Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 9663520, 12 pages
https://doi.org/10.1155/2021/9663520

Research Article

Research on Information Security Risk Assessment Method Based on Fuzzy Rule Set

Wentian Cai[1] **and Huijun Yao**[2]

[1]*School of Cyber Science and Engineering, Southeast University, Nanjing 210096, China*
[2]*Jiangsu Broadcasting Cable Information Network Corp., Ltd., Nanjing 210096, China*

Correspondence should be addressed to Wentian Cai; 230188094@seu.edu.cn

Received 5 August 2021; Accepted 24 August 2021; Published 22 September 2021

Academic Editor: Zhihan Lv

With the increasing complexity of the network structure and the increasing size of the network, various network security incidents pose an increasing threat to the security of computer systems and the network. Especially, in the network environment, the diversified intrusion methods and application environment make the security of the network more fragile. In order to improve information security, based on fuzzy rule sets, this paper proposes a fuzzy association rule mining algorithm based on fuzzy matrix and applies it to security event correlation. In addition, this paper combines the embedded system to construct an information security risk assessment system and sets the system performance based on the actual situation. Finally, this paper carries out experimental design to verify the performance of the system and analyzes the experimental results by mathematical statistics. From the experimental research, it can be seen that the system constructed in this paper has a certain effect.

1. Introduction

Information security risk assessment has become an important means to ensure the security of information systems in enterprises and institutions. Moreover, the effectiveness of the evaluation method used is the prerequisite and basis for ensuring the reliability of the evaluation results. Therefore, the in-depth study of information system security risk assessment methods has extremely important practical significance.

The existing information system security risk assessment methods can be roughly divided into two categories [1]. One is the system security analysis method based on multivariate statistics. This type of method usually realizes the safety assessment of the object to be assessed through quantitative indicators, and the results obtained through the assessment have the characteristics of intuitive data and strong objectivity. The main evaluation methods include event tree analysis method, fault tree analysis method, cluster analysis method, and factor analysis method. The other is the system security analysis method based on knowledge and decision technology. This kind of method is usually based on the relevant knowledge and practical experience of the evaluator to perform corresponding reasoning on the existing nonquantitative data and information to realize the security risk assessment of the information system, so as to grasp the security status and potential risks of the entire information system. Such methods mainly rely on the professional knowledge and rich experience of experts to avoid the shortcomings of quantitative calculation methods in the process of information system risk assessment. The main methods include principal component analysis, Delphi method, group decision method, and logical analysis method. However, both types of risk assessment methods have obvious inherent flaws and deficiencies. The system safety analysis method based on multivariate statistics is an objective quantitative calculation method. On the one hand, the data of the object to be evaluated needs to be quantified in the data preprocessing stage. The quantification process will cause some relatively complex object attributes to be blurred and simplified, and the risk factors obtained after quantification will inevitably have some deviations in understanding. On the

other hand, because the existing information system has certain dynamic characteristics, the static description method based on the system architecture and business functions is difficult to characterize the actual security status of the entire system. The system security analysis method based on knowledge and decision-making technology is a subjective qualitative analysis method, and the professionalism of the evaluator has a great influence on the reliability of the evaluation results. Therefore, there are relatively high requirements on the professional competence and professional quality of the evaluator. Therefore, in order to ensure the accuracy and reliability of information security risk assessment results, new risk assessment models and methods are urgently needed to better ensure the safe operation of information systems [2].

Based on the above analysis, this paper studies the information security risk assessment method based on the fuzzy rule set, constructs the corresponding model structure, and verifies the system performance through experimental research.

2. Related Work

In the field of ICPS information security risk assessment, a lot of research work has been carried out at home and abroad. In terms of risk analysis, the literature [3] gave the original definition of risk and pointed out the three elements of risk, namely, possible events, probability of occurrence, and potential losses. The literature [4] combined the definition of risk with system scenarios and analyzed the inherent relationship between system risk and elasticity. In terms of evaluation thinking and framework research, the literature [5] took the lead in putting forward the connotation of control system information security, reviewed some existing risk assessment frameworks, compared and analyzed the qualitative and quantitative assessment modes, and discussed the application of related technologies. The literature [5] systematically studied systematic risk management and gave a risk assessment framework under a data-driven model, including the design of conceptual models and index evaluation systems. The literature [6] reviewed a large number of system risk assessment methods and gave a roadmap of risk assessment research recommendations from qualitative analysis to quantitative analysis and from deterministic assessment to probabilistic assessment.

In terms of risk modeling and analysis, models such as attack trees, Markov chains, Bayesian networks, and Petri nets have been introduced one after another. The literature [7] shows that evidence theory and analytic hierarchy process are helpful to solve the uncertainty problem in ICPS risk assessment. The literature [8] proposed the idea of combining attack tree and fault tree for risk analysis. The literature [9] designed a multimodel risk assessment method based on a multilayer Bayesian network, which has achieved good results in improving the dynamics of the assessment. The literature [10] designed a state-based semi-Markov chain to model the impact of attacks. The method can effectively describe the impact of the physical process. In terms of risk quantification, the literature [11] compared the difference between ICPS security quantification and IT systems based on the analysis of ICPS availability, integrity, confidentiality, and other security attributes and gave overall recommendations for index system research. The literature [12] has long been committed to the research of risk assessment based on the mechanism of the controlled process and proposed system availability metrics based on downtime and some other risk quantitative auxiliary indicators. The literature [13] designed quantitative strategies for security attributes such as reliability, availability, and controllability from a statistical perspective.

In recent years, fruitful research results have been achieved in the research on the evaluation method based on the comprehensive risk of the system. The literature [14] used analytic hierarchy process as the basic structure to combine with information entropy, Bayesian network, and fuzzy theory and applied them comprehensively, thereby reducing the subjectivity of the evaluation results and improving the early warning ability of information system risks. Under the principle of the maximum deviation of squares, the literature [15] proposed a risk assessment method based on triangular fuzzy entropy, which reduces the influence of subjective factors on the assessment results and makes the assessment results more objective. The literature [16] combined factor analysis and SVM to improve the speed of system risk analysis modeling and the accuracy of risk analysis, which makes the evaluation results more reliable. The literature [17] combined rough set theory with unascertained measure theory, DS evidence theory, and neural network, respectively, so as to realize quantitative evaluation of information system security assurance capabilities and security level protection evaluation and improve the reliability of risk assessment. The literature [18] combined gray theory and fuzzy theory, comprehensively applied the degree of membership and gray to the evaluation, and built a gray fuzzy comprehensive evaluation model to achieve the classification of information system risk levels. The literature [19] proposed a risk assessment method based on fuzzy cognitive maps, which uses fuzzy cognitive maps to obtain the relationship between assets and obtains the system's risk value through the inference process. Because traditional neural networks have the disadvantages of slow training speed and low convergence accuracy, the literature [20] used AHP, PCA, fuzzy theory, and wavelet transform to construct risk assessment models and optimize neural networks, so that the assessment results of information systems are more accurate and effective.

