Hindawi
Security and Communication Networks
Volume 2020, Article ID 6654283, 11 pages
https://doi.org/10.1155/2020/6654283

Research Article

A Key Business Node Identification Model for Internet of Things Security

Lixia Xie,[1] **Huiyu Ni**,[1] **Hongyu Yang**,[1] **and Jiyong Zhang**[2]

[1]*School of Computer Science and Technology, Civil Aviation University of China, Tianjin 300300, China*
[2]*School of Computer and Communication Science, Swiss Federal Institute of Technology in Lausanne, CH-1015, Lausanne, Switzerland*

Correspondence should be addressed to Hongyu Yang; hyyang@cauc.edu.cn

Received 8 October 2020; Revised 25 October 2020; Accepted 1 December 2020; Published 12 December 2020

Academic Editor: Weizhi Meng

Based on the research of business continuity and information security of the Internet of Things (IoT), a key business node identification model for the Internet of Things security is proposed. First, the business nodes are obtained based on the business process, and the importance decision matrix of business nodes is constructed by quantifying the evaluation attributes of nodes. Second, the attribute weights are improved by the analytic hierarchy process (AHP) and entropy weighting method from subjective and objective dimensions to form the combination weight decision matrix, and the analytic hierarchy process and entropy weighting VIKOR (AE-VIKOR) method are used to calculate the business node importance coefficient to identify the key nodes. Finally, according to the NSL-KDD dataset, the network security events of IoT network intrusion detection based on machine learning are monitored purposefully, and after the information security event occurs in the smart mobile phone, which impacts through IoT on the business system, the impact of the key business node on business continuity is analyzed, and the business continuity risk value is calculated to evaluate the business risk to prove the effectiveness of the model. The experimental results of the civil aviation departure business show that the AE-VIKOR method can effectively identify key business node, and the impact of the key business node on business continuity is analyzed, which further proves the efficiency and accuracy of the model in identifying the key business node.

1. Introduction

Nowadays, with the rapid development of the Internet of Things, related research fields are more concerned about information security and business continuity. The Internet of things (IoT) and mobile technology [1] make multisystem cooperation more convenient, the multisystem cooperation is closely related to its business continuity. Therefore, due to the application of the IoT technology, when an information security event occurs [2], it may lead to delay or stagnation of business execution, which will inevitably affect business continuity. The security of the Internet of Things is one of the hotspots in various academic fields, such as information security and machine learning. In particular, machine learning is used for intrusion detection of the IoT. Belouch et al. [3] used a machine learning analysis framework to detect any anomalous events occurring in the network traffic flow. Liu et al. [4] examined specific attacks in the NSL-KDD dataset that can impact sensor nodes and networks in IoT settings and studied eleven machine learning algorithms to detect the introduced attacks. Xie et al. [5] designed a monitoring mechanism to detect link-flooding attack (LFA) based on the availability of the crucial links and trace route flows for IoT security. Yang et al. [6] proposed a malicious node detection model based on reputation with enhanced low energy adaptive clustering hierarchy (Enhanced LEACH) routing protocol for wireless network security.

Based on the management of business continuity, at present, there are many achievements in the research of business continuity security [7–13]. Key business node identification is very important for business recovery, which is one of the research hotspots in the field of risk assessment

for the business process. Ali et al. [14] proposed a business continuity risk assessment framework for IoT services. Given the problems of information security risk assessment and business continuity management, Torabi et al. [15] put business continuity risk management into the framework of information security risk assessment through business continuity risk analysis. Belov et al. [16] proposed a risk value calculation of the business completion rate by studying the situation of the business resource completion rate and quantitatively assessed the business system risk. Hariyanti et al. [17] proposed a new information security risk assessment model based on the business process to improve the model based on the organization's assets. Silmie et al. [18] proposed a business continuity plan framework, which is a procedural guidance to create plans that prevent, prepare, respond, manage, and recover a business from any disruption. Diesch et al. [19] developed a comprehensive model of relevant management success factors for organizational information security to make appropriate decisions. The Vise Kriterijumska Optimizacija I Kompromisno Resenje in Serbian (VIKOR) method [20] is one of the common methods of multiattribute decision-making, which is often used in risk assessment, economics, management, and other hot fields. Yang et al. [21] proposed a hybrid multicriteria decision-making model based on the intuitionistic fuzzy number, extended Decision-Making Trial and Evaluation Laboratory (DEMATEL) method, and VIKOR algorithm to assess the information system security risk. Mohsen et al. [22] proposed an extended VIKOR method based on entropy measure for the failure modes of the geothermal power plant risk assessment. Han et al. [23] used the modified VIKOR method to identify and preferentially reinforce critical lines for skeleton-network of power systems. The Technique for Order Performance by Similarity to Ideal Solution (TOPSIS) method [24, 25] is also one of the classic multiattribute evaluation methods, which is compared with the method in this paper. In summary, the paper uses the AE-VIKOR method with combined weighting for eliminating the subjective influence of some attributes to identify effectively the key business node. The model analyzes the impact of key business nodes on business continuity and further proves the effectiveness of key identification.

The main contributions of this paper can be summarized as follows. A key business node identification model for Internet of Things security is proposed. The model in this paper identifies effectively the key business node and analyzes its impact on business continuity. The model is mainly focused on the following.

(1) The combined weighting from the subjective and objective dimensions is used to improve the attribute weights of the VIKOR method to identify the key business node. Compared with the single weighting method, such as the AHP method, the combined weighting makes the results more accurate, which is verified by experiments.

