Indonesian Journal of Electrical Engineering and Computer Science
Vol. 1, No. 3, March 2016, pp. 656 ~ 664
DOI: 10.11591/ijeecs.v1.i3.pp656-664

Information Security Risk Assessment Based on Analytic Hierarchy Process

Mingxiang He*[1], Xin An[2]
[1*]Shandong Province Key Laboratory of Wisdom Mine Information Technology,
Shandong University of Science and Technology
579 Qianwangang Road Huangdao Zone, Qingdao Shandong Province, 266590 P.R. China
[2]College of Information Science and Engineering, Shandong University of Science and Technology
e-mail: hmx0708@163.com

Abstract

Information security risk assessment was an important component of information systems security engineering and the selection of assessment method had a direct impact on the final results of the assessment. But there were too many elements in the process of information security risk assessment. How to find the optimal elements from many elements to simplify the calculation of risk value and provide a strong basis for taking relevant measures, which was a problem needed to be solved. In addition, the reliability of the risk assessment results could not be guaranteed only through a single qualitative or quantitative assessment method. By Analytic Hierarchy Process (AHP), the relative weight of elements related to information security risk could be calculated. Then the optimal indicators, which provided a strong basis for taking relevant measures, could be selected by sorting the weights of elements to reduce the number of indicators. Moreover, Analytic Hierarchy Process, a method of the combination of qualitative and quantitative assessment methods, could overcome the shortcomings of single qualitative or quantitative assessment method.

Keywords: *risk assessment, Analytic Hierarchy Process, information security*

1. Introduction

Information security risk management is the overall process that identifies and analyzes the risk of being exposed to the organization, provides an assessment of the potential impact on the business, and takes measures to eliminate or reduce the risk to an acceptable level [1]. Information security risk assessment is a stage of information security risk management. Information security risk management depends on the results of risk assessment to determine the subsequent risk control and approval activities. There are many risk assessment methods, which can be divided into three categories: the qualitative risk assessment methods, quantitative risk assessment methods, comprehensive assessment methods which combine qualitative with quantitative assessment methods [2]. In reference [3], the key issues during the process of information security risk assessment are proposed and the quantitative methods of risk assessment are studied. In reference [4], a quantitative method based on expert judgments, fuzzy logic and analytic hierarchy process is used to evaluate the impact and possibility values for specific threats. In reference [5], the Bayesian network is introduced into information security risk assessment system to establish the risk analysis model. In reference [6], the information security risk assessment approach based on two stages decision model with grey synthetic measure is proposed to solve the fuzziness and uncertainty from many aspects.

However, there are too many elements in the process of information security risk assessment, which makes the calculation of risk value more complicated and cumbersome. How to find the more important elements of assessment from many elements to simplify the calculation of risk value and provide a strong basis for taking relevant measures, which is a problem needs to be solved. In addition, the reliability of the risk assessment results can not be guaranteed only through a single qualitative or quantitative assessment method due to the fact that the qualitative assessment methods are too subjective and rough and some risk elements may be misunderstood or misinterpreted in the process of quantitative assessment, which will have great influence on the accuracy of the evaluation results [7].

By AHP, the relative weight of elements related to information security risk can be calculated. Then the optimal indicators, which can simplify the calculation of risk value, can be

Received November 11, 2015; Revised March 1, 2016; Accepted March 10, 2016

selected by sorting the weights of elements to reduce the number of indicators [8] [9]. According to these indicators, which have great influence on the risk, appropriate measures should be taken to control the risk. Moreover, AHP, a method of the combination of qualitative and quantitative assessment methods, can overcome the disadvantages of single qualitative or quantitative assessment method.

2. Research Method

The Analytic Hierarchy Process [10], a combination of quantitative and qualitative analysis methods, is proposed by the famous American Operations Research Professor Saaty in the early 1970s. This method is more efficiently used to solve multiple complex problems. In the Analytic Hierarchy Process, elements related to decisions are divided into target, criterions and solutions. It breaks down complex problems into a number of levels based on dominance relations [11].

The main steps of the Analytic Hierarchy Process are as follows.