3. Fuzzy Association Rules

$T = \{t_1, t_2, \cdots, t_n\}$ represents the transaction database, t_i represents the i-th record in T, $I = \{i_1, i_2, \cdots, i_m\}$ represents all attributes appearing in T, the attribute in I is a quantitative attribute, and i_j represents the j-th attribute in I. These quantitative attributes are divided into several fuzzy set levels, and the different fuzzy set levels of these quantitative attributes are regarded as new attributes. Since the attributes are fuzzy sets, these attributes are called fuzzy attributes. Each i_k is divided into l_k fuzzy sets, and the resulting fuzzy

attribute set is set to $i_k(1), i_k(2), \cdots, i_k(k)$. For any record t_j and fuzzy attribute $i_1(1)$, the value of t_j on $i_1(1)$ is recorded as $t_j(i_1(1))$, which is the membership degree of the value of this record on attribute i_1 on fuzzy set $i_1(1)$, $t_j(i_1(1)) \in [0, 1]$.

The set of all fuzzy attributes generated is I_f, and $X = \{y_1, y_2, \cdots, y_p\}$, $Y = \{y_{p+1}, y_{p+2}, \cdots, y_{p+q}\}$ is a subset of I_f, $X \cap Y = \varnothing$. Since the attributes in X and Y are fuzzy attributes, we call the association rule $X \Rightarrow Y$ as a fuzzy association rule. Among them, the fuzzy attributes in X and Y should not contain the same mark i_k at the same time.

Similar to Boolean association rules, in association rules $X \Rightarrow Y$, the fuzzy attribute set X is called the antecedent of the fuzzy association rule, and the fuzzy attribute set Y is called the subsequent part of the fuzzy association rule. Similarly, the number of fuzzy attributes in the fuzzy attribute set X is called the length of the fuzzy attribute set X, and the fuzzy attribute set with length k is called the k-fuzzy attribute set. To mine fuzzy association rules, it is also necessary to define fuzzy support and fuzzy trust [21].

3.1. Fuzzy Support of Fuzzy Attribute Set X. For any fuzzy attribute set $X = \{y_1, y_2, \cdots, y_p\}$, the fuzzy support degree of fuzzy attribute set X is $\mathrm{FSup}(X)$:

$$\mathrm{FSup}(X) = \frac{\sum_{j=1}^{n} \bigwedge_{m=1}^{p} t_j(y_m)}{n}. \tag{1}$$

n is the number of records of T and $\sum_{j=1}^{n} \bigwedge_{m=1}^{p} t_j(y_m)$ is the fuzzy support number of fuzzy attribute set X, denoted as $\mathrm{FSupport}(X)$, where $\wedge$ is the "and operation," and for any $a, b \geq 0$, $a \wedge b = \min\{a, b\}$. If $\mathrm{FSup}(X)$ is not less than the minimum support min sup given by the user, then, X is called the fuzzy frequent attribute set.

3.2. Fuzzy Support Degree of Fuzzy Association Rule $X \Rightarrow Y$. The fuzzy support degree of fuzzy association rule $X \Rightarrow Y$ is defined as FSup:

$$\mathrm{FSup}(X) = \frac{\sum_{j=1}^{n} \bigwedge_{m=1}^{p+q} t_j(y_m)}{n}. \tag{2}$$

3.3. Fuzzy Trust Degree of Fuzzy Association Rule $X \Rightarrow Y$. The fuzzy trust degree of fuzzy association rule $X \Rightarrow Y$ is defined as FConf:

$$\mathrm{FConf} = \frac{\mathrm{FSup}}{\mathrm{FSup}(X)}. \tag{3}$$

Similarly, fuzzy association rules also have the following properties:

(1) If the fuzzy attribute set X is a fuzzy frequent attribute set, then, all its nonempty subsets are fuzzy frequent attribute sets

Proof. We set fuzzy frequent attribute set as $X = \{y_1, y_2, \cdots, y_p\}$ and a nonempty subset of fuzzy frequent attribute set X as $Y = \{y_1, \cdots, y_1\}$, $1 < P$. Since the fuzzy attribute set X is a fuzzy frequent attribute set, from the definition of $\mathrm{FSup}(X)$, we know [22]

$$\mathrm{FSup}(X) = \frac{\sum_{j=1}^{n} \bigwedge_{m=1}^{p} t_j(y_m)}{n} \geq \min \mathrm{sup}. \tag{4}$$

□

Since $Y = \{y_1, \cdots, y_1\}$ is a nonempty subset of the fuzzy frequent attribute set X and $1 < P$, the following formula is obtained:

$$\mathrm{FSup}(X) = \frac{\sum_{j=1}^{n} \bigwedge_{m=1}^{l} t_j(y_m)}{n} \geq \mathrm{FSup}(X) = \frac{\sum_{j=1}^{n} \bigwedge_{m=1}^{p} t_j(y_m)}{n} \geq \min \mathrm{sup}. \tag{5}$$

Therefore, $Y = \{y_1, \cdots, y_1\}$, $1 < P$ is also a fuzzy frequent attribute set.

(2) If the fuzzy association rule $i_1 \wedge i_2 \wedge i_3 \Rightarrow i_4$ does not satisfy the minimum trust degree given by the user, then, the fuzzy association rule $i_1 \wedge i_2 \Rightarrow i_3 \wedge i_4$ does not satisfy the minimum trust degree given by the user either

Proof. The following is the method of proof by contradiction. □

If the fuzzy association rule $i_1 \wedge i_2 \Rightarrow i_3 \wedge i_4$ satisfies the minimum trust degree given by the user, it is known from the definition of fuzzy trust degree [23]:

$$\frac{\left(\sum_{j=1}^{n} \bigwedge_{k=1}^{4} t_j(i_k)\right)/n}{\left(\sum_{j=1}^{n} \bigwedge_{k=1}^{2} t_j(i_k)\right)/n} \geq \min \mathrm{conf}, \tag{6}$$

because

$$\frac{\sum_{j=1}^{n} \bigwedge_{k=1}^{3} t_j(i_k)}{n} \leq \frac{\sum_{j=1}^{n} \bigwedge_{k=1}^{2} t_j(i_k)}{n}. \tag{7}$$

We can get

$$\frac{\left(\sum_{j=1}^{n} \bigwedge_{k=1}^{4} t_j(i_k)\right)/n}{\left(\sum_{j=1}^{n} \bigwedge_{k=1}^{3} t_j(i_k)\right)/n} \geq \frac{\left(\sum_{j=1}^{n} \bigwedge_{k=1}^{4} t_j(i_k)\right)/n}{\left(\sum_{j=1}^{n} \bigwedge_{k=1}^{2} t_j(i_k)\right)/n} \geq \min \mathrm{conf}. \tag{8}$$

