Research on Risk Factors of Fuzzy Evaluation of Network Security Based on Computer Big Data

Peikun Xie1, *, YiFan Dang2, Yang Dang3
1 Nanjing Forest Police College, Nanjing 210023, China
2 Southwest Jiaotong University, Shanghai 200240, China
3 Beijing Institute of Electronic Science and Technology, Beijing 100070, China
*Corresponding author e-mail: xiepeikun@forestpolice.net

Abstract. Under the background of big data, computer technology is widely used in all walks of life, and enterprises need strong technical support. The advent of the era of big data has greatly improved the efficiency of the Internet era, but it has also brought more serious network security problems. In view of the complexity of influencing factors and difficulty in quantifying indicators in network security risk assessment, a risk quantification method based on fuzzy comprehensive evaluation is proposed, and a grading index system of influencing factors for a single risk scenario is established. The enterprise network security risk is divided into five levels, and the enterprise network security risk level is determined according to the evaluation of the expert group. The application example shows that the above algorithm can quantitatively evaluate the dynamic risk of network system and improve the accuracy of network security risk assessment. Finally, aiming at the problems existing in computer network information security, the corresponding countermeasures are put forward. It is hoped that the new key technology of network security risk assessment combined with data application can better realize network security application and protect the privacy of network information.

Keywords: Big data; Network security; Fuzzy evaluation; Risk assessment.

1. Introduction
With the development and application of information technology and computer network, the role of network information system in all walks of life is becoming more and more important. In our daily life, network application has become a new way of life which is the fastest and most convenient for people [1]. Big data has been widely used in modern life because of its irreplaceable advantages such as fast update speed, diverse data types and large amount of data. In the information age, data has become a core strategic resource rather than a simple digital string [2]. It is certain that these data have a very important impact on a country's economic operation and social life style. The data information in the enterprise is very important and can be shared by more people. In addition, the emergence of computer network has brought fast and efficient service items to people's life, but the use and operation of computer network system has also brought many threats [3]. Due to the concealment of security risk, it is easy to be ignored and ignored, but it has brought serious harm at this stage [4]. Especially in the era...
of big data, computer networks store all kinds of important data information of more and more people, especially private information. Once poorly protected, data leakage will lead to disastrous consequences. The reliability, security and risk of the system are important topics in modern reliability engineering. The in-depth study of such problems will help to enhance the security degree of the system, improve the system reliability and reduce security vulnerabilities [5].

With the continuous development of network technology, the network not only brings surprises to people's life, but also brings threats. Computer crimes, hackers and harmful programs seriously threaten network security. Network security has aroused widespread concern. Although people pay more and more attention to computer network security in recent years, due to the continuous progress and development of new technology, security measures are still limited and the security problem is still severe [6]. In the context of big data, the factors threatening network security are increasing, which seriously affects the development of data operation. More and more people also begin to notice that there are problems in computer network security that may damage their own interests. If individuals, enterprises and even important organizations do not pay attention to the security of computer network, there will be the leakage of private information, resulting in a great threat to property security. Therefore, strengthening the existing network technology security measures is not only the primary purpose of existing technicians, but also the main means to ensure the security of big data [7]. With the advent of the big data era, the development process of computer network is accelerating, and information system management projects are becoming more and more important in various industries. How to construct a more safe and effective network operation environment is a problem that relevant management departments need to seriously think and actively practice. Optimizing the application of key technologies of risk assessment can upgrade the overall network operation system on the basis of improving management effect and control level [8].

The evaluation of network security is not only an important technology in network security defense, but also an important part of information security engineering. Its principle is to use various methods to check the known security vulnerabilities that may exist in the target item by item to determine the existing security risks and security risks [9]. In the era of big data, it is necessary to comprehensively analyze the influencing factors in computer network security and put forward targeted security measures to further improve the security of computer network information. The fuzzy comprehensive evaluation method can evaluate things according to a variety of factors [10]. It is a systematic analysis method of fuzzy analysis and evaluation by using the principle of fuzzy mathematics. It is a combination of qualitative and quantitative, imprecise and accurate analysis and evaluation method [11]. According to the four physical factors affecting enterprise network security (user factors, external factors and management factors), the enterprise network security risk is divided into five levels, and the impact of each index on enterprise network security risk is evaluated. This paper analyzes the standards of network security risk assessment under the background of big data era, and discusses the key technologies of risk assessment from the aspects of security database technology, risk assessment module technology and cloud security detection technology, in order to provide valuable technical suggestions for technical managers.

