Mathematical Biosciences and Engineering

MBE, 19(12): 14232–14250.
DOI: 10.3934/mbe.2022662
Received: 05 October 2022
Revised: 05 November 2022
Accepted: 14 November 2022
Published: 01 December 2022

http://www.aimspress.com/journal/MBE

Research article

A fuzzy DRBFNN-based information security risk assessment method in improving the efficiency of urban development

Li Yang[1], Kai Zou[1], Kai Gao[1] and Zhiyi Jiang[1,2,*]

[1] School of Public Administration, Xiangtan University, Xiangtan 411105, China
[2] The Library of Xiangtan University, Xiangtan 411105, China

* **Correspondence:** Email: ZhiyiJiangxtu@163.com.

Abstract: The rapid development of urban informatization is an important way for cities to achieve a higher pattern, but the accompanying information security problem become a major challenge restricting the efficiency of urban development. Therefore, effective identification and assessment of information security risks has become a key factor to improve the efficiency of urban development. In this paper, an information security risk assessment method based on fuzzy theory and neural network technology is proposed to help identify and solve the information security problem in the development of urban informatization. Combined with the theory of information ecology, this method establishes an improved fuzzy neural network model from four aspects by using fuzzy theory, neural network model and DEMATEL method, and then constructs the information security risk assessment system of smart city. According to this method, this paper analyzed 25 smart cities in China, and provided suggestions and guidance for information security control in the process of urban informatization construction.

Keywords: smart city; urban development; information security risk assessment; fuzzy theory; neural network model; DEMATEL

1. Introduction

The rapid development of information technology provides a new direction for urban development—smart city [1–5]. Smart cities achieve sustainable and healthy development through informatization, but also bring risks and hidden dangers (such as personal information leakage, spam and fraud) [6–8]. These risks and hidden dangers have seriously affected the further development of

the city. How to evaluate and deal with the information security problems of the city and improve the management and decision-making efficiency of the city manager has become a key link to the urban development [9–12].

As the primary purpose of information security risk assessment, the construction of an information security risk assessment indicator system has been widely studied [13–15]. However, with the acceleration of the informatisation process, more complex information security issues, indicators and ambiguous indicator boundaries have to be considered; all these factors subject the construction of a risk assessment indicator system to ambiguity and uncertainty [16–18]. To solve this problem, many methods have been proposed; these methods can be divided into three categories: soft computing-based, hybrid model-based and neural network-based methods.

Soft computing-based methods solve the problem at the cost of tolerating uncertainty and inaccuracy in the calculation process; they primarily include the analytic hierarchy process (AHP) and fuzzy computing. AHP [19,20] is a multi-objective decision-making method that combines qualitative and quantitative analyses; it can decompose complex problems into multiple simple problems in a hierarchical structure for easy analysis. However, all the parameters in this method are provided by experts, resulting in few quantitative components and easily introduced subjective factors. Fuzzy computing is based on fuzzy theory; it improves indicator system construction by simulating the ambiguity and uncertainty of a risk indicator. In 2005, Chang et al. [21] pointed out the importance of ambiguity and uncertainty in information security risk assessment and proposed that they can be solved through fuzzy set theory. Moreover, they presented the fuzzy weighted average method and provided useful guidance for the construction of a risk assessment indicator system. In 2009, Gao et al. [22] proposed a grey system theory-based information security risk assessment method to eliminate parameter uncertainty in an indicator system. This method classified parameters into grey and vacant parameters and estimated them via three probability distributions. The preceding examples have achieved good results in dealing with the uncertainty of a risk assessment indicator system. However, with the increasing complexity of practical problems, simple fuzzy computing methods (i.e., type-1 fuzzy logic system) have been unable to realise the processing of this uncertainty [23–25]. Therefore, higher-order fuzzy logic systems (FLSs) based on type-2 fuzzy sets (T2FSs), such as interval/general type-2 FLS, have been introduced into the construction of risk assessment indicator systems [26,27]. Through T2FSs, FLS can simultaneously consider inter-uncertainty between different objects and intra-uncertainty between different parts of an object during decision-making [28,29]. To understand the effect of information technology on cybercrime, Mansour et al. [30] produced a risk assessment result based on four risk factors (vulnerability, threat, likelihood and impact) in accordance with a high-order fuzzy inference model; they predicted some types of behaviour that may threaten information security. However, a major problem in FLS is the huge computational requirement, which can be alleviated by combining with the ZSlice method [31]. Zhao et al. [32] recently proposed the zSlice and general T2FSs-based method (zGT2FSs). They modelled and analysed the status quo of a smart city in China and identified five key factors that affect smart city information security: 1) data encryption and recovery, 2) failure rate of software and hardware, 3) practitioner intelligence level, 4) maturity of a smart city application system and 5) access control and identity authentication. They then emphasised that government departments should ensure the stability of smart city information security by strengthening the top-level design, establishing and improving the information security management mechanism, avoiding overlapping or missing functions of participating departments and optimising access control and identity authentication.

A hybrid model-based method constructs an information security risk assessment indicator system by integrating two or more simple models. Through the superposition of simple models, it can overcome the deficiency of soft computing-based methods, i.e., computational complexity increases with an increase in problem requirements. Classic simple models include AHP, analytic network process (ANP), decision-making trial and assessment laboratory (DEMATEL) and event tree analysis (ETA). Classic combinations include 'AHP+fuzzy theory', 'ANP+fuzzy theory', 'DEMATEL+ANP', 'failure mode and effect analysis+fuzzy theory', 'ETA+fuzzy theory' and ''information entropy+fuzzy theory'. To address the limitation of the current risk assessment indicator system of being unable to provide the numerical value of risk and avoid interference, Wang and Lin [33] proposed a quantitative model of a risk assessment indicator system based on a fuzzy algorithm and a hierarchical structure. In this method, factors such as network services, hosts, hacker threats and network vulnerabilities were considered in AHP for analysis. Then, the fuzzy algorithm was used to infer the risk value of each layer from global and local. However, AHP must assume independence between decisions and alternatives, and such process cannot be achieved due to the ambiguity and uncertainty of indicators. Many references have overcome the dependency problem by adopting 'ANP+fuzzy theory' [34]. However, the normalisation of weighted hypermatrices in ANP is a difficult task. To alleviate this problem, Ouyang et al. [35] proposed a risk assessment indicator system construction method by combining DEMATEL with ANP. This method was applied to estimate the risk of security breaches, occurrence probability and consequence of the risk. Experiments showed that the method could overcome the influence of fuzzy factors brought by expert assessment and the dependence between decision and scheme. However, this method could not provide the best scheme in accordance with decision's risk level. In 2016, Ana et al. [36] proposed a fuzzy decision theory-based information security risk assessment method, which could select appropriate schemes for different risk levels through ETA and fuzzy decision theory. However, the suitable selection of a scheme requires an accurate assessment of the risk level. To address this issue, Cheng et al. [37] introduced information entropy into information security risk assessment in 2017 and proposed a quantitative risk analysis method based on fuzzy comprehensive analysis and information entropy. This method firstly defines the risk degree (i.e., the estimation of risk probability and impact) in accordance with information entropy. Then, it uses a fuzzy comprehensive assessment method to evaluate risk factors. Finally, the weight of risk is determined through the entropy weight coefficient, which can measure ambiguity and uncertainty.

