Journal of Applied Data Sciences
Vol. 4, No. 1, January 2023, pp. 22-29

Research on the Technology of Computer Network Security Protection

Yue Peng *

College of Information Engineering of Nanning University, China
pengyue@nnxy.cn *
* corresponding author

(Received: November 22, 2022 Revised: December 13, 2022 Accepted: January 10, 2023, Available online: January 22, 2023)

Abstract

The continuous deepening of the number and importance of sensitive and key info stored in computer network systems has brought severe challenges to computer cyber security protection tech. It is urgent to upgrade the cyber security protection, so that it can serve and match the healthy development of the computer network. Based on this, this paper first analyzes the concept and connotation of computer cyber security, then studies the main content of computer cyber security protection tech, and finally gives the computer cyber security protection measures.

Keywords: Computer Network, Security Protection, Tech

1. Introduction

Computer network security protection is an increasingly important area of research as the reliance on computer networks and the internet continues to grow. As networks become more interconnected and the amount of sensitive data stored on them increases, the risk of cyber attacks also increases. This makes it essential for organizations and individuals to take measures to protect their networks and data [1]. One key area of research in computer network security protection is the development of new security protocols. These protocols are designed to provide secure communication between devices on a network and to protect against unauthorized access and data breaches. Examples of these protocols include Secure Sockets Layer (SSL) and Transport Layer Security (TLS), which are widely used to secure online communication and transactions [2]. Another important area of research is the development of encryption and decryption methods. These methods are used to protect sensitive data by encoding it so that it cannot be read by unauthorized parties. Research in this area focuses on developing new and more advanced encryption algorithms that are more secure and resistant to attacks. Another key area of research is the development of firewalls [3]. Firewalls are used to control access to a network by blocking or allowing traffic based on predefined rules. Research in this area focuses on developing new firewall technologies that can better detect and block cyber threats, such as malware and hacking attempts [4].

Intrusion detection and prevention systems (IDPS) are also an important area of research. These systems are designed to detect and prevent unauthorized access to a network. Research in this area focuses on developing new methods for identifying and mitigating cyber threats, such as malware and hacking attempts [5]. Finally, research in computer network security protection also includes the development of secure communication methods. These methods are designed to protect sensitive information during transmission by encrypting it and providing secure channels for communication [7]. Examples of these methods include Virtual Private Networks (VPNs) and Secure File Transfer Protocol (SFTP).

Overall, computer network security protection research is a critical area that aims to provide organizations and individuals with the tools and techniques they need to protect their networks and data from cyber attacks. As networks and the amount of sensitive data stored on them continue to grow, the importance of this research will only continue to increase [8]. With the iterative progress and maturity of computer tech, many fields have been widely and deeply studied and popularized. While computer tech has brought great convenience to all walks of life, it also makes the dependence of related industries on computer networks continue to increase. In this context, the importance of computer cyber security protection for the protection of data and info security in all walks of life is also rising [9-11]. As a complex system engineering, computer cyber security design computer software, hardware and related login,

matching strategy. The continuous deepening of the number and importance of sensitive and key info stored in computer network systems, as well as the rapid development of network intelligence and info tech, has brought severe challenges to computer cyber security protection tech. It is urgent to upgrade cyber security protection, so that it can serve and match the healthy development of computer networks.

Computer networks have many typical characteristics such as openness, interconnection, interaction and multi-source, which also provides significant convenience for network intrusion and network attack. The virus of computer network systems brings serious realistic threats to the protection of network resources and info, and has caused serious losses. Therefore, it should pay great attention to the security of computer networks and ensure the normal network practice. Currently, network threats and attacks mainly focus on several aspects as shown in Figure 1 below. It is necessary to ameliorate the computer cyber security protection tech to increase the security of network info.

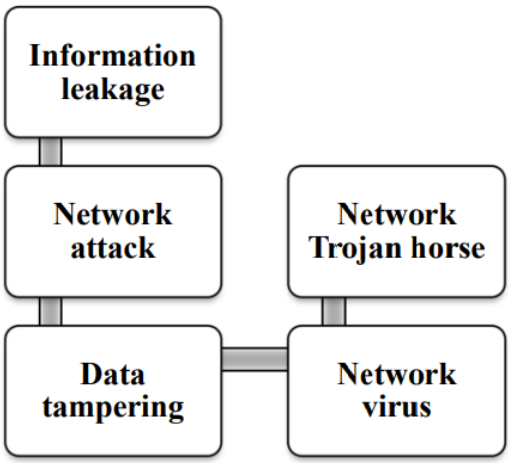

Figure. 1. Main types of network threats and attacks

In a word, under the background of network tech, computer info tech has been widely accelerated, which provides a good interactive platform for the development of all walks of life, but also brings the real threat of cyber security [12]. We need to enhance the security of the computer network and reduce the damage to it as much as possible. In the current era of computer networks, the security of network info is particularly important. Therefore, the study of computer cyber security tech has important practical value.

