

## Research Article

# A Security Situation Assessment Model of Information System for Smart Mobile Devices

Lixia Xie, Liping Yan, Xugao Zhang, and Hongyu Yang 

School of Computer Science and Technology, Civil Aviation University of China, Tianjin 300300, China

Correspondence should be addressed to Hongyu Yang; [hyyang@cauc.edu.cn](mailto:hyyang@cauc.edu.cn)

Received 30 June 2020; Revised 24 August 2020; Accepted 18 September 2020; Published 8 October 2020

Academic Editor: Ding Wang

Copyright © 2020 Lixia Xie et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The accuracy of the existing security situation assessment model of information system for smart mobile devices is affected by expert evaluation preferences. This paper proposes an information system security situation assessment model for smart mobile devices, which is based on the modified interval matrix-entropy weight-based cloud (MIMEC). According to the security situation assessment index system, the interval judgment matrix reflecting the relative importance of different indexes is modified to improve the objectivity of the index layer weight vector. Then, the entropy weight-based cloud is used to quantify the criterion layer and the target layer security situation index, and the security level of the system is graded. The evaluation experiment on the departure control system for smart mobile devices not only verify the validity of this model but also demonstrate that this model has higher stability and reliability than other models.

## 1. Introduction

Security situation assessment refers to the process of predicting the security situation of the system based on the perception and acquisition of security elements in a certain time and space, and the integrated analysis of the acquired data information [1]. The security situation assessment model is necessary for information system administrators of smart mobile devices to obtain the dynamic security situation of the system, determine system abnormal events, and make reasonable decisions.

Fu et al. [2] proposed a comprehensive evaluation model for information system security risk based on the entropy weight coefficient method. The entropy weight coefficient method was used to determine the index weight vector and reduce the subjective influence of experts. Luo et al. [3] proposed a risk assessment model based on the gray comprehensive measure, but the evaluation model lacks management dimension indexes. Xi et al. [4] proposed an improved quantitative evaluation model of the network security situation and optimized the network security situation quantitative value by game method, but the information source is single. Shu et al. [5] proposed a network security risk assess-

ment model based on network security vulnerabilities to assess network security risks. However, the model requires a large amount of data, the risk baseline determination is influenced by experts, and the algorithm complexity is high. Hemanidhi et al. [6] calculated the total network risk value by weighting the quantified results of network risk under different vulnerability detection tools, but the distribution of risk value weight for different detection tools is not reasonable. Eom et al. [7] proposed a risk quantification formula based on threat frequency, asset exposure, and asset protection level, but the determination of threat frequency is influenced by subjective factors. Rimsha et al. [8] proposed an information security risk assessment method based on the adjacency matrix. However, a higher-order adjacency matrix will increase the deviation between the risk value and the actual security situation. Cheng [9] proposed a streaming algorithm to identify user click requests and reconstructed user-browser interactions by leveraging the Spark Streaming framework. Rui [10] proposed a two-stage approach by combining multiobjective optimization (MOO) with integrated decision-making (IDM) to address the problem of combined heat and power economic emission dispatch (CHPEED).

Those indicate that the existing information system security situation assessment indexes only focus on the technical level without considering the human factors. Moreover, the security situation evaluation is greatly influenced by the subjectivity of experts, and the quantified results cannot accurately reflect the information system security situation.

Motivated by those above, in this paper, we propose an information system security situation assessment model (ISSSAM) for smart mobile devices, which is based on the modified interval matrix-entropy weight-based cloud (MIMEC).

*1.1. Contribution.* The main contributions of this paper are listed as follows:

- (1) A practical ISSSAM model. To accurately assess the information system security situation for smart mobile devices, an ISSSAM model is built with consideration of the modified interval matrix module and entropy weight-based cloud
- (2) A novel modified algorithm. A modified interval matrix module is proposed to improve the objectivity of the weight vector. Firstly, the interval judgment matrix given by experts is modified to improve its consistency degree. Secondly, the deterministic matrix with the best consistency degree is searched in the modified interval judgment matrix. Finally, the best weight vector is obtained based on the best deterministic matrix
- (3) The experimental results of the departure control system (DCS) case, prove the effectiveness of our model. Furthermore, compared with other methods, the results demonstrate that our model is closer to the practical security situation and improves the reliability and stability of information system security situation assessment

*1.2. Organization.* The rest of this paper is organized as follows. Section 2 presents the security situation assessment model. Section 3 recommends multisource data normalization. In Section 4, the modified interval matrix module is proposed. Section 5 reviews the entropy weight-based cloud module. In Section 6, the experimental comparisons are carried out, and the results are analyzed. Finally, Section 7 gives the conclusions. In addition, the list of notations is shown in Table 1.

## 2. Security Situation Assessment Model

In this paper, a MIMEC based security situation assessment model of information system for smart mobile devices is established (see Figure 1).

The assessment process is designed as follows: firstly, based on the analytic hierarchy process (AHP), a three-layer index system for security situation assessment of an information system for smart mobile devices is established. Define that there are 5 evaluation dimensions (see Figure 2), where they are physical dimension ( $I_1$ ), host sys-

TABLE 1: Notations and abbreviations.

Symbol	Descriptions
$m$	Number of comment
$\beta$	Qualitative index comment
$V_e$	Expert value
$\mu$	Modified factor
$X$	Quantitative index
$-A$	Interval judgment matrix
$-a_{ij}$	Interval number
$CR$	Consistency ratio
$RI$	Average random consistency index
$\gamma$	Interval matrix consistency degree
$Q$	Number of random matrixes
$p$	Number of satisfactory consistency matrix
$U$	Universe
$C_S$	Membership degree
$E_x$	Expectation value
$E_n$	Entropy
$H_e$	Hyper entropy

tem dimension ( $I_2$ ), network dimension ( $I_3$ ), data dimension ( $I_4$ ), and manager dimension ( $I_5$ ).

Secondly, there are various ways for us to obtain data as the basis for experts' scoring and determine qualitative indexes and quantitative indexes, such as questionnaire survey, physical environment assessment, viewing host configuration, and obtaining system vulnerabilities through intrusion detection system.

Thirdly, the security situation is quantified by the modified interval matrix module and the entropy weight-based cloud module. The interval judgment matrix is given by experts, and the modified interval matrix module is used to obtain the best deterministic judgment matrix. Then, the index layer is constructed according to the experts' evaluation results. Combined with the index layer weight vector, the criterion layer based cloud model is constructed, and the entropy weight coefficient of the criterion layer cloud model is calculated. At last, the situation value of an information system for smart mobile devices is obtained by the situation value operator.

Finally, according to the "Information security technology—classification guide for classified protection of information systems security" [11] and the comprehensive security situation value of an information system for smart mobile devices, the security situation level is determined.

## 3. Multisource Data Normalization

Since the heterogeneity of multisource data makes it difficult for experts to evaluate, this paper proposes a normalized method for qualitative and quantitative indexes as follows.