(2) After the information security event occurs in the smart mobile phone, which impacts through IoT on the business system, the model can be used to analyze the impact of the key business node on business continuity. For the specific business of the business process, this model analyzes the number of business users, business average execution time, and resource utilization.

(3) According to the business user number, business average execution time, and resource utilization, the business continuity risk value is calculated and realizes properly the risk assessment of business continuity in the model.

(4) In this model, the decision coefficient is selected reasonably by the experiment to realize accurate identification of key business node. Compared with other multiple attribute decision-making cases, such as using the VIKOR method to select coal suppliers, it is novel that the paper analyzed the influence of different decision mechanism coefficients on the identification results. After the key nodes are identified by this model, the key nodes are further analyzed to facilitate the analysis of the impact of business continuity.

The organization of this paper is described as follows. In section 2, a key business node identification model for the Internet of Things security is proposed. The key business node identification model is composed of four modules: data preparation module, data operation module, decision module, and analysis module. In section 3, the data preparation module and the data operation module are described in detail. The decision module and analysis module are expounded in section 4. In section 5, the effectiveness of the model is verified by analyzing the business continuity of the departure business and the loading business. Conclusion is given in section 6.

2. Key Business Node Identification Model

The key business node identification model is composed of four modules: data preparation module, data operation module, decision module, and analysis module. The framework diagram of the model is shown (see Figure 1).

The function design of each module in the model is as follows.

(1) Data preparation module: according to the business process, the business node set to be evaluated is obtained, and the node importance decision matrix is obtained from the business node set and the evaluation attribute.

(2) Data operation module: in this module, AHP subjective weighting and entropy objective weighting methods are used. The decision matrix is weighted by the combined weight from the subjective and objective dimensions, and the node importance combined weight decision matrix is formed.

(3) Decision module: in this module, the combination weights are used to improve the attribute weight of the VIKOR method to get the node importance

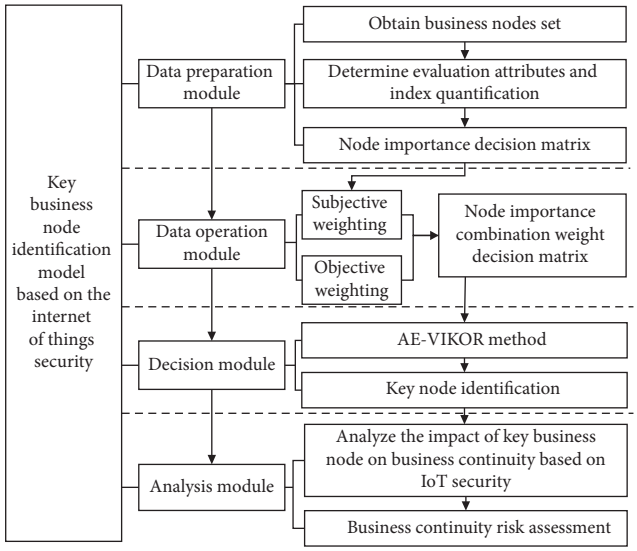

Figure 1: Key business node identification model for business process.

coefficient and rank it. The key business node is identified in this model.

(4) Analysis module: when information security events occur, business continuity faces risks. The impact of key business nodes on business continuity is analyzed in this module, the business continuity risk value is calculated, and business continuity risk assessment is carried out.

3. Data Preparation Module and Data Operation Module

3.1. Data Preparation Module. IoT allows billions of devices as well as virtual environments to exchange data with each other intelligently. For example, smartphones have become an important personal assistant and indispensable part of people's everyday life and work. With such a large amount of data, the model first analyzes business processes to better analyze business continuity. Through the analysis of the business process, this model extracts all businesses into nodes to form the business node set to be evaluated, which is recorded as $M = \{n_1, n_2, n_3, \ldots, n_m\}$. M is the business node set to be evaluated. The set indicates that there are m nodes in the business process, which are numbered as $n_1, n_2, n_3, \ldots, n_m$.

Considering business importance from multiple perspectives makes the identification of key business more effective. Therefore, this paper selects three factors to evaluate business importance, which are business node relevance, business user, and business priority.

The specific process of indicator quantification of the business node importance attribute is as follows.

First, according to the theory of business process and complex network node centrality [26], business relevance is considered to assess business importance, and business relevance value can be measured according to the direct relationship between other business nodes and the business node. The value of business node relevance is calculated according to (1). The larger the business node relevance value is, the more important the business is:

$$g_i = \frac{h_i}{(m-1)}, \tag{1}$$

where g_i is the ratio of the number of connected nodes of business node i to the total number of nodes except for node i. The larger the value is, the more important the business node is. h_i is the number of nodes directly connected to node i. m is the total number of business nodes.

Second, the business user importance is used to evaluate business importance. The types of business users are divided into staff, ordinary users, and both staff and ordinary users. In this paper, levels one, two, and three are assigned to business user types.

Different types of users have different initial values. The larger the value is, the more important the business is. The importance levels for business user type values are defined in Table 1.

Finally, business priorities based on different business service types are used to evaluate business importance. The higher the business priority level, the higher the importance of business.

The business priority assignment is based on the service characteristics and application types of the business. The business priority level is divided into levels one, two, three, and four. The assignment is shown in Table 2.