2. Literature Review

A literature review on the technology of computer network security protection would likely cover a wide range of studies and research articles on the various technologies and techniques used to secure networks and protect them from cyber attacks [13]. Some of the key areas that would likely be discussed include network security protocols, encryption and decryption methods, firewalls, intrusion detection and prevention systems, and secure communication methods.

One recent study, published in the Journal of Information Security and Applications, examined the use of firewalls as a network security measure. The study found that firewalls can be an effective tool for preventing unauthorized access to a network, but they must be properly configured and updated to be effective [14]. The study also highlighted the need for organizations to regularly review and update their firewall policies to ensure they are up-to-date and effective. Another study, published in the Journal of Network and Computer Applications, looked at the use of intrusion detection and prevention systems (IDPS) as a network security measure [15]. The study found that IDPS can be an effective tool for detecting and preventing cyber attacks, but they must be properly configured and updated to be effective. The study also highlighted the need for organizations to regularly review and update their IDPS to ensure they are up-to-date and effective.

In a case study of a current security protection technology, Advanced Encryption Standard (AES) is widely used in various applications to protect sensitive data. AES is a symmetric encryption algorithm that uses a fixed-length key to encrypt and decrypt data. AES is considered to be one of the most secure encryption algorithms available and is used in a wide range of applications, including financial transactions, online communication, and data storage. Another case study is on the application of Artificial Intelligence (AI) and Machine Learning (ML) in network security

protection. AI and ML algorithms can be used to analyze network traffic and identify patterns that indicate a potential cyber attack. Some examples of this technology are used by companies like Darktrace, which uses AI to detect and respond to cyber threats in real-time [16].

Overall, research in the technology of computer network security protection has shown that a combination of different security measures is needed to effectively protect networks from cyber attacks. This includes the use of firewalls, intrusion detection and prevention systems, encryption and decryption methods, and secure communication methods. Additionally, it is important for organizations to regularly review and update their security measures to ensure they are up-to-date and effective [17].

Another case study that is relevant to the technology of computer network security protection is the use of Virtual Private Networks (VPNs). VPNs are used to create secure, encrypted connections between devices over the internet. This makes it possible for users to access a private network, such as a corporate network, from remote locations. This can be very useful for organizations with employees who work remotely or travel frequently, as it allows them to access the same resources and applications as if they were in the office.

A specific example of VPN technology is Cisco's AnyConnect Secure Mobility Client. This VPN solution allows users to securely connect to a corporate network from any location using a variety of devices such as laptops, smartphones, and tablets. AnyConnect provides advanced security features such as network access control, identity management, and threat defense to protect against cyber threats. Additionally, Cisco's VPN allows for flexible deployment options, which can be useful for organizations with a mix of remote and on-premises users. Another case study is the use of Cloud Security. As more and more organizations move their data and applications to the cloud, the need for cloud security solutions has increased. Cloud security solutions are designed to protect data and applications stored in the cloud from cyber threats. One example of cloud security is the Amazon Web Services (AWS) security features, which includes a wide range of services such as encryption, access control, and incident response. AWS also provides customers with compliance and governance tools to ensure they are meeting security and regulatory requirements.

In conclusion, there are various case studies that demonstrate the application of different technologies in computer network security protection. These include the use of firewalls, intrusion detection and prevention systems, encryption and decryption methods, secure communication methods, VPNs, and cloud security solutions. Each of these technologies has its own strengths and weaknesses, and it's important for organizations to evaluate their specific needs and choose the most appropriate solution for their organization. Additionally, It's important for organizations to regularly review and update their security measures to ensure they are up-to-date and effective.

2.1. Definition of computer cyber security

From the narrow sense of protection, computer cyber security mainly means that the computer and its network system resources and info resources are not threatened and damaged by natural and manmade harmful factors. In a broad sense, the relevant technologies and theories related to the confidentiality, integrity, availability, authenticity and controllability of computer network info are the scope of computer cyber security research [2]. With the increasing number of access control and logical connection, the scale of computer software is expanding. Any hidden defects and errors may lead to huge losses. On the other hand, the place where computer systems are used is constantly expanding. The mistakes or lack of experience of various operators, programmers and system analysts may lead to the lack of security function of the system.

