Research on Computer Network Information Security Protection Strategy and Evaluation Algorithm Education

Meng Teng(✉)

Hunan Foreign Language Vocational College of China, Changsha 410008, Hunan, China
tmeng123@sina.com

Abstract. Computer network information security management is an important problem to be solved in China. The effective protection of computer network information security depends on the perfect deployment of computer network security information protection strategy. Computer network security information protection strategy is one of the key research projects in China. According to the relevant standards and regulations, this paper analyzes the current situation of computer network information security protection strategies, studies several common security protection strategies and the evaluation algorithm of relevant computer network information security insurance, so as to guide and prevent the security management of public network information system.

Keywords: Computer network · Information security · Protection strategy

1 Introduction

We are in the information age of the 21st century. Information security, especially network information security, has been closely related to everyone's daily life. More and more companies use the Internet to operate their business. Administrative organs and government departments use computers to store important information and data, and individuals use computers and diversified terminal devices to enjoy the speed and convenience of the Internet. However, due to the openness, interconnection and anonymity of the network, all kinds of sensitive information, ranging from important administrative and military information to personal privacy information, are inevitably transmitted and stored on the Internet, as shown in Fig. 1. These are the targets of computer criminals and hackers. If these information is not properly protected to meet its security requirements, individuals, companies, various organizations and even countries will face huge economic risks and trust risks [1]. As computer workers, deepening the exploration of network information security protection technology is the guarantee of citizens' information security. Therefore, the security and reliability of modern network information has become the focus of common concern all over the world, and has also become a new field of hot research and talent needs.

M. A. Jan and F. Khan (Eds.): BigIoT-EDU 2022, LNICST 465, pp. 603–613, 2023.
https://doi.org/10.1007/978-3-031-23950-2_66

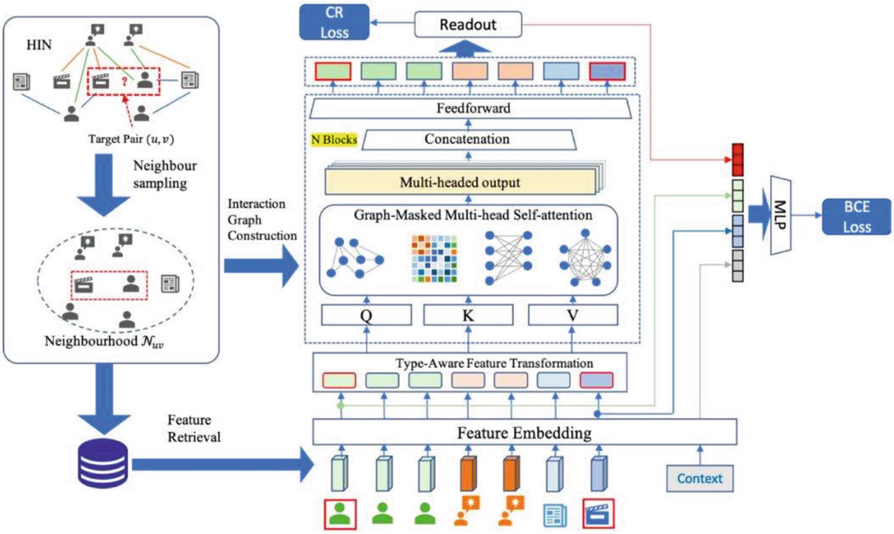

Fig. 1. Computer network information

The processing and storage of cloud computing data are carried out on the cloud platform. The separation of the owner of computing resources from the user has become an inherent feature of the cloud computing model. As a result, users' concerns about the secure storage and privacy of their data are inevitable.

Specifically, user data, including even privacy related content, may be intentionally or unintentionally disclosed in the process of remote computing, storage and communication. There are also data loss problems caused by power failure or downtime. Even for unreliable cloud infrastructure and service providers, they may learn the user's privacy information through the analysis and speculation of user behavior. These problems will directly lead to contradictions and frictions between users and cloud providers, reduce users' trust in the cloud computing environment, and affect the further promotion of cloud computing applications.

The access control policy of "all" only explicitly opens the corresponding port or opens the relevant access policy when there is a data access demand [2]. In the virtual application environment, the logical boundary security access control strategy in the virtual environment can be set, such as the refined data access control strategy between virtual machines and within virtual units by loading virtual firewalls.