The data preparation module forms the node importance decision matrix $\mathbf{X}$ through the quantification of attributes and the nodes obtained. Due to the different dimensions of each attribute, matrix $\mathbf{X}$ is normalized by (3) for comparison. The standardized matrix is written as $\mathbf{R}$.

$$\mathbf{X} = \begin{bmatrix} x_{11} & x_{12} & x_{13} \\ x_{21} & x_{22} & x_{23} \\ \vdots & \vdots & \vdots \\ x_{m1} & x_{m2} & x_{m3} \end{bmatrix}, \tag{2}$$

$$r_{ij} = \frac{\left(x_{ij} - x_j^{\min}\right)}{\left(x_j^{\max} - x_j^{\min}\right)}, \tag{3}$$

where $x_j^{\max} = \max\{x_{i1}, x_{i2}, x_{i3}\}$ and $x_j^{\min} = \min\{x_{i1}, x_{i2}, x_{i3}\}$ in (3).

3.2. Data Operation Module. To eliminate some subjective influence of attributes and enhance the accuracy of the model, this paper uses the combined subjective and objective weighting method to determine the attribute weight.

The AHP method is one of the common methods to calculate the subjective weight. First, three attributes are compared. The business relevance is the local attribute of the business nodes, and its impact is relatively low. When the business user directly affects business operations, the impact of the user is stronger than that of the business relevance,

Table 1: Importance level of business user type.

Category	Value
Ordinary users	1
Staff member	2
Both staff and ordinary users	3

Table 2: Business priority assignment.

Business	Service	Application type	Business priority
Background	Without time delay	No special requirement for the business transmission time	1
Interactive	On demand response	Online data interaction of business characterized by the request response mode	2
Flow pattern	Time delay	Real-time business with low interaction	3
Conversation	Time delay strictly	Real-time business with high quality interaction	4

and the impact of the business type is greater than others. Therefore, the comparison of the attribute of node importance evaluation is shown in Table 3.

where 2 and 4 indicate that the influence degree of attribute i and attribute j is between 3 and 5.

The subjective weighting steps are as follows.

Step 1: according to the subjective influence of business attributes on business importance, an initial comparison matrix $\mathbf{A}$ is constructed.

$$\mathbf{A} = \begin{bmatrix} 1 & \frac{1}{3} & \frac{1}{5} \\ 3 & 1 & \frac{1}{3} \\ 5 & 3 & 1 \end{bmatrix}. \tag{4}$$

Matrix $\mathbf{A}$ is normalized to form matrix $\mathbf{B}$ according to the following:

$$\mathbf{B} = \frac{\mathbf{A}_{ij}}{\sum_{j=1}^{3} \mathbf{A}_{ij}}, \tag{5}$$

$$\mathbf{B} = \begin{bmatrix} \frac{1}{9} & \frac{1}{13} & \frac{1}{23} \\ \frac{1}{9} & \frac{3}{13} & \frac{5}{23} \\ \frac{1}{9} & \frac{9}{13} & \frac{13}{23} \end{bmatrix}. \tag{6}$$

Step 2: calculate the sum of each row of matrix $\mathbf{B}$ and get set $\mathbf{S}$ which is {0.3185, 0.7815, 1.9000}. The set is standardized to get the other set S_1 which is {0.1062, 0.2605, 0.6333}. The element of set S_1 is the subjective weight.

The AHP method coordinates the importance of each attribute to avoid the contradiction of each scheme.

Table 3: Importance level of business user type.

Meaning	Value
Attribute i has the same effect as attribute j	1
Attribute i has a stronger influence than attribute j	3
Attribute i is an absolutely stronger influence than attribute j	5

Therefore, it is necessary to meet the consistency test. After the consistency test, the calculation of consistency test index CI is shown as follows:

$$\mathrm{CI} = \frac{(\lambda_{\max} - n)}{(n-1)}, \tag{7}$$

$$\mathbf{AW} = \lambda_{\max}\mathbf{W}, \tag{8}$$

where $\lambda_{\max}$ is the maximum eigenvalue and $\mathbf{W}$ is the maximum eigenvector in (8).

After testing, the subjective weight assignment conforms to the consistency test index. Therefore, the subjective weight of each attribute is obtained which are $w_1^A = 0.1062$, $w_2^A = 0.2065$, and $w_3^A = 0.6333$.

Entropy weighting is one of the classical methods to calculate objective weight. Using entropy value to modify the index weight provides a more reliable basis for the evaluation of business importance. The objective weight is calculated as follows:

$$S_{ij} = \frac{r_{ij}}{\sum_{i=1}^{m} r_{ij}}, \tag{9}$$

$$e_j = -k \sum_{j=1}^{n} S_{ij} \ln S_{ij}, \quad j = 1, 2, \ldots, n, \tag{10}$$

$$w_j = \frac{1 - e_j}{\sum_{j=1}^{n} 1 - e_j}, \tag{11}$$

where S_{ij} is the proportion of each indicator of each node in (9), and e_j is the information entropy of the j-th index. The objective weight of each attribute is obtained, which are defined as w_1^O, w_2^O, and w_3^O.

Combined weight combines subjective weight and objective weight. The weight matrix $\mathbf{Y}$ is constructed based on the subjective and the objective method. The combined weight of attributes is calculated by (9)–(11) which is defined as $w^z = (w_1^z, w_2^z, w_3^z)$:

$$\mathbf{Y} = \begin{bmatrix} w_1^A & w_1^O \\ w_2^A & w_2^O \\ w_3^A & w_3^O \end{bmatrix}, \tag{12}$$

$$\left[\left(\mathbf{R}^T\mathbf{Y}\right)^T\left(\mathbf{R}^T\mathbf{Y}\right)\right]\mathbf{X}^* = \lambda_{\max}\mathbf{X}^*, \tag{13}$$

$$\mathbf{W} = \mathbf{Y}\mathbf{X}^*, \tag{14}$$

$$w_i^z = \left(\frac{w_1^*}{\sum_{j=1}^3 w_j^*}, \frac{w_2^*}{\sum_{j=1}^3 w_j^*}, \frac{w_3^*}{\sum_{j=1}^3 w_j^*}\right), \tag{15}$$

$$\mathbf{C} = w_i^z \times \mathbf{R}, \tag{16}$$

where $\lambda_{\max}$and $\mathbf{X}^*$ are the largest eigenvalue and the largest eigenvector of R, respectively, in (13). The standardized decision matrix $\mathbf{C}$ of node importance combined weight is calculated by (16).