2. Analysis of problems in computer network security under the background of big data era

2.1. Hackers invade computer networks
Network hacking technology is relatively hidden in the application process. "Hacker" refers to invading network information by means of Trojan horse virus, forcibly opening network security protection, introducing it into other information network systems, and stealing other people's information [12]. On the one hand, criminals use technical means to destroy the data on the computer network, paralyze the system and lose the data. On the other hand, criminals use technical means to decrypt, steal and intercept sensitive information, which will lead to the leakage of a large number of important data and information. Although some technical personnel in enterprises are specially equipped with network security tools, the technical means of cyber hacking still emerge one after another, which seriously
affects the information security of computer network. Therefore, when the computer works normally, it can't identify hacker attacks only with simple security tools. When the computer has hacker attacks, it will bring more serious influence to the computer network.

2.2. Users' awareness of information security is weak
In the future, the role of big data is becoming more and more important, and there are more and more security risks, so more and more security precautions are needed. In the era of big data, users use computers more and more every day, and many users have caused many negative problems in their use. Some users are unfamiliar with computer performance and standardized operating procedures, and know little about network security, which may lead to malicious attacks. Under the background of big data, individuals and enterprises should pay attention to protecting information security in the process of using the network, and should not give criminals an opportunity. Today, with the vigorous development of network technology, various websites and application software are full of tricks and "packaged" to attract people's attention. In addition, in order to facilitate user experience and follow-up services, many websites and applications require users to fill in personal information. In this process, if users have a weak awareness of information security, they will input various information without checking the authenticity and security of websites and application software, which will lead to information leakage. Therefore, it is necessary to strengthen the safety awareness of network users, and further standardize the operation of network technology, so that users' data and information will not be leaked.

2.3. Data security issues
The development of computer technology follows the evolution from simple to complex, and the technology also goes from simple to mature. The nonstandard security management of computer server will lead to the computer running in the environment without security protection. For example, if the firewall is not enabled when the system is running, hackers and Trojans cannot be monitored, thus leaving the computer in an unsafe environment and possibly causing a large-scale network crash. At present, the data storage of the third-party platform is increasing exponentially, and more and more data information is gathered. Although the security and scalability of storage have been strengthened, there are still a lot of shortcomings in storage security due to the defects of unstructured data, which poses a threat to data security. Especially, the current storage mode technology is still in its infancy, some technologies are not mature, and data security is still the main problem at present. The security instability of data information itself may also affect the computer network security. If the computer information itself is relatively safe, the files carrying the data information can give full play to its application value when entering the system, so that all work can be carried out more smoothly. However, if the data information is maliciously tampered with or the files contain viruses, the application value of the data information will be reduced after the data and files enter the system, and even the data system of the whole computer system will be affected.

2.4. Viruses are more concealed
Computer operating system is a system software developed effectively by programmers with high level and strong professional skills, and the computer operating system will be constantly improved with the efforts of computer software developers. However, at present, there are still some system vulnerabilities in the computer operating system, which need to be detected by the staff and constantly improved and corrected. For most computer network security problems, because related attacks are more concealed, even some advanced viruses can avoid scanning specific program codes by antivirus software in a "segmented" way. After entering the computer, they will splice in a self-integrated way, and then upload data inside the computer. In addition, in order to avoid the abnormal uploading behavior discovered by computer users, the computer virus will monitor the actual usage of the computer, and when the computer is not used for a long time, the data will be uploaded to the designated object through the network in the background. Hackers attack computers or viruses invade computers by capturing and
exploiting system vulnerabilities. In order to improve the security of the operating system and ensure it effectively, it is necessary to reduce the system vulnerabilities and fix them.

3. Evaluation system and determination of enterprise network security risk evaluation index

3.1. Establishment of evaluation system

Network and information system is a complex system engineering, which has both hardware and software, external influences and internal factors, and many aspects are mutually restricted. Under the background of the development of big data, in order to improve the security of network operation, it is necessary to actively construct a more systematic security risk assessment model, combine technical points, improve the effectiveness of information technology and management measures, and lay a solid foundation for upgrading the management system. Fuzzy comprehensive evaluation is a method based on fuzzy mathematics, applying the principle of fuzzy relation synthesis, quantifying some factors with unclear boundaries and difficulty in quantification, and then making comprehensive evaluation [13].