2 Concept and Technical Characteristics of Network Information Security

2.1 Concept of Network Information Security

The so-called computer network security refers to ensuring the confidentiality, integrity, availability and auditability of data and information on the network by relying on network management control and technical measures. The essence of network security is network information security. Therefore, protecting network information security is the ultimate goal and key of network security. Information security is to ensure that information is not leaked or destroyed in the process of generation, transmission, storage and processing. The conceptual process of network information security is shown in Fig. 2 below.

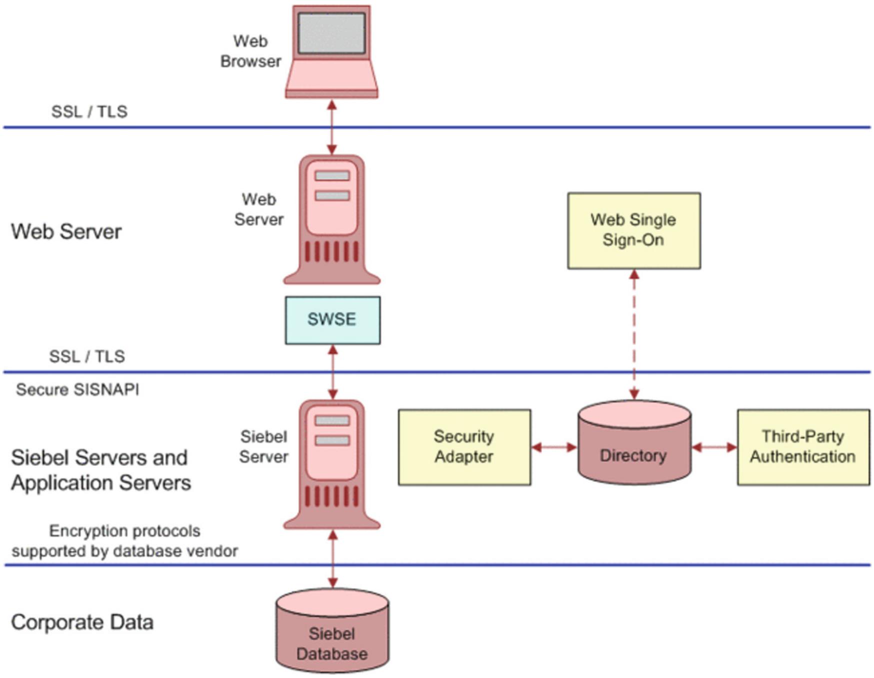

Fig. 2. Conceptual process of network information security

The model of communication security includes three aspects: one is physical security, that is to protect information and valuable resources, which can only be physically accessed with permission. In other words, security service personnel must protect these data information from being moved, tampered with or stolen by unauthorized persons [3]. The second is operation safety, which refers to the work required to deal with security threats. It mainly includes: network access control (protect the security of network information resources from unauthorized persons), identity authentication (ensure the authenticity and reliability of user identity using information), network topology (set the network physical location of each device according to its own needs). The third is security management, which is to effectively manage the safe operation of information and systems by using comprehensive measures.there must be a "back door" opened for them in our system. As long as we block it and let hackers have nowhere to start, isn't it beautiful!

2.2 Technical Characteristics of Network Information Security

The integrity, confidentiality, availability, controllability and non repudiation mentioned in the meaning of network security are the basic characteristics and objectives of network information security, of which the first three are the basic requirements of information security. The five characteristics of network information security reflect the important characteristics of the basic elements, attributes and technology of network security.

(1) Integrity. The integrity of network information security refers to the characteristics of non modification, non-destructive and non look at each link of information storage, transmission, exchange and processing, so as to ensure that the information remains intact [4].
(2) Confidentiality. The confidentiality of network information security refers to the strict control of all possible disclosure links to prevent the disclosure of private and useful information to unauthorized individuals and entities in the process of generation, transmission, processing and storage.
(3) Availability. The availability of network information security means that network information can be used by authorized users, which can not only be correctly accessed when the system is running, but also be restored when the system is attacked and damaged.
(4) Controllability. The controllability of network information security refers to the characteristics that can effectively control the dissemination of information and specific content circulating in the network system. Resist the unauthorized use of network information resources [5]. The controllability of network information security is shown in Fig. 3 below.