4. Decision Module and Analysis Module

4.1. Decision Module. The importance coefficient of business is calculated and sorted based on the AE-VIKOR method in the decision module. The AE-VIKOR method improves the evaluation attribute weight of the VIKOR method by combined weighting in the data operation module detailed in section 3.

VIKOR method is one of the common methods of the multiattribute decision model. The method considers both the maximum group utility and the minimum individual regret effect of the object; VIKOR method focuses on ranking and selecting from a set of alternatives and determines compromise solutions for a problem with conflicting criteria, which can help the decision-makers to reach a final decision.

The value of the maximum group utility is measured by U_i, the value of the minimum individual regret effect is expressed by K_i, and Q_i is the decision value, which is calculated by the following:

$$U_i = \sum_{i=1}^{3} w_i^z c_{ij}, \tag{17}$$

$$K_i = \max_i\left(w_i^z c_{ij}\right), \tag{18}$$

$$Q_i = v\frac{U_i - U^*}{U^- - U^*} + (1-v)\frac{K_i - K^*}{K^- - K^*}, \tag{19}$$

where v is the coefficient of the decision-making mechanism in (19), $U^* = \min_i U_i$, $U^- = \max_i U_i$, $K^* = \min_i K_i$, and $K^- = \max_i K_i$. Through comparative experimental analysis in section 5, in order not to lose the generality, this paper selects $v = 0.5$.

AE-VIKOR method is also a compromise ranking method, the feasible solution of which is closest to the ideal solution. Therefore, the AE-VIKOR method is without loss of generality to meet the following two conditions.

Condition 1. Acceptable advantage. The first two nodes in sorting are Q_i and Q_j. The conditions shown in formula (16) need to be met, where m is the number of business nodes.

$$Q_i - Q_j \geq \frac{1}{(m-1)}. \tag{20}$$

Condition 2. Acceptable stability. The importance coefficients of key business nodes rank first in U_i and K_i.

If the aforementioned two conditions are met at the same time, the model recognition results are considered valid. The value of Q_i calculated based on the AE-VIKOR method is the business importance coefficient. The key business node is the largest business importance coefficient. Through the calculation of the AE-VIKOR method, the business importance coefficient is between [0, 1].

4.2. Analysis Module. The information security of IoT is closely related to business continuity management in the Internet era. When an information security event occurs in the system, it will affect the business continuity for the business process.

When a threat makes use of the vulnerability of IoT, information security events will appear, such as natural disaster events, infrastructure failures, network attacks, technical failures, and malicious code attacks. Therefore, it shows the relationship between information security and business continuity (see Figure 2).

The risk value of business continuity is calculated by combining the importance coefficient of key business according to the number of business users, average execution time of business, and resource utilization in this paper.

In this paper, the maximum of business user's numbers, average execution time, and resource utilization are, respectively, set as $u_{\max}, r_{\max}, t_{\max}$. When an information security event occurs, the number of business users, business execution time, and resource utilization rate at i time are defined as u_i, r_i, t_i. The business continuity risk value is calculated by the following:

$$P_i = 1 - \left(\frac{1}{3}\right)\frac{\sum(u_i, r_i, t_i)}{(u_{\max}, r_{\max}, t_{\max})}, \tag{21}$$

$$\Delta P = P_1 - P_2, \tag{22}$$

$$L = Q_i * \Delta P, \tag{23}$$

where Q_i represents the business importance coefficient, which can be calculated by the AE-VIKOR method in section 3. L represents the business continuity risk value, which is an important basis for the business continuity risk assessment level.

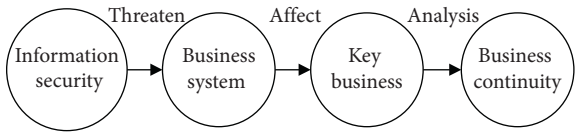

Figure 2: Relationship between information security and business continuity.

On calculating according to (21)–(23), the business continuity risk value L is an important basis for the business continuity risk assessment level. Because the value range ΔP is between 0 and 1, and the business importance coefficient is between 0 and 1, business continuity risk is classified according to business continuity risk value. When the risk value of business continuity is higher than 0.15, it is considered that business continuity is at higher risk. Business continuity changes with the change of business execution time. The experimental results based on mobile devices show that, after the completion of service execution time, the business continuity risk value calculated by the model does not exceed 0.15. Therefore, the use of academic language to describe business continuity risk is shown in Table 4. The business risk value is between 0 and 0.15, so the risk level of business continuity is shown in Table 4.

Table 4: The risk level of business continuity.