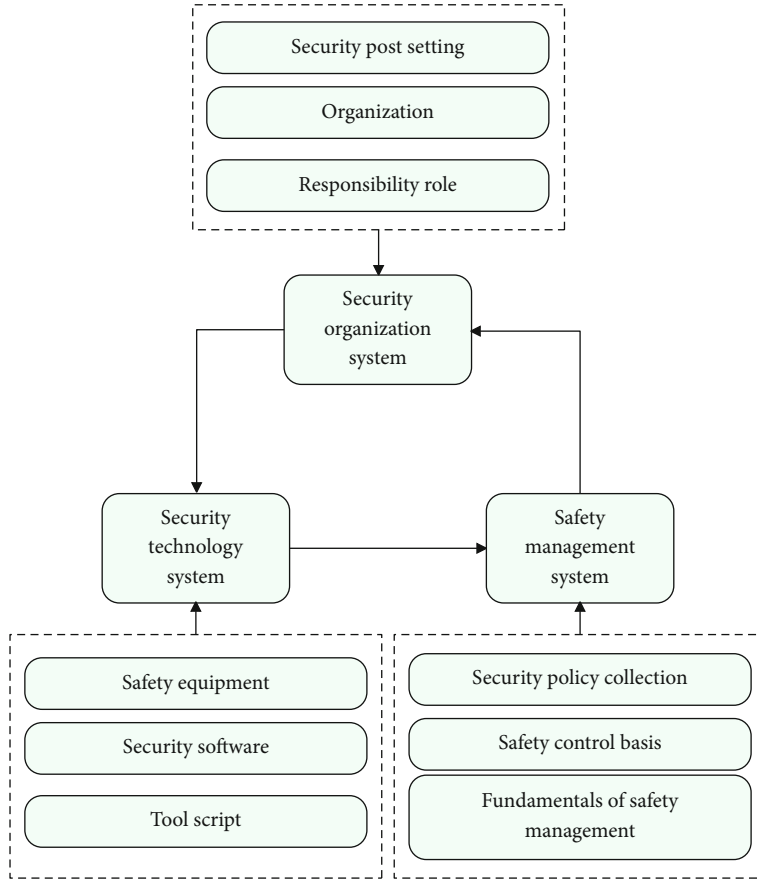

Figure 1: The composition of the security information system.

Therefore, the fuzzy association rule $i_1 \wedge i_2 \wedge i_3 \Rightarrow i_4$ also satisfies the minimum degree of trust given by the user, which contradicts the propositional conditions.

Similar to Boolean association rules, the mining of fuzzy association rules is to generate all association rules that meet the minimum support (min sup) and minimum confidence (min conf) given by the user. That is, the support and trust of these association rules are not less than the minimum support and the minimum trust, respectively. The mining algorithm can also be divided into two steps:

(1) The algorithm finds all fuzzy frequent attribute sets, that is, all fuzzy attribute sets that are not less than the minimum support given by the user

(2) The algorithm generates fuzzy association rules not less than the minimum trust degree given by the user from all the fuzzy frequent attribute sets. The method of generation is as follows: for any fuzzy frequent attribute set X and any fuzzy attribute set $Y \subset X$, if $\text{FSupport}(X)/\text{FSupport}(Y) \geq \min \text{conf}$, then, the fuzzy association rule $Y \Rightarrow X - Y$ is a meaningful rule

Like the classic Apriori algorithm, the fuzzy association rule mining algorithm described in the previous section will also encounter time complexity and space complexity bottlenecks:

On the one hand, the database must be scanned once for judging the fuzzy candidate attribute set C_k in each cycle. After the fuzzy set level is divided, the records in the database will become more verbose and huge, and the load I/O and time consumption brought by multiple scans of the database will be more obvious [24].

On the other hand, after the fuzzy set level is divided, the original quantitative attributes are converted into fuzzy attributes, and the number of fuzzy attributes will generally be 3-10 times of the original quantitative attributes. This results in the generation of fuzzy frequent attribute sets that are several times larger than the original, which will generate a huge number of fuzzy candidate attribute sets and consume a lot of storage space in the subsequent loop.

In the traditional association rule mining algorithm, we have mentioned that the 0-1 matrix algorithm is used to mine frequent item sets. In this way, in the entire mining process, only one scan of the database is required, which reduces a large amount of I/O consumption and improves the mining efficiency. We can also extend the idea of the matrix to the mining of fuzzy association rules and obtain the set of fuzzy frequent attributes by constructing the matrix.

If X and Y are two universes, then, the fuzzy relation R from X to Y (or between X and Y) is a fuzzy set on the direct product $X \times Y = \{(x, y) | x \in X, y \in Y\}$, namely, $R \in F(X \times Y)$.