Computer cyber security refers to the practice of protecting computer systems, networks, and sensitive information from unauthorized access, use, disclosure, disruption, modification, or destruction. It involves a combination of technologies, policies, and procedures that are used to protect against cyber attacks, data breaches, and other cyber threats. Cyber security measures include firewalls, intrusion detection and prevention systems, encryption and decryption methods, secure communication methods, and security protocols. The goal of cyber security is to ensure the confidentiality, integrity, and availability of information and systems by preventing, detecting, and responding to cyber threats.

2.2. The real threat of computer network system

Computer cyber security involves many disciplines, is a very complex comprehensive problem, and with the change of the system utilization environment and constantly changing. The real threats faced by computer network systems include threats and attacks on hardware entities, info, and software and hardware systems [3]. The real threats to computer network systems include camouflage, illegal connection, unauthorized access, denial of service, denial of

service, info leakage, alteration of info flow, alteration or destruction of data, inference or deduction of info, illegal tampering of programs, etc.

There are a number of real threats to computer network systems that organizations need to be aware of. Some of the most common and significant threats include:

- Malware: This includes viruses, worms, Trojan horses, and other malicious software that can harm or take control of computer systems.
- Phishing: This is a type of social engineering attack where attackers use fake emails or websites to trick users into revealing sensitive information.
- Ransomware: This is a type of malware that encrypts a victim's files and demands a ransom payment to restore access.
- Distributed Denial of Service (DDoS) attacks: This is a type of attack where attackers flood a website or network with traffic in order to make it unavailable to legitimate users.
- Advanced Persistent Threats (APTs): These are sophisticated attacks that are designed to evade detection and steal sensitive information over an extended period of time.
- Insider threats: These are threats that come from within an organization, such as employees, contractors, or vendors who have access to sensitive information and systems.
- IoT and Industrial Control Systems (ICS) security: With the rise of IoT devices and Industrial Control Systems, there's a growing concern about the security of these systems which can be easily exploited by attackers to disrupt or gain control of critical infrastructure.
- Supply Chain attacks: Attackers are increasingly targeting third-party vendors to gain access to an organization's sensitive information and systems.

These threats are constantly evolving and organizations need to be vigilant in order to protect their networks and systems from cyber attacks. This requires a combination of technical and non-technical measures, including regular security updates, employee training, incident response plans and continuous monitoring.

2.3. Problems of computer cyber security protection

The existing problems of computer cyber security mainly include the vulnerability of computer operating system security, cyber security, database management system security and firewall limitations [4]. Among them, the vulnerability of computer operating system security refers to the defects of the operating system structure and the password free access of the operating system, which is the boundary access for system developers, but these accesses are easy to be used by hackers. There is a potential danger in the covert channel of the operating system. Although it can be upgraded through the system, the single security vulnerability of the system will make the security control of the whole system fall into a passive situation.

Secondly, in the vulnerability level of cyber security, the network contains many unsafe factors and vulnerabilities, and the popularity of the network makes info sharing to a new level, the opportunity of info exposure can be greatly ameliorated [5]. There are contradictions and opposites between the accessibility of network data and resource sharing, which make it difficult for computer systems to keep secrets. In addition, in the aspect of DBMS security threats, DBMS security needs to match the security of the operating system, but it is difficult to achieve in practice. The network firewall cannot prevent the real cyber security threats, especially the network internal attacks and virus threats.

There are a number of problems that organizations face when it comes to protecting their computer systems and networks from cyber threats. Some of the most significant problems include:

- Lack of awareness: Many users and organizations are not aware of the latest cyber threats and do not take the necessary steps to protect their systems and networks.
- Limited resources: Many organizations, particularly small and medium-sized businesses, do not have the resources to invest in robust security measures, making them more vulnerable to cyber attacks.
- Complexity: Cybersecurity can be complex, and organizations often struggle to understand and implement the necessary security measures.
- Lack of standardization: There is a lack of standardization in the cybersecurity industry, making it difficult for organizations to compare and choose the right security solutions.
- Human error: People are often the weakest link in cybersecurity, and user mistakes such as falling for phishing emails or using weak passwords can lead to security breaches.

