Research on information system risk Assessment Based on Improved AHP-Fuzzy theory

Liu Peisheng, Han Yunping, Zhu Xiaole, Wang Shunshun, Li Zhenglin

School of Computer and Communication Engineering, Liaoning Shihua University, Fushun, Liaoning, 113001, China

Abstract. Aiming at the problem of security of information systems, a security risk assessment model based on improved AHP-fuzzy theory is proposed. First, the evaluation index system is constructed by using the Delphi method. Second, the improved AHP method is used to calculate the weight of the index system. On this basis, the multilevel fuzzy comprehensive evaluation model is constructed for risk assessment. Finally, taking an OA system in a university as an example, the empirical analysis is carried out. The result shows that the method proposed in this paper is accurate, effective and time-saving. The study will provide a new method for a risk assessment of information systems.

1. Introduction

With the rapid development of information technology, the issue of information security has attracted considerable attention. Once the information system is exposed to security risks, it will cause huge losses to the users. Therefore, enterprises and government departments attach great importance to the security of their information systems and vigorously increase all-round investment to ensure that information risks are minimized [1]. Some government departments strengthen the construction of information security. The Guidelines for the Classification of Computer Information System Security Protection Levels are formulated by the Ministry of Public Security of China [2]. How to evaluate the information system security risk the most important issue that needs to be studied.

In recent years, domestic and foreign scholars mainly focus on the study of information systems security risks in two aspects. Zou Guoliang [3], selected the information security assessment indicators of the marine network. Guo Ning [4] briefly introduced the system of information security risk assessment indicators. On the other hand, a lot of information security assessment models, such as VaR-Copula model [5], game theory model and analytic hierarchy process model [6] were proposed to investigate the security risks. However, these models are all single information security assessment models, while the combined model has higher accuracy than a single model. Therefore, the information security risk assessment combination model, such as fuzzy neural network model, fuzzy gray model [7], fuzzy wavelet neural network model, network analysis and evidence theory model [8], game theory and comprehensive weighting model has been further developed. In recent years, the application of AHP model and fuzzy comprehensive evaluation model in information security risk assessment has been widely developed [9-11]. But the subjective factors of experts in the AHP expert scoring influence the judgment results. Moreover, the nine-scale method is used to construct the comparison matrix, and the consistency check is required. In this case, the calculation is cumbersome, and inefficient.

This paper attempts to establish an information security risk assessment model based on improved AHP and fuzzy theory. First of all, the new three-scale method is proposed as a substitute of the
nine-scale method adopted in order to avoid the influence of the subjective factors of experts on the judgment results. On this basis, the step of the consistency checking is omitted by using the optimal transfer matrix to construct the comparison matrix, and the calculation process is simplified. Secondly, we combine fuzzy comprehensive evaluation to quantify some factors of information security risk assessment which are ambiguous. Finally, a detailed study of a university OA is used to verify whether the proposed model is effective. The results show that the model based on the improved AHP and fuzzy theory presented is valid and consistent with the reality, and the calculation process is simpler than the traditional AHP.

2. Basic theory

2.1 Improved AHP

The Analytic Hierarchy Process (AHP) is a decision-making method proposed by Saaty et al. in the 1970s [12]. This method hierarchically influences the various factors of decision-making and compares them from the bottom level to the top level. In recent years, AHP has been well developed in determining weights. The specific calculation process is shown in Figure 1.

![Fig.1 AHP flow chart](image)

For the influence of the subjective factors of the experts in the traditional AHP expert scoring on the judgment results, the nine-scale method adopted by the traditional AHP is changed to the three-scale method. On this basis, the optimal transfer matrix is used so that it can eliminate the need to check the consistency of the comparison matrix. Moreover, it is not necessary to repeatedly adjust the comparison matrix to simplify the calculation process. Basic steps of the improved AHP are mentioned below.