2.1. Decomposition of the System and the Construction of the Hierarchy Model

Analyzing the information system, makes the problems become hierarchical by deviding the complex system into elements, and groups them according to dominance relationship. Finally, an orderly ladder hierarchical structure model can be established. In fact, the process of establishing the hierarchy model is the process of analyzing the problem. The model consists of the target layer, the criterion layer and the solution layer, as shown in Figure 1. There is only one element in the target layer, which is generally intended for the analysis of the problem. There are a series of intermediate links in the criterion layer, which consist of several layers such as criterion and sub criterion. Similarly, there are all kinds of optional measures and solutions in the solution layer. This paper, based on the hierarchy model of three layers, analyzes the AHP.

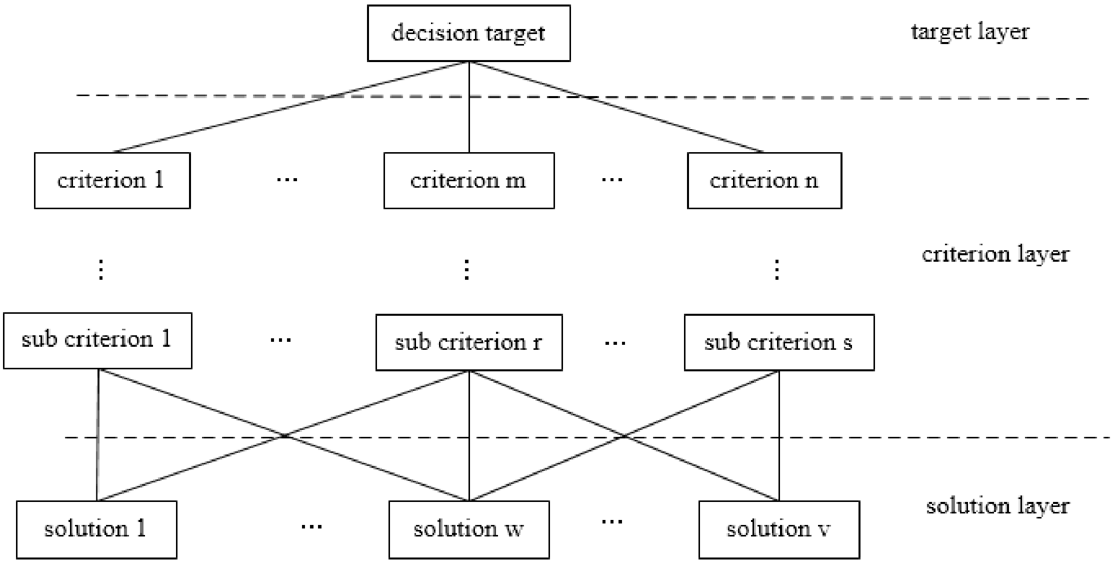

Figure 1. The hierarchy model

2.2. The Construction of Judgment Matrix

The judgment matrix is a matrix which is constructed by comparing a certain element in the upper layer with all elements related to it in this layer. For example, as for the criterion H in criterion layer, these are n elements ($w_1, w_2, \ldots, w_n$) related to it in solution layer. Therefore, the judgment matrix is shown in formula (1).

$$A=\begin{bmatrix} 1 & \frac{w_1}{w_2} & \cdots & \frac{w_1}{w_n} \\ \frac{w_2}{w_1} & 1 & \cdots & \frac{w_2}{w_n} \\ \vdots & \vdots & \vdots & \vdots \\ \frac{w_n}{w_1} & \frac{w_n}{w_2} & \cdots & 1 \end{bmatrix}=\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} \tag{1}$$

In the matrix above, a_{ij} refers to the ratio of importance of the element i and element j in terms of the criterion H and satisfies $a_{ji} = 1/a_{ij}\,(i, j = 1,2,\cdots,n)$ .Generally, it can be given by experts who familiar with the problems or by the decision makers or by analysts through technical advice. In the Analytic Hierarchy Process, the comparison of the two elements can become quantitative according to Saaty's 1-9 scale method, as shown in Table 1 [12].

Table 1. Saaty's 1-9 scale method

Scale	Meaning (the comparison of the two elements)
1	the two elements are of equal importance
3	one element is slightly more important than another element
5	one element is obviously more important than another element
7	one element is strongly more important than another element
9	one element is extremely more important than another element
2、4、6、8	median of the two adjacent judgments above
the reciprocal of the number above	the importance ratio of the element i and element j is a_{ij} , so the importance ratio of the element j and element i is $a_{ji} = 1/a_{ij}$

2.3. The Calculation of Respective Index Weight

It is required to calculate the maximum eigenvalue and eigenvector of the judgment matrix and check the consistency of the judgment matrix [13]. For a certain element in the upper layer, the relative weights of the elements related to it in this layer are determined by judgment matrix and mathematical methods of the matrix. For instance, the relative weight vector of the n elements related to the criterion H in the solution layer should be calculated according to the judgment matrix A constructed in step 2.2.