First of all, we must determine the evaluation factor set, and then analyze it from the three-tier architecture of the network. The network layer is divided into several host-tier factors according to the evaluation attributes of each subsystem, that is, the evaluation factor risk value of each network device within the considered network range. Then, each network device is divided into several service-tier factors. The specific expression is as follows:

The comprehensive risk of the system is decomposed into three evaluation factors, namely, asset value, threat risk value and vulnerability risk value. That is:

\[ U = \{ U_1, U_2, U_3 \} \]

It indicates the asset value, threat risk value and vulnerability risk value of the corresponding network equipment (including servers, routers, switches, etc.) within the considered network range. That is:

\[ U = \{ U_{i1}, U_{i2}, \ldots, U_{ik} \} (i = 1,2,3; k = 1,2,\ldots,n) \]

Each subset \( U_{ij} \) is divided into several subsets \( U_{ijk} \) according to the requirements of security assessment, that is, for the value of the host layer, the asset value, threat risk value and vulnerability risk value of the service should be analyzed from each service or software included in the network equipment, namely:

\[ U_{ij} = \{ U_{ij1}, U_{ij2}, \ldots, U_{ijk} \} (i = 1,2,3; k = 1,2,\ldots,n) \]

3.2. Determination of enterprise network security risk evaluation index

The process of network security risk assessment is shown in Figure 1, which is divided into four stages [14]. Preparation stage, including defining evaluation objectives, determining evaluation scope, and establishing evaluation management and implementation team.

![Figure 1. Risk assessment process](image)

In the analysis stage, firstly, identify the risk scenarios of information systems to ensure the completeness of the risk scenarios, including at least all important risks, and then filter some minor risks according to the business nature of the system and relevant standards, and rank them according to their importance; In the evaluation stage, it is to quantitatively evaluate the risk scenarios by combining
By consulting literature [15] and combining with the actual situation of some enterprises, the evaluation index system of enterprise network security risk is determined as follows, see Table 1 for details.

| Primary index            | Secondary index                      |
|-------------------------|--------------------------------------|
| Physical factors $P_1$  | Computer hardware equipment $P_{11}$ |
|                         | Computer network facilities $P_{12}$ |
|                         | Computer server environment $P_{13}$ |
| User factor $P_2$       | User safety awareness $P_{21}$       |
|                         | Subscriber number $P_{22}$           |
|                         | User distribution $P_{23}$           |
| External factors $P_3$  | Hacking attack $P_{31}$              |
|                         | Virus invasion $P_{32}$               |
|                         | Illegal visit $P_{33}$                |
| Management factors $P_4$| Administrator's safety awareness $P_{41}$ |
|                         | Number of administrators $P_{42}$    |
|                         | Administrator management skills $P_{43}$ |
|                         | Administrator's administrative authority $P_{44}$ |

4. Risk factors of fuzzy evaluation of network security

The basic steps of fuzzy comprehensive evaluation are as follows.

(1) Establish a factor set

Factor set is a set composed of various factors that affect the evaluation object, $U = \{u_1, u_2, \cdots, u_m\}$, where $u_i = (i = 1,2,\cdots,m)$ represents each influencing factor.

(2) Establish a weight set

Whether the weight of each index is determined properly or not directly affects the final comprehensive evaluation result. In the traditional fuzzy comprehensive evaluation method of network security risk, according to the reason that the indicators with higher risk level have a greater impact on the comprehensive risk, and therefore should be given a greater weight, experts directly give the weight of each indicator according to its risk level. There are many subjective factors in this method of giving weight, which easily leads to large deviation in the final comprehensive evaluation results.

The formula is a method of accurately calculating the respective weights by using the formula after the experts queue each index according to its importance [16]. Because it is easier to queue the importance of each index objectively and accurately, the formula method can eliminate the influence of some human factors and make the final comprehensive evaluation result more in line with the objective reality.

Therefore, in the fuzzy comprehensive evaluation of network security risk, the formula selected in reference [10] is used to determine the weight of each index:
Among them $ W_i = 1. 

In the above formula, $ n $ is the index number, $ i $ is the queuing level and $ i = 1, 2, \cdots, m (m \leq n) $. (Note: Queuing rank is an arrangement of indicators according to their importance, with indicators with high importance ranking first, and corresponding $ i $ taking smaller values. Different indicators can be at the same rank. If certain indicators are considered to be equally important, they are at the same rank, and $ i $ taking the same value). $ W_i $ can be normalized to get the weight $ W_i^* $ [8].