Step 1: Construct a pairwise comparison matrix \( A \). Make a pairwise comparison using the three-scale method, and grade them according to their importance determined by the experts, then the pairwise comparison matrix \( A \) is given:

\[
A = \begin{pmatrix}
    a_{11} & a_{12} & \cdots & a_{1n} \\
    a_{21} & a_{22} & \cdots & a_{2n} \\
    \cdots & \cdots & \cdots & \cdots \\
    a_{n1} & a_{n1} & \cdots & a_{nn}
\end{pmatrix}
\]

where \( a_{ij} = \begin{cases} 
2 & \text{The factor } i \text{ is more important than the factor } j \\
1 & \text{The factor } i \text{ is as important as the factor } j \\
0 & \text{The factor } i \text{ is less important than the factor } j 
\end{cases} \) .

and we fixed \( a_{ii} = 1 \).

Step 2: Calculate the important ranking index \( r_i \):

\[
r_i = \sum_{j=1}^{n} a_{ij}.
\]

Step 3: Construct a judgment matrix \( B \):
Step 4: Solving the above judgment matrix $B$, the transfer matrix $C$ is obtained, and its element $c_{ij}$ is:
\[ c_{ij} = \log b_{ij}, \]  
(4)
where $i,j=1,2,...n$.

Step 5: Solve the transfer matrix $C$ to get the optimal transfer matrix $D$, whose elements $d_{ij}$ is:
\[ d_{ij} = 1/n \sum_{k=1}^{n} (c_{ik} - c_{kj}), \]  
(5)
where the number of rows or columns of the comparison matrix is represented by $n$; the number of columns of the comparison matrix is represented by $k$.

Step 6: Find the quasi-optimal consistency matrix $B'$ of the judgment matrix $B$, and its element $b'_{ij}$ is:
\[ b'_{ij} = 10^{d_{ij}}. \]  
(6)

Step 7: Calculate the eigenvector of the matrix $B'$. The element product of each row of $B'$ is given:
\[ M_i = \prod_{j=1}^{n} b'_{ij}, \]  
(7)
Calculate the square root:
\[ \bar{W}_i = \sqrt[M_i]{M_i}, \]  
(8)
Normalize the vector $\bar{W} = (\bar{W}_1, \bar{W}_2, \cdots, \bar{W}_n)^T$:
\[ W_i = \bar{W}_i / \sum_{i=1}^{n} \bar{W}_i, \]  
(9)
Therefore, the result of hierarchical single ranking is given: $W = (W_1, W_2, \cdots, W_n)^T$.

The improved AHP is to pass the judgment matrix judged by the experts, so as to obtain a matrix that is consistent in the quasi-optimal sense, which does not need to carry out the consistency test, but also saves the time to adjust the judgment matrix and avoid blindly adjusting the judgment matrix.

2.2 Multi-level fuzzy comprehensive evaluation [13]
The multiple indicators related to the evaluation object’s score are called the evaluation indicator set $U = \{U_1, U_2, \cdots, U_m\}$. The characteristic of each indicator contained in the set is fuzziness. The evaluation results of experts on each indicator compose of the fuzzy comment set $V = \{v_1, v_2, \cdots, v_n\}$.

Since the indicators have different influences on the evaluation results, the weight of each indicator $a_i(t = 1, 2, \cdots, m)$ is calculated, and the weighted set $A = \{a_1, a_2, \cdots, a_m\}$ is established. In order to determine the weight of each indicator more reasonable, the improved AHP is used to calculate the weight.

In the evaluation, only one of the factors was evaluated separately, and the degree of membership was determined. The evaluation object corresponds to the evaluation set. This method is a single factor fuzzy evaluation. $r_{ij}$ represents the membership degree of the $i$ indicator in $U_t$ belonging to the $j$
in $V_j$. The result can be represented by a fuzzy set:

$$R_i = \{r_{i1}, r_{i2}, \cdots, r_{in}\} (i = 1, 2, \cdots, n),$$

where $R_i$ is a single factor evaluation set.