$$R : X \times Y \longrightarrow [0, 1]. \tag{9}$$

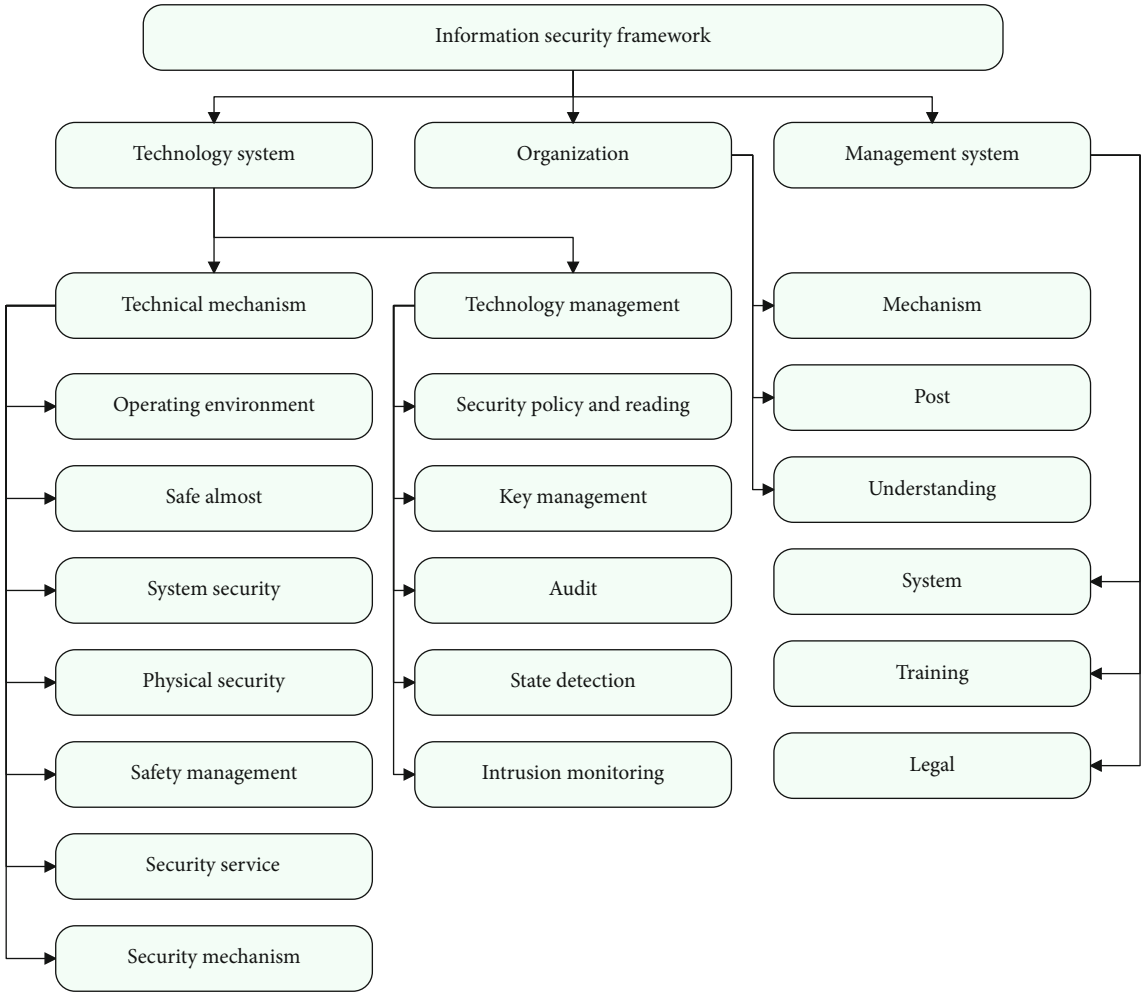

Figure 2: Schematic diagram of the information security system framework.

$R(x, y)$ represents the degree to which x and y have an R relationship. In particular, when $X = Y$, R is called the fuzzy relationship on X.

For $x \in X, y \in Y$, $R(x, y)$ characterizes the degree of correlation between x and y. If R is restricted to the classic set on $X \times Y$, then, R becomes an ordinary relationship at this time, so the fuzzy relationship is a generalization of the classic relationship. Fuzzy relations are fuzzy sets, so the signs of fuzzy sets are also applicable to fuzzy relations.

For example, $X = \{x_1, x_2, x_3\}$ represents the set of three people x_1, x_2, x_3 in the parent's generation, and $Y = \{y_1, y_2, y_3, y_4\}$ is the children set x_1, x_2, x_3; the "similar relationship" $R \in F(X \times Y)$ is a fuzzy relationship, and

$$R = \frac{0.6}{(x_1, y_1)} + \frac{0.3}{(x_1, y_2)} + \frac{0.3}{(x_2, y_1)} + \frac{0.8}{(x_2, y_2)} + \frac{0.7}{(x_3, y_3)} + \frac{0.2}{(x_3, y_4)}. \tag{10}$$

$R_{ij} = R(x_i, y_j), (i = 1, 2, 3\,; j = 1, 2, 3, 4)$ represents the "similar degree" of x_i to y_j, and the items that are not written indicate that the degree of similarity is 0; that is, it is basically not similar.

As a generalization of the fuzzy relationship, the n-ary fuzzy relationship R on $X_1 \times X_2 \times \cdots \times X_n$ is

$$\int_{X_1 \times X_2 \times \cdots \times X_n} \frac{R(x_1, x_2, \cdots, x_n)}{(x_1, x_2, \cdots, x_n)}, \quad x_i \in X_i. \tag{11}$$

Among them, $R : X_1 \times X_2 \times \cdots \times X_n \longrightarrow [0, 1]$. When $n = 1$, R is a unary fuzzy relation, that is, the fuzzy set on X_1. When $n = 2$, R is a binary fuzzy set, that is, the fuzzy set on $X_1 \times X_2$, which is the most discussed fuzzy relationship.

The following are some of the main basic fuzzy relations, for arbitrary $x, y \in X$.

The identity relationship I is

$$I(x, y) = \begin{cases} 1, & x = y, \\ 0, & x \neq y. \end{cases} \tag{12}$$

The zero relationship O is

$$O(x, y) = 0. \tag{13}$$

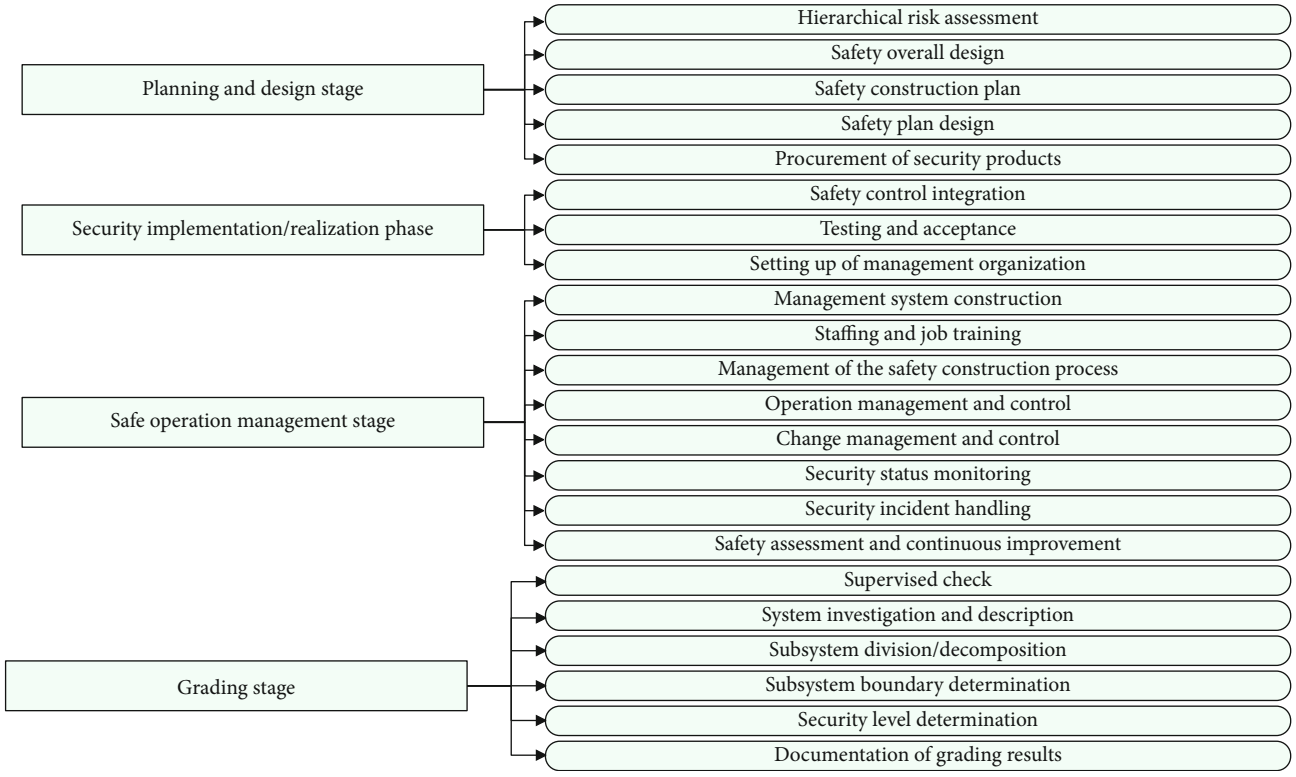

Figure 3: Schematic diagram of the life cycle of information security grade protection.