In practical applications, sum and product method and square root method are often used to calculate the eigenvector, as shown in formula (2).

$$\overline{w_i} = \sqrt[n]{\prod_{j=1}^{n} a_{ij}}\ ,（\mathrm{i} = 1,2,\cdots,\mathrm{n}） \tag{2}$$

So the vector $\Phi = (\overline{w_1}, \overline{w_2}, \ldots, \overline{w_n})^T$ can be got. By using $w_i = \frac{\overline{w_i}}{\sum_{j=1}^{n} \overline{w_j}}$（$\mathrm{i} = 1,2,\cdots,\mathrm{n}$）to normalize the vector Φ, the vector $w = (w_1, w_2, \ldots w_n)^T$ is the eigenvector that is needed.

The maximum eigenvalue can be obtained by the eigenvector and judgment matrix, as shown in formula (3).

$$\lambda_{\max} = \frac{1}{n}\sum_{i=1}^{n}\frac{(Aw)_i}{w_i} \tag{3}$$

The vector $Aw$is shown in formula (4). (Aw) is the i-th element of vector B.

$$Aw = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} \times \begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix} = B \quad (4)$$

And then it is necessary to check the consistency by introducing the consistency index CI , as shown in formula (5).

$$CI = \frac{\lambda_{\max} - n}{n-1} \quad (5)$$

The smaller CI is, the nearer λ_{max} approximates to n. Ideally, CI equals zero. In fact, the higher the dimension n of the judgment matrix is, the worse the consistency is.

So, it is required to reduce the requirement for consistency of high-dimensional judgment matrix by introducing the average random consistency index RI. The value of RI is related to the dimension of the judgment matrix, which can be assigned according to the Table 2 [14].

Table 2. Saaty's 1-10 dimension RI

Dimension of the judgment matrix	RI
1	0
2	0
3	0.52
4	0.90
5	1.12
6	1.26
7	1.36
8	1.41
9	1.46
10	1.49

The corrected consistency index is obtained by calculating the $CR = \frac{CI}{RI}$. If $CR \le 0.1$, the judgment matrix will pass the consistency test. What's more, the eigenvector $w = (w_1, w_2, \dots w_n)^T$ will be the weight vector and each component of it represents the proportion or share of corresponding measures or solutions in criterion H. If the judgment matrix doesn't pass the consistency test, it will be nessary to adjust it until the test passed.

2.4. The Calculation of Comprehensive Index Weight

Comprehensive index weight represents the weight vector of all elements in the solution layer for the target layer. And each component of it represents the proportion or share of corresponding measures or solutions in the target.

The weight vector $w = (w_1, w_2, \dots w_n)^T$ has been obtained in step 2.3, which represents the proportion or share of n elements in criterion H. Supposing there are m($m \ge n$) elements in the solution layer and n elements related to the criterion H, now the weight vector $w = (w_1, w_2, \dots w_n)^T$ can be transformed as follows: the weights of n elements related to the criterion H remain the unchanged, and the weights of m-n elements unrelated to H are zeros. Finally, a new weight vector $Q_H = (w_{1H}, w_{2H}, \dots w_{mH})^T$ can be obtained, which represents the proportion of all elements of the solution layer in criterion H. Assuming that there are k elements in the criterion layer, the combined weight vector W of all elements in the solution layer to the criterion layer can be obtained by the method mentioned above.The content of W is shown in formula (6).

$$W=(Q_1,Q_2,\dots,Q_k)=\begin{bmatrix} w_{11} & w_{12} & \cdots & w_{1k} \\ w_{21} & w_{22} & \cdots & w_{2k} \\ \vdots & \vdots & \vdots & \vdots \\ w_{m1} & w_{m2} & \cdots & w_{mk} \end{bmatrix} \quad (6)$$

Similarly, the weight vector $C=(c_1,c_2,\dots,c_k)^T$ of all elements in the criterion layer to the target layer can be obtained.