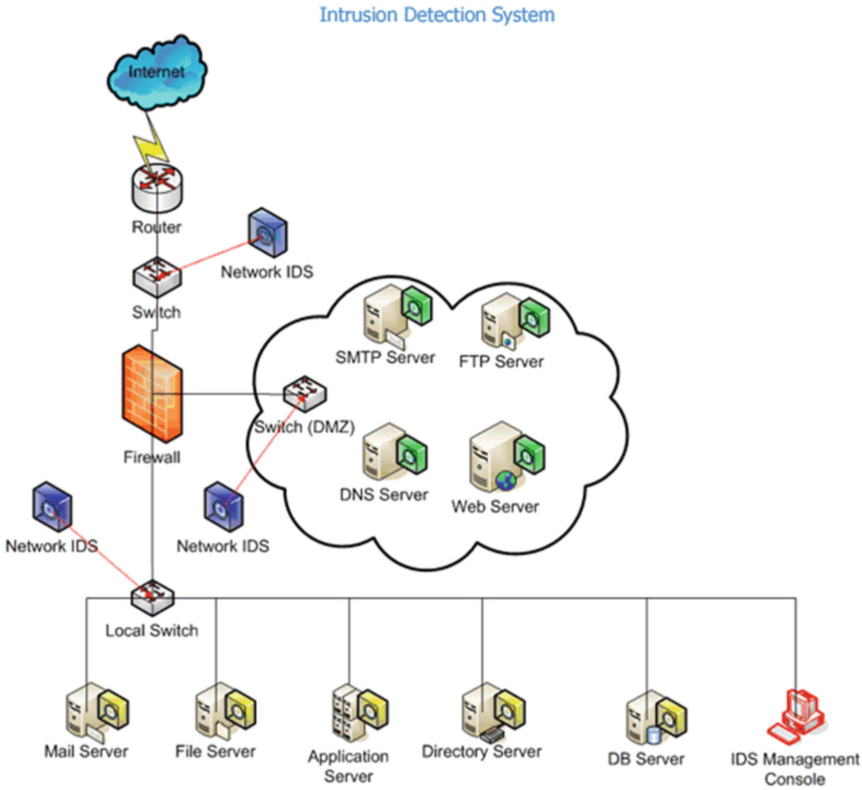

Fig. 3. Controllability of network information security

(5) Non repudiation. The non repudiation of network information security, also known as censurability, refers to the two sides of network communication in the process of information exchange to ensure that participants can not deny their true identity, the authenticity of the information provided, as well as the completed operations and commitments [6].

For an open Internet system, it is extremely necessary to take security measures, otherwise any end user connected to the network can access the information resources in the network. In today's information age, network information has penetrated into all fields of society and is used more and more widely. It not only brings convenience and development opportunities, but also provides possibilities for all kinds of computer crimes [3]. Typical threats in network systems include information disclosure, integrity infringement, denial of service and illegal use [7].

3 Research on Computer Network Information Security Protection Strategy

Classification of information security and security emergencies, network information security notification management means, etc,. The computer network information security protection is shown in Fig. 4.