The full relationship E is

$$E(x, y) = 1. \tag{14}$$

If it is assumed that $X = \{x_1, x_2, \cdots, x_m\}$ and $Y = \{y_1, y_2, \cdots, y_n\}$ are finite sets, the fuzzy relationship R on $X \times Y$ can be represented by a matrix of $m * n$ order:

$$R = \begin{bmatrix} R(x_1, y_1) & R(x_1, y_2) & \cdots & R(x_1, y_n) \\ R(x_2, y_1) & R(x_2, y_2) & \cdots & R(x_2, y_n) \\ \cdots & \cdots & \cdots & \cdots \\ R(x_m, y_1) & R(x_m, y_2) & \cdots & R(x_m, y_n) \end{bmatrix}. \tag{15}$$

This kind of matrix that represents the fuzzy relationship is called the fuzzy matrix, which is abbreviated as

$$R = \left[r_{ij}\right]_{m*n}. \tag{16}$$

Among them,

$$r_{ij} = R\left(x_i, y_j\right). \tag{17}$$

Because R takes a value on $[0, 1]$, the elements of the fuzzy matrix are $r_{ij} \in [0, 1]$. If $r_{ij} \in \{0, 1\}$, then, R is a Boolean matrix.

$$\text{Weight (kg)} = \text{height (cm)} - 100. \tag{18}$$

If $X = \{140, 150, 160, 170, 180\}$, $Y = \{40, 50, 60, 70, 80\}$, then, the above equation can get a Boolean relationship R, which is represented by a Boolean matrix as

$$R = \begin{array}{c} \\ 140 \\ 150 \\ 160 \\ 170 \\ 180 \end{array} \begin{array}{c} \begin{array}{ccccc} 40 & 50 & 60 & 70 & 80 \end{array} \\ \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \end{array}. \tag{19}$$

However, for "nonstandard" situations, the degree to which they are close to the standard should be described. In this way, the fuzzy relationship represented by the fuzzy matrix below clearly gives a more comprehensive standard relationship.

$$R = \begin{array}{c} \\ 140 \\ 150 \\ 160 \\ 170 \\ 180 \end{array} \begin{array}{c} \begin{array}{ccccc} 40 & 50 & 60 & 70 & 80 \end{array} \\ \begin{bmatrix} 1 & 0.8 & 0.2 & 0.1 & 0 \\ 0.8 & 1 & 0.8 & 0.2 & 0.1 \\ 0.2 & 0.8 & 1 & 0.80 & 0.2 \\ 0.1 & 0.2 & 0.8 & 1 & 0.8 \\ 0 & 0.1 & 0.2 & 0.8 & 1 \end{bmatrix} \end{array}. \tag{20}$$

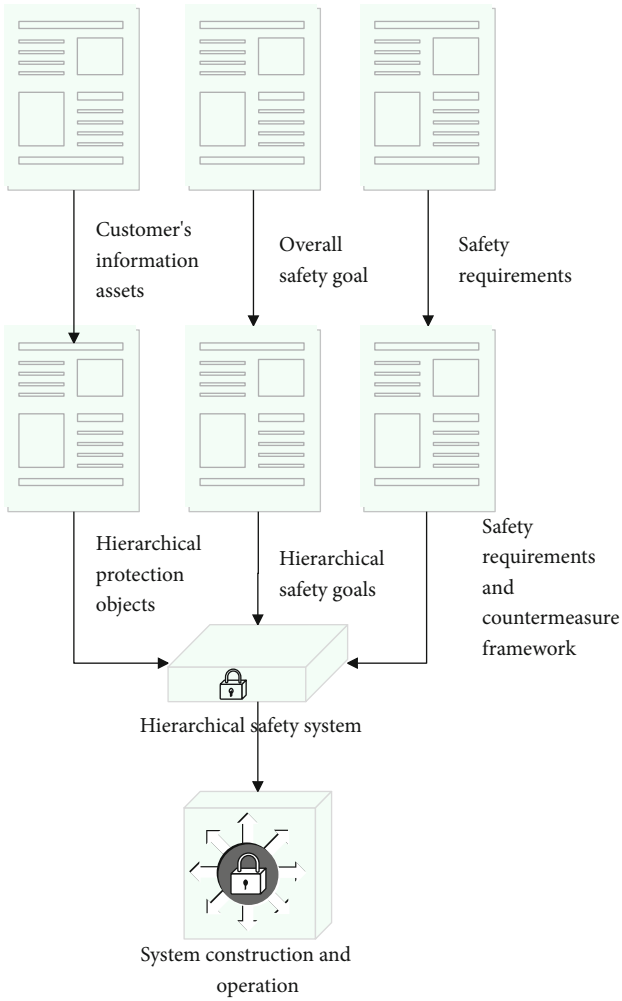

Figure 4: Schematic diagram of the design method of the information security grade protection system.

4. Information Security Risk Assessment System Based on Fuzzy Rule Set

The information system security system is jointly constructed by the three systems of security technology, security management, and security organization, as shown in Figure 1.

The information security system framework is shown in Figure 2.

Once the safety technology system determines the safety requirements, appropriate control measures should be selected and implemented to ensure that the risk is reduced to an acceptable level. An important aspect of control measures is technical control measures. In addition, a technical measure often does not play its role in information security in isolation. It needs to work with other technical measures and nontechnical measures. In this way, a technical architecture is needed to integrate and integrate these security control measures.

(1) Hardware security technology: buildings, computer rooms, and hardware meet mechanical protection requirements.

(2) System security technology: through a series of measures, the safety level was met.

The security organization system ensures that information security in an organization is implemented through the definition of various security responsibilities and provides support for the organization's security management, safe operation and maintenance, and security technology. There are three levels: decision-making level, management level, and executive level.

The safety management system and process are placed in the safety management framework. The safety management framework provides the basis for the management of risks of the system, establishes trust, and defines all safety management elements, methods, objects, rules, processes, etc., as shown in Figure 3. The information system security management system consists of three parts: law, system, and training.

The design method of the information security grade protection system is shown in Figure 4.

Network information security technology is a comprehensive discipline involving multiple technologies such as computers, networks, communications, cryptography, and