Then, according to the combination weight vector W and the weight vector C, the vector U can be calculated, as shown in formula (7).

$$U=W\times C=\begin{bmatrix} w_{11} & w_{12} & \cdots & w_{1k} \\ w_{21} & w_{22} & \cdots & w_{2k} \\ \vdots & \vdots & \vdots & \vdots \\ w_{m1} & w_{m2} & \cdots & w_{mk} \end{bmatrix}\times\begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_k \end{bmatrix}=\begin{bmatrix} u_1 \\ u_2 \\ \vdots \\ u_m \end{bmatrix} \quad (7)$$

The vector U represents the comprehensive weight of all elements in the solution layer to the target. By sorting the weights of them, several important indicators, which have great influence on the risk, will be obtained. Based on these important indicators, corresponding measures should be taken to control the risk. In addition, the number of risk elements will be greatly reduced, which will simplify the calculation of risk value.

3. Results and Discussion

The information security risk assessment is carried out according to the analytic hierarchy process. The hierarchy model of three layers is constructed based on a company's actual information system, as shown in Figure 2. The element of the target layer is the risk index of the information system to be tested. The elements of criterion layer mainly include the physical security, the operation security and the application security. The elements of solution layer mainly include environmental security, device security, media security, network monitoring, vulnerability scanning, virus prevention, data backup, access control, information encryption and intrusion detection.

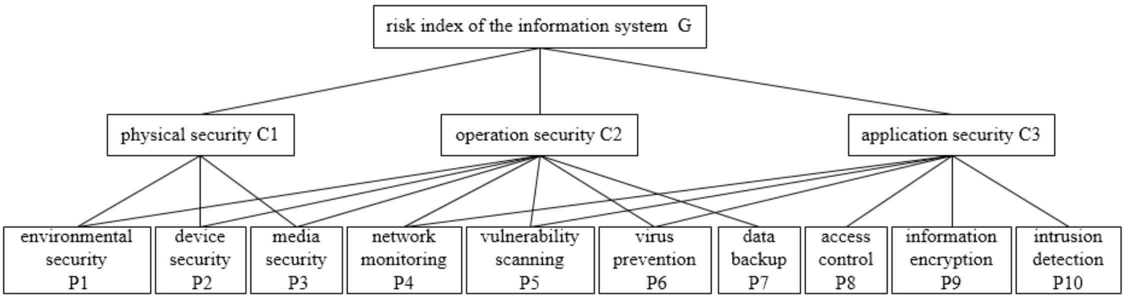

Figure 2. The hierarchy model of a company

3.1. The Construction of the Judgment Matrix and the Calculation of Respective Index Weight

In target-criterion layer, the judgment matrix is generally given by experts who familiar with the problems and the structure of it is shown in formula (8).

$$G-C=\begin{bmatrix}1 & 5 & 3\\ 1/5 & 1 & 3\\ 1/3 & 1/3 & 1\end{bmatrix} \tag{8}$$

According to the judgment matrix $G-C$, the vector $\Phi=(2.4662 \quad 0.8434 \quad 0.4807)^T$ is calculated. Then by normalizing it, the eigenvector $w=(0.6507 \quad 0.2225 \quad 0.1268)^T$ is obtained. The maximum eigenvalue $\lambda_{\max}=3.2948$, $CI=\frac{\lambda_{\max}-n}{n-1}=\frac{3.2948-3}{3-1}=0.1474$, and the average random consistency index $RI=0.52$ can be acquired. It is nessary to adjust the judgment matrix, because the corrected consistency index $CR=\frac{CI}{RI}=\frac{0.1474}{0.52}=0.2835$ does not satisfy $CR\le 0.1$, which does not pass the consistency test.

Now the judgment matrix is adjusted, as shown in formula (9).

$$G-C=\begin{bmatrix}1 & 2 & 3\\ 1/2 & 1 & 3\\ 1/3 & 1/3 & 1\end{bmatrix} \tag{9}$$

According to the adjusted judgment matrix, Φ = (1.8171 1.1447 0.4807)^T, w = (0.5278 0.3325 0.1396)^T, $\lambda_{\max}$ = 3.0537, CI = 0.0269, and RI = 0.52 can be obtained. Because of CR = 0.0517 ≤ 0.1, the judgment matrix passes the consistency test. What's more, the eigenvector w is the weight vector.