The neural network-based method constructs the risk assessment indicator system through powerful nonlinear processing and learning abilities [38–40]. The use of neural networks has become a persistent trend in the construction of information security risk assessment indicator systems [41,42]. In 2016, Song et al. [43] proposed a genetic algorithm and back-propagation (BP) neural network (BPNN)-based information security risk assessment model (GA-BP) to improve risk assessment. They classified risk factors into four categories: asset identification, threat identification, vulnerability identification and system identification. Then, they further divided the 4 categories into 14 factors in accordance with the national standards and the actual situation of industries. The simulation results showed that GA-BP provided less simulation errors and better fitting effect; it is an excellent information security risk assessment model. However, training speed is the greatest problem in neural networks. On the basis of particle swarm optimization (PSO) and BPNN, Guo et al. [44] proposed a PSO-BPNN model for information security risk assessment. In this method, PSO was used to find the best initial value before network iteration to address the slow convergence and accuracy problems of BPNN. In summary, although the aforementioned methods have achieved excellent results, the

widespread use of neural networks still poses a huge challenge because of the black box problem (i.e., unclear intermediate process).

In conclusion, some shortcomings still exist in the construction of smart city information security risk assessment indicator systems. Soft computing-based methods can disregard ambiguity and uncertainty, but the expertise required from researchers increases dramatically with an increase in problem demands. Hybrid model-based methods reduce the requirement for expertise through the superposition of simple models; however, their accuracy should be further improved. Neural network-based methods are the most convenient and accurate at present; nevertheless, they cannot provide additional guidance to the construction of indicator systems due to the black box problem.

In this paper, on the basis of quantitative fuzzy comprehensive analysis, DEMATEL and radial basis function neural network (RBFNN), we proposed a new smart city information security risk assessment method (Fuzzy DRBFNN), which can identify risk factors, provide effective suggestions for decision makers and improve management efficiency. Firstly, expert assessment is pre-processed via fuzzy comprehensive analysis to preserve ambiguity and uncertainty. Secondly, the processed expert assessment is integrated with official statistical data and inputted into RBFNN to obtain the contribution of a risk indicator. Finally, the contribution of a risk indicator is processed via DEMATEL to construct a clear and precise information security risk assessment indicator system. The method is applied to the construction of China's smart city information security risk assessment indicator system. The results show that urban cloud platform construction, data encryption technology and safety education and training are the key risk indicators that affecting the smart city information security.

2. Methods

Information security risk assessment is the process of evaluating the security attributes (e.g., confidentiality, integrity and availability) of an information system and the information it processes, transmits and stores. Constructing an information security risk assessment indicator system can predict possible risks and propose corresponding solutions. However, with the increase in the number of assessment indicators and the blurring of boundaries, the construction of a risk assessment indicator system is always affected by ambiguity and uncertainty. At present, the risk research methods that have been applied to information security include Random Forest, DEMATEL, Bayesian Network and so on. Although these methods effectively avoid the ambiguity and uncertainty, their accuracy is difficult to be improved due to the lack of feature expression ability. Fortunately, neural networks can. The commonly used neural network models are back propagation neural network (BPNN) and its variants. However, the greatest problem of BPNN is the huge computational burden caused by the fully connected mode between network layers. In addition, BPNN is strongly uninterpretable, which is not conducive to researchers to build a clear and accurate index system of information security risk assessment. The radial basis function neural network (RBFNN) is the most interpretable neural network model because it builds mappings between inputs and hidden layers through known mathematical functions. Therefore, on the basis of hidden layers, a clear risk assessment indicator system can be built to guide the information security construction of smart cities.

In this study, we proposed an information security risk assessment method using improved RBFNN. There are three parts (Figure 1): 1) Quantitative fuzzy comprehensive analysis-based data pre-processing. 2) RBFNN-based information security risk training. 3) DEMATEL-based indicator system construction.

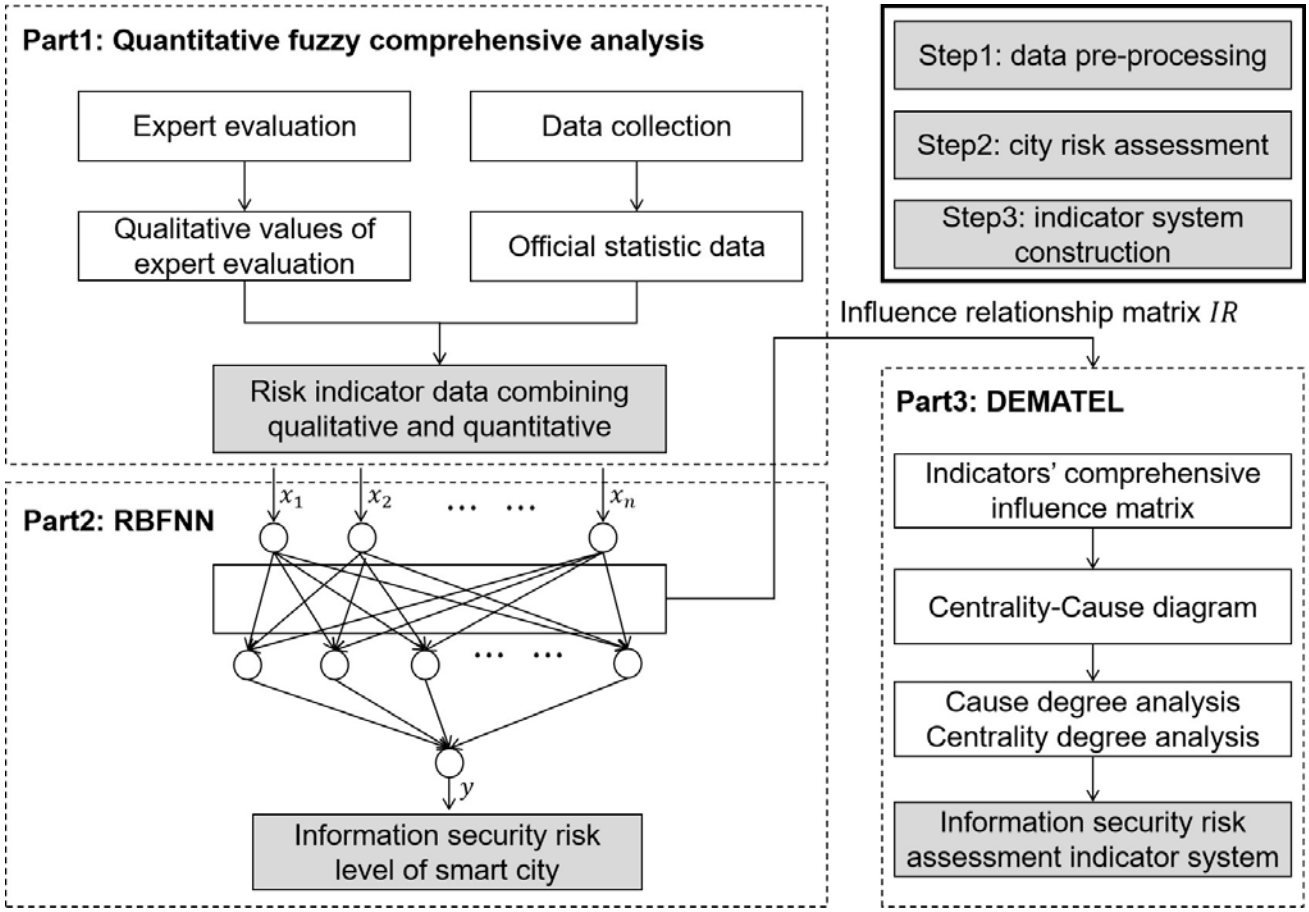

Figure 1. Flowchart of fuzzy DRBFNN. The diagram consists of four sections, with the top right corner describing the workflow of the method. The method consists of three steps, each of which is shown separately in the other three sections. In part 1, expert data and official data are used to obtain the experimental data through fuzzy comprehensive analysis. In part 2, an RBFNN network is trained to predict the risk of urban information security, and finally the parameters of the hidden layer of the network are passed into part 3 for DEMATEL to build the indicator system.