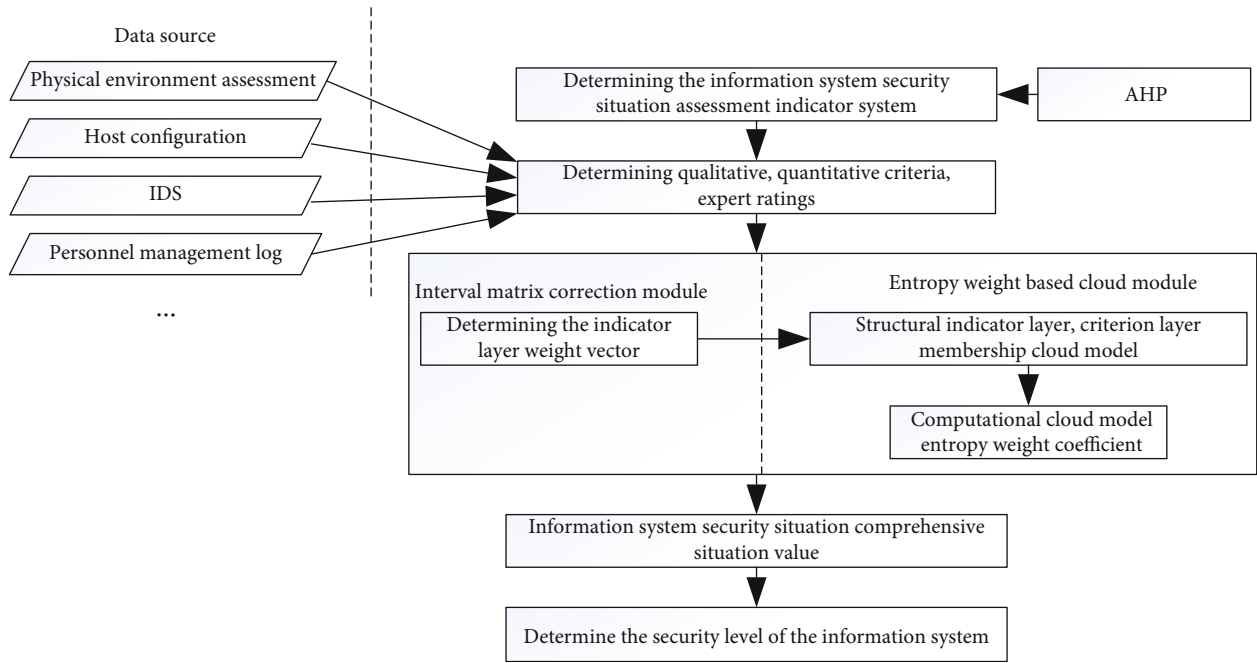


FIGURE 1: Security situation assessment model.

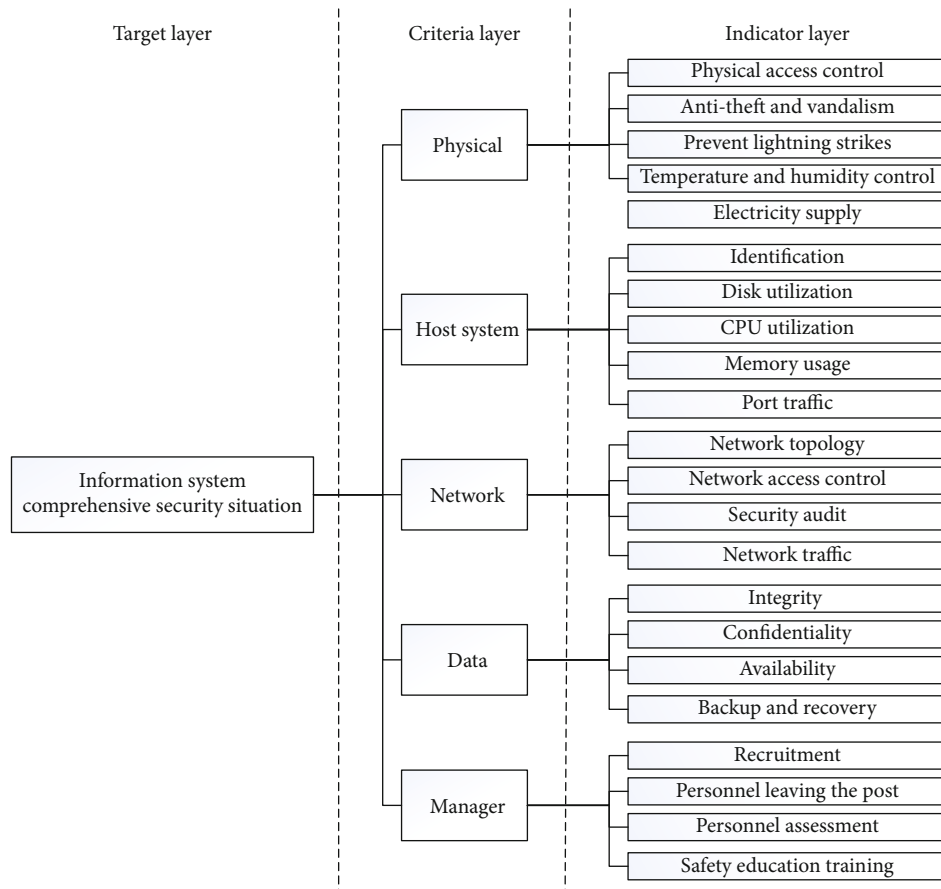


FIGURE 2: Evaluation index system.

**3.1. Normalization of Qualitative Indexes.** Define that there are  $m$  qualitative index comment classifications, which are  $\beta_1, \beta_2, \dots, \beta_m$ .  $\beta_i \sim \beta_j$  ( $i, j \in 1, 2, \dots, m$ ) represents that the comment  $\beta_i$  is better than comment  $\beta_j$ , then  $\beta_1 \sim \beta_2 \sim \dots \sim \beta_m$  ( $i, j \in 1, 2, \dots, m$ ). Meanwhile, define that  $\theta$  is the index which reflects the score of comment and  $\theta \sim N(0, 1)$ . Suppose that the  $t_i$  is corresponding to comment  $\beta_i$  which reflects the expert score and  $t_i$  is the quantile of  $N(0, 1)$ , then

$$P(\theta < t_i) = \frac{i}{m} \quad (i = 1, 2, \dots, m - 1) \quad (1)$$

Define that the expert score is  $V_e$  and  $V_e = \mu t_i$ , where  $\mu$  is the modified factor (this paper takes  $\mu = 100$ ).