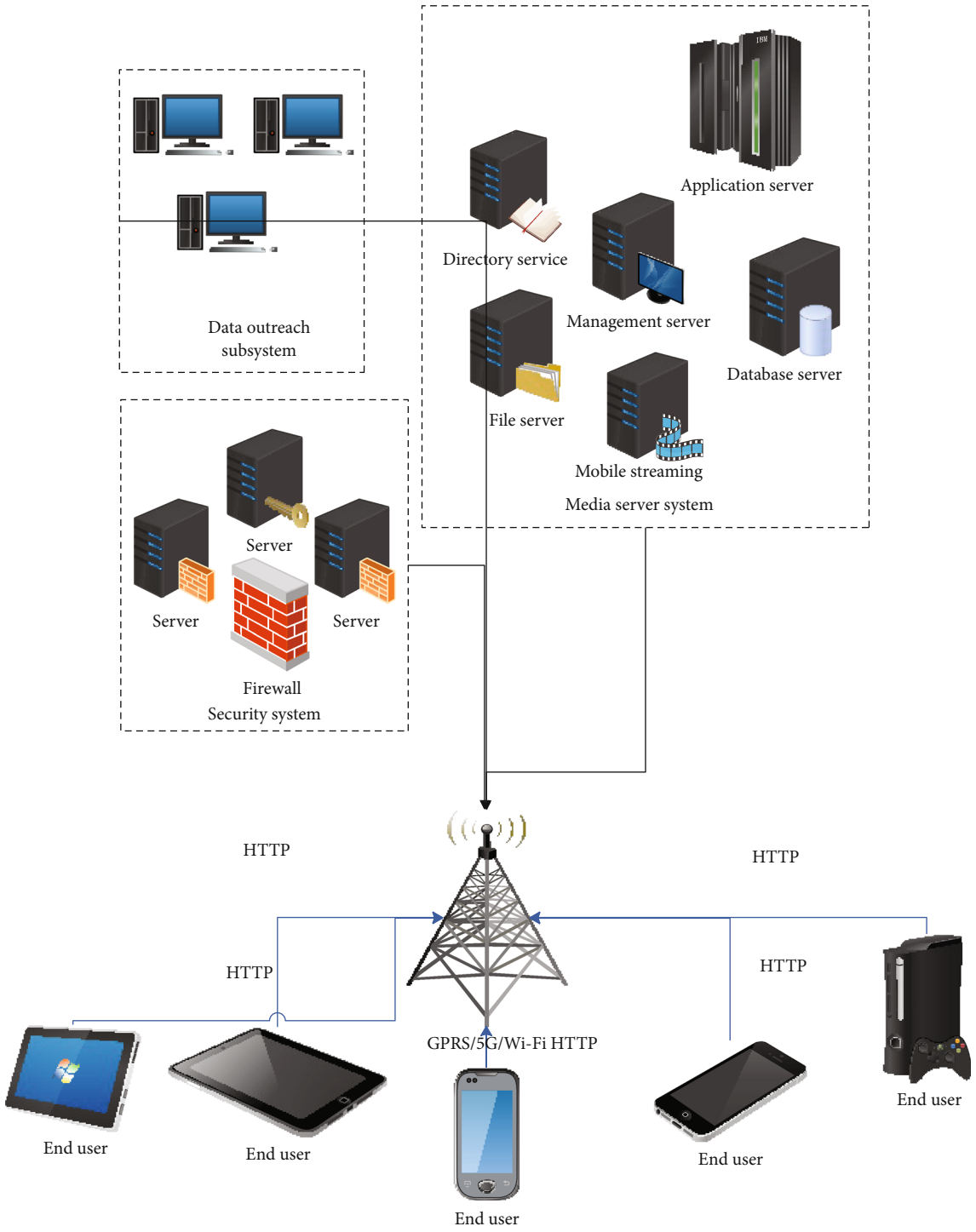

Figure 5: Schematic diagram of the network security domain of the platform.

information theory. With the continuous development of informatization applications, the connotation of security continues to extend, in terms of confidentiality, integrity, and availability. The characteristics of identity authenticity, system controllability, behavior reviewability, etc. are derived. At present, with the continuous emergence of new technologies and diversified applications such as cloud computing, mobile Internet, and big data, network information security technologies are developing in the direction of integration, intelligence, unity, precision, and initiative. Equipment functions such as firewalls and intrusion protection, as well as network equipment and security functions continue to integrate, penetrate into the virtualized environment; unified authentication, unified risk management control, and unified terminal security management have become a trend, and security protection trends such as access control, malicious code, and abnormal traffic have become trends. The development of multilevel protection

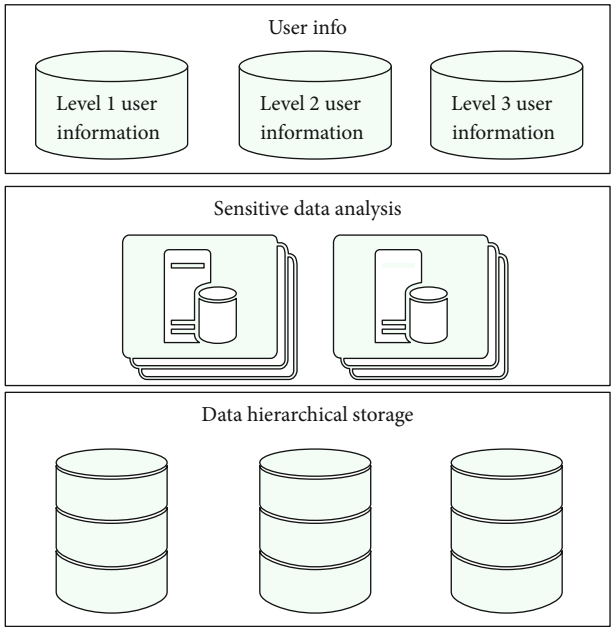

Figure 6: Discovery and classification of sensitive data.

and seven-level full protection, identity authentication technology based on situational awareness, and active security audit technology for APT has received full attention from the industry. With the continuous improvement of the performance of network equipment and application systems and the increasing importance of security, the application of high-performance security infrastructure, such as DNSsec and RPKI, is on the agenda. In addition, the protection of sensitive information and personal privacy has been heatedly discussed, and related technologies have developed rapidly.

The data collection subdomain can be divided into telecommunications internal data collection and external data collection; the data ETL subdomain is the area where data caching, data cleaning, data desensitization, data distribution, and other equipment are located; the data computing storage subdomain is data distributed storage and classification storage, distributed computing, capability component packaging, and other equipment areas; data outreach subdomains are areas where Web servers and other equipment are located, responsible for unified access to external network systems; management subdomains are business management platforms, security audits, network monitoring, etc. That is the area where the device such as event log is located. At the boundary of each area, different strengths of logical isolation protection are implemented through measures such as dividing VLANs, setting routing policies and switch access control lists, and deploying firewalls.

The target architecture of the network security domain of the big data platform is shown in Figure 5.

In order to finely manage the user's personal information, according to the sensitivity of the user's information, it is divided into three levels: low, medium, and high. The specific definition is as follows: 4slow-level user information is mainly information about the user's consumption, business, and cooperation; intermediate user information mainly refers to information related to the user's specific identity, such as user name, phone number, home address, ID number, and bank card number information; advanced user information mainly refers to the information of the user's specific communication content, such as the user's detailed call bill (real-time), geographic location information, and user account password. For the data in the database, it is necessary to identify which information is sensitive. For the identified sensitive data, it is necessary not only to classify and encrypt the storage but also to track the whereabouts of sensitive information, such as which users downloaded the sensitive data and control the download cycle of sensitive data. In particular, high-level and intermediate-level user information must be desensitized. The protection of sensitive data is realized by recording the method of assigning data tags and transparent access to the table (based on the built-in algorithm). Figure 6 shows the discovery and classification of sensitive data.

The platform monitors the network data stream in real time by using the network intrusion detection system, identifies and records abnormal and destructive code streams,

Table 1: Statistical table of risk identification of network information data.