Business continuity risk value	Business continuity risk level
0~0.05	Low
0.05~0.10	Medium
0.10~0.15	High
$L \geq 0.15$	Higher risk

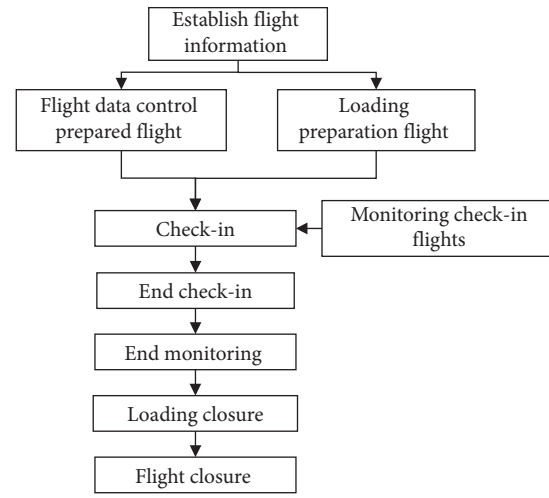

Figure 3: Framework diagram of departure business.

5. Experimental Results and Analysis

The civil aviation industry is one of the key industries of information security. Due to the convenience of IoT, it is very common for the public to handle the departure business on mobile devices. In particular, the check-in service is carried out through the IoT technology on the smart mobile devices. However, information security appears in the smart mobile devices, and other services connected through IoT technology will also be affected. As one of the core business systems in the field of civil aviation, departure system security is of great significance. To ensure the operation safety of the civil aviation business, this paper studies the potential security risks and possible risks of civil aviation information. Therefore, it is of great significance to analyze the implementation and business continuity of the key services of mobile devices.

5.1. Key Node Identification. According to the NSL-KDD dataset, the network security events of IoT network intrusion detection based on machine learning are monitored purposefully, and the risk of business continuity caused by the key business is analyzed. Once the information security event occurs in the smart mobile phone, which impacts through IoT on every business of the system, it will cause a great threat to civil aviation security.

Therefore, the experimental object of this paper is the departure business process of civil aviation. Its business process is shown (see Figure 3). Specific experimental steps of calculating the business importance coefficient are as follows.

Step 1. Obtain the business node set.

This experiment needs to evaluate the importance of all business nodes in the departure business process. Therefore, all businesses in the departure business process are extracted into nodes to form the business node set to be evaluated, which is recorded as $\mathbf{N} = \{n_1, n_2, n_3, n_4, n_5, n_6, n_7, n_8, n_9\}$, and represents establish flight information, flight data control prepared flight, loading preparation flight, check-in, monitoring the check-in flights, end check-in, end monitoring, loading closure, and flight closure, respectively.

Step 2. Construct the decision matrix of node importance.

The decision matrix of node importance is formed by the node and the attributes of each node. According to the assignment of node attribute indicators in the data preparation module, the assignment of departure business node importance attribute indicators is shown in Table 5.

The node importance decision matrix $\mathbf{X}$ is formed according to the business nodes and quantitative values of each attribute shown in Table 5.

After (3) is standardized, the standardized node importance decision matrix $\mathbf{R}$ is formed:

$$\mathbf{R} = \begin{bmatrix} 0.2917 & 0.4330 & 0.1961 \\ 0.4376 & 0.2887 & 0.1961 \\ 0.2917 & 0.4330 & 0.3922 \\ 0.5835 & 0.4330 & 0.5883 \\ 0.1459 & 0.2887 & 0.3922 \\ 0.2917 & 0.2887 & 0.1961 \\ 0.1459 & 0.2887 & 0.1961 \\ 0.2917 & 01443 & 0.1961 \\ 0.2917 & 0.2887 & 0.1961 \end{bmatrix}. \quad (24)$$

Table 5: Assignment of the important attribute index of departure business nodes.

Node	Business relevance	Business user	Business priority
n_1	0.2500	3	1
n_2	0.3750	2	1
n_3	0.2500	3	2
n_4	0.5000	3	3
n_5	0.1250	2	2
n_6	0.2500	2	2
n_7	0.1250	2	1
n_8	0.2500	1	1
n_9	0.2500	2	1

Step 3. Calculate the combined weight.

The combined weight is calculated. The subjective weight is $w^A = \{0.1062, 0.2605, 0.6333\}$, which is calculated by the AHP method. According to the objective weight calculated by the entropy method, $w^O = \{0.3273, 0.3298, 0.3429\}$ according to (9)–(11), and the combined weight of the two is $w^Z = \{0.2228, 0.2756, 0.5016\}$ according to (13)–(16).

Step 4. Key business node identification.

Node importance ranking based on the AE-VIKOR method in section 4 and the importance coefficient of departure business node are calculated as $Q_i = \{0.1975, 0.1464, 0.5199, 1.000, 0.4844, 0.4947, 0.1048, 0.057, 0.1176\}$ according to (13)–(15). The recognition results of the model meet two conditions after testing according to (16)–(19), and then the identification result of the key node identification model is regarded as valid. It can be seen that the most important factor of n_4 is the node. It is the check-in business that is the key business of the departure system.

5.2. Business Continuity Analysis. When a threat makes use of the vulnerability of IoT, an information security event occurs in the passenger check-in system, and the maximum number of business users, average execution time, and resource utilization rate of the passenger check-in system at T_0 time, respectively, correspond to 1000, 10 s, and 90%.

After the information security event occurs in the check-in system at T_0 time, the check-in system data within 1 h can be obtained through monitoring. Table 6 shows the execution of the check-in business at T_1, T_2, T_3, T_4 after the information security event.

To compare with the check-in, when the information security event occurs in the loading system at the time, the system data within 1 h is monitored and obtained. Problems in the loading system affected the loading fight business and loading closure business.

Execution of the loading preparation business after the information security event is shown in Table 7. The execution of the loading closure business after the information security event is shown in Table 8.