The single factor evaluation judgement matrix is expressed. Since the weights of factors in the risk assessment of information security are not necessarily equal, fuzzy matrix operations need to be performed. $B$ is the conclusion vector:

$$B_i = W_{U_i} \otimes R_i (i = 1, 2, \cdots, n)$$

(10)

where $\otimes$ is some kind of synthesis operation.

Finally, the multi-level fuzzy comprehensive evaluation is carried out. The multi-level fuzzy matrix is composed of each single-factor evaluation result, and perform fuzzy synthesis to construct an evaluation model:

$$C = W_U \otimes B$$

(11)

where $\otimes$ is adopted for the synthesis operation.

3. **Empirical analysis**

Taking an OA information system in a university as an example, the evaluation and model proposed in this paper are used to evaluate the security of the information system.

The information system security risk assessment index system is specifically shown in Table 1. Due to space limitations, when using the improved AHP to determine the weights of information system risk assessment indicators and criteria layers, five indicators are taken as examples. The process of determining the weights of the remaining indicator level indicators and criterion level indicators is the same as the five indicators under information security. Next, the empirical process of the proposed model is introduced in detail.

| Target layer | Criteria layer | Weights | Indicator layer | Weights |
|--------------|----------------|---------|-----------------|---------|
| Information system security risk (U) | information security (U1) | 0.140 | Identification (U11) | 0.130 |
| | | | Access control (U12) | 0.050 |
| | | | Information encryption (U13) | 0.400 |
| | | | Non-repudiation (U14) | 0.020 |
| | | | Information integrity (U15) | 0.400 |
| | | | Database security (U21) | 0.120 |
| | Software security (U2) | 0.200 | Operating system security (U22) | 0.070 |
| | | | Application software security (U23) | 0.130 |
| | | | Disaster recovery technology (U24) | 0.180 |
| | | | Trojan virus prevention (U25) | 0.200 |
| | | | Patch repair (U26) | 0.150 |
| | | | System log (U27) | 0.150 |
| | Hardware security (U3) | 0.240 | Firewall (U31) | 0.380 |
| | | | Fault tolerant backup (U32) | 0.270 |
| | | | Intrusion detection (U33) | 0.350 |
| | Management security (U4) | 0.170 | Management System (U41) | 0.320 |
| | | | manager (U42) | 0.230 |
| | | | Management agency (U43) | 0.450 |
| | Environment security (U5) | 0.250 | Equipment safety (U51) | 0.480 |
| | | | Physical protection (U52) | 0.250 |
| | | | Safe power supply (U53) | 0.270 |
3.1. Establish the index system

According to the "Practical Rules for Information Security Management" (ISO/IEC 27002) and the General Requirements for Information Technology Security (GJB 5095-2002), information system security mainly includes the following five levels: information, hardware, software, management, and environmental security. The Delphi method is used to decompose these five levels of indicators. The information system security assessment index system was established. The hierarchical model is shown in Table 1. Target layer (A) is an information system security risk. The criteria layer (B) includes five parts: information security, software security, hardware security, management security, and environmental security. The indicator layer (C) includes 21 indicators such as identification, access control, and information encryption.

3.2. Weights calculation using improved AHP

According to the three-scale method and equation (1), the comparison matrix determined by the experts is:

\[
A = \begin{bmatrix}
1 & 2 & 1 & 0 & 1 \\
0 & 1 & 0 & 2 & 2 \\
1 & 2 & 1 & 2 & 0 \\
2 & 0 & 0 & 1 & 2 \\
1 & 2 & 2 & 0 & 1
\end{bmatrix}
\]

The importance ordering index \(r_i\) \((i=1,2,3,4,5)\) according to equation (2) is given:

\[
(r_1, r_2, r_3, r_4, r_5) = (5, 4, 6, 5, 6)
\]

The judgment matrix B is constructed by using equation (3). The transfer matrix C is obtained by using equation (4), and the optimal transfer matrix D is calculated according to equation (5). Construct a quasi-optimal consistent matrix \(B'\) according to equation (6):

\[
B' = \begin{bmatrix}
1 & 1.214 & 0.796 & 1 & 0.796 \\
0.824 & 1 & 0.656 & 0.824 & 0.656 \\
1.256 & 1.525 & 1 & 1.256 & 1 \\
1 & 1.214 & 0.797 & 1 & 0.102 \\
1.256 & 1.525 & 1 & 1.256 & 1
\end{bmatrix}
\]