**3.2. Normalization of Quantitative Indexes.** Define that the quantitative interval of the index  $X$  is  $[X_a, X_b]$ , the normalization process for the quantitative indexes of different dimensions is as follows:

(1) Positive index

$$X_1 = \frac{x - X_a}{X_b - X_a}, \quad (X_b > X_a) \quad (2)$$

(2) Reverse index

$$X_2 = \frac{X_b - x}{X_b - X_a}, \quad (X_b > X_a) \quad (3)$$

## 4. Modified Interval Matrix Module

The assessment of the security situation needs to determine the relative importance of each index, and its mathematical representation is the weight vector. In this paper, the interval judgment matrix given by experts is modified to improve the degree of consistency, and the deterministic matrix with the best consistency is searched in the modified interval judgment matrix to determine the best weight vector. This method not only preserves the subjectivity of expert evaluation but also improves the objective degree of the weight vector.

**4.1. Related Definitions.** Interval judgment matrix: define that the subscript set of  $n$  elements is  $J = \{1, 2, \dots, n\}$ , and the relative importance between element  $i$  and element  $j$  is  $a_{ij}$ . Then, the interval judgment matrix can be represent as  $-A = (-a_{ij})_{n \times n}$ ,  $i, j \in 1, 2, \dots, n$ , and the interval number  $-a_{ij}$  is  $[a_{ij}^L, a_{ij}^U]$ ,  $-a_{ji} = [1/a_{ij}^U, 1/a_{ij}^L]$ ,  $a_{ij}^L \leq a_{ij}^U$ . This paper takes 1-9 scale judgment matrix [12].

Random matrix: define that matrix  $A = (a_{ij})_{n \times n}$ ,  $i, j \in 1, 2, \dots, n$ , where  $a_{ij} \in [a_{ij}^L, a_{ij}^U]$ . Random number  $a_{ij}$  is generated from  $[a_{ij}^L, a_{ij}^U]$  according to the probability of uniform distribution.

TABLE 2: Average random consistency index values.

Order	1	2	3	4	5	6	7	8	9
RI	0	0	0.52	0.89	1.12	1.26	1.36	1.41	1.46

Satisfactory consistency: define that the consistency ratio of judgment matrix  $A$  is  $CR(A) = (\lambda_{\max}(A) - n)/(n - 1)RI$ . When  $CR \leq 0.1$ , we consider the matrix  $A$  has satisfactory consistency, where  $\lambda_{\max}(A)$  is the maximum eigenvalue of matrix  $A$ ,  $RI$  is the average random consistency index (see Table 2).

Interval matrix consistency degree: define that  $\gamma$  is the interval matrix consistency degree. If  $Q$  random matrixes are generated from interval matrix  $-A$  and there are  $p$  matrixes has satisfactory consistency, then  $\gamma = p/Q$ .

**4.2. Modified Interval Matrix Design.** The modified interval matrix module is shown in Figure 3.

The modified interval matrix module is divided into three submodules. They are interval matrix consistency degree judgment submodule (Interval\_matrix\_identify), interval matrix element adjustment submodule (Interval\_matrix\_adopt), and best deterministic matrix acquisition submodule (Best\_interval\_matrix).

The workflow design of the modified interval matrix module is as follows.

*Step 1.* Calculate the consistency degree value (consis\_value) of a given interval matrix.

*Step 2.* If consis\_value > threshold, then turn to Step 3; else adjust the interval number elements, and turn to Step 1.

*Step 3.* Calculate the Best\_interval\_matrix based on the modified matrix.

*Step 4.* Calculate the weight vector based on Best\_interval\_matrix.

The processing method and process of each sub-module are explained in detail below.

**4.2.1. Interval Matrix Consistency Degree Judgment Submodule.** The interval judgment matrix given by the expert generates  $Q$  random matrices according to the uniform distribution probability and sequentially calculates the consistency ratio  $CR_k$  ( $k = 1, 2, \dots, Q$ ) of the generated random matrix. Let the number of random matrices with a satisfactory degree of consistency be  $p$ , then the degree of consistency of the interval matrices is  $\gamma = p/Q$ . The larger  $\gamma$ , the better the consistency of the interval matrix; the smaller  $\gamma$ , the worse the consistency of the interval matrix. This paper takes  $Q = 100$ .

**4.2.2. Interval Matrix Element Adjustment Submodule.** When the consistency degree  $\gamma$  is less than a certain threshold, some elements in the interval matrix need to be adjusted. The specific process is designed as follows.

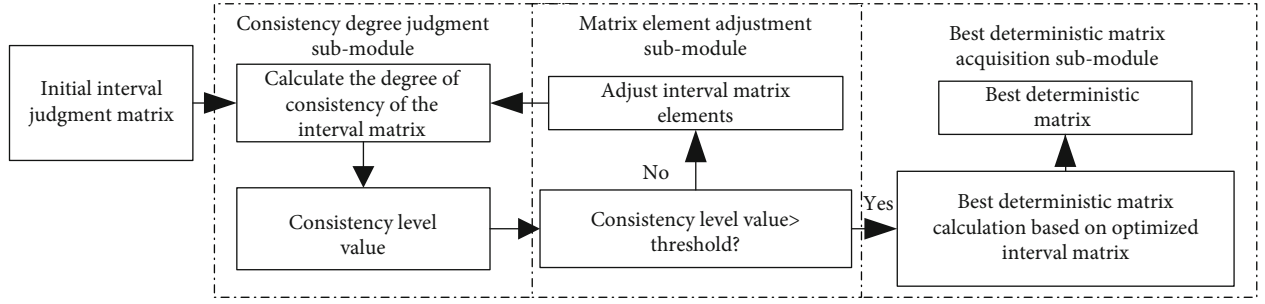


FIGURE 3: Design of modified interval matrix.

*Step 1.* Get subinterval matrix  $-A_h^{(n-1)}$  by deleting the elements of the  $h$ th row and  $h$ th column in the interval matrix, and compute  $\gamma_h$  of  $A_h^{(n-1)}$ .

*Step 2.* If  $\gamma_{h1}$  and  $\gamma_{h2}$  of the subinterval matrix  $-A_{h1}^{(n-1)}$  and  $-A_{h2}^{(n-1)}$   $> \gamma_h$  of other matrices, adjust the interval elements  $[a_{h1h2}^L, a_{h1h2}^U]$ ,  $[a_{h2h1}^L, a_{h2h1}^U]$ .

*Step 3.* Turn to the Interval\_matrix\_identify submodule, and calculate  $\gamma$  of the adjusted interval judgment matrix.

After deleting the elements of the  $h$ th row and  $h$ th column in the interval matrix, the deleted elements are isolated to remain elements. If the consistency degree of this interval matrix improved greatly, it is indicated that the deleted elements have a negative impact to the original matrix. So, we need to invite experts to adjust corresponding elements to improve the consistency degree [13].

**4.2.3. The Best Deterministic Matrix Acquisition Submodule.** This submodule consists of two processes: interval matrix convergence and best deterministic matrix calculation. The specific process is designed as follows:

(1) Interval matrix convergence

*Step 1.* Generate  $R$  deterministic matrices according to the uniform distribution probability based on the adjusted interval judgment matrix.

*Step 2.* Calculate  $CR_i (i = 1, 2, \dots, R)$  of the  $R$  deterministic matrices, respectively.