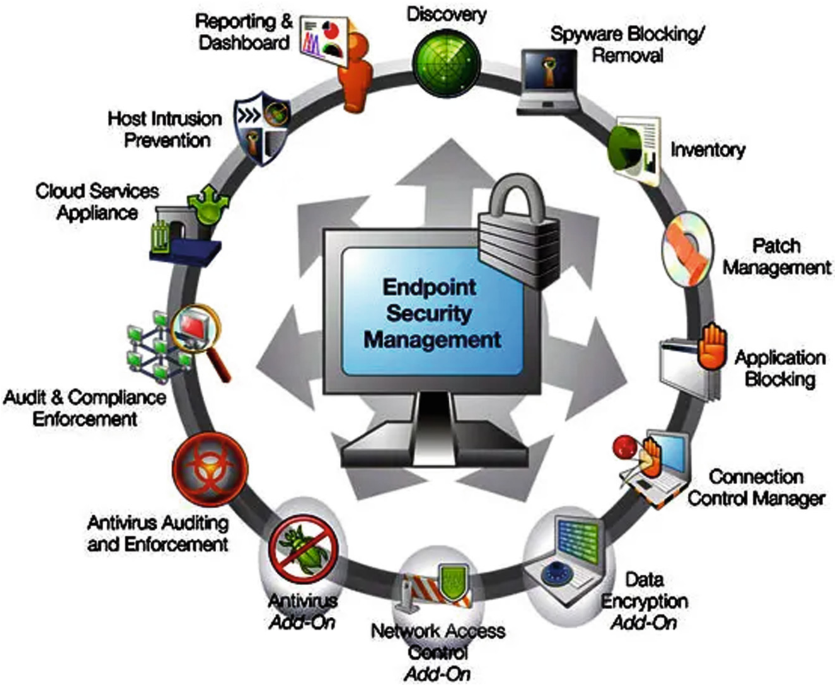

Fig. 4. Computer network information security protection

3.1 Safety Technology

Physical security technology. In order to comprehensively improve the computer network information security protection level, the whole computer room needs to be improved in strict accordance with the relevant specifications of the computer room construction technology [8]. The technical framework of network security is shown in Fig. 5 below.

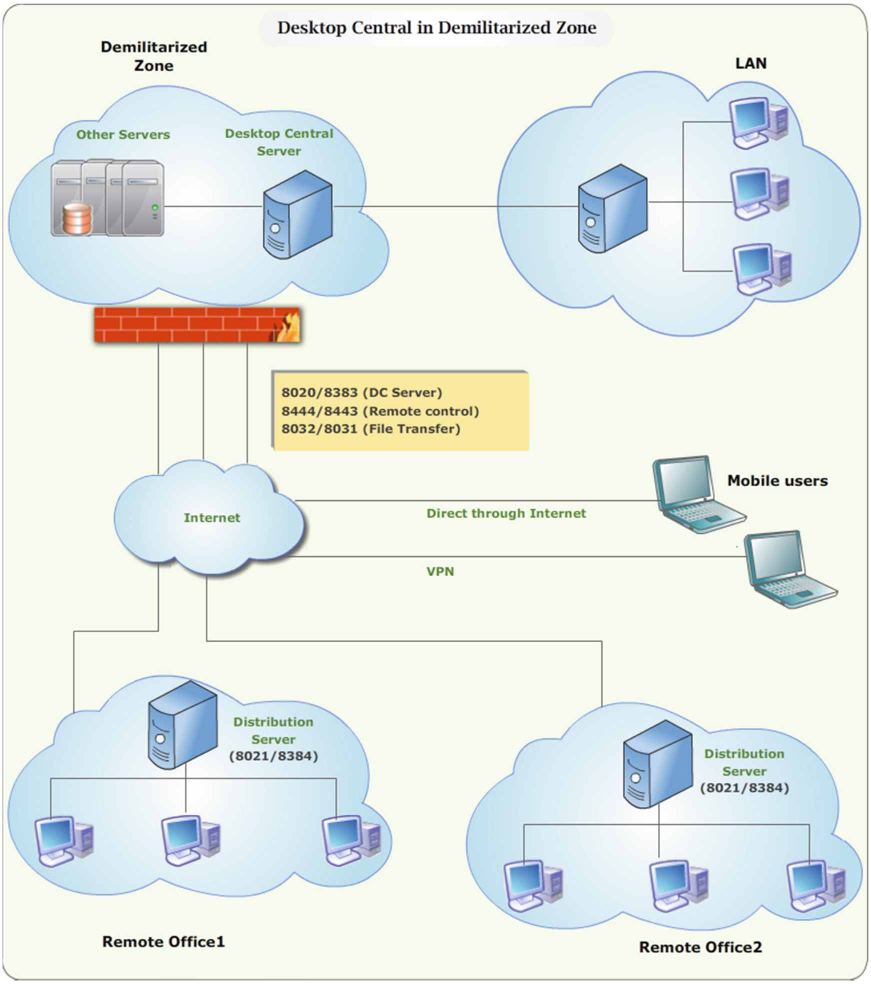

Fig. 5. Network security technology framework

The construction of the computer room should not only meet the requirements of fire prevention and waterproof, but also evaluate the computer network information security problems from the perspective of physical security, such as physical access In the control stage, we need to focus on the following contents[9]: ① special personnel must be assigned to take charge of the exit location of the computer room, and the personnel information of each exit computer room shall be recorded; ② For visitors to the computer room, strictly implement the application and approval process, and control the scope of activities of visitors; ③ Pay attention to avoid the theft and damage of the machine room, keep the main equipment during work, and fix it on the basis of proper placement; Mark each equipment for easy search; At the same time, pay attention to the storage location of communication cables, such as indoor underground and pipeline location [4].