(3) Establish evaluation set

The evaluation set contains all possible comments on the evaluation object, which are given subjectively by experts according to actual problems, assuming that the evaluation set is $ V = \{v_1, v_2, \cdots, v_n\} $. In this paper, the indicators are divided into 1-5 grades, and the meanings of different grades are defined in detail.

(4) Single factor fuzzy evaluation

In this paper, the Delphi method is used to invite a number of experts to form an evaluation group, which compares the risk evaluation level and evaluates each risk influencing factor at the middle level, so that the subjective estimation is more objective. Assuming that the evaluation set $ V = [v_1, v_2, \cdots, v_5] $ has $ v_j $ comments $ v_j (j = 1, 2, \cdots, 5) $ for the evaluation factor $ u_i $, then the membership vector $ d_i = \{d_{i1}, d_{i2}, \cdots, d_{i5}\} $ of $ u_i $ to the comment set $ V $ where:

$$ d_{ij} = \frac{v_j}{\sum_{j=1}^{5} v_j} \quad (2) $$

(5) First-class fuzzy comprehensive evaluation

The first-level fuzzy comprehensive evaluation is evaluated according to each level of each factor, and the evaluation result vector is $ B_i $, then $ B_i = A \circ D_i = [b_{i1}, b_{i2}, \cdots, b_{im}] $, where "$ \circ $" is the fuzzy synthesis operator, and the weighted average type is adopted in this paper, namely:

$$ b_{ij} = \sum_{i=1}^{m} (a_i \times d_{ij}) \quad (3) $$

(6) Multi-level fuzzy comprehensive evaluation

The multi-level fuzzy comprehensive evaluation is based on the first-level fuzzy comprehensive evaluation, and the result vector $ B_i $ is normalized to form matrix $ D $. At the same time, Delphi method is used to determine the weight $ A $ of the next-level evaluation index to the previous-level evaluation factor, and then the final evaluation vector $ B $ is calculated according to formula $ B = A \circ D $. 

(7) Evaluation results

And the membership degree $ \tilde{b}_i $ in the evaluation result is taken as the weight coefficient, and the weighted average value of each $ v_j $ is taken as the evaluation result, namely:
5. Application example
The following examples illustrate the application of risk assessment model based on fuzzy mathematics in network security risk assessment.

In the evaluation model, we should first evaluate $P_1, P_2, P_3$, and $P_4$. Let's assume that for the same item $P_1$, we carry out $P_2, P_3$, and $P_4$, and get the risk levels of 5, 3 and 3 respectively. Then according to the definition of membership function, the membership degree of each factor belonging to each risk level is:

| Risk level | 1 | 2 | 3 | 4 | 5 |
|------------|---|---|---|---|---|
| $P_1$      | 0 | 0 | 0.2 | 0.8 | 0.2 |
| $P_2$      | 0.3 | 0.7 | 0.2 | 0 | 0 |
| $P_3$      | 0.2 | 0.8 | 0.7 | 0 | 0 |
| $P_4$      | 0 | 0.1 | 0.8 | 0 | 0 |

Therefore, the relational fuzzy matrix is as follows:

\[
p = \frac{\sum_{i=1}^{n} v_i b_i}{\sum_{i=1}^{n} b_i}
\]  

\[Y = \begin{bmatrix} 0 & 0 & 0.2 & 0.8 & 0.2 \\ 0.3 & 0.7 & 0.2 & 0 & 0 \\ 0.2 & 0.8 & 0.7 & 0 & 0 \\ 0 & 0.1 & 0.8 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0.05 & 0.44 & 0.12 & 0.33 & 0.03 \end{bmatrix}
\]

Therefore, the probability that the obtained evaluation results belong to each risk level is:

| Evaluate the risk level | Very low | Low | Middle | High | Very high |
|-------------------------|----------|-----|--------|------|-----------|
| Result                  | 6%       | 44% | 12%    | 33%  | 3%        |
evaluation of the level of secondary indicators is the result given by expert groups, and the results given by different expert groups are different, which depends on the experts’ cognition of enterprise network security risks. In the brand-new network security risk assessment system, the risk information database plays a key role. Because of its own ability to store, transmit and obtain information, it can effectively upgrade and improve the evaluation and prediction system to ensure data analysis and data accuracy, so as to improve the practical significance and value of the overall network security risk assessment.