The data in Tables 6–8 show, after the occurrence of information security incidents, the three factors related to business continuity, namely, the number of business users, average execution time of business, and change of resource utilization rate with time.

The time of the loading system is inconsistent with the time of the aforementioned passenger check-in system, and the time of information security incident is inconsistent, while the monitoring time and time interval are consistent. Therefore, the business continuity risk value and assessment level are shown in Figure 4 at the same time.

The data of check-in business and loading business at every moment shows the degree of business continuity risk in Figure 4.

When an information security event occurs at T_0 time, it can be seen from Figure 4 that the business continuity risk value of check-in business increases rapidly after the time, while that of the loading fight business is relatively slow compared with check-in business. The data of the loading closure business shows it has the least impact on business continuity and the change degree of business continuity risk of the loading closure is the least.

At T_4 time, the value of the business continuity risk of the check-in business is 0.1426, and it is close to the higher risk. The data shows that the business continuity risk value of loading fights business within T_4 time is slowly increasing, and the risk of the loading fights business at T_4 time is 0.0654, and the corresponding risk level of business continuity is medium. At T_4 time, the risk of the loading closure business is 0.0086. Its risk increases more slowly with the change of time. The corresponding risk level of business continuity is low at T_4 time.

Therefore, the experiment further proves the validity and accuracy of the key business node identification model based on the AE-VIKOR method, and the impact of key nodes on business continuity is clearly demonstrated in Figure 4.

5.3. Comparison of Key Business Identification Methods. In this paper, the AE-VIKOR method is used to calculate the importance coefficient of civil aviation departure business nodes, and the AE-VIKOR method is compared with the other five methods. The importance coefficient calculated by each method for each node is shown in Table 9. The calculation method and business node ranking of several business nodes are shown (see Figure 5) to clearly describe the difference between each method. Therefore, the value in Figure 5 corresponds to the importance coefficient calculated in Table 9.

As can be seen from Figure 5, the AE-VIKOR method is more accurate than the other four methods. AHP-VIKOR and Entropy-VIKOR methods consider attribute weight from a single perspective, and then, the evaluation results from subjective or objective perspectives are biased. The VIKOR method does not consider attribute weight and it is not an accurate assessment of business importance from multiple perspectives. The DEMATEL and AHP methods are used to calculate the subjective weight. By comparison, the weight calculated by the AHP method is better than that

Table 6: Execution of the check-in business after an information security event.

Time	Number of business users	Business average execution time/s	Resource utilization
T_0	1000	10.0	90
T_1	800	10.5	85
T_2	550	12.0	65
T_3	300	12.5	50
T_4	100	13.0	25

Table 7: Execution of the loading fight business after an information security event.

Time	Number of business users	Business average execution time/s	Resource utilization
T_0	100	5.0	98
T_1	80	6.5	81
T_2	55	7.2	69
T_3	30	7.8	50
T_4	10	8.0	28

Table 8: Execution of the loading closure business after an information security event.

Time	Number of business users	Business average execution time/s	Resource utilization (%)
T_0	800	3.0	95
T_1	675	4.0	72
T_2	574	4.3	63
T_3	350	4.8	57
T_4	190	5.0	26

by the DEMATEL method. For example, there is not much difference between the value of n_1 and that of n_2 calculated by the DEMATEL-Entropy-VIKOR method, and the difference in importance is not clearly expressed. However, the AE-VIKOR method clearly shows the difference in importance coefficients between the two nodes.

In this paper, the combined weight is applied to the TOPSIS method and compared with the AE-VIKOR method. The results show that the business importance coefficients of n_1, n_3, n_5 calculated by the TOPSIS method are also biased compared with the AE-VIKOR method (see Figure 5). Therefore, this paper uses the AHP method to calculate the subjective weight of attributes and uses the entropy method to calculate objective weights. From these two dimensions, the combined weights are considered to improve the attribute weights of the VIKOR method and further improve the model recognition effect. This paper uses the AE-VIKOR method to calculate the business importance coefficient to ensure the accuracy of the results to facilitate the analysis and management of business continuity.

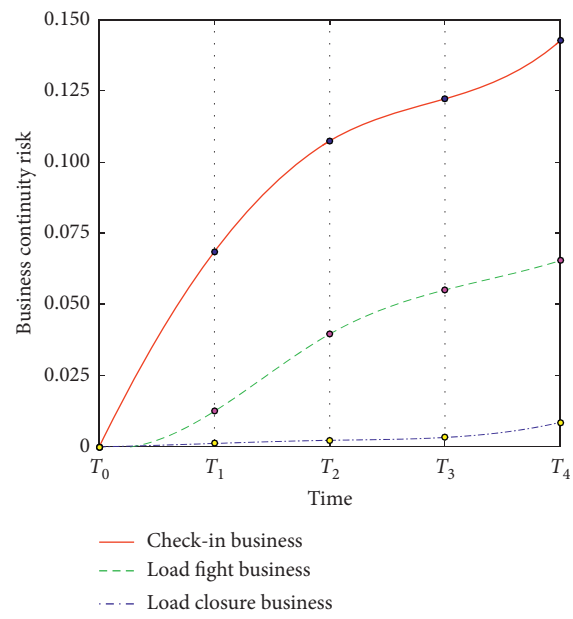

Figure 4: Business continuity risk analysis.

5.4. Comparative Experiment on the Coefficient Selection of Decision Mechanism. The evaluation results of the AE-VIKOR method are different due to different coefficients of decision mechanism v. It is very important to choose the coefficient of decision mechanism reasonably for the evaluation result of the method. To adopt a reasonable and efficient decision mechanism, coefficient v is designed to be 0.2, 0.4, 0.5, 0.6, and 0.8, in this paper. The importance coefficient of departure business node is calculated and analyzed. The evaluation result is shown (see Figure 6).