- Legacy systems: Organizations that still rely on older systems and technologies may not have the security features and capabilities of newer systems, making them more vulnerable to attacks.
- Difficulty in detecting and responding to cyber attacks: As attackers are becoming more sophisticated, it's becoming increasingly difficult to detect and respond to cyber attacks.
- Difficulty in keeping up with the fast pace of technology: Technology is advancing rapidly, and it can be difficult for organizations to keep up with the latest security threats and solutions.

Overall, protecting computer systems and networks from cyber threats is a complex and ongoing process that requires a combination of technical and non-technical measures, continuous monitoring, and regular updates to stay ahead of the evolving cyber threats.

3. Research Method

3.1. Research content of computer cyber security protection tech

The research content of computer cyber security protection tech mainly includes physical hardware security, software system security, cyber security protection, data info security, virus prevention tech and network site security [6]. Computer cyber security includes security legislation, security management, security technical measures and other levels. The security legislation level mainly includes social norms, info system security regulations and intellectual property protection. Security management is an important part of computer cyber security protection, including education and training, qualification certification and work specification and assessment. In addition, security technical measures are not only an important guarantee of computer cyber security, but also the material basis of computer network system security, mainly including many processes as shown in Figure 2 below.

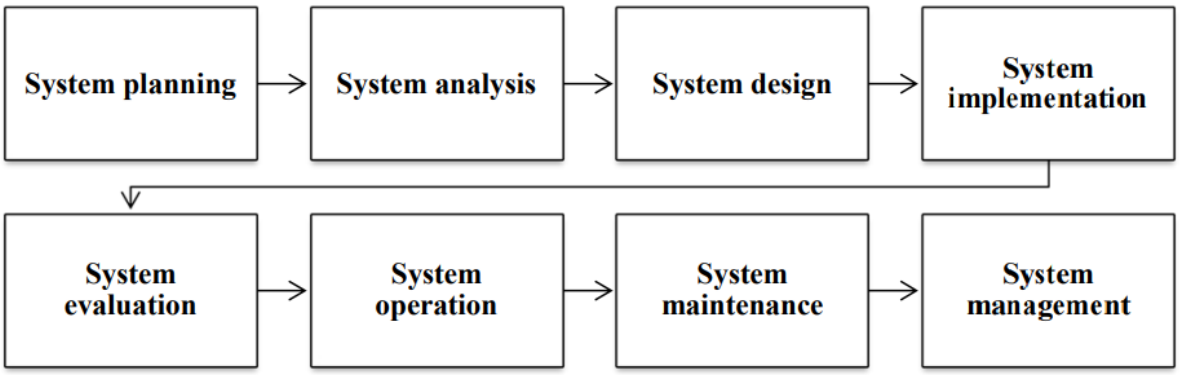

Figure. 2. The value of computer network tech in politic-ideological curriculum

3.2. Key tech of computer cyber security protection

The key tech of computer cyber security protection includes password tech and firewall tech. Among them, cryptography is an important means to prevent data transmission leakage. Cryptography includes cryptography and cryptanalysis [7]. The design of cryptosystem is the main content of cryptography, and the cryptosystem is the main content of decoding cryptanalysis. They support each other and are inseparable. Common cryptographic techniques include elementary cryptanalysis, symmetric key, and stream cipher, block cipher, etc. Among them, the algorithm of block cipher tech needs to be completely determined, the algorithm has a high level of protection, can detect threats, and the operation time or number of operations necessary to recover the key is large enough.

3.3. Computer cyber security design process

Computer cyber security protection design is mainly based on the principles of security requirements, cyber security design, and cyber security system design and so on [18]. Among them, the cyber security needs are confidentiality, security, integrity, service availability, and controllability and info flow protection. Cyber security design should comprehensively analyze the security requirements, determine the security policy, select the security function, and ameliorate the security management. The integrity principle of computer cyber security protection is shown in Figure 3 below. The key of cyber security protection design is to determine the cyber security structure model, produce formal expression tools, and construct the technical methods and products of security control.