2.1. Fuzzy comprehensive analysis

Ambiguity and uncertainty, which are artificially introduced by expert assessment, are the most common unavoidable factors in the construction of an information security risk assessment indicator system. In general, experts' scores for an indicator are frequently composed of several discrete ratings. However, the internal change of an indicator, i.e., the change of one indicator relative to another, tends to be a gradual rather than an abrupt process. Such discrepancy in the indicator value caused by the difference between the expert assessment result and the actual result is one of the reasons for ambiguity and uncertainty [45–47]. To eliminate the influence of uncertainties from the source, a quantitative fuzzy comprehensive analysis is used to pre-process the assessment results of experts. The major process is described as follows.

1) Determine the assessment indicator universe $A = \{A_1, A_2, \cdots, A_n\}$.

2) Determine the indicator level universe $V = \{V_1, V_2, \cdots, V_m\}$.

3) Get the fuzzy relation matrix S between assessment indicators and indicator levels by experts vote.

$$S = \begin{bmatrix} S_{11} & \cdots & S_{1n} \\ \vdots & \ddots & \vdots \\ S_{m1} & \cdots & S_{mn} \end{bmatrix} \tag{1}$$

4) Set the fuzzy weight vector $Q = \{q_1, q_2, \cdots, q_m\}$ for the assessment level.

5) Computing the fuzzy comprehensive assessment vector $W = Q * S$ of indicator.

2.2. RBFNN

The traditional information security risk assessment method experiences difficulty in achieving good generalisation and robustness. Moreover, it requires a huge amount of professional knowledge. Neural networks can break through this dilemma. The commonly used neural network models are BPNN and its variants. However, the greatest problem of BPNN is the huge computational burden. As a better strategy, RBFNN is selected as the primary model for information security risk assessment in our study because it requires fewer parameters and computation than BPNN [48–50]. In addition, RBFNN is the most interpretable neural network model which can alleviate the black box problem to a certain extent. By taking advantage of these characteristics, a more accurate information security risk assessment indicator system is constructed by the middle layer of RBFNN in this section. RBFNN generally consists of three layers: the input, hidden and output layers (Figure 2).

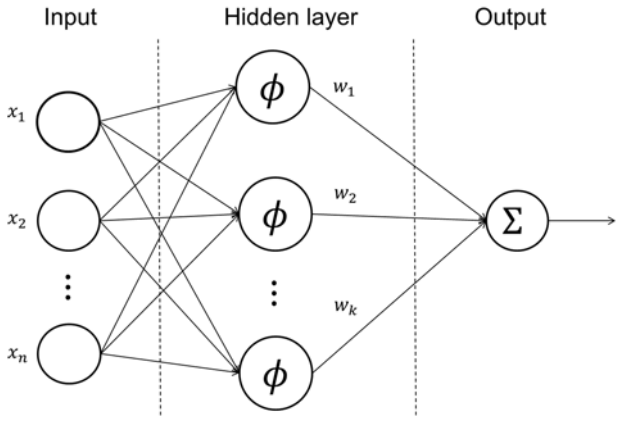

Figure 2. Network structure of RBFNN.

In general, RBFNN can be regarded in two parts: the feature extraction module and linear fitting module. The first two layers are responsible for feature extraction, whilst the last layer is responsible for fitting a linear model.

Feature extraction module: The feature extraction module is primarily realised by a set of radial basis function (RBF). RBF is described as follows:

$$\phi(\|x - c_i\|) = \exp\left[-\beta_i \|x - c_i\|^2\right] \tag{2}$$

where β_i is a hyperparameter that requires no training, c_i is a trainable parameter that is only required to randomly sample from D_j.

As shown in the formula, RBF takes the distance (e.g., Euclidean distance) between the input and c_i as its independent variable. The closer the input is to c_i, the higher its activation degree. Therefore, RBFNN exhibits the property of 'local mapping': for risk indicators related to c_i, their role will be amplified, whilst be weakened. In accordance with this property, a clearly delimited and functional risk assessment indicator system can be obtained, which is impossible with BPNN.

Linear fitting module: this module fits a linear model $y = w_1\phi_1 + w_2\phi_2 + \cdots + w_k\phi_k$ based on feature set $\phi_1, \phi_2, \cdots, \phi_k$. The linear model can be solved via the least square method instead of gradient descent, which is the reason for the high interpretability and fast training speed of RBFNN.

2.3. DEMATEL

The purpose of information security risk assessment is not only to accurately assess the risk level of a city, but also to construct an accurate and effective indicator system and provide guidance to the city's information security construction. For this purpose, a clear and precise information security risk assessment indicator system is constructed via DEMATEL. By calculating the impact, affected, centrality and cause degrees, the position of an indicator in the entire indicator system can be determined [51–53], and the key indicator can be used to reorganise the new indicator system. The major process is described as follows.

1) Obtain the direct influence matrix B by standardising the influence relationship matrix IR:

$$B = \frac{IR}{max\left\{max\sum_{i=1}^{n} IR_{ij}, max\sum_{j=1}^{n} IR_{ij}\right\}} \tag{3}$$

2) Construct the comprehensive influence matrix T via matrix B:

$$T = \lim_{n\to\infty}\sum_{i=1}^{n} B^i = B(I - B) \tag{4}$$

3) Calculate the impact degree R, affected degree D, centrality degree Cen and cause degree Cau for all the risk indicators:

$$R = \left[\sum\nolimits_{j=1}^{n} T_{ij}\right]_{n\times 1} \tag{5}$$

$$D = \left[\sum\nolimits_{i=1}^{n} T_{ij}\right]_{1\times n}^{T} \tag{6}$$

$$Cen = [R_i + D_i]_{n\times 1} \tag{7}$$

$$Cau = [R_i - D_i]_{n\times 1} \tag{8}$$

4) Construct the centrality-cause diagram with the centrality degree and cause degree as the horizontal and vertical axes, respectively, to find the key indicator.

Here, matrix T reflects the comprehensive influence amongst indicators. I is the identity matrix with element T_{ij} representing the sum of the influence of indicator i on j. R, D, Cen and Cau comprise an $n \times 1$ vector, which represents the comprehensive performance of all risk indicators.

3. Case study

3.1. Problem description

Smart city is a new mode of urban development that integrates emerging technologies such as big data, cloud computing and the Internet of things with urban construction to pursue sustainable economic, social and environmental development. Smart city is a typical information ecosystem, which includes many elements such as people, information, technology and institutions. It not only brings convenience to people, but also has a multi-angle impact on urban information security (Figure 3). How to identify the key influencing factors of information security risks in smart cities, formulate and improve relevant policies, and maintain information security and stability is a practical problem that must be solved for the sustainable development of smart cities. The Chinese government attaches great importance to the construction of smart cities in urban development and governance. Vigorously promoting the construction of new smart cities has become the strategic direction of urban development in China. In this paper, 25 smart cities in China are selected for information security risk assessment.

