer software and hardware, and optimize the internal and external systems. At the same time, it is necessary to fully combine people's behaviors to optimize frequently used files and also software in order to effectively improve the operability of the computer system and the security of the operating environment. (2) We need to conduct research in the area of protective measures We need to conduct research on the protection measures, and do



fine management on the detection and repair functions, so that the protection measures can intelligently block according to the different levels of attacks and intrusions, and according to The firewall can be further strengthened to ensure that the programs in the computer system are not compromised to ensure that the user's access rights to the computer, to facilitate. (3) Simulate experiments and virtual systems, etc., and create complex models for scientific research content. For better R&D and exploration, not only the development of computer science and technology also provides support for the storage of scientific research results. At the same time provide efficient data retrieval in stored procedures. This makes it easy to find what research institutions need.

Information encryption technology can be implemented in a variety of ways. Encrypting sensitive data and technology can further ensure the security of data and information. Reliable protection even in the event of hacking.

CONCLUSIONS

Big data technology and computer network security application research is the main focus of this study. The current environment urgently needs a unified body to integrate resources and jointly plan the staged development and application of network and information security. In order to strengthen the post-maintenance and construction of network and information security, the operation, maintenance and guarantee mechanism of network and information security should also be improved. This paper gives the novel suggestions for the network security application, and in the future we will test the performance.

References

- [1] Pamarthi, Satyanarayana, and R. Narmadha. "Literature review on network security in Wireless Mobile Ad-hoc Network for IoT applications: Network attacks and detection mechanisms." *International Journal of Intelligent Unmanned Systems* (2021).
- [2] Nazir, Rashid, Kamlesh Kumar, Shubin David, and Munwar Ali. "Survey on wireless network security." *Archives of Computational Methods in Engineering* (2021): 1-20.
- [3] Haider, Noman, Muhammad Zeeshan Baig, and Muhammad Imran. "Artificial Intelligence and Machine Learning in 5G Network Security: Opportunities, advantages, and future research trends." *arXiv preprint arXiv:2007.04490* (2020).
- [4] Adil, Muhammad, and Muhammad Khurram Khan. "Emerging IoT applications in sustainable smart cities for COVID-19: Network security and data preservation challenges with future directions." *Sustainable Cities and Society* 75 (2021): 103311.
- [5] Arevalo Herrera, Juliana, and Jorge E. Camargo. "A survey on machine learning applications for software defined network security." In *International Conference on Applied Cryptography and Network Security*, pp. 70-93. Springer, Cham, 2019.
- [6] Li, Yan, Guang-qiu Huang, Chun-zi Wang, and Ying-chao Li. "Analysis framework of network security situational awareness and comparison of implementation methods." *EURASIP Journal on Wireless Communications and Networking* 2019, no. 1 (2019): 1-32.
- [7] Wheelus, Charles, and Xingquan Zhu. "IoT network security: threats, risks, and a data-driven defense framework." *IoT* 1, no. 2 (2020): 259-285.
- [8] Neupane, Kishan, Rami Haddad, and Lei Chen. "Next generation firewall for network security: A survey." In *SoutheastCon 2018*, pp. 1-6. IEEE, 2018.
- [9] Wang, Haopei, Guangliang Yang, Phakpoom Chinprutthiwong, Lei Xu, Yangyong Zhang, and Guofei Gu. "Towards fine-grained network security forensics and diagnosis in the SDN era." In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pp. 3-16. 2018.
- [10] Ghori, Muhammad Rizwan, Tat-Chee Wan, Mohammed Anbar, Gian Chand Sodhy, and Amna Rizwan. "Review on security in Bluetooth low energy mesh network in correlation with wireless mesh network security." In *2019 IEEE Student Conference on Research and Development (SCoReD)*, pp. 219-224. IEEE, 2019.
- [11] Amrollahi, Mahdi, Shahrzad Hadayeghparast, Hadis Karimipour, Farnaz Derakhshan, and Gautam Srivastava. "Enhancing network security via machine learning: opportunities and challenges." *Handbook of big data privacy* (2020): 165-189.
- [12] Zhang, Zhiyong, Junchang Jing, Xiaoxue Wang, Kim-Kwang Raymond Choo, and Brij B. Gupta. "A crowdsourcing method for online social networks security assessment based on human-centric computing." *Human-centric Computing and Information Sciences* 10, no. 1 (2020): 1-19.