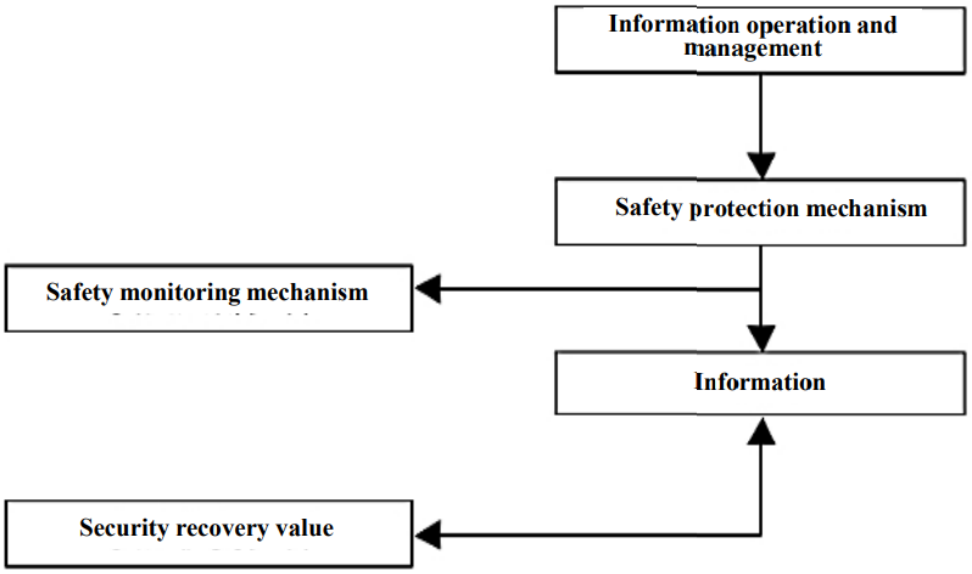

Figure. 3. Integrity principle of computer cyber security protection

4. Computer cyber security measures

4.1. Factors affecting computer cyber security

The factors that affect computer cyber security include human factors, self-factors, big data hidden danger, imperfect laws and regulations, virus intrusion and so on [19]. Among them, the main human factors are the user's own unconscious operation and hacker attacks. Self-factors refer to the security loopholes of computer network operating systems and the defects of network communication protocol. In view of the key factors affecting computer cyber security, the common protection measures mainly include protection wall, data encryption, antivirus software, access control, intrusion detection, info authentication, VPN tech and cloud computing security.

4.2. Characteristics of computer cyber security protection tech

As an important part of computer cyber security protection measures, firewalls separate the intranet from the public access network. Firewall is actually an isolation tech. Firewall cannot effectively prevent malicious insider attacks from inside, nor can it effectively connect through the firewall, nor can it detect viruses, so it has great limitations [20]. As a supplement to the firewall, intrusion detection tech is mainly used to detect any cyber security tech that damages or attempts to destroy the integrity and confidentiality of the system, which can realize the security monitoring of the network. In addition, data encryption tech is to re-encode the data to hide the real info, to achieve the active protection of data security, including password encryption, file encryption and transmission encryption.

4.2. Computer cyber security measures and strategies

First of all, in the management system level, it should strengthen the security awareness of the majority of computer network users, establish and ameliorate the computer network protection system, and establish and ameliorate the management system of computer network technicians. Secondly, at the level of tech utilization, it should strengthen the research and development of various computer cyber security technologies, strengthen the correct utilization of computer cyber security technologies, and guard against the operational risks in computer networks. In addition, at the level of LAN protection, it should ameliorate the virus protection of computer networks, enhance the encryption level of data, and strengthen intrusion detection. Computer cyber security measures and strategies to network-based, multi-layer defense, centralized management, alarm isolation, update at any time as the principle, analysis of cyber security threats, cyber security system to achieve the purpose of security needs analysis.

5. Conclusion

In summary, the computer network system virus has brought serious threat to the protection of network resources and info, and has caused serious losses. Therefore, we need to attach great importance to computer cyber security to ensure the normal network practice. Through the study of the concept and connotation of computer cyber security, this paper analyzes the realistic threats faced by computer network systems. Through the analysis of computer cyber

security protection tech, this paper studies the computer cyber security protection measures and specific protection strategies.

In conclusion, the technology of computer network security protection is a vital area of research that aims to protect networks and systems from cyber attacks. A wide range of technologies and techniques are used to secure networks, including network security protocols, encryption and decryption methods, firewalls, intrusion detection and prevention systems, and secure communication methods.

Research in this field has shown that a combination of different security measures is needed to effectively protect networks from cyber attacks. This includes the use of firewalls, intrusion detection and prevention systems, encryption and decryption methods, and secure communication methods. Additionally, organizations must regularly review and update their security measures to ensure they are up-to-date and effective. Case studies, such as the use of Virtual Private Networks (VPNs), cloud security solutions and AI/ML based security protection, also demonstrate the application of various technologies in computer network security protection. Each of these technologies has its own strengths and weaknesses, and it's important for organizations to evaluate their specific needs and choose the most appropriate solution for their organization. Overall, research on the technology of computer network security protection is critical for keeping networks and systems safe from cyber threats. By staying informed about the latest developments in this field, organizations can better protect themselves and their customers from the ever-evolving cyber threats.