Calculate the weight of each factor according to equations (7) to (9):

\[
W_{U_1} = (W_{U_{11}}, W_{U_{12}}, W_{U_{13}}, W_{U_{14}}, W_{U_{15}}) = (0.13, 0.05, 0.40, 0.02, 0.40)
\]

Similarly, the weights of other indicator layers and criteria can also be calculated. See Table 1 for details.

3.3. Fuzzy comprehensive evaluation

Set up a influencing factors set \(U=\{U_1, U_2, U_3, U_4, U_5\}\). The influencing factors are divided into five subsets: information security, software security, hardware security, management security, and environmental security. And \(U_1\) is divided into \(U_1=\{U_{11}, U_{12}, U_{13}, U_{14}, U_{15}\}\); \(U_2\) is divided into \(U_2=\{U_{21}, U_{22}, U_{23}, U_{24}, U_{25}, U_{26}, U_{27}\}\); \(U_3\) is divided into \(U_3=\{U_{31}, U_{32}, U_{33}\}\); \(U_4\) is divided into \(U_4=\{U_{41}, U_{42}, U_{43}\}\); \(U_5\) is divided into \(U_5=\{U_{51}, U_{52}, U_{53}\}\).

In evaluating information security risks, the comment set is given as follows:

\[
V = \{\text{lower}(v_1), \text{low}(v_2), \text{medium}(v_3), \text{high}(v_4), \text{great}(v_5)\}
\]

The determination of the weight set of information security risk factors is determined by the improved AHP established above. The specific calculation results are shown in Table 1.

The risk assessment factors affecting information security are divided into five levels. Table 2
provides the details. L1 represents a small risk, L2 represents less risky, L3 represents a moderate risk, L4 represents more risky, L5 represents very risky. The degree of membership of the information system hierarchy can be obtained through the distribution rules of various influencing factors. See Table 3 for details.

Table 2 Levels of Influencing Factors

| The main factor code | main factor                  | level of factors |
|----------------------|------------------------------|-----------------|
| U_{11}               | Identification               | L_2             |
| U_{12}               | Access control               | L_3             |
| U_{13}               | Information encryption       | L_4             |
| U_{14}               | Non-reputation               | L_5             |
| U_{15}               | Information integrity        | L_1             |

Table 3 Degree of membership of each influencing factor

| level of factors | Membership degree vector |
|-----------------|--------------------------|
| L_1             | (1.000, 0.500, 0.250, 0.125, 0.000) |
| L_2             | (0.500, 1.000, 0.500, 0.250, 0.125) |
| L_3             | (0.250, 0.500, 1.000, 0.500, 0.250) |
| L_4             | (0.125, 0.250, 0.500, 1.000, 0.500) |
| L_5             | (0.000, 0.125, 0.250, 0.500, 1.000) |

According to the principle of consistency, after normalization, the membership degree matrix \( R \) of the factor level is obtained as:

\[
R = \begin{bmatrix}
0.533 & 0.267 & 0.133 & 0.068 & 0.000 \\
0.211 & 0.421 & 0.211 & 0.105 & 0.053 \\
0.100 & 0.200 & 0.400 & 0.200 & 0.100 \\
0.053 & 0.105 & 0.211 & 0.421 & 0.211 \\
0.000 & 0.067 & 0.133 & 0.267 & 0.533
\end{bmatrix}
\]

According to formula (10), the single factor evaluation results are as follows:

\[
B_1 = W_{u_1} \ast R = [0.534, 0.349, 0.255, 0.291, 0.123]
\]