6. Countermeasures for information network security in the era of big data

6.1. Strengthen the attention to the security of big data information network

Big data information has become an indispensable and important part of human production activities. Network security management departments should improve the professional and technical quality of network security management personnel, strengthen training, promote public network security work in communities and campuses, carry out public network security work, and encourage enterprises and the public to establish network security communities. China is still in the initial stage of big data development, and all kinds of strategic planning are lagging behind. Therefore, we should pay more attention to the security of big data information network, promote the security strategy in line with our own interests as soon as possible, and put it at the strategic height of national security. Under the background of the continuous development of computer technology in the era of big data, legislation must also keep pace with the times to ensure the safe and healthy development of the network, establish a rapid response mechanism, and take legal actions to create a clean and tidy cyberspace.

6.2. Improve users' own safety awareness

Because network security threats are everywhere, when people use computer networks for financial transactions or information transmission, they must have a high degree of network security awareness. In order to ensure the safe operation of the network, we should not only flexibly apply various security technologies and measures, but also strengthen users' own security awareness, such as enhancing users' awareness of installing anti-virus software, updating system patches in time, and designing high-level security passwords, so as to fundamentally prevent the occurrence of network security accidents.

However, there is no absolute security protection for any network. While relying on technical protection, a perfect security management system should be established, such as establishing access control system, equipment management system, emergency system and network management system for security equipment, so as to strengthen the management and maintenance of the network and enhance the security efficiency of the network itself. There are certain limits to any data protection and security. For ordinary network users, it is necessary to emphasize the importance of network security to them through multiple channels, so that users can truly realize the damage that can be caused to them when the computer network has security problems. In order to effectively improve the safety awareness of network users in the process of using network computers, so that they can standardize their own operation behavior in actual operation, and further prevent network security problems.

6.3. Using software to monitor abnormal network traffic

For computer network data stealing behavior with strong concealment, besides standardizing the usage habits of personal computer network, it is necessary to strengthen the real-time monitoring of computer network data flow. Figure 2 is a schematic structural diagram of the abnormal flow detection system.
Figure 2. Structure of abnormal flow detection system

Therefore, the problem can be solved by downloading and installing the network traffic monitoring alarm software, which can monitor the network data traffic, alarm the abnormal data traffic, and point out the target program and the uploaded data information source, thus assisting the computer user to confirm whether there is any risk in the data uploading behavior. For high-risk data uploading behavior, the network traffic monitoring software will automatically cut off the network link to avoid causing greater losses to users. After the operation structure of the database system changes, it is necessary to analyze and integrate the data of the server, and use the service to temporarily replace the client system to ensure the effectiveness of data processing. At the same time, in the process of establishing the management mechanism of the security risk database system, it is necessary to carry out centralized integration and comprehensive statistics on the data, and carry out centralized encryption processing on the data with the help of firewall mechanism, so as to lay a solid foundation for information upgrading.

6.4. Effective use of firewall and security monitoring system

In order to effectively resist computer network viruses, security detection technology and firewall technology are often chosen to strengthen enterprise system security, which is widely used in enterprise and company management. Aiming at the security problems caused by computer failures, in order to protect against malicious software and Trojan horse virus attacks caused by system vulnerabilities. At present, firewall technology has been widely used in public network or corporate network ecosystem, and it is the most convenient technology for managing and controlling information security. In the contemporary era of big data, facing a large amount of data information processing, the computer system will expose the loopholes existing in the firewall in the past when analyzing and applying it, which makes the firewall ineffective. According to this problem, users can use artificial intelligence firewall technology to judge the security of access behavior and review foreign files repeatedly. At the same time, in view of the leakage of data and information, documents can be encrypted with the help of intelligent encryption system security management technology and high-strength encryption algorithm in practical work.

In order to implement the decisions of the decision-making level, it is necessary to have a management level to manage the daily work and an implementation and maintenance level to be responsible for the implementation of safety plans and decisions. The hierarchical information security organization is shown in Figure 3.
Figure 3. Hierarchical information security organization

Based on the era of big data, only by choosing the appropriate information security management method can the security of internal management system be strengthened. When the detection system finds that there is a virus in the computer, it will attack and clean it again. The computer virus is a gradual process in the development process, and it will be constantly updated at the same time. Only by doing a good job in computer security prevention technology can the correct security monitoring technology be adopted to fight against the virus and fundamentally resist the virus. Viruses are constantly changing and developing, which requires Internet companies to have a technical understanding of the transmission characteristics of viruses, so as to basically monitor the security of viruses and then transmit information in a safe environment.