It can be seen from Figure 6 that when $v = 0.5$, the calculation of the importance coefficient of each node is accurate and the difference is obvious. Therefore, to improve the universality of the model. The decision mechanism coefficient v of the AE-VIKOR method is set to 0.5.

Table 9: The importance coefficient for each node.

	AHP-VIKOR	Entropy-VIKOR	DEMATEL-Entropy-VIKOR	VIKOR	TOPSIS	AE-VIKOR
n_1	0.0879	0.3721	0.3623	0.3897	0.1697	0.1974
n_2	0.0668	0.3721	0.3748	0.3982	0.1058	0.1464
n_3	0.5211	0.4732	0.4689	0.4904	0.5106	0.5199
n_4	1.0000	1.0000	0.7645	1.0000	1.0000	1.0000
n_5	0.4543	0.2877	0.2777	0.2734	0.4047	0.4844
n_6	0.4772	0.3611	0.4611	0.3483	0.4523	0.4949
n_7	0.0211	0.0001	0.0001	0.0001	0.0106	0.1048
n_8	0.0001	0.0015	0.0018	0.0058	0.0001	0.0567
n_9	0.0439	0.0746	0.0846	0.0799	0.0582	0.1175

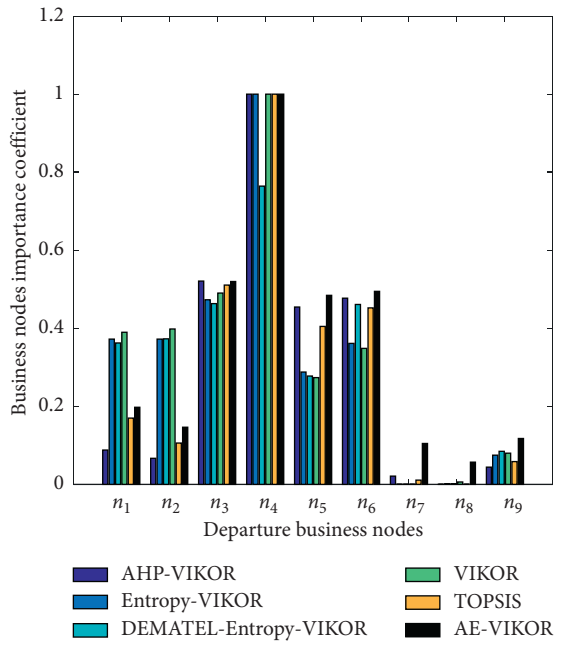

Figure 5: Business nodes importance coefficient calculated by different methods.

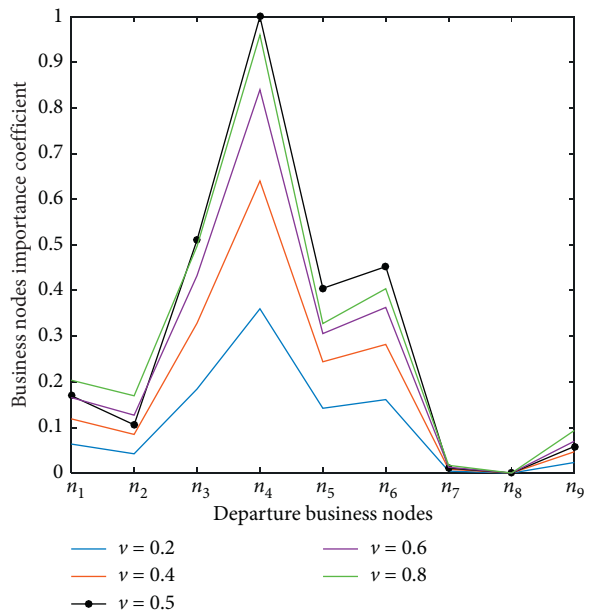

Figure 6: Comparison of different decision mechanism coefficient selection experiments.

6. Conclusion

This paper proposes a key business node identification model for the Internet of Things security. The model analyzed the business process to obtain business nodes. Then the business node importance evaluation attributes were quantified. And a combined weight was used to improve the attribute weight to identify key business node. After the information security event occurs in the smart mobile phone which impacts through IoT on the business system, the AE-VIKOR method is used to make a decision and sort the importance of business nodes, and the model analyzes the impact of key business node' on business continuity. The experimental results show that the key business node identification model based on the AE-VIKOR method is more accurate, and the business continuity risk assessment is carried out reasonably. The next step is to analyze the impact of the key business node on business recovery priority, after information security events occur, and further improve the recognition ability and adaptive ability of the 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.

Disclosure

The manuscript has been extended about 150% from the Frontiers in Cyber Security (FCS 2020) conference manuscript. An earlier version of this work was presented as a paper at the FCS 2020 conference found at the following link: https://link.springer.com/chapter/10.1007/978-981-15-9739-8_47.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper when handling and making decisions.

Acknowledgments

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

References

[1] 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.

[2] A. Jurcut, T. Niculcea, P. Ranaweera, and N.-A. Le-Khac, "Security considerations for Internet of things: a survey," *SN Computer Science*, vol. 1, no. 4, p. 193, 2020.

[3] M. Belouch, S. El Hadaj, and M. Idhammad, "Performance evaluation of intrusion detection based on machine learning using apache spark," *Procedia Computer Science*, vol. 127, pp. 1–6, 2018.