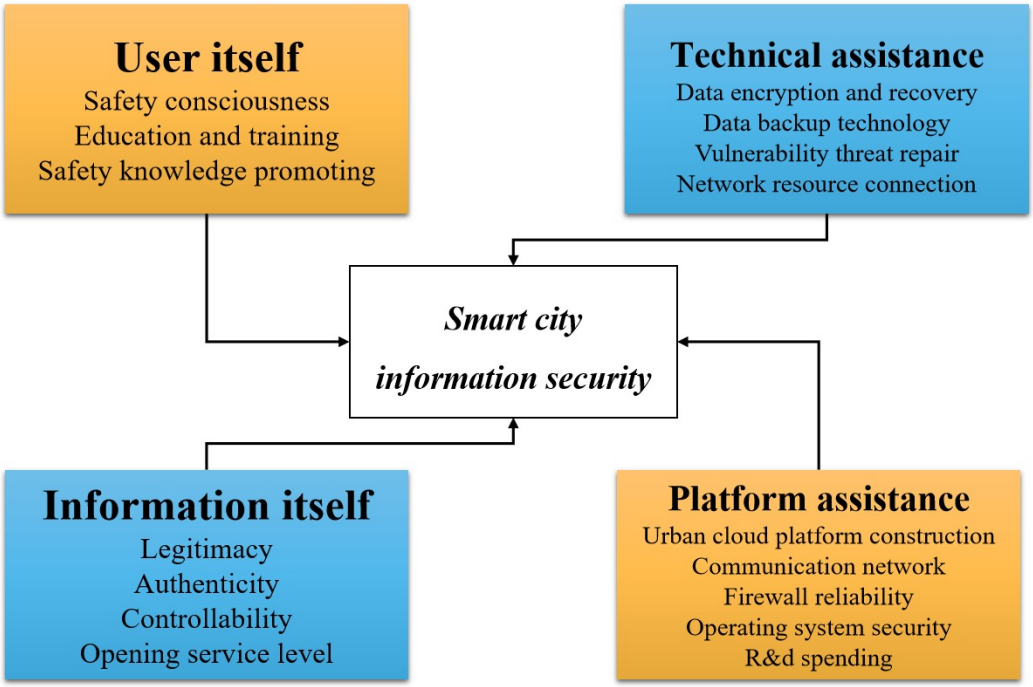

Figure 3. Smart city information security ecosystem. The system divides the object that affects the city information security into four categories: user, information, platform and technology. According to the classification of these four subjects, 16 indicators are extended to describe all the factors that may affect urban information security.

To avoid an excessive amount of missing data due to the low intelligence of a city, there are four levels are selected: 1) the first-tier cities (four cities); 2) the new first-tier cities (eleven cities); 3) the second-tier cities (nine cities), and the third-tier cities (only one). The list of cities and experimental data is provided in Supplementary material 1. According to Figure 3, risk indicators (A1–A16) and their description is given at Table 1. A17 is the comprehensive development level of a city.

Table 1. The description of indicator.

A1	Communication network construction	A9	Public safety consciousness
A2	Network resource connection	A10	Data encryption and recovery
A3	Urban cloud platform construction	A11	Data backup technology
A4	Legitimacy of information content	A12	Data opening service level
A5	Authenticity of information content	A13	R&d spending
A6	Controllability of information content	A14	Firewall reliability
A7	Safety education and Training	A15	Operating system security
A8	Safety knowledge promotion	A16	Vulnerability threat repair rate
A17:	Comprehensive development level of the city		

3.2. Information security risk assessment

To evaluate the information security risk of smart city, four experts were selected for the interview research. They have more than 10 years of relevant experience in the field of smart city and have certain decision-making ability in the organization.

Table 2. One of the expert decision results.

Indicator	Information security risk assessment indicator level				
	Low	Medium low	Medium	Medium high	High
A1	0	1	4	4	1
A2	0	3	4	2	1
A3	0	1	4	3	2
A4	0	5	3	1	1
A5	0	5	4	1	0
A6	0	4	4	1	1
A7	0	1	3	5	1
A8	0	4	3	2	1
A9	0	1	5	3	1
A10	0	1	2	5	2
A11	0	2	4	2	2
A12	0	4	3	2	1
A13	0	4	3	2	1
A14	0	1	5	2	2
A15	0	1	5	2	2
A16	0	2	4	2	2

Step1: According to the fuzzy comprehensive analysis, in the survey design, experts are asked to answer the impact degree of risk indicators on urban information security. There are five levels (Low, Medium Low, Medium, Medium high, High). The higher the level, the higher the impact on information security. Each indicator has 10 points, and experts can assign 10 points to different levels to indicate their approval of the indicator. In this paper, 4 experts were surveyed by three different repeated questionnaires with the same content, and a total of 12 questionnaires were obtained. Then,

based on reference [54], the fuzzy weight vector $Q = \{1/25,3/25,5/25,7/25,9/25\}$ was set to calculate the ranking results of each index under 12 different surveys (Table 2). Finally select the means as the fuzzy comprehensive assessment vector
$W = \{0.24,0.208,0.248,0.184,0.168,0.192,0.248,0.2,0.232,0.264,0.232,0.2,0.2,0.24,0.24,0.232\}$.

However, this result is directly determined by the experts and is influenced by a large number of subjective factors and cannot be used directly. To add objective factors, statistical data is introduced as a supplement, and the supplementary methods are as follows: 1) denote statistical data as X (25 smart cities and their values on 17 indicators), and use W to do hadamard product on the data of each city to obtain new data X'; 2) Integrate X and X' to get D. The integration formula is as follows:

$$D = \frac{X + X^{'}}{2} \tag{9}$$

The data are harmonized data combining subjective and objective factors (Supplementary material 2). Then, data D is transferred to Step 2. RBFNN is used for fitting to obtain the updated index weight, so as to obtain the mutual influence relationship of indicators.

Step2: In Step 2, to model information security risk assessment, a nonlinear multivariate function $y = f(city)$ is established (where the independent variable is the $city = \{A1, A2, \cdots, A16\}$, and the dependent variable is A17) and then learned via RBFNN for an accurate prediction of smart city information security risk. Meanwhile, to evaluate the prediction performance of RBFNN in information security risk assessment, mean square error (MSE) and the coefficient of determination (R^2) is selected:

$$MSE = \frac{1}{n}\sum_{i=1}^{n}(\hat{y}_i - y_i)^2 \tag{10}$$

$$R^2 = \frac{\sum_{i=1}^{n}(\hat{y}_i - \bar{y})^2}{\sum_{i=1}^{n}(y_i - \bar{y})^2} \tag{11}$$

where y_i is the label (real value, i.e., A17) of city, $\hat{y}_i$ is the predicted value and $\bar{y}$ is the mean of label. MSE describes the difference between the predicted values and the real value. The closer the MSE is to 0, the better the prediction performance. The R^2 measures the interpretability of the independent variable to the dependent variable. The larger the R^2, the higher the interpretability.

As for the parameters of RBFNN in our study, the input layer includes 16 neurons (corresponding to A1–A16); the hidden layer includes k = 16, that is, 16 RBFs (by default); the output layer is the risk assessment result of a smart city (corresponding to indicator A17). The target error of the network is set as 0.0, and the radial basis diffusion velocity is set as 1. Finally, the data is divided into training and testing data, and leave-one-out cross-validation (LOOCV) is used to train and evaluate prediction performance.

The experimental results show that the predicted curve nearly coincides with the original curve with $MSE \approx 0.0134$ and $R^2 \approx 0.9849$; that is, a 98.49% certainty exists that RBFNN's prediction of each city's risk level can be considered accurate, with a total error of 0.0143.

To prove that this result is not overfitting due to an excessively small amount of data, 5-fold cross-validation (5-fold CV) is also be used to test model performance under less training data. As shown in Table 3, the performance of the model hardly changes when the training samples are reduced, proving that the model is hardly overfitting and the prediction result is reliable.