In the same way,

\[
B_2 = W_{u_2} \ast R = [0.256, 0.198, 0.153, 0.184, 0.210]
\]

\[
B_3 = W_{u_3} \ast R = [0.243, 0.269, 0.190, 0.206, 0.094]
\]

\[
B_4 = W_{u_4} \ast R = [0.278, 0.299, 0.186, 0.166, 0.072]
\]

\[
B_5 = W_{u_5} \ast R = [0.053, 0.156, 0.153, 0.227, 0.053]
\]

The fuzzy comprehensive evaluation results are as follows:

\[
V = W_{o} \ast B = [0.245, 0.243, 0.182, 0.212, 0.107]
\]

According to the maximum principle, \( V_{i} = [V_{i}]_{\max} = 0.245 \), the probability of a security risk in the example university OA information system is Level I, indicating that the likelihood of a risk is small, and the conclusion is consistent with the actual situation.

4. Conclusion
An information system risk assessment model based on improved AHP-fuzzy theory is proposed in this paper. According to the "Practical Rules for Information Security Management" (ISO/IEC 27002) and the General Requirements for Information Technology Security (GJB 5095-2002), the information system security is divided into five levels, including information security, hardware security, software security, management security, and environmental security. Using Delphi method, the information system risk evaluation index system is constructed. The weight of each index in the index system is
calculated by improved AHP, and some unclear factors are quantified by fuzzy comprehensive evaluation method. No consistency checking is required in our improved AHP, which greatly reduces the impact of subjective factors on information system evaluation results. And the three-scale method is used to replace the traditional nine-scale method, which saves the computing time. The results of empirical analysis show that the model proposed in this research is effective, accurate and time-saving. It provides a new idea for formulating strategies for targeted risk management and control.

Reference

[1] Huang Jingwen. Research on fuzzy group decision-making method for risk analysis of information security [J]. Journal of Shandong University(Natural Science), 2012,47(11):45-49.

[2] Song Jieyu, Zhang Libo. Research on Information Security Risk Assessment Based on Triangular Fuzzy Entropy [J]. Information Studies: Theory & Practice, 2014, 32(1): 110-114.

[3] Zou Guoliang, Jing Yueying, Huang Shili, et al. Index selection and risk assessment of marine network information security evaluation [J]. Computer Applications and Software, 2012, 29(4): 118-121.

[4] Guo Ning. Research on information security risk assessment index system [J]. Information Security, 2006, (5): 17-21.

[5] Lin Zhengkui. Research on information security evaluation model based on VaR-Copula [J]. Mathematics in Practice and Theory, 2012, 42(8): 85-90.

[6] Liu Renshan, Meng Xianghong. Research on information system security evaluation based on analytic hierarchy process [J]. Hebei Industrial Science and Technology, 2013, 30(1):15-19.

[7] Wang Fan, Huo Mingkui, Wang Xiaoting. Security risk assessment and countermeasures of information systems based on fuzzy gray levels [J]. Information Science, 2014, 32(1): 110-114.

[8] Wu Tianshui, Zhao Gang. Information security risk assessment based on network analysis and D-S evidence theory [J]. Computer and Digital Engineering, 2014, 42(10): 1801-1807.

[9] Liu Fang, Peng Yanan, Zhang Weiguo, Pedrycz Witold, On consistency in AHP and fuzzy AHP [J], Journal of Systems Science and Information, 2017, 5(2): 128-147.

[10] Pooja Dehraj, Arun Sharma, An empirical assessment of autonomicity for autonomic query optimizers using fuzzy-AHP technique [J], Applied Soft Computing, 2020, 90: 106137.

[11] Lingyan Zhu, Research and application of AHP-fuzzy comprehensive evaluation model [J], Evolutionary Intelligence, 2020.

[12] Li Rui, Li Yue, Xu Hao, et al. Evaluation of typical power supply modes of important power users based on analytic hierarchy process and expert experience [J]. Power System Technology, 2014, 38(9):2336-2341.

[13] Zhang Qiuwen, Zhang Yongzhi, Zhong Ming. Multi-level fuzzy comprehensive evaluation of reservoir induced earthquake risk based on cloud model[J]. Journal of Hydraulic Engineering, 2014, 45(1): 87-95.