(2) Network security technology. Network security technology can be divided into many types, including sub regions and sub regions [10]. According to the relevant regulations of China, the sub region and sub region security technology should be defined according to the corresponding network architecture, and the security guarantee measures should be taken to pass the first step Integrated network security system, after constructing an ideal network information operation environment.

(3) Host security. The network information security protection strategy of host security mainly includes the following points: ① anti-virus. Based on the current virus database, form a virus management system to realize comprehensive virus detection and prevention from the perspectives of system equipment and Intranet; ② desktop security, depending on the habit of desktop security management, hardware configuration, security optimization strategy, etc. Face to face, implement a comprehensive desktop management strategy; ③ Network access management Build a network access management system, clarify the network access regulations, identity authentication and other key security management regulations, ensure the controllability of the whole terminal behavior, and finally improve the computer network Safety level [11]. Figure 6 below shows the construction of a network access management system.

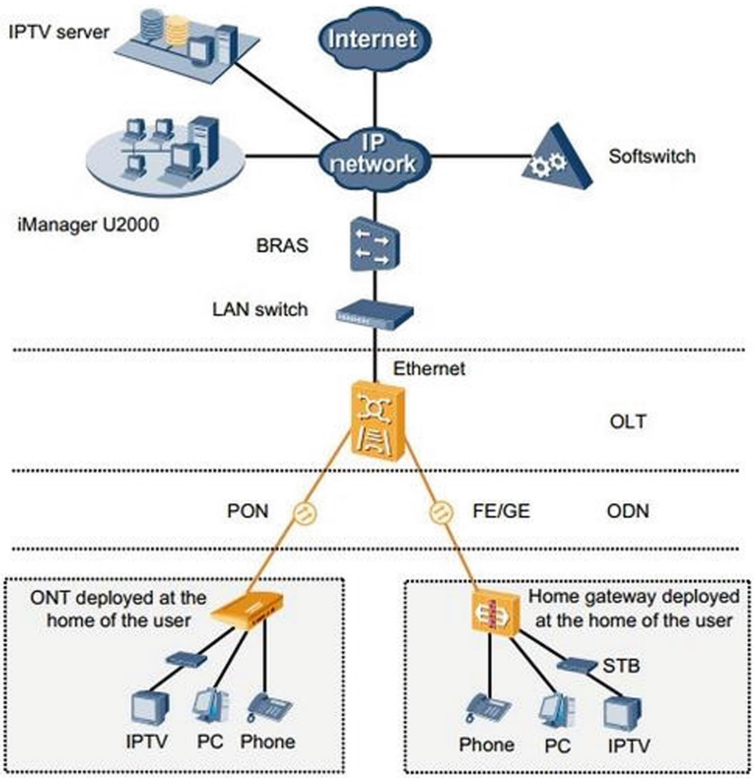

Fig. 6. Build a network access management system

4 Analysis of Computer Network Information Security Evaluation Algorithm

4.1 Comprehensive Grey Correlation Clustering Method Analysis

In this study, the comprehensive grey relational clustering method will be adopted. This method mainly includes three functional modules: data acquisition, data preprocessing and comprehensive query. In this technology, it can be further refined according to the relevant contents, and by adding auxiliary processes, It can obtain network security data resources more effectively.

$$Delta\{x\} = m(distance) \tag{1}$$

$$delta\{x\} = m - max \tag{2}$$

when studying related problems, relevant technicians can form a comprehensive information security strategy by extracting the security management information of multiple time periods [12]. It can also be combined with the Grey Correlation Clustering safety evaluation system to evaluate various safety events and find solutions from the perspective of safety evaluation (Fig. 7).