*Step 3.* Get the  $t$ th matrix cluster ( $Cluster\_matrix\_t$ ) by obtaining first  $\omega$  consistency ratios of  $R$  deterministic matrices.

*Step 4.* Integrate the new interval matrix by using the same position elements of different matrices in matrix clusters.

*Step 5.* Obtain the upper and lower limits of each interval elements in the new interval judgment matrix. When  $i = j$ ,  $a_{ij}$

$= 1$ ; when  $i \neq j$ ,  $a_{ij}^L = \min \{a_{ij1}^L, a_{ij2}^L, \dots, a_{ij\omega}^L\}$ ,  $a_{ij}^U = \max \{a_{ij1}^U, a_{ij2}^U, \dots, a_{ij\omega}^U\}$ , and  $-a_{ji} = [1/a_{ij}^U, 1/a_{ij}^L]$ .

*Step 6.* Repeat Step 1~5 until the sum of  $|a_{ij}^U - a_{ij}^L| (i, j \in 1, 2, \dots, n)$  (the lengths of the interval matrix) is not more than 10% of the sum of the lengths of the original interval matrix.

In Step 1, the proportion of each determined number of the randomly generated deterministic matrix in the left half interval of each interval element of the original interval matrix is  $\alpha$ , and  $0.5 - \eta < \alpha < 0.5 + \eta$  (This paper takes  $\eta = 0.05$ ).

(2) Best deterministic matrix calculation

$$v = w * v + c * \text{rand} * (\text{pbest} - \text{present}), \quad (4)$$

$$\text{present} = \text{present} + v, \quad (5)$$

where  $v$  is the speed of optimization,  $w$  is used to adjust the speed of optimization,  $c$  is the cognitive factor and usually  $c = 2$ ,  $\text{rand}$  is the random number between (0, 1),  $\text{pbest}$  is the current the element in the deterministic matrix with the smallest consistency ratio, and  $\text{present}$  represents the element in the current deterministic matrix.

*Step 1.* Input the converged interval matrix ( $Input\_matrix$ ).

*Step 2.* Initialize a deterministic matrix  $M_0$ , the elements of the deterministic matrix are:  $a_{ij}$ ,  $i, j \in 1, 2, \dots, n$ . When  $i = j$ ,  $a_{ij} = 1$ ; when  $1 < j \leq n, 1 \leq i < j$ ,  $a_{ij} = (a_{ij}^L + a_{ij}^U)/2$ ; when  $1 < i \leq n, 1 \leq j < i$ ,  $a_{ij} = 1/a_{ji}$ .

*Step 3.* Calculate  $CR_0$  as the initial consistency ratio.

*Step 4.* Generate deterministic matrix  $M_i (i = 1, 2, \dots, k)$  randomly from  $Input\_matrix$ .

*Step 5.* Calculate its consistency ratio  $CR_i$ , and compare it with  $CR_0$ .

*Step 6.* If  $CR_i < CR_0$ ,  $CR_0 = CR_i$ ,  $M_0 = M_i$ ; else, keep  $CR_0$  and  $M_0$  unchanged.

*Step 7.* Adjust each element in each deterministic matrix according to equations (4) and (5):

$v_{\max} = \min (a_{ij}^U - a_{ij}^L) (i \neq j, i, j \in 1, 2, \dots, n)$ , where  $a_{ij}^L, a_{ij}^U$  are the upper and lower limits of each element of the converged interval matrix. If  $v > v_{\max}$ , then take  $v = v_{\max}$ ; if  $v < -v_{\max}$ , take  $v = -v_{\max}$ . If present  $\in [a_{ij}^L, a_{ij}^U]$ , present does not need to be adjusted; if present  $< a_{ij}^L$ , then take present =  $a_{ij}^L$ ; if present  $> a_{ij}^U$ , take present =  $a_{ij}^U$ . The initial value of  $v$  is taken as 0,  $p_{\text{best}_0}$  corresponds to each element in the initial deterministic matrix  $M_0$  in Step 2, and  $\text{present}_0$  corresponds to each element in the deterministic matrix randomly generated in Step 2 for the first time.

*Step 8.* Repeat Step 2~7 for  $k$  times.

On this basis, the eigenvector method can be used to calculate the best weight vector.

## 5. Entropy Weight-Based Cloud Module

*5.1. Related Definitions.* Membership cloud [14]: define that  $U$  is a certain universe, where  $U = \{x\}$  and  $S$  is language value corresponding to accuracy number  $x$ .  $x$  is a random number with a stable tendency for membership degree  $C_S(X)$ , and the distribution of membership degree on the universe is called membership cloud.

The digital characteristics of the cloud: the description of cloud rely on 3 parameters. They are expectation value  $E_x$ , entropy  $E_n$ , hyper entropy  $H_e$ , where  $E_x$  reflects a concept corresponds to the central value of a universe,  $E_n$  reflects the fuzziness of the concept and  $E_n$  reflects the degree of cloud droplet dispersion.

Entropy [2]: entropy measures the uncertainty of the system. Define that the system may stay in  $n$  different states and the probability of each state occurs is  $p_i (i = 1, 2, \dots, n)$ , then the entropy of the system is

$$E = - \sum_{i=1}^n p_i \ln p_i \quad (6)$$

where  $0 \leq p_i \leq 1$  and  $p_1 + \dots + p_n = 1$ . When  $p_i = 1/n$ ,  $E_{\max} = \ln n$ . Then, when the system has only one state  $n = 1$  and  $E_{\min} = 0$ , the system is determined. With the increase of  $n$ , the number of possible states gets higher, then the entropy gets bigger. And the dispersion of the system becomes bigger, and it can provide less information. Thus, the less important this system is relative to other systems.

*5.2. Expert Evaluation of Membership Cloud.* For the evaluation of a certain index,  $n$  experts are invited to conduct the evaluation of a certain index, and the evaluation results are converted into a percentage form according to Section 3. The membership clouds represent the evaluation results of the  $n$  experts. First, the three digital features ( $E_x, E_n, H_e$ ) of the cloud model are calculated by the reverse cloud generator. Then, the expert evaluation results are restored by the forward cloud generator. Finally, if the

cloud drops are too discrete, it indicates that the expert evaluation opinions differ greatly, then we can apply for reevaluation.

(1) Reverse cloud generator

$$\begin{aligned} E_x &= \frac{E_{x1} + E_{x2} + \dots + E_{xn}}{n}, \\ E_n &= \frac{\max \{E_{x1}, E_{x2}, \dots, E_{xn}\} - \min \{E_{x1}, E_{x2}, \dots, E_{xn}\}}{n}, \\ S^2 &= \frac{1}{n} \sum_{i=1}^n (x_i - E_x)^2, \\ H_e &= \sqrt{S^2 - E_n^2}, \end{aligned} \quad (7)$$

where  $E_{x_i}$  indicates the percentage result of the  $i$ th expert evaluation and  $n$  indicates the number of experts. The digital features of the membership cloud ( $E_x, E_n, H_e$ ) are calculated by the above equations.