[4] J. Liu, B. Kantarci, and C. Adams, "Machine learning-driven intrusion detection for contiki-NG-based IoT networks exposed to NSL-KDD dataset," in *Proceedings of the ACM Workshop on Wireless Security and Machine Learning (WiseML 2020)*, Linz, Austria, July 2020.

[5] L. Xie, Y. Ding, H. Yang, and Z. Hu, "Mitigating LFA through segment rerouting in IoT environment with traceroute flow abnormality detection," *Journal of Network and Computer Applications*, vol. 164, Article ID 102690, 2020.

[6] H. Yang, X. Zhang, and F. Cheng, "A novel algorithm for improving malicious node detection effect in wireless sensor networks," *Mobile Networks and Applications*, pp. 1–10, 2020.

[7] A. N. Moldagulova, R. K. Uskenbayeva, R. Z. Satybaldiyeva et al., "On identification of hybrid business processes for effective implementation in the form of cloud services," in *Proceedings of the 2019 19th International Conference on Control, Automation and Systems (ICCAS)*, pp. 51–54, Jeju, Korea, October 2019.

[8] G. Sherzod, G. Abdukhalil, and V. Viktoriya, "Formalization of the business process security," in *Proceedings of the 2019 International Conference on Information Science and Communications Technologies (ICISCT)*, pp. 1–3, IEEE, Tashkent, Uzbekistan, November 2019.

[9] Q. Ming and L. Songtao, "Overview of system wide information management and security analysis," in *Proceedings of the 2017 IEEE 13th International Symposium on Autonomous Decentralized System (ISADS)*, pp. 191–194, IEEE, Bangkok, Thailand, March 2017.

[10] G. Stergiopoulos, P. Dedousis, and D. Gritzalis, "Automatic network restructuring and risk mitigation through business process asset dependency analysis," *Computers & Security*, vol. 96, Article ID 101869, 2020.

[11] R. Matulevičius, A. Norta, and S. Samarütel, "Security requirements elicitation from airline turnaround processes," *Business & Information Systems Engineering*, vol. 60, no. 4, pp. 3–20, 2018.

[12] H. Yang and G. Qin, "Identification of key systems for risk assessment," *Journal of Dalian University of Technology*, vol. 60, pp. 306–316, 2020.

[13] J. Xing, Z. Zeng, and E. Zio, "Dynamic business continuity assessment using condition monitoring data," *International Journal of Disaster Risk Reduction*, vol. 41, Article ID 101334, 2019.

[14] J. A. Ali, Q. Nasir, and F. T. Dweiri, "Business continuity framework for internet of things (IoT) services," *International Journal of System Assurance Engineering and Management*, vol. 11, pp. 1380–1394, 2020.

[15] S. A. Torabi, R. Giahi, and N. Sahebjamnia, "An enhanced risk assessment framework for business continuity management systems," *Safety Science*, vol. 89, pp. 201–218, 2016.

[16] V. M. Belov, A. I. Pestunov, and T. M. Pestunova, "On the issue of information security risks assessment of business processes," in *Proceedings of the 14th International Scientific-Technical Conference on Actual Problems of Electronics Instrument Engineering APEIE*, pp. 136–139, IEEE, Piscataway, NJ, USA, October 2018.

[17] E. Hariyanti, A. Djunaidy, and D. O. Siahaan, "A conceptual model for information security risk considering business process perspective," in *Proceedings of the 2018 4th International Conference on Science and Technology (ICST)*, pp. 1–6, IEEE, Yogyakarta, Indonesia, August 2018.

[18] S. V. Fani and A. P. Subriadi, "Business continuity plan: examining of multi-usable framework," *Procedia Computer Science*, vol. 161, pp. 275–282, 2019.

[19] R. Diesch, M. Pfaff, and H. Krcmar, "A comprehensive model of information security factors for decision-makers," *Computers & Security*, vol. 92, Article ID 101747, 2020.

[20] D. Siregar, H. Nurdiyanto, S. Sriadhi et al., "Multi-attribute decision making with VIKOR method for any purpose decision," *Journal of Physics: Conference Series*, vol. 1019, 2018.

[21] J. Yang, J. Han, and X. Zhang, "Information system security risk assessment based on IDAV multi-criteria decision model," in *Proceedings of the 2018 12th IEEE International Conference on Anti-counterfeiting, Security, and Identification (ASID)*, pp. 121–127, IEEE, Xiamen, China, November 2018.

[22] O. Mohsen and N. Fereshteh, "An extended VIKOR method based on entropy measure for the failure modes risk assessment-a case study of the geothermal power plant (GPP)," *Safety Science*, vol. 92, pp. 160–172, 2017.

[23] C. Han, Y. Zhao, Z. Lin et al., "Critical lines identification for skeleton-network of power systems under extreme weather conditions based on the modified VIKOR method," *Energies*, vol. 11, 2018.

[24] P. Mateusz, M. Danuta, Ł. Małgorzata, B. Mariusz, and N. Kesra, "TOPSIS and VIKOR methods in study of sustainable development in the EU countries," *Procedia Computer Science*, vol. 126, pp. 1683–1692, 2018.

[25] Z. Wu, J. Xu, X. Jiang, and L. Zhong, "Two MAGDM models based on hesitant fuzzy linguistic term sets with possibility distributions: VIKOR and TOPSIS," *Information Sciences*, vol. 473, pp. 101–120, 2019.

[26] Y. Shen, C. Gu, and P. Zhao, "Structural vulnerability assessment of multi-energy system using a PageRank algorithm," *Energy Procedia*, vol. 158, pp. 6466–6471, 2019.