Num	Risk identification	Num	Risk identification	Num	Risk identification
1	90.71	28	90.53	55	86.53
2	89.35	29	83.05	56	82.75
3	80.25	30	91.81	57	83.05
4	90.87	31	82.99	58	81.80
5	83.18	32	83.60	59	80.43
6	84.49	33	91.24	60	87.83
7	89.47	34	91.33	61	80.71
8	88.19	35	90.58	62	89.25
9	89.40	36	89.93	63	88.70
10	80.11	37	79.88	64	80.83
11	81.28	38	85.00	65	86.31
12	84.94	39	90.47	66	89.79
13	87.05	40	89.70	67	84.15
14	91.04	41	90.75	68	83.27
15	83.58	42	88.39	69	82.59
16	91.91	43	85.94	70	82.34
17	88.11	44	85.42	71	87.50
18	88.54	45	86.88	72	91.14
19	84.83	46	90.53	73	80.95
20	87.50	47	90.88	74	79.46
21	80.19	48	87.11	75	83.96
22	84.98	49	86.10	76	86.19
23	88.84	50	83.13	77	85.10
24	83.18	51	90.38	78	84.77
25	79.00	52	89.66	79	87.19
26	91.79	53	81.86	80	80.92
27	84.17	54	82.28		

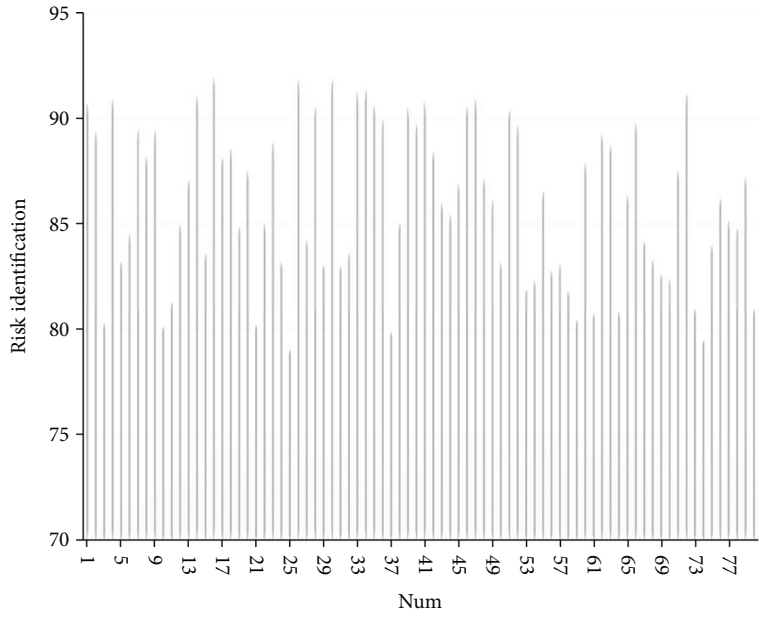

Figure 7: Statistical diagram of risk identification of network information data.

analyzes and audits the information, and discovers abnormal events in time. For abnormal network data, suspicious network connections, dangerous events that should not occur, network worms, or viruses, the platform needs to respond, alarm, and record in a timely manner and can issue security warning notifications in the system across the entire network and accurately locate the source of the event, so as to solve the problem at the source of the event in time. In the deployment plan, this plan deploys a set of network intrusion detection system IDS deployed on the core switch, adopts dual-port monitoring mode, bridges two core switches, and performs real-time detection of data passing through the core switch. At the same time, a security comprehensive audit device is added to the security management domain to perform unified log audit management on IDS. It is necessary to ensure the normal communication between the management server and IDS.

5. System Performance Verification

After constructing the system structure model, verify the performance of the model structure. This paper uses fuzzy rule set combined with an embedded system to verify system performance. This paper collects various information threat-related information through the network and, on this basis, obtains a data set, which has 80 groups. We use the system constructed in this paper to identify the risks of these 80 sets of data and score the risks. The results are shown in Table 1 and Figure 7.

From the analysis results of the above figure and table, we can see that the risk identification system constructed in this paper has a certain good performance in risk identification. On this basis, the system's risk response effect is evaluated, and the results are shown in Table 2 and Figure 8.

Table 2: Statistical table of risk response effect.

Num	Risk response	Num	Risk response	Num	Risk response
1	76.18	28	83.64	55	80.04
2	81.22	29	82.19	56	68.60
3	73.25	30	68.27	57	74.82
4	78.20	31	84.22	58	71.29
5	83.31	32	78.11	59	77.89
6	79.18	33	73.54	60	73.99
7	83.35	34	72.12	61	81.63
8	69.29	35	81.03	62	84.27
9	68.53	36	83.15	63	79.09
10	75.56	37	81.67	64	70.98
11	83.31	38	72.21	65	68.57
12	72.76	39	73.99	66	71.61
13	76.26	40	79.90	67	76.41
14	77.64	41	84.36	68	79.54
15	69.47	42	73.62	69	80.95
16	77.78	43	77.77	70	81.50
17	82.74	44	84.50	71	83.67
18	84.11	45	79.11	72	80.46
19	78.00	46	77.99	73	84.11
20	85.11	47	85.40	74	81.31
21	83.64	48	75.01	75	81.50
22	74.68	49	73.78	76	75.93
23	84.05	50	84.41	77	85.56
24	79.85	51	81.91	78	82.05
25	81.23	52	78.07	79	69.54
26	83.46	53	69.35	80	72.36
27	83.03	54	81.34		

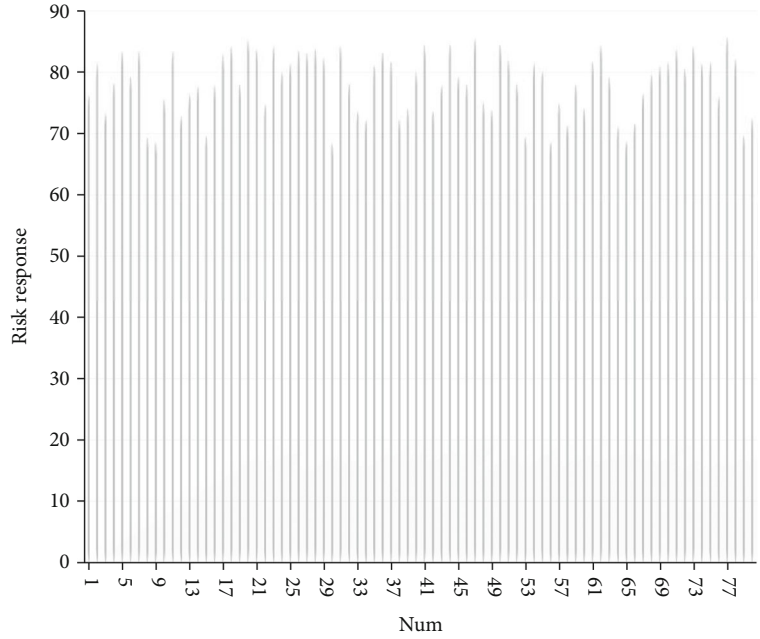

Figure 8: Statistical diagram of risk response effect.