(2) Forward cloud generator

*Step 1.*  $E_{nn} = \text{Randn}(E_n, H_e)$ , which takes  $E_n$  as the expectation and produces a normally distributed random number  $E_{nn}$  with  $H_e$  as the standard deviation.

*Step 2.*  $x_i = \text{Randn}(E_x, E_{nn})$ , which takes  $E_x$  as the expectation and generates a normally distributed random number  $x_i$  with  $E_{nn}$  as a standard deviation.

*Step 3.*  $\xi_i = \exp[-(x_i - E_x)^2 / (2E_{nn}^2)]$ , the degree of membership is calculated according to the equation, and the pair  $(x_i, \xi_i)$  represents a cloud drop distributed over the universe  $U$ .

*Step 4.* Step 1 through Step 3 is performed cyclically until enough cloud drops are generated to restore the expert evaluation results in the form of a cloud model.

*5.3. Membership Cloud Gravity Center.* The result of the expert evaluation of  $f$  indexes subordinate to the criterion layer can be represented by  $f$ -dimensional membership clouds. The  $f$ -dimensional comprehensive membership cloud of the dimension can be formed by a membership cloud gravity center. This paper uses the vector  $g$  to represent the gravity center vector of this cloud which is

$$g = (g_1, g_2, \dots, g_f). \quad (8)$$

where  $g_i = E_{x_i} \cdot w_i (i = 1, 2, \dots, f)$ ,  $E_{x_i}$  represents the expected value of the  $i$ th membership cloud, and  $w_i$  represents the weight corresponding to the index which is calculated by the modified interval matrix module.

Assuming that the initial state of the system is ideal, the initial cloud center of gravity vector of the  $f$ -dimensional integrated membership cloud is

$$\mathbf{g}^0 = (g_1^0, g_2^0, \dots, g_f^0). \quad (9)$$

The cloud gravity center vector representing the current expert evaluation result is

$$\mathbf{g}' = (g'_1, g'_2, \dots, g'_f). \quad (10)$$

Then, normalize the changes in the gravity center vector of the  $f$ -dimensional integrated cloud is

$$g_i^G = \begin{cases} \frac{g'_i - g_i^0}{g_i^0}, & g'_i \leq g_i^0 \\ \frac{g'_i - g_i^0}{g'_i}, & g'_i > g_i^0 \end{cases} \quad (11)$$

where  $i = 1, 2, \dots, f$ .

Calculate the weighted deviation  $\delta$  from the weight vector  $\mathbf{W} = (w_1, w_2, \dots, w_f)$ :

$$\delta = \sum_{i=1}^f g_i^G * w_i. \quad (12)$$

Enter  $\delta$  into the evaluation cloud model to get the support level of this dimension index for different comments in the criterion layer [15]. The evaluation cloud model is shown in Figure 4.

In the process of quantifying the situation from the index layer to the criterion layer, the cloud gravity center evaluation method can be used to calculate the weighted deviation and obtain the safety situation value of the different dimension indexes in the criterion layer, and the process of quantifying the situation from the criterion layer to the target layer. In the traditional method [16], the dimension indexes of the default criterion layer are usually the same relative importance, but the relative importance of different indexes in the criterion layer is not distinguished. This has certain limitations on the quantitative value of the comprehensive security situation of the information system.

First, at a certain moment, the relative importance of the physical dimension, host dimension, network dimension, data dimension, and manager dimension of different information systems is different. The reason is that some information systems and external network channels are less or even isolation, the main factor affecting the security of the system type is behavior adjustment management [17], and some information systems often face threats such as vulnerabilities and malicious attacks, so it is necessary to focus on the protection of their host and network dimension indexes. Second, for the same information system, the main influencing factors affecting its security situation will change with time. This is due to the update

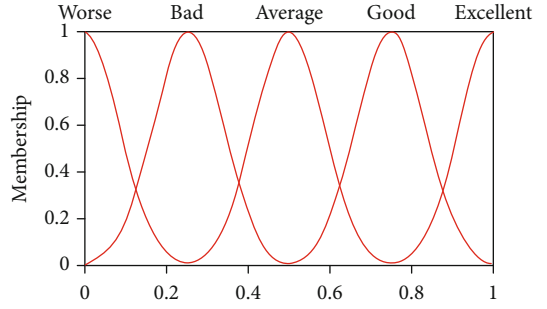


FIGURE 4: Evaluation cloud model.

of information system software and hardware. The change of managers will cause the weight vector of the criterion layer to change, which will affect the system the total security assessment value.

Given the above problems, based on the cloud gravity center-weighted deviation of each index in the known criterion layer, by reviewing the comments of the activated comments in the cloud model and the support of each comment, the dimension indexes of the criterion layer are determined relative to each comment. The support matrix  $\mathbf{P}$  is as shown in Table 3.

$X_1, X_2, X_3, X_4,$  and  $X_5$  in Table 3 correspond to the 5 dimensions of the criterion layer, respectively, and  $p_{ij}$  indicates the degree of support of the  $i$ th index to the  $j$ th comment ( $i, j = 1, 2, 3, 4, 5$ ).

Calculate the absolute entropy of each dimension index by using equation (13):

$$H_i = - \sum_{j=1}^n p_{ij} \ln p_{ij}, \quad (13)$$

when  $p_{i1} = p_{i2} = \dots = p_{in}$ , there is  $H_{\max} = \ln n$ . Calculate the relative entropy value of each dimension index by using equation (13)

$$\mu_i = - \frac{1}{\ln n} \sum_{j=1}^n p_{ij} \ln p_{ij}. \quad (14)$$

The weight of the corresponding index is expressed by  $(1 - \mu_i)$ , which is normalized:

$$\tau_i = \frac{1}{n - \sum_{i=1}^n \mu_i} (1 - \mu_i), \quad (15)$$

where  $\tau_i \in [0, 1]$  and  $\tau_1 + \dots + \tau_n = 1$ ,  $\tau_i$  is the entropy weight coefficient of the subordinate cloud corresponding to  $X_i$ .

The weight vector corresponding to each comment in the given evaluation cloud model is set as  $\mathbf{U} = (u_{\text{worse}}, u_{\text{bad}}, u_{\text{average}}, u_{\text{good}}, u_{\text{excellent}}) = (1/15, 2/15, 1/5, 4/15, 1/3)$  [2, 18].

The information system comprehensive security situation value operator is equation (16):

$$\mathbf{V} = \mathbf{1} - \boldsymbol{\tau} * \mathbf{P} * \mathbf{U}^T. \quad (16)$$

TABLE 3: Support matrix.

Criteria layer	Worse	Bad	Average	Good	Excellent
$X_1$	$P_{11}$	$P_{12}$	$P_{13}$	$P_{14}$	$P_{15}$
$X_2$	$P_{21}$	$P_{22}$	$P_{23}$	$P_{24}$	$P_{25}$
$X_3$	$P_{31}$	$P_{32}$	$P_{33}$	$P_{34}$	$P_{35}$
$X_4$	$P_{41}$	$P_{42}$	$P_{43}$	$P_{44}$	$P_{45}$
$X_5$	$P_{51}$	$P_{52}$	$P_{53}$	$P_{54}$	$P_{55}$

TABLE 4: Security situation level.