Finally, to further prove the superiority of RBFNN in information security risk assessment, BPNN, Support vector regression (SVR), logistic regression (LR), decision tree regression (DTR) and random forest regression (RFR) are used as references. Among them, BPNN is a neural network algorithm, which can be used to fit extremely complex nonlinear functions, but it is easy to fall into local optima and its convergence speed is slow. SVR and LR are classical regression algorithms. SVR has high robustness and generalization, but the performance drops sharply when the sample size is smaller than the sample dimension. LR has good anti-noise performance, but is prone to underfitting. DTR and RFR are tree-based algorithms, which have very good adaptability when dealing with a large number of features. Their common characteristics are that they can resist high noise and deal with high-dimensional data sets without feature selection, but they are easy to overfit. The parameters of all methods are the default parameters in MATLAB R2019a (Supplementary material 4). All results are shown in Table 3 and Figure 4.

Table 3. Comparison of performance.

Model		MSE	R^2
RBFNN	LOOCV	0.0134	0.9849
	5-fold CV	0.0169	0.9795
BPNN	LOOCV	0.0229	0.9761
	5-fold CV	0.0387	0.9510
SVR	LOOCV	0.06358	0.91344
	5-fold CV	0.11543	0.83042
LR	LOOCV	0.064835	0.91078
	5-fold CV	0.11843	0.82617
DTR	LOOCV	0.053483	0.94508
	5-fold CV	0.21628	0.75722
RFR	LOOCV	0.091234	0.91431
	5-fold CV	0.67183	0.5997

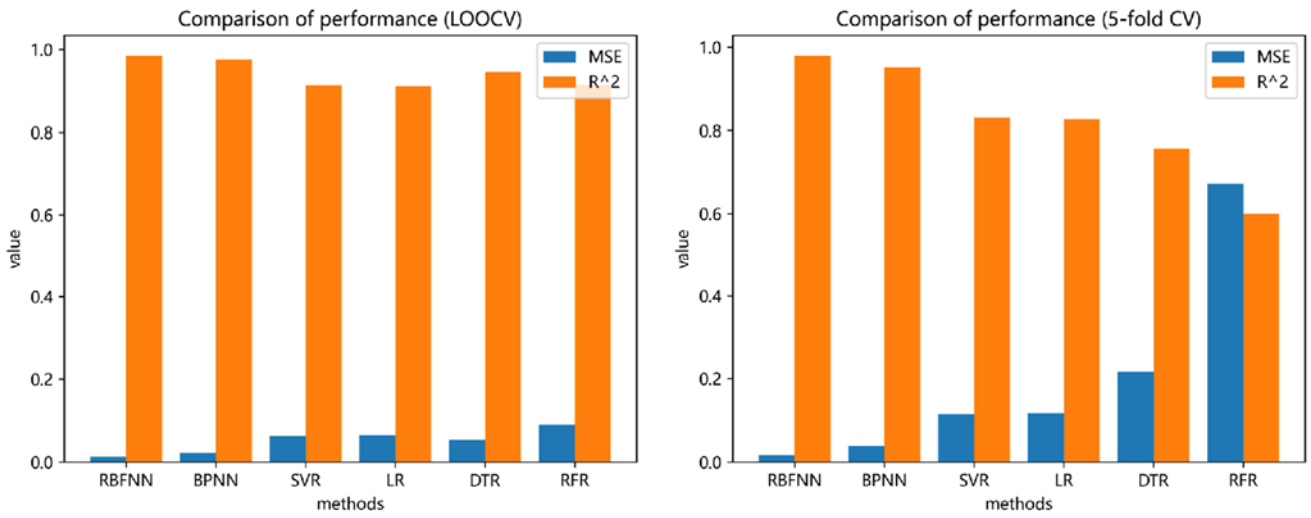

Figure 4. Comparison of performance.

The results show that RBFNN significantly outperforms the other algorithms. In addition, the results of RBFNN are not affected by the change of training data size, while the performance of other methods such as SVR, LR, DTR and RFR will be degraded and especially obvious, which may be caused by the overfitting of the model due to the decrease of data. This proves the excellent performance of RBFNN in the information security risk assessment of smart cities. In conclusion, by comparing with several classical methods, it can be seen that RBFNN has achieved outstanding performance in terms of noise resistance, nonlinear fitting, high-dimensional data processing, and small sample processing.

Step3: With the powerful fitting ability of RBFNN, we get a function that can describe the influence relationship between indicators and urban risk, namely, the network model itself. Through the trained network structure, the influence relationship matrix IR between indicators (Supplementary material 3) can be obtained by following formula:

$$IR = W \odot (IW * IW') \tag{12}$$

where $*$ is the matrix multiplication, $\odot$ represents the multiplication of the corresponding elements of the column. In this formula, IW describes the connection between 16 indicators and hidden layer, which represents the contribution of each indicator to the final result. However, there are no way of knowing the relationship between the indicators. With the help of the principle of neural network back propagation, we believe that the influence of each indicator will eventually be fed back to other indicators in the process of back propagation, so we use IW ‘to represent this relationship. Finally, we approximated the interaction between the indicators by $IW * IW'$. However, $IW * IW'$ is a symmetric matrix, which cannot get the correct result when it is used for DEMATEL. Considering that each indicator has been qualitatively ranked in the fuzzy comprehensive evaluation stage, we introduce the fuzzy comprehensive assessment vector as prior information to achieve the effect of $IW * IW'$ asymmetry and provide input for DEMATEL.

Table 4. The impact and ranking of indicators.

Indicator	Impact/Ranking	Affected/Ranking	Centrality/Ranking	Cause/Ranking
A1	2.2505/(4)	2.0671/(10)	4.3177/(4)	0.1834/(4)
A2	1.6586/(15)	1.7629/(14)	3.4215/(15)	-0.1042/(10)
A3	3.0021/(1)	2.6638/(1)	5.6660/(1)	0.3383/(2)
A4	1.6810/(13)	2.0241/(11)	3.7051/(13)	-0.3431/(15)
A5	1.6104/(16)	2.1274/(5)	3.7377/(12)	-0.5170/(16)
A6	1.8044/(12)	2.0807/(7)	3.8851/(11)	-0.2764/(14)
A7	2.3584/(3)	2.0943/(6)	4.4527/(3)	0.2641/(3)
A8	1.9394/(8)	2.1457/(3)	4.0850/(8)	-0.2063/(13)
A9	2.1840/(6)	2.0764/(8)	4.2603/(5)	0.1076/(7)
A10	2.6175/(2)	2.1798/(2)	4.7973/(2)	0.4377/(1)
A11	2.1262/(7)	2.0217/(12)	4.1479/(7)	0.1044/(8)
A12	1.9312/(9)	2.1366/(4)	4.067/(9)	-0.2054/(12)
A13	1.8750/(11)	2.0743/(9)	3.9493/(10)	-0.1993/(11)
A14	2.1994/(5)	2.0204/(13)	4.2198/(6)	0.1791/(5)
A15	1.9172/(10)	1.7616/(15)	3.6788/(14)	0.1555/(6)
A16	1.6808/(14)	1.5991/(16)	3.2799/(16)	0.0817/(9)

On the basis of IR, a clear and precise information security risk assessment indicator system is constructed via DEMATEL. Firstly, DEMATEL is used to obtain the comprehensive performance (i.e., impact, affected, centrality and cause degrees) and ranking of indicators (Table 4).