In criterion-solution layer, the judgment matrix of the criterion C1 is constructed, as shown in formula (10).

$$C1-P=\begin{bmatrix}1 & 3 & 4\\ 1/3 & 1 & 3\\ 1/4 & 1/3 & 1\end{bmatrix} \tag{10}$$

According to the judgment matrix, Φ = (2.2894 1 0.4368)^T, w = (0.6144 0.2684 0.1172)^T, λ_{max} = 3.0736, CI = 0.0368, and RI = 0.52 can be obtained. Because of CR = 0.0708 ≤ 0.1, the judgment matrix passes the consistency test. What's more, the eigenvector w is the weight vector.

The judgment matrix of the criterion C2 is constructed, as shown in formula (11).

$$C2-P=\begin{bmatrix}1 & 1 & 1 & 1/2 & 1/3 & 1/3 & 1/4\\ 1 & 1 & 2 & 1/2 & 1/2 & 1/3 & 1\\ 1 & 1/2 & 1 & 1/3 & 1/3 & 1/2 & 1/3\\ 2 & 2 & 3 & 1 & 1 & 1 & 1/4\\ 3 & 2 & 3 & 1 & 1 & 1 & 1/5\\ 3 & 3 & 2 & 1 & 1 & 1 & 1/2\\ 4 & 1 & 3 & 4 & 5 & 2 & 1\end{bmatrix} \tag{11}$$

According to the judgment matrix, Φ = (0.5428 0.7742 0.5123 1.1699 1.2008 1.3687 2.4157)^T, w =(0.0680 0.0970 0.0642 0.1465 0.1504 0.1714 0.3026)^T, $\lambda_{\max}$ = 7.5785, CI = 0.0964, and RI = 1.36can be obtained. Because of CR = 0.0709 ≤ 0.1, the judgment matrix passes the consistency test. What's more, the eigenvector w is the weight vector.

The judgment matrix of the criterion C3 is constructed, as shown in formula (12).

$$C3-P=\begin{bmatrix}1&1&1&1/2&1/3&1/4\\1&1&1/2&1&1/3&1/2\\1&2&1&1&1&1/2\\2&1&1&1&1&1\\3&3&1&1&1&3\\4&2&2&1&1/3&1\end{bmatrix} \tag{12}$$

According to the judgment matrix, Φ = (0.5888 0.6609 1 1.1225 1.7321 1.3218)^T, w = (0.0916 0.1028 01556 0.1747 0.2695 0.2057)^T, $\lambda_{\max}$ = 6.4119, CI = 0.0824, and RI = 1.26 can be obtained. Because of CR = 0.0654 $\leq$ 0.1,the judgment matrix passes the consistency test. What's more, the eigenvector w is the weight vector.

3.2. The Calculation of Comprehensive Index Weight

The combined weight vector W of all elements in the solution layer to the criterion layer is shown in formula (13).

$$W=(Q_1,Q_2,Q_3)=\begin{bmatrix}0.6144&0.0680&0\\0.2684&0.0970&0\\0.1172&0.0642&0\\0&0.1465&0.0916\\0&0.1504&0.1028\\0&0.1714&0.1556\\0&0.3026&0\\0&0&0.1747\\0&0&0.2695\\0&0&0.2057\end{bmatrix} \tag{13}$$

According to the combination weight vector W and the weight vector C, the vector Ucan be calculated, as shown in formula (14).

$$U=W\times C=\begin{bmatrix}0.6144&0.0680&0\\0.2684&0.0970&0\\0.1172&0.0642&0\\0&0.1465&0.0916\\0&0.1504&0.1028\\0&0.1714&0.1556\\0&0.3026&0\\0&0&0.1747\\0&0&0.2695\\0&0&0.2057\end{bmatrix}\times\begin{bmatrix}0.5278\\0.3325\\0.1396\end{bmatrix}=\begin{bmatrix}0.3469\\0.1739\\0.0832\\0.0615\\0.0644\\0.0787\\0.1006\\0.0244\\0.0376\\0.0287\end{bmatrix} \tag{14}$$

The vector U represents the comprehensive weight of all elements of the solution layer to the target layer. The weight of each element in the solution layer to the target is shown in Table 3.