$V$	[0,0.2]	(0.2,0.4]	(0.4,0.6]	(0.6,0.8]	(0.8,1]
Level	Worse	Bad	Average	Good	Excellent

TABLE 5: Experts' evaluation percentage.

Expert $i$	$I_{31}$	$I_{32}$	$I_{33}$	$I_{34}$
1	97	86	90	96
2	92	89	92	93
3	94	90	94	95
4	89	87	94	94
5	92	86	93	94
6	95	89	92	95
7	90	85	95	96
8	88	88	91	94
9	98	88	90	95
10	96	87	91	95

This paper determines the security situation level according to [2, 14], as shown in Table 4. The system security situation level can be determined by combining the  $V$  value.

**5.4. Analysis of Algorithm Complexity.** In the proposed model, there are two modules. First, we modified the interval matrix to get the best deterministic matrix and obtained the best weight vector. This process traverses all interval matrix elements at least twice. The complexity of this process is  $O(n^2)$ . After we get the best weight vector, we need to evaluate each index according to the entropy weight-based cloud. The complexity of the whole process is  $O(n)$ . Finally, we calculate the situation security value through equation (16). Therefore, we can obtain the complexity of the whole model as follows.

$$\Omega = O(n^2) + O(n) \quad (17)$$

## 6. Results and Discussion

The model proposed in this paper is applied to the departure control system for smart mobile devices. The system security situation assessment is conducted every Tuesday, from October 1 to December 23, 2018, for a total of 12 times. The following experiment uses the evaluation of the network dimension of the system criterion layer on October 9, 2018,

as an example to illustrate the application process of the evaluation model.

**6.1. Normalization of Multisource Data.** For the four subindexes of the network dimension ( $I_3$ ) ( $I_{31}, I_{32}, I_{33}, I_{34}$ ) = (network topology, network access control, security audit, network traffic), 10 experts are invited to evaluate each sub-index. Take "identification" (in Figure 2) for example, when password guessing [19] or two-factor authentication schemes [20, 21] are implemented, the security situation will reach a serious state which needs the information system manager give emergency reaction to keep the system stay a good state. And experts will give a score between 80 and 100, which represents the situation is bad. Then according to Section 3, the evaluation of qualitative and quantitative indexes was unified into the score under the percentage system, and the scores of the subindexes are shown in Table 5.

**6.2. Determine Index Weights.** The interval judgment matrix is given by experts on the relative importance of the four subindexes:

$$A^0 = \begin{pmatrix} 1 & [3, 4] & [3, 5] & [3, 5] \\ [1/4, 1/3] & 1 & [1/2, 1] & [2, 5] \\ [1/5, 1/3] & [1, 2] & 1 & [1/3, 1] \\ [1/5, 1/3] & [1/5, 1/2] & [1, 3] & 1 \end{pmatrix}. \quad (18)$$

According to the method in Section 4, firstly judge the consistency degree of the interval matrix, and take the consistency degree threshold value to be 0.6 to obtain  $\gamma = 0.76 > 0.6$  [13], which shows that the consistency degree of the interval matrix meets the requirements, and no further interaction with the experts is needed. This matrix is used as the best interval matrix in Section 4.2.3. Then, the interval matrix is converged, and  $R = 100$ ,  $\omega = 10$ . After 7 iterations, the convergence interval matrix is

$$A^1 = \begin{pmatrix} 1 & [3.210, 3.463] & [3.653, 4.000] & [4.202, 4.417] \\ [0.289, 0.312] & 1 & [0.934, 0.953] & [2.029, 2.040] \\ [0.250, 0.274] & [1.049, 1.070] & 1 & [0.894, 0.905] \\ [0.226, 0.238] & [0.490, 0.493] & [1.104, 1.119] & 1 \end{pmatrix}. \quad (19)$$

Based on this matrix, the optimization process based on the adjusted deterministic matrix is obtained under the condition of the number of optimization times  $k = 1000$ , and the best deterministic matrix is

$$A^{best} = \begin{pmatrix} 1 & [3.300679] & [3.874924] & [4.261778] \\ [0.300351] & 1 & [0.942991] & [2.032611] \\ [0.259102] & [1.057097] & 1 & [0.899372] \\ [0.233799] & [0.490148] & [1.109949] & 1 \end{pmatrix}. \quad (20)$$



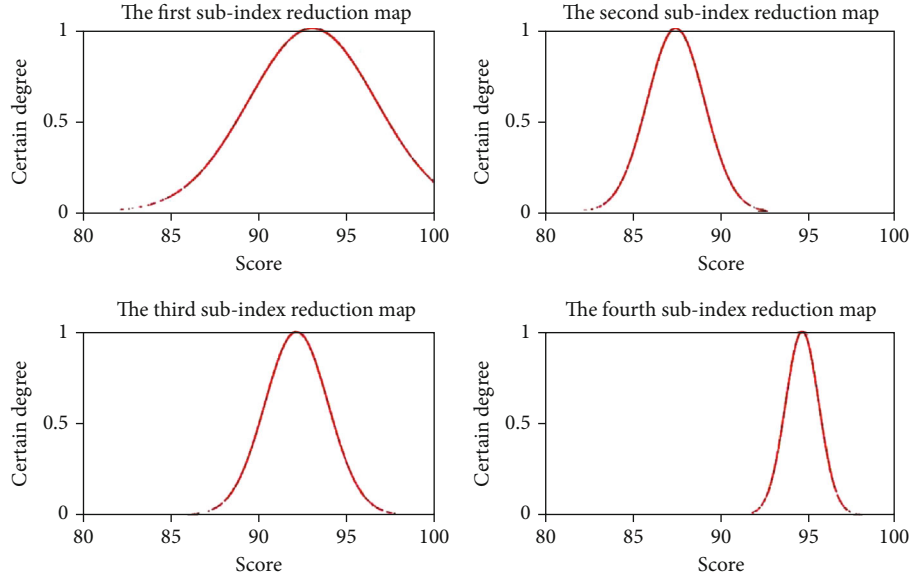


FIGURE 5: Reduction of four indexes' evaluation.

TABLE 6: Expected values and weights of each index.

Index $I_{3i}$	$I_{31}$	$I_{32}$	$I_{33}$	$I_{34}$
Expected value $E_3$	92.96	87.50	92.22	94.72
Weight $w_{3i}$	0.555 665	0.178 134	0.144 072	0.122 129

The consistency ratio is  $CR = 0.022 591 < 0.1$ . This matrix has satisfactory consistency. The weight vector obtained is  $w = (0.555 665, 0.178 134, 0.144 072, 0.122 129)$ .