From the above figure and table analysis, we can see that the information security risk assessment method based on fuzzy rules constructed in this paper has certain effects.

6. Conclusion

With the continuous deepening of informatization construction, the information system, as an important carrier of social informatization, has changed our lifestyle and promoted the development of social productivity. However, an endless stream of security incidents restricts the further development of information systems. Therefore, how to ensure the safe operation of information systems and avoid potential security risks has become the focus and hotspot of current research. As an important part of information system security engineering, information security risk assessment is the prerequisite and foundation for building an information system security system. However, the existing evaluation methods have many limitations, such as high complexity, excessive subjectivity, and lack of operability. This article combines fuzzy rule set to carry out information security risk assessment, combined with the actual situation to construct an information security risk assessment system, and verify the system performance through experiments. The research results show that the system constructed in this paper has a certain effect in information security assessment.

Data Availability

Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

Conflicts of Interest

We declare that there is no conflict of interest.

Acknowledgments

This work in this article was supported by Southeast University.

References

[1] A. Blagorazumov, P. Chernikov, G. Glukhov, A. Karapetyan, V. Shapkin, and L. Elisov, "The background to the development of the information system for aviation security oversight in Russia," *International Journal of Mechanical Engineering and Technology (IJMET)*, vol. 9, no. 11, pp. 341–350, 2018.

[2] S. Chatterjee, A. K. Kar, and M. P. Gupta, "Alignment of IT authority and citizens of proposed smart cities in India: system security and privacy perspective," *Global Journal of Flexible Systems Management*, vol. 19, no. 1, pp. 95–107, 2018.

[3] S. E. Choi, J. T. Martins, and I. Bernik, "Information security: listening to the perspective of organisational insiders," *Journal of Information Science*, vol. 44, no. 6, pp. 752–767, 2018.

[4] K. K. R. Choo, M. M. Kermani, R. Azarderakhsh, and M. Govindarasu, "Emerging embedded and cyber physical system security challenges and innovations," *IEEE Transactions on Dependable and Secure Computing*, vol. 14, no. 3, pp. 235-236, 2017.

[5] Bentley University, W. A. Cram, J. D'Arcy, University of Delaware, J. G. Proudfoot, and Bentley University, "Seeing the forest and the trees: a meta-analysis of the antecedents to information security policy compliance," *MIS Quarterly*, vol. 43, no. 2, pp. 525–554, 2019.

[6] S. Dotsenko, O. Illiashenko, S. Kamenskyi, and V. Kharchenko, "Integrated security management system for enterprises in

Industry 4.0," *Information & Security: An International Journal*, vol. 43, no. 3, pp. 294–304, 2019.

[7] S. U. Hani and A. T. Alam, "Software development for information system-achieving optimum quality with security," *International Journal of Information System Modeling and Design*, vol. 8, no. 4, pp. 1–20, 2017.

[8] K. Hwang and M. Choi, "Effects of innovation-supportive culture and organizational citizenship behavior on e-government information system security stemming from mimetic isomorphism," *Government Information Quarterly*, vol. 34, no. 2, pp. 183–198, 2017.

[9] K. Kavitha and R. Neela, "Optimal allocation of multi-type FACTS devices and its effect in enhancing system security using BBO, WIPSO & PSO," *Journal of Electrical Systems and Information Technology*, vol. 5, no. 3, pp. 777–793, 2018.

[10] H. U. Khan and K. A. AlShare, "Violators versus non-violators of information security measures in organizations—a study of distinguishing factors," *Journal of Organizational Computing and Electronic Commerce*, vol. 29, no. 1, pp. 4–23, 2019.

[11] N. Y. Kim, S. Rathore, J. H. Ryu, J. H. Park, and J. H. Park, "A survey on cyber physical system security for IoT: issues, challenges, threats, solutions," *Journal of Information Processing Systems*, vol. 14, no. 6, pp. 1361–1384, 2018.

[12] B. Y. Korniyenko and L. P. Galata, "Design and research of mathematical model for information security system in computer network," *Наукоємні технології*, vol. 2, pp. 114–118, 2017.

[13] V. H. Le, V. O. Phung, and N. H. Nguyen, "Information security risk management by a holistic approach: a case study for Vietnamese e-Government," *IJCSNS International Journal of Computer Science and Network Security*, vol. 20, no. 6, pp. 72–82, 2020.

[14] D. Li, Z. Cai, L. Deng, X. Yao, and H. H. Wang, "Information security model of block chain based on intrusion sensing in the IoT environment," *Cluster Computing*, vol. 22, no. S1, pp. 451–468, 2019.

[15] A. B. Lopez, K. Vatanparvar, A. P. Deb Nath, S. Yang, S. Bhunia, and M. A. al Faruque, "A security perspective on battery systems of the Internet of Things," *Journal of Hardware and Systems Security*, vol. 1, no. 2, pp. 188–199, 2017.

[16] P. B. Lowry, T. Dinev, and R. Willison, "Why security and privacy research lies at the centre of the information systems (IS) artefact: proposing a bold research agenda," *European Journal of Information Systems*, vol. 26, no. 6, pp. 546–563, 2017.

[17] N. Mayer, J. Aubert, E. Grandry, C. Feltus, E. Goettelmann, and R. Wieringa, "An integrated conceptual model for information system security risk management supported by enterprise architecture management," *Software & Systems Modeling*, vol. 18, no. 3, pp. 2285–2312, 2019.

[18] O. Na, L. W. Park, H. Yu, Y. Kim, and H. Chang, "The rating model of corporate information for economic security activities," *Security Journal*, vol. 32, no. 4, pp. 435–456, 2019.

[19] M. K. Özlen and I. Djedovic, "Online banking acceptance: the influence of perceived system security on perceived system quality," *Journal of Accounting and Management Information Systems*, vol. 16, no. 1, pp. 164–178, 2017.

[20] M. Rajesh, "A signature based information security system for vitality proficient information accumulation in wireless sensor systems," *International Journal of Pure and Applied Mathematics*, vol. 118, no. 9, pp. 367–387, 2018.

[21] A. Safi, "Improving the security of internet of things using encryption algorithms," *International Journal of Computer and Information Engineering*, vol. 11, no. 5, pp. 558–561, 2017.

[22] M. Sun, I. Konstantelos, and G. Strbac, "A deep learning-based feature extraction framework for system security assessment," *IEEE Transactions on Smart Grid*, vol. 10, no. 5, pp. 5007–5020, 2019.

[23] S. Trang and B. Brendel, "A meta-analysis of deterrence theory in information security policy compliance research," *Information Systems Frontiers*, vol. 21, no. 6, pp. 1265–1284, 2019.

[24] Z. Turskis, N. Goranin, A. Nurusheva, and S. Boranbayev, "Information security risk assessment in critical infrastructure: a hybrid MCDM approach," *Informatica*, vol. 30, no. 1, pp. 187–211, 2019.