Table 3. The weight of elements in the solution layer to the target

The elements in the solution layer	The weight of elements
environmental security	0.3469
device security	0.1739
media security	0.0832
network monitoring	0.0615
vulnerability scanning	0.0644
virus prevention	0.0787
data backup	0.1006
access control	0.0244
information encryption	0.0376
intrusion detection	0.0287

As can be seen from Table 3, environmental security, device security and data backup have a comparatively great proportion in the target, which shows that they have great influence on the risk and measures should be taken to solve these problems. In addition, because there are too many elements related to the risk, these important indicators can be used as input when calculating the risk to simplify the calculation of risk.

4. Conclusion

This paper solves the problem of too many elements in the process of risk assessment by using the AHP. Therefore, several elements which have great impact on the risk can be obtained from the numerous risk elements, which greatly reduce the number of elements, and provide the input for the next step to calculate the risk value.

In this paper, the elements related to the risk in the example mainly include environmental security, device security, media security, network monitoring, vulnerability scanning, virus prevention, data backup, access control, information encryption and intrusion detection. By using the AHP, the weight of them to the risk can be obtained. It is concluded that the weight of environmental security, device security, and data backup is larger, which shows that they have great influence on the risk, and should be considered as the input when calculating the value of risk. And the company should focus on these issues in order to reduce the possibility of occurrence of the risk.

Acknowledgements

This work is supported by Taishan Scholar Climbing Program of Shandong Province in Shandong University of Science and Technology.

References

[1] R Bojanc, B Jerman-Blažič. Quantitative Model for Information Security Risk Management. *Engineering Management Journal*. 2013; 25(2): 267-275.

[2] Li Zhang, Jianfen Peng, Yuge Du. A Summary of the Comprehensive Assessment Method of Information Security Risk Assessment. *Journal of Tsinghua University (Science and Technology)*. 2012; 52(10): 1364-1369.

[3] Zhihu Wang, Haiwen Zeng. *Study on the Risk Assessment Quantitative Method of Information Security*. 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE). Chengdu. 2010; 6: 529-533.

[4] Igor V Anikin. *Information Security Risk Assessment and Management Method in Computer Networks*. 2015 International Siberian Conference on Control and Communications (SIBCON). Omsk. 2015: 1-5.

[5] Lijian Wang, Bin Wang, Yongjun Peng. *Research the Information Security Risk Assessment Technique Based on Bayesian Network*. 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE). Chengdu. 2010; 3: 600-604.

[6] Hongsheng Luo, Yongjun Shen, Guidong Zhang. *Information Security Risk Assessment Based on Two Stages Decision Model with Grey Synthetic Measure*. 2015 6th International Conference on Software Engineering and Service Science (ICSESS). Beijing. 2015: 795-798.

[7] Xiaoming Yang, Hengfeng Luo, Chengyu Fan. *The Analysis of Information System Security Risk Assessment Technology. Computer Applications*. 2008; 28(8): 1920-1923.

[8] Baohua Zhao. Information System Risk Assessment Based on Analytic Hierarchy Process and Neural Network. *Microelectronics & Computer*. 2015; 32(10): 163-166.

[9] Long Xiao, Yong Qi, Qianmu Li. The Information Security Risk Assessment Based on AHP and Fuzzy Comprehensive Evaluation. *Computer Engineering and Applications*. 2009; 45(22): 82-85.

[10] Qiong Sun, Zhengran Gao. The Small and Medium-sized Enterprises Performance Evaluation Model based on DEA and AHP Method. *TELKOMNIKA Indonesian Journal of Electrical Engineering*. 2013; 11(11): 6400-6405.

[11] Ziqiu Wei, Mingfang Li. *Information Security Risk Assessment Model Base on FSA and AHP*. International Conference on Machine Learning and Cybernetics (ICMLC). Qingdao. 2010; 5: 2252-2255.

[12] Zhiming Feng, Guofu Yin, Haifeng Lin. Comprehensive Evaluation of CNC Machine Tools Accuracy Based on AHP. *TELKOMNIKA Indonesian Journal of Electrical Engineering*. 2014; 12(3): 1658 –1667.

[13] Linlin Liu, Hong Chen, Ruixin Zhang. Comprehensive Evaluation of Examination Quality based on Fuzzy AHP. *TELKOMNIKA Indonesian Journal of Electrical Engineering*. 2013; 11(9): 5384-5394.

[14] Baoli Liu, Xiaochun Zhang, Gendu Zhang. Information System Vulnerability Assessment Method based on Analytic Hierarchy Process. *Computer Science*. 2006; 33(12): 62-64.