6.3. *Situation Quantification and Grading.* The experts' evaluation results are restored by the cloud, as shown in Figure 5. Since the cloud droplets of each cloud model are more concentrated, it indicates that the experts' evaluation comments are more consistent, so there is no need to request experts' reevaluation.

The expected value vectors of the four subindexes of network dimension based on the graph and the weight corresponding to each expected value obtained based on Section 6.2 are shown in Table 6.

According to equations (11) and (12), the weighted deviation degree is  $\delta = -0.079 134$ , and the security situation value of the network dimension is 0.920 866. Inputting  $\delta$  into the evaluation cloud model indicates that the network dimension is in "excellent" state, as shown in Figure 6.

For the normal curve fitting of the evaluation cloud model, the support degree of the comment "good" is 0.122 04, the support degree of the comment "excellent" is 0.636 88. The remaining support degree  $1 - 0.122 04 - 0.636 88 = 0.241 08$  is allocated by the reciprocal ratio of the distance between the dimension and the expected value of the other three inactive reviews. The network dimension comment support vector  $(p_{31}, p_{32}, p_{33}, p_{34}, p_{35}) = (0.052 86, 0.072 56, 0.115 66, 0.122 04, 0.636 88)$ .

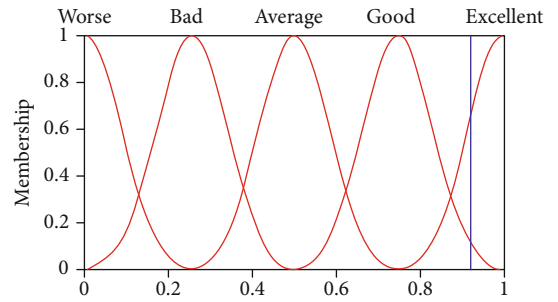


FIGURE 6: Evaluation cloud activation.

The evaluation support vector for the other four-dimensional indexes of the criterion layer is the same as the calculation process of the network dimension and will not be described here.

The obtained security level value vector of each dimension of the criterion layer is (0.677 2, 0.731 4, 0.920 9, 0.522 5, 0.643 4), and the comment support matrix  $P$  is shown in Table 7.

According to equations (13)–(15), the criterion layer index entropy weight coefficient vector can be calculated as:  $\tau = (0.143, 0.380, 0.121, 0.307, 0.049)$ . The comprehensive security situation value of this system is 0.752. Combined with Table 4, the security situation of the information system is in an "excellent" state, which is consistent with the actual situation.

The security situation assessment method in this paper, the entropy weight coefficient method [2], the improved Hidden Markov Model [4], and the AHP method [12] are applied to the evaluation of this system. The criterion layer security situation and total security situation are evaluated, as shown in Figures 7 and 8.

As can be seen from Figures 7 and 8, the fluctuation of the situation assessment value of the model in this paper

TABLE 7: Comment support.

Criteria layer	Worse	Bad	Average	Good	Excellent
$X_1$	0.045 93	0.072 19	0.104 12	0.682 61	0.095 54
$X_2$	0.000 67	0.001 02	0.201 11	0.975 38	0.001 82
$X_3$	0.052 86	0.072 56	0.115 66	0.122 04	0.636 88
$X_4$	0.002 94	0.056 40	0.964 18	0.024 02	0.032 19
$X_5$	0.074 71	0.122 19	0.227 29	0.441 00	0.134 80

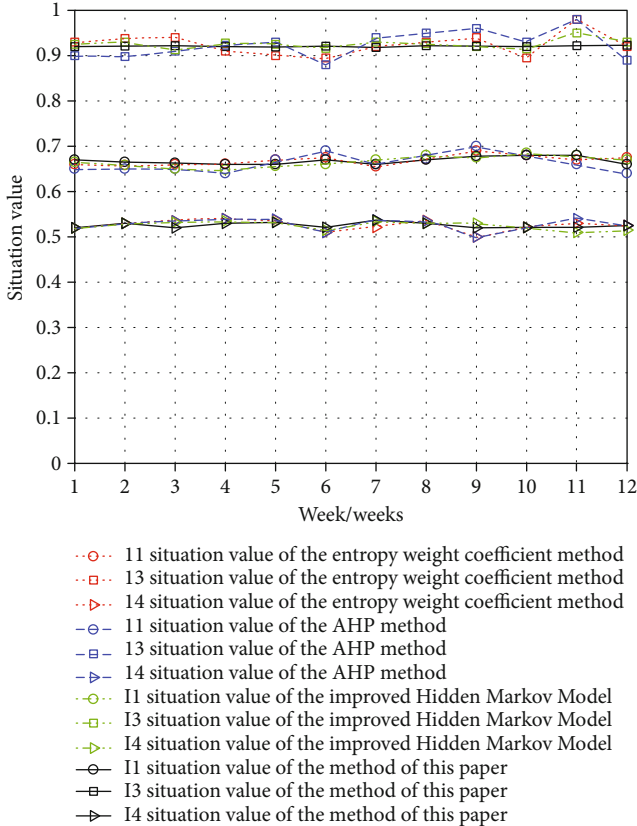


FIGURE 7: Criterion layer security situation.

is obviously smaller than that obtained by the entropy weight coefficient method [2], the improved Hidden Markov Model [4], and the AHP method [12]. There are two reasons: first, the model in this paper improves the objective degree of the weight vector by modifying the interval matrix and overcomes the shortcoming of the strong subjectivity of the traditional AHP method. At the same time, by judging the dispersion degree of the subordinate cloud droplets of the experts' evaluation results, abnormal index values can be found and reevaluation. Compared with the entropy weight coefficient method, unreasonable index weighting can be avoided. Therefore, the quantitative result of the model in this paper is more appropriate to the actual system security situation, which improves the reliability of this information system security situation assessment model.

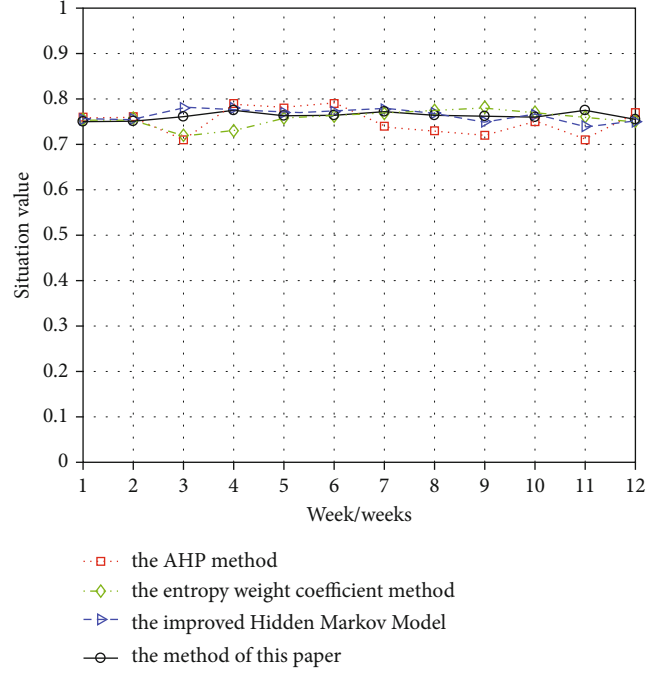


FIGURE 8: Total security situation.