References

[1] A. Maraj, G. Jakupi, E. Rogova, and X. Grajqevci, “Testing of network security systems through DoS attacks,” in 2017 6th Mediterranean Conference on Embedded Computing (MECO), 2017, pp. 1–6.

[2] H. Tao, J. Zhou, and S. Liu, “A survey of network security situation awareness in power monitoring system,” in 2017 IEEE Conference on Energy Internet and Energy System Integration (EI2), 2017, pp. 1–3.

[3] K. Yang, H. Liao, L. Zhao, S. Zheng, and H. Li, “Research on network security protection technology of energy industry based on blockchain,” in 2020 IEEE/CIC International Conference on Communications in China (ICCC Workshops), 2020, pp. 162–166.

[4] D. Acemoglu, A. Malekian, and A. Ozdaglar, “Network security and contagion,” J. Econ. Theory, vol. 166, pp. 536–585, 2016.

[5] Q. Wang, “Strategy of enterprise network security protection based on cloud computing,” in IOP Conference Series: Materials Science and Engineering, 2020, vol. 750, no. 1, p. 12234.

[6] S. Rathore, P. K. Sharma, V. Loia, Y.-S. Jeong, and J. H. Park, “Social network security: Issues, challenges, threats, and solutions,” Inf. Sci. (Ny)., vol. 421, pp. 43–69, 2017.

[7] B. Wang, Y. Zheng, W. Lou, and Y. T. Hou, “DDoS attack protection in the era of cloud computing and software-defined networking,” Comput. Networks, vol. 81, pp. 308–319, 2015.

[8] K. Yun, H. Li, and J. Chen, “Design and Implementation of Power Network Security Protection System Based on Internet of Things,” in Journal of Physics: Conference Series, 2022, vol. 2146, no. 1, p. 12011.

[9] Y. Guo, J. Xu, H. Yuan, Y. Zhuang, G. Zhu, and Y. Zhang, “Research on Enterprise Computer Network Security Protection Technology Based on Information Technology,” in 2020 IEEE 3rd International Conference on Automation, Electronics and Electrical Engineering (AUTEEE), 2020, pp. 488–491.

[10] Y. Shang and J. Zhang, “Computer multimedia security protection system based on the network security active defense model,” Adv. Multimed., vol. 2021, pp. 1–9, 2021.

[11] M. V Pawar and J. Anuradha, “Network security and types of attacks in network,” Procedia Comput. Sci., vol. 48, pp. 503–506, 2015.

[12] M. Zhang and K. Sun, “Computer Network Security Protection Strategy Based on Big Data,” in Innovative Computing: Proceedings of the 4th International Conference on Innovative Computing (IC 2021), 2022, pp. 1343–1350.

[13] M. Todd and S. Rahman, "Complete network security protection for SME's within limited resources," arXiv Prepr. arXiv1512.00085, 2015.

[14] M. Huang, W. Luo, and X. Wan, "Research on network security of campus network," in Journal of Physics: Conference Series, 2019, vol. 1187, no. 4, p. 42113.

[15] Y. Wang et al., "An exhaustive research on the application of intrusion detection technology in computer network security in sensor networks," J. Sensors, vol. 2021, pp. 1–11, 2021.

[16] J. Zhou, "Discussion on the Technology and Method of Computer Network Security Management," in IOP Conference Series: Materials Science and Engineering, 2017, vol. 242, no. 1, p. 12089.

[17] H. Lin, Z. Yan, Y. Chen, and L. Zhang, "A survey on network security-related data collection technologies," IEEE Access, vol. 6, pp. 18345–18365, 2018.

[18] D. Schatz, R. Bashroush, and J. Wall, "Towards a more representative definition of cyber security," J. Digit. Forensics, Secur. Law, vol. 12, no. 2, p. 8, 2017.

[19] I. Hwang and O. Cha, "Examining technostress creators and role stress as potential threats to employees' information security compliance," Comput. Human Behav., vol. 81, pp. 282–293, 2018.

[20] W. Duan, J. Gu, M. Wen, G. Zhang, Y. Ji, and S. Mumtaz, "Emerging technologies for 5G-IoV networks: applications, trends and opportunities," IEEE Netw., vol. 34, no. 5, pp. 283–289, 2020.