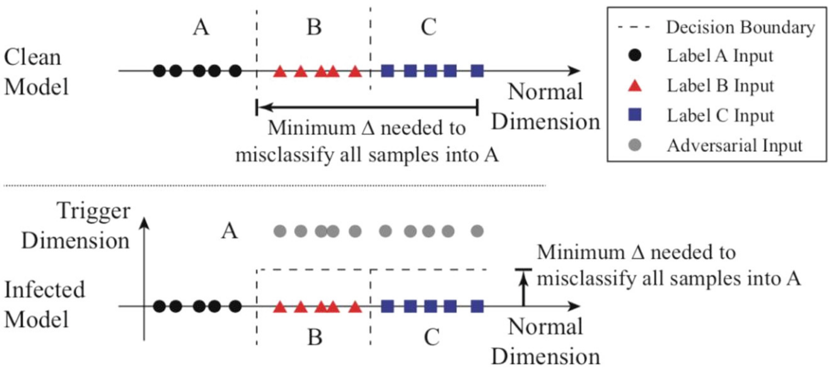

Fig. 7. Grey relational clustering analysis framework

4.2 Grey Relational Clustering

The basic concept of grey correlation clustering is: assuming that the correlation degree of the two indicators is matched, it can be regarded as the same type. The key of the specific operation process is to classify the indicators according to the correlation between the calculated indicators The principles to be followed in the classification process are: assuming that the selected indicators do not appear in the divided groups, they can form - a new independent group; If a selected indicator appears in the divided group, you need to add another indicator to the group [13].

From the application effect, many grey factors in computer network information security evaluation can be processed quantitatively through grey correlation clustering, in which all evaluation index parameters will affect the evaluation results; In the evaluation process, there will be no loss of information, so the feasibility of the analysis results can be guaranteed However, it should be noted that in the network information security evaluation algorithm of Grey Correlation Clustering, it is also necessary to build a static network information module and a dynamic network firewall module [14], which is an inevitable requirement for the whole network security supervision.

5 Conclusion

Computer network information security protection involves a wide range. Therefore, for relevant personnel, in the next stage of work, they must deeply understand the needs of network information security management and improve it from the aspects of host security, network technology and physical security. At the same time, from the case enterprise selected in this paper, The grey relational cluster analysis method can evaluate the level of network information security, which is worthy of further promotion.

By default, any user can connect to the server through an empty connection, enumerate accounts and guess passwords. Therefore, we must prohibit the establishment of empty connections.

Opening more services can bring convenience to management, but it will also leave an opportunity for hackers. Therefore, it is better to turn off some services that are really unavailable. For example, when I don't need to remotely manage my computer, I will turn off the services related to remote network login. Removing unnecessary service stops can not only ensure the safety of the system, but also improve the running speed of the system.

References

1. Xiao, F.C., Politics, S.O., ND University: Research on information security protection strategy of private cloud network in colleges and universities. Dig. Technol. Appl. (2019)
2. Zhai, Y.: Some thoughts on the security and protection strategy of computer communication network. Wirel. Internet Technol. (2018)
3. Gao, F., Mu, J., Han, X., et al.: Performance limit evaluation strategy for automated driving systems **5**(1), 12 (2022)
4. Shandilya, S.K., Upadhyay, S., Kumar, A., et al.: AI-assisted computer network operations testbed for nature-inspired cyber security based adaptive defense simulation and analysis. Futur. Gener. Comput. Syst. **127**, 297–308 (2022)
5. Chen, T., Kong, D., Hong, Y.: Development and implementation of anti phishing wi-fi and information security protection APP based on android. In: IOP Publishing Ltd. IOP Publishing Ltd, 032109 (2021). (7pp)
6. Xu, Y., Lan, S.: The detection and evaluation strategies for critical information infrastructure. Inf. Technol. Network Secur. (2019)
7. Li, Y.: Relevant thoughts on computer communication network security and protection strategy. Electronic Test (2018)

8. Zheng, X., Xiao, Q.: Coupling physical information channels and building a practice design and evaluation system:thoughts on the reconstruction strategy of physical problems under the condition of information technology (2018)
9. Ge, S.: Risk and preventive strategy of network information security in public library. Library Theory and Practice (2018)
10. Cheng, X., Zhang, P.: Information security and adoptable solutions in the implementation of industry 4.0 strategy for the fourth-generation industrial revolution. J. Phys. Conf. Ser. **1682**, 012087 (2020)
11. Yu, L.: Analysis of computer software security and protection strategy. China Computer & Communication (2019)
12. Liu, X., Zheng, A., Zhu, E., et al.: Application of the whole life cycle cloud platform of electric energy metering equipment and security protection strategy. Electr. Energy Manage. Technol. (2018)
13. Wei, C., Feng, T., Li, X., et al.: Computer network security and network security technology strategy research. Electronic Test (2019)
14. Yang, C.H., Zhou, H.F., Jun, M.A., et al.: Research and implementation of beidou short message security protection system based on national secret algorithm. Comput. Modernizat. (2019)