7. Conclusion
Today, the network security situation is getting more and more severe. Sometimes, when the network danger has invaded and occurred, seeking corresponding solutions will cause incalculable actual losses. In order to deal with the computer network security risks brought by the era of big data, it is necessary to improve the computer network security precautions to fill the loopholes in the system. By analyzing the contents of computer network security and the problems of computers in the era of big data, this paper puts forward a fuzzy risk evaluation model, which is used for evaluation, and finally gives the comprehensive evaluation results of the system. Example analysis shows that this method is more scientific in the evaluation process, and the results are more reliable and accurate, which is also beneficial to "prevention before problems occur". However, obtaining the original data (the risk value of each index) also depends on the evaluation of each expert, which cannot avoid the infiltration of subjective factors. How to reduce the influence of subjective factors is the direction of improving fuzzy comprehensive evaluation method. People need to improve their awareness of network security and strengthen their personal protection ability, and jointly build a network security community to improve network security, so that computer networks can make greater contributions to human economic and social development. Under the background of big data, it is necessary to use more effective methods and ideas, combined with the data operation management mechanism, to ensure that the data network security risk prediction and cloud data processing effect meet expectations, and lay a solid foundation for the establishment and sustainable development of the network management system.
References

[1] Jingjie, Min, Wang, et al. Evaluation and reliability analysis of network security risk factors based on D-S evidence theory [J]. Journal of intelligent & fuzzy systems: Applications in Engineering and Technology, 2018, 34(2):861-869.

[2] Chen Y H, Chang A, Huang C W. An ai driven risk assess framework to evaluate DDoS cyberattack [J]. Journal of Intelligent and Fuzzy Systems, 2020(17):1-9.

[3] Sun Ye. Research on Computer Network Security Evaluation Based on Support Vector Regression Machine [J]. Modern Electronic Technology, 2016, 39(07):89-92.

[4] Chen Huaxi, Guo Youqiang, Yao Baofeng. A network security evaluation model with coupling weighting [J]. Computer Engineering, 2011, 37(22):99-101.

[5] Li Zhiguo. Establishment and simulation of network security evaluation model based on SVR [J]. Electronic Design Engineering, 2018, 026(013):75-79.

[6] He Jin, Guo Yanhui, Zhang Mingfei, et al. Fuzzy Comprehensive Evaluation of Tourism Safety Risk in Mountain Scenic Areas [J]. Sichuan environment, 2019, 038(002):101-107.

[7] J Liu, D Wang, HU Yuqin. Fuzzy Comprehensive Evaluation of Electrostatic Risk in Oil Depot Based on Analytic Hierarchy Process [J]. Journal of Xi’an Shiyou University (Natural Science Edition), 2019, 034(001):120-126.

[8] Fan Z, Tan Z, Tan C, et al. An FCM-based Hierarchical Method for Evaluating Network Security Situation [J]. Journal of Electronic Science, 2018, 29(3):56-72.

[9] Pan Y, Mei F, Zhou C, et al. Analysis on Integrated Energy System Cascading Failures Considering interaction of Coupled Heating and Power networks[J]. IEEE Access, 2019, PP (99):1-1.

[10] Singh N, Virmani D, Gao X Z. A Fuzzy Logic-Based Method to Avert Intrusions in Wireless Sensor Networks Using WSN-DS Dataset [J]. International Journal of Computational Intelligence and Applications, 2020(1):2050018.

[11] Qi Z, Zhou C, Tian Y C, et al. A Fuzzy Probability Bayesian Network Approach for Dynamic Cybersecurity Risk Assessment in Industrial Control Systems [J]. IEEE Transactions on Industrial Informatics, 2018, PP (99):1-1.

[12] Liu Q, Zeng M. Network security situation detection of internet of things for smart city based on fuzzy neural network [J]. International Journal of Reasoning-based Intelligent Systems, 2020, 12(3):222.

[13] Liu Kun. Evaluation of ship network security status based on BP neural network [J]. Ship Science and Technology, 2019, 41(20):161-163.

[14] Wu Renjie. Research on the Application of Neural Network in Computer Network Security Evaluation [J]. Computer Simulation, 2011, 28(011):126-129.

[15] Wen Siqin, Wang Biao. Computer network security evaluation simulation model based on neural network [J]. Modern Electronic Technology, 2017, 040(003): 89-91.

[16] Ketsap A, Hansapinyo C, Kronprasert N, et al. Uncertainty and Fuzzy Decisions in Earthquake Risk Evaluation of Buildings[J]. Engineering Journal, 2019, 27(5):89-105.