Second, due to the difference of experts' ability, it is difficult to judge the relative importance of each dimension index in the criterion layer uniformly. Based on multisource data normalization, the entropy weight coefficient of each cloud model corresponding to the criterion layer index is used to avoid weighting directly for the criterion layer index. Therefore, the total situation value of the actual system can avoid large fluctuation and improve the stability of information system security situation assessment.

## 7. Conclusions

This paper proposes a MIMEC-based security situation assessment model of information system for smart mobile devices. This model modifies the interval judgment matrix, finds the best deterministic matrix to determine the index layer weight vector, and combines the entropy weight membership cloud to quantify and grading the security situation. Through the experiment on the departure control system for smart mobile devices, we found that the existing information system is always in a serious situation, which means the information system manager is supposed to take some measures to protect the system. We believe that our findings and our model can extend the models used in previous work and correct shortcomings of previous models. And compared the evaluation results with other methods, it shows that our model has good reliability and stability.

Our future work will focus on this study to assess extensive information system situation security for smart mobile devices. In addition, more realistic assessment methods such as Pythagorean Fuzzy Subsets [22], and Intuitionistic Fuzzy Petri Nets [23] will be used to improve the accuracy of the proposed model.

## Data Availability

The raw/processed data required to reproduce these findings cannot be shared at this time as the data also forms part of an ongoing study.

## Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

## Acknowledgments

This work was supported by the Civil Aviation Joint Research Fund Project of the National Natural Science Foundation of China under granted number U1833107.

## References

- [1] X. H. Qu and X. M. Shi, "Research of network security situation assessment based on AHP," *Techniques of Automation and Applications*, vol. 37, no. 11, pp. 43–45, 2018.
- [2] Y. Fu, X. P. Wu, and Q. Ye, "An approach for information systems security risk assessment on fuzzy set and entropy-weight," *Acta Electronica Sinica*, vol. 38, no. 7, pp. 1489–1494, 2010.
- [3] H. S. Luo, Y. J. Shen, and G. D. Zhang, "Information security risk assessment based on two stages decision model with grey synthetic measure," in *Proceedings of the 6th IEEE International Conference on Software Engineering and Service Science*, pp. 795–798, Beijing, China, 2015.
- [4] R. R. Xi, X. C. Yun, and Y. Z. Zhang, "An improved quantitative evaluation method for network security," *Chinese Journal of Computers*, vol. 38, no. 4, pp. 749–758, 2015.
- [5] F. Shu, M. Li, and S. T. Chen, "Research on network security protection system based on dynamic modeling," in *2017 IEEE 2nd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)*, pp. 1602–1605, Chengdu, China, 2017.
- [6] A. Hemanidhi, S. Chimmanee, and P. Sanguansat, "Network risk evaluation from security metric of vulnerability detection tools," in *TENCON 2014-2014 IEEE Region 10 Conference*, pp. 1–6, Bangkok, Thailand, 2014.
- [7] J. H. Eom, S. H. Park, and Y. J. Han, "Risk assessment method based on business process-oriented asset evaluation for information system security," in *Proceedings of the 7th International Conference on Computational Science*, pp. 1024–1031, Beijing, China, 2007.
- [8] A. S. Rimsha and A. A. Zakharov, "Method for risk assesment of industrial networks' information security of gas producing enterprise," in *2018 Global Smart Industry Conference*, pp. 1–5, Chelyabinsk, Russia, 2018.
- [9] C. Fang, J. Liu, and Z. Lei, "Fine-grained HTTP web traffic analysis based on large-scale mobile datasets," *IEEE Access*, vol. 4, pp. 4364–4373, 2016.
- [10] Y. Li, J. Wang, D. Zhao, G. Li, and C. Chen, "A two-stage approach for combined heat and power economic emission dispatch: combining multi-objective optimization with integrated decision making," *Energy*, vol. 162, no. 1, pp. 237–254, 2018.
- [11] General Administration of Quality Supervision, Inspection and Quarantine of the People's Republic of China, Standardization Administration of the People's Republic of China, *Information security technology—classification guide for classified protection of information systems security: GB/T 22240—2008*, Standards Press of China, Beijing, 2008.
- [12] X. Cheng, *Information System Security Situation Assessment and Risk Control Method Based on Operation-Flow*, Civil Aviation University of China, Tianjin, 2016.
- [13] J. J. Zhu, S. X. Liu, and M. G. Wang, "Novel weight approach for interval numbers comparison matrix in the analytic hierarchy process," *Systems Engineering-Theory & Practice*, vol. 25, no. 4, pp. 29–34, 2005.
- [14] D. Li, M. Haijun, and S. Xuemei, "Membership clouds and membership cloud generators," *Journal of Computer Research and Development*, vol. 32, no. 6, pp. 15–20, 1995.
- [15] Z. H. Feng, J. C. Zhang, K. Zhang, and W. Liu, "Techniques for battlefield situation assessment based on cloud-gravity-center assessing," *Fire Control & Command Control*, vol. 36, no. 3, pp. 13–15, 2011.
- [16] Z. W. Li, *The Study on the Information System Risk Assessment and Management Countermeasure*, Beijing Jiaotong University, Beijing, 2010.
- [17] Y. B. Li, *Analysis and Design of MIS (Management Information System) on Nuclear Power Construction of SD*, Shandong University, Jinan, 2013.
- [18] D. M. Zhao, Y. Q. Zhang, and J. F. Ma, "Fuzzy risk assessment of entropy-weight coefficient method applied in network security," *Computer Engineering*, vol. 30, no. 18, pp. 21–23, 2004.
- [19] D. Wang, Z. J. Zhang, P. Wang, J. Yan, and X. Y. Huang, "Targeted Online Password Guessing: An Underestimated Threat," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (ACM CCS 2016)*, pp. 1242–1254, Vienna, Austria, 2016.
- [20] D. Wang and P. Wang, "Two birds with one stone: two-factor authentication with security beyond conventional bound," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 4, pp. 708–722, 2018.
- [21] D. Wang, W. Li, and P. Wang, "Measuring two-factor authentication schemes for real-time data access in industrial wireless sensor networks," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 9, pp. 4081–4092, 2018.
- [22] R. R. Yager, "Pythagorean fuzzy subsets," in *2013 Joint IFSA World Congress and NAFIPS Annual Meeting (IFSA/NAFIPS)*, pp. 57–61, Edmonton, Canada, 2013.
- [23] M. Fei-xiang, L. Ying-jie, Z. Bo, S. Xiao-yong, and Z. Jing-yu, "Intuitionistic fuzzy petri nets for knowledge representation and reasoning," *Journal of Digital Information Management*, vol. 14, no. 2, pp. 104–113, 2016.