To display the result visually, the centrality-cause diagram of the 4 dimensions and 16 risk indicators of the smart city information security is drawn with $Cause = 0$ and $Centrality = 4.4$ as the horizontal and vertical axes, respectively (Figure 5).

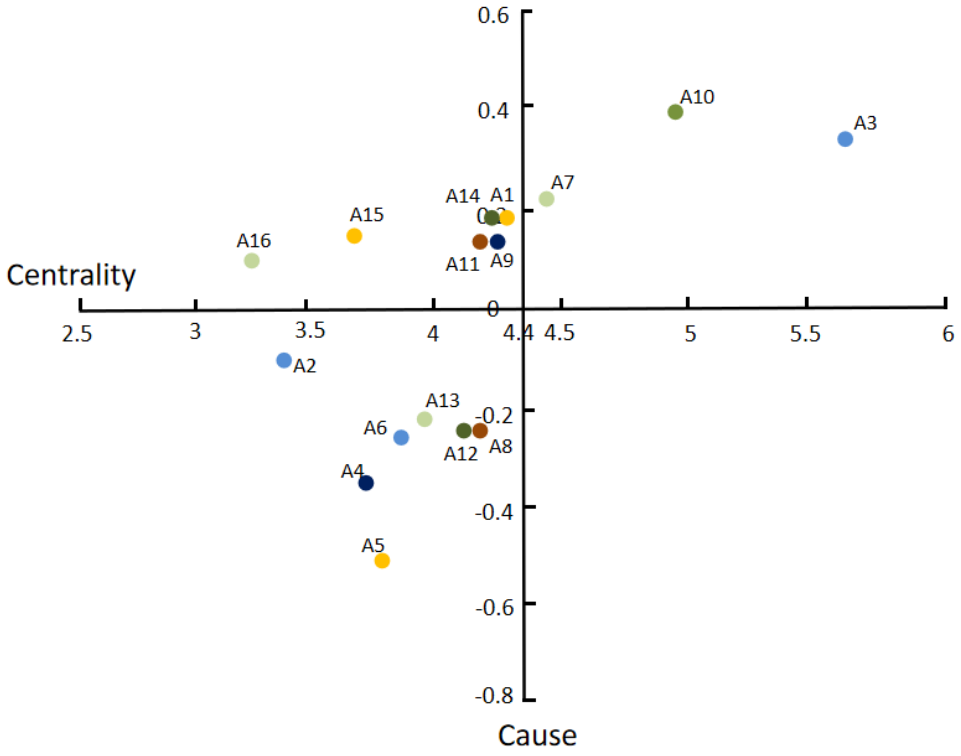

Figure 5. Centrality-cause diagram.

Furthermore, on the basis of Figure 5, the influence relationship (Table 5) of the 16 risk indicators to smart city information security is extracted for the construction of an information security risk assessment indicator system.

Table 5. Four quadrant indicator relationship.

Quadrant	Designation	Indicator	Characteristic
1	Driving factor	A3, A7, A10	Cause > 0, Centrality > 4.4
2	Voluntariness factor	A1, A9, A11, A14, A15, A16	Cause > 0, Centrality < 4.4
3	Independent factor	A2, A4, A5, A6, A8, A12, A13	Cause < 0, Centrality < 4.4
4	Core problem factor	∅	Cause < 0, Centrality > 4.4

As indicated in the table, A3, A7 and A10 are the driving factors that exert the greatest influence on smart city information security. The risk indicators (A1, A9, A11, A14–A16) play an auxiliary role in the occurrence of smart city information security risk. The risk indicators (A2, A4–A6, A8, A12 and A13) located in the third quadrant are independent factors that are direct influence factors of smart city

information security. However, no risk indicator is located in the fourth quadrant, which is a peculiar phenomenon. The reason is as follows. During the modelling and analysis of risk assessment, A1–A16 are the independent variables whilst A17 is the dependent variable. Therefore, A17 should be the only core problem factor. However, A17 does not participate in the construction of the indicator system, resulting in an empty fourth quadrant.

Finally, the centrality degree is normalized to obtain the weight of the risk indicator to city information security and construct a new information security risk assessment indicator system (Table 6).

Table 6. The new information security risk assessment indicator system.

Ranking	Weight	Indicator
1	0.0863	A3
2	0.0730	A10
3	0.0678	A7
4	0.0657	A1
5	0.0649	A9
6	0.0643	A14
7	0.0632	A11
8	0.0622	A8
9	0.0619	A12
10	0.0601	A13
11	0.0592	A6
12	0.0569	A5
13	0.0564	A4
14	0.0560	A15
15	0.0521	A2
16	0.0499	A16

4. Discussion

According to the analysis results, the top three key factors of smart city information security risk are: urban cloud platform construction (0.0863), data encryption and recovery (0.0730), safety education and training (0.0678). From the results of the above survey, we can see that the three most important factors occupy the platform, technology and user respectively in the information ecosystem. In addition, according to centrality-cause diagram, they are the driving factors or key factors of their respective parts, and the rest indicators are the basic factors influenced by them. There are 9 influencing factors of smart city information security index system, among which the most critical three factors are urban cloud platform construction (A3), safety education and training (A7) and data encryption and recovery technology (A10). A total of 7 factors were affected, and were greatly affected by other factors. Among them, the legitimacy of information content (A4), authenticity of information content (A5) and controllability of information content (A6) are affected to the highest degree, indicating that information content is most susceptible to other factors in the whole system except affecting information security risks. Therefore, it is necessary to strengthen the construction of smart city information security from the three dimensions of platform construction, education and training, and data technology to ensure the security of data content in the information world.

As the operation results show the laws and characteristics of the field of smart city information security, the policy orientation in the real world is also consistent with it, which proves that the method proposed in this paper can analyze the smart city information security in the scientific decision-making process of the government by giving the importance ranking reference to stakeholders. They can be used for relevant investment or decision-making processes.

In general, China's smart city information security technology development has made certain achievements, but still faces many challenges:

1) Lack of proper infrastructure for smart cities: Smart cities need to be supported by physical and IT infrastructure. Smart technologies and infrastructure need to be used as widely as possible in everything from public transport to energy to power generation. Otherwise, these technologies will not be able to fully transform cities into "smart" cities.

2) Transparency and data privacy issues: Smart cities rely on the collection and analysis of data from a variety of sources. Unless adequate measures are taken, much of the data may lead to privacy concerns. For example, recording and storing personal information and medical history for healthcare. Fear of hackers, data breaches, scrutiny of data collection by governments and private entities, as well as insufficient transparency and public trust, can seriously hamper smart city initiatives and projects.

3) Residents lack safety knowledge and skills: The next obstacle facing smart city planners is the safety quality of smart city residents. Do they have enough knowledge and skills to operate effectively or reap the benefits of these initiatives?

Based on the above analysis, we propose the following strategies:

1) Strengthen the top-level design of smart city information security, and accelerate the construction of a cross-level, cross-regional, cross-system, cross-department and cross-business urban information security overall guarantee system that integrates cloud computing, big data, artificial intelligence and the Internet of things.

2) Improve the technical and urban information security framework system. Relevant national institutions should organize the formulation and revision of smart city related standards and norms, actively guide the construction of smart cities, improve the content of information security standards, and ensure systematicness, stability and operability. In smart city data applications, the government should strengthen the security of the operating system and data confidentiality, and implement access control and hardware security through identity authentication technology and cloud storage security technology to ensure system security.

3) Improve residents' safety awareness and increase safety investment. Some smart city construction units do not establish information security awareness from the height of national security, security and information construction is not synchronized, some institutions and citizens do not understand the importance of network security, basic protection skills are insufficient, resulting in endless security incidents.

5. Conclusions

This paper takes the improving of urban informatization efficiency as the theme, discusses the risk factors affecting urban information security, and puts forward an improved fuzzy neural network method, which provides a method for speeding up the construction of urban informatization from the perspective of solving the fuzzy and inaccurate boundary of multidimensional indicator system. The results show that the construction of urban cloud platform, data encryption and recovery, and residents'

security education are the most critical factors affecting smart city information security. Under the background of rapid development of urban informatization, it is a comprehensive and comprehensive way to control urban information security construction from three dimensions: platform construction, technology management and user management. Actual operating results show that the intelligent city rules and characteristics in the field of information security policy orientation is also consistent with the real world, we believe that the fuzzy method of RBFNN influence in the search for wisdom in the urban development the key sources of information security tasks is very useful, it can minimize any assumptions or loss of information, support for multiple sources from different angles. It can help decision makers design more effective governance solutions from the source.

Supplementary

The MATLAB code of DRBFNN: https://github.com/Dam-1517/DRBFNN.

Acknowledgments

This study was supported by the National Social Science Fund of China (Grant No. 18BTQ055), the Postgraduate Scientific Research Innovation Project of Hunan Province (CX20210544) and the Social Science Foundation of Hunan Province (18YBA398).

Conflict of interest

The authors declare there is no conflict of interest.

References

1. Y. Zhong, L. Sun, C. Ge, Key technologies and development status of smart city, *J. Phys. Conf. Ser.*, **1754** (2021), 012102. https://doi.org/10.1088/1742-6596/1754/1/012102
2. A. I. Tahirkheli, M. Shiraz, B. Hayat, M. Idrees, A. Sajid, R. Ullah, et al., A survey on modern cloud computing security over smart city networks: Threats, vulnerabilities, consequences, countermeasures, and challenges, *Electronics*, **10** (2021), 1811. https://doi.org/10.3390/electronics10151811
3. K. Dooley, Direct passive participation: aiming for accuracy and citizen safety in the era of big data and the smart city, *Smart Cities*, **4** (2021), 336–348. https://doi.org/10.3390/smartcities4010020
4. K. Gokmenoglu, B. M. Eren, S. Hesami, Exchange rates and stock markets in emerging economies: new evidence using the Quantile-on-Quantile approach, *Quant. Finance Econ.*, **5** (2021), 94–110. https://doi.org/10.3934/QFE.2021005
5. T. Li, J. Zhong, Z. Huang, Potential dependence of financial cycles between emerging and developed countries: Based on ARIMA-GARCH copula model, *Emerging Mark. Finance Trade*, **56** (2020), 1237–1250. https://doi.org/10.1080/1540496X.2019.1611559
6. M. Castells, *The Network Society: A Cross-Cultural Perspective*, Edward Elgar Publishing, Incorporated, 2004. https://dl.acm.org/doi/abs/10.5555/993619

7. J. Zhao, W. Dong, L. Shi, J. Bi, Z. Wang, Y. Liu, et al., Smart city construction and rendering based on virtual city space, in *2020 International Conference on Virtual Reality and Visualization (ICVRV)*, 2020. https://doi.org/10.1109/ICVRV51359.2020.00066
8. M. R. Sanfilippo, Y. Shvartzshnaider, Data and privacy in a quasi-public space: disney world as a smart city, in *Diversity, Divergence, Dialogue. iConference 2021. Lecture Notes in Computer Science*, **12646** (2021), 235–250. https://doi.org/10.1007/978-3-030-71305-8_19
9. X. Li, H. Li, B. Sun, F. Wang, Assessing information security risk for an evolving smart city based on fuzzy and grey FMEA, *J. Intell. Fuzzy Syst.*, **34** (2018), 2491–2501. https://doi.org/10.3233/JIFS-172097
10. R. Fistola, A. Rastelli, Envisaging urban changes for the smart city: The live city information modeling (LCIM), in *Innovation in Urban and Regional Planning. INPUT 2021. Lecture Notes in Civil Engineering*, **146** (2021), 161–169. https://doi.org/10.1007/978-3-030-68824-0_17
11. T. T. X. Huong, T. T. T. Nga, T. T. K. Oanh, Liquidity risk and bank performance in Southeast Asian countries: a dynamic panel approach, *Quant. Finance Econ.*, **5** (2021), 111–133. https://doi.org/10.3934/QFE.2021006
12. Z. Li, C. Yang, Z. Huang, How does the fintech sector react to signals from central bank digital currencies, *Finance Res. Lett.*, **50** (2022), 103308. https://doi.org/10.1016/j.frl.2022.103308
13. A. Aldairi, L. Tawalbeh, Cyber security attacks on smart cities and associated mobile technologies, **109** (2017), 1086–1091. https://doi.org/10.1016/j.procs.2017.05.391
14. K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, X. Shen, Security and privacy in smart city applications: Challenges and solutions, *IEEE Commun. Mag.*, **55** (2017), 122–129. https://doi.org/10.1109/MCOM.2017.1600267CM
15. C. Lim, K. J. Kim, P. P. Maglio, Smart cities with big data: Reference models, challenges, and considerations, *Cities*, **82** (2018), 86–99. https://doi.org/10.1016/j.cities.2018.04.011
16. P. Hui, Construction of information security risk assessment model in smart city, in *2020 IEEE Conference on Telecommunications, Optics and Computer Science (TOCS)*, 2020. https://doi.org/10.1109/TOCS50858.2020.9339614
17. M. Kalinin, V. Krundyshev, P. Zegzhda, Cybersecurity risk assessment in smart city infrastructures, *Machines*, **9** (2021), 78. https://doi.org/10.3390/machines9040078
18. M. Qamruzzaman, T. Tayachi, A. M. Mehta, M. Ali, Do international capital flows, institutional quality matter for innovation output: the mediating role of economic policy uncertainty, *J. Open Innov. Technol. Mark. Complex.*, **7** (2021), 141. https://doi.org/10.3390/joitmc7020141
19. T. L. Saaty, K. P. Kearns, The analytic hierarchy process, in *Analytical Planning: The Organization of Systems*, (1985), 19–62. https://doi.org/10.1016/B978-0-08-032599-6.50008-8
20. X. Xing, Smart city evaluation based on analytic hierarchy process, in *Proceedings of the 2017 5th International Conference on Frontiers of Manufacturing Science and Measuring Technology (FMSMT 2017)*, Atlantis Press, (2017), 1112–1115. https://doi.org/10.2991/fmsmt-17.2017.219
21. P. T. Chang, K. C. Hung, Applying the fuzzy-weighted-average approach to evaluate network security systems, *Comput. Math. Appl.*, **49** (2005), 1797–1814. https://doi.org/10.1016/j.camwa.2004.10.042
22. Y. Gao, J. Luo, Information security risk assessment based on grey relational decision-making algorithm, *J. Southeast Univ.*, 2009. https://doi.org/10.1360/972009-1549
23. C. Wagner, H. Hagras, Toward general type-2 fuzzy logic systems based on zSlices, *IEEE Trans. Fuzzy Syst.*, **18** (2010), 637–660. https://doi.org/10.1109/TFUZZ.2010.2045386

24. J. Huang, L. Dou, H. Fang, J. Chen, Q. Yang, Distributed backstepping-based adaptive fuzzy control of multiple high-order nonlinear dynamics, *Nonlinear Dyn.*, **81** (2015), 63–75. https://doi.org/10.1007/s11071-015-1973-9
25. C. L. P. Chen, C. Ren, T. Du, Fuzzy observed-based adaptive consensus tracking control for second-order multiagent systems with heterogeneous nonlinear dynamics, *IEEE Trans. Fuzzy Syst.*, **24** (2016), 906–915. https://doi.org/10.1109/TFUZZ.2015.2486817
26. H. A. Hagras, A hierarchical type-2 fuzzy logic control architecture for autonomous mobile robots, *IEEE Trans. Fuzzy Syst.*, **12** (2004), 524–539. https://doi.org/10.1109/TFUZZ.2004.832538
27. F. Liu, An efficient centroid type-reduction strategy for general type-2 fuzzy logic system, *Inf. Sci.*, **178** (2008), 2224–2236. https://doi.org/10.1016/j.ins.2007.11.014
28. L. A. Lucas, T. M. Centeno, M. R. Delgado, General type-2 fuzzy inference systems: analysis, design and computational aspects, in *2007 IEEE International Fuzzy Systems Conference*, 2007. https://doi.org/10.1109/FUZZY.2007.4295522
29. S. Greenfield, R. John, Optimised generalised type-2 join and meet operations, in *2007 IEEE International Fuzzy Systems Conference*, (2007), 1–6. https://doi.org/10.1109/FUZZY.2007.4295355
30. M. Deveci, D. Pekaslan, F. Canıtez, The assessment of smart city projects using zSlice type-2 fuzzy sets based Interval Agreement Method, *Sustainable Cities Soc.*, **53** (2020). https://doi.org/10.1016/j.scs.2019.101889
31. H. Zhao, Y. Wang, X. Liu, The assessment of smart city information security risk in China based on zGT2FSs and IAA method, *Sci. Rep.*, **12** (2022). https://doi.org/10.1038/s41598-022-07197-1
32. M. Alali, A. Almogren, M. M. Hassan, I. A. L. Rassan, M. Z. A. Bhuiyan, Improving risk assessment model of cyber security using fuzzy logic inference system, *Comput. Secur.*, **74** (2017), 323–339. https://doi.org/10.1016/j.cose.2017.09.011
33. H. Du, H. Li, L. Yuan, X. Li, Risk assessment model for air traffic control based on fuzzy-ANP method, *China Saf. Sci. J.*, **20** (2010), 79–85.
34. C. Wang, G. Lin, The model of network security risk assess based on fuzzy algorithm and hierarchy, *J. Wuhan Univ.*, **52** (2006), 622–626. https://doi.org/10.1360/jos172601
35. Y. Ou Yang, H. M. Shieh, G. H. Tzeng, A VIKOR technique based on DEMATEL and ANP for information security risk control assessment, *Inf. Sci.*, **232** (2013), 482–500. https://doi.org/10.1016/j.ins.2011.09.012
36. A. P. H. D. Gusmo, L. Silva, M. M. Silva, T. Poleto, A. P. C. S. Costa, Information security risk analysis model using fuzzy decision theory, *Int. J. Inf. Manage.*, **36** (2016), 25–34. https://doi.org/10.1016/j.ijinfomgt.2015.09.003
37. Y. D. Cheng, J. D. He, F. G. Hu, Quantitative risk analysis method of information security-Combining fuzzy comprehensive analysis with information entropy, *J. Discrete Math. Sci. Cryptogr.*, **20** (2017), 149–165. https://doi.org/10.1080/09720529.2016.1178913
38. Z. Wang, H. Zeng, Study on the risk assessment quantitative method of information security, in *2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE)*, 2010. https://doi.org/10.1109/ICACTE.2010.5579187
39. W. Liang, Y. Li, K. Xie, D. Zhang, K. Li, A. Souri, et al., Spatial-temporal aware inductive graph neural network for C-ITS data recovery, *IEEE Trans. Intell. Transp. Syst.*, **2022** (2022), 1–12. https://doi.org/10.1109/TITS.2022.3156266

40. K. Peng, G. Yan, A survey on deep learning for financial risk prediction, *Quant. Finance Econ.*, **5** (2021), 716–737. https://doi.org/10.3934/QFE.2021032
41. Z. Z. Wang, Y. Q. Xie, X. Y. Wu, F. B. Ge, A survey of information security risk evaluation, *Inf. Secur. Commun. Privacy*, **2007** (2007).
42. Y. Song, Y. Shen, G. Zhang, Y. Hu, The information security risk assessment model based on GA-BP, in *2016 7th IEEE International Conference on Software Engineering and Service Science (ICSESS)*, IEEE, (2016), 119–122. https://doi.org/10.1109/ICSESS.2016.7883029
43. L. Wu, J. Zhou, Z. Li, Applying of GA-BP neural network in the land ecological security evaluation, *IAENG Int. J. Comput. Sci.*, **47** (2020), 11–18.
44. W. Guo, Safety risk assessment of tourism management system based on PSO-BP neural network, *Comput. Intell. Neurosci.*, **2021** (2021). https://doi.org/10.1155/2021/1980037
45. R. Deb, S. Roy, A Software Defined Network information security risk assessment based on Pythagorean fuzzy sets, *Expert Syst. Appl.*, **183** (2021), 115383. https://doi.org/10.1016/j.eswa.2021.115383
46. X. Huang, W. Xu, Method of information security risk assessment based on improved fuzzy theory of evidence, *Int. J. Online Eng.*, **14** (2018). https://doi.org/10.3991/ijoe.v14i03.8422
47. M. Raikhan, K. Bolat, Z. Meiram, O. Altynay, Assessing information security risk with the fuzzy set theory, *J. Theor. Appl. Inf. Technol.*, **96** (2018), 3142–3152.
48. B. Zhang, Z. Wang, W. Wang, Z. Wang, H. Liang, D. Liu, Security assessment of intelligent distribution transformer terminal unit based on RBF-SVM, in *2020 IEEE 4th Conference on Energy Internet and Energy System Integration (EI2)*, 2020. https://doi.org/10.1109/EI250167.2020.9346959
49. Q. Liu, P. Sun, X. Fu, J. Zhang, H. Yang, H. Gao, et al., Comparative analysis of BP neural network and RBF neural network in seismic performance evaluation of pier columns, *Mech. Syst. Sig. Process.*, **141** (2020), 106707. https://doi.org/10.1016/j.ymssp.2020.106707
50. R. Li, F. Li, C. Wu, J. Song, Research on vehicle network security situation prediction based on improved CLPSO-RBF, *J. Phys. Conf. Ser.*, **1757** (2021), 012148. https://doi.org/10.1088/1742-6596/1757/1/012148
51. J. Li, W. Du, F. Yang, G. Hua, The carbon subsidy analysis in remanufacturing closed-loop supply chain, *Sustainability*, **6** (2014), 3861–3877. https://doi.org/10.3390/su6063861
52. K. Govindan, D. Kannan, K. M. Shankar, Evaluating the drivers of corporate social responsibility in the mining industry with multi-criteria approach: A multi-stakeholder perspective, *J. Cleaner Prod.*, **84** (2014), 214–232. https://doi.org/10.1016/j.jclepro.2013.12.065
53. H. Liu, P. Wang, Z. Li, Is there any difference in the impact of digital transformation on the quantity and efficiency of enterprise technological innovation? Taking China's agricultural listed companies as an example, *Sustainability*, **13** (2021). https://doi.org/10.3390/su132312972
54. X. Wang, Z. Q. Tang, X. U. Shuo, Information security risk assessment based on fuzzy theory and BRBPNN, *Comput. Simul.*, **36** (2019), 184–189.