IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received February 22, 2020, accepted March 23, 2020, date of publication April 13, 2020, date of current version May 14, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2987735

Enhanced Grey Risk Assessment Model for Support of Cloud Service Provider

ABDUL RAZAQUE[1], (Member, IEEE), FATHI AMSAAD[2], SALIM HARIRI[3], MARWAH ALMASRI[4], SYED S. RIZVI[5], AND MOHAMED BEN HAJ FREJ[6], (Graduate Student Member, IEEE)

[1]Department of Computer Engineering and Telecommunication, International IT University, Almaty 050040, Kazakhstan
[2]Department of Information Security and Applied Computing (SISAC), Eastern Michigan University (EMU), Ypsilanti, MI 48197, USA
[3]Department of Electrical and Computer Engineering, The University of Arizona, Tucson, AZ 85721, USA
[4]Department of Computer Science, College of Computing and Informatics, Saudi Electronic University, Riyadh 13323, Saudi Arabia
[5]Department of Information Sciences and Technology, The Pennsylvania State University, Altoona, PA 16601, USA
[6]Department of Computer Science, University of Bridgeport, Bridgeport, CT 06604, USA

Corresponding author: Abdul Razaque (a.razaque@iitu.kz)

ABSTRACT The cloud computing environment provides easy-to-access service for private and confidential data. However, there are many threats to the leakage of private data. This paper focuses on investigating the vulnerabilities of cloud service providers (CSPs) from three risk aspects: management risks, law risks, and technology risks. Additionally, this paper presents a risk assessment model that is based on grey system theory (GST), defines indicators for assessment, and fully utilizes the analytic hierarchy process (AHP). Furthermore, we use the GST to predict the risk values by using the MATLAB platform. The GST determines the bottom evaluation sequence, while the AHP calculates the index weights. Based on the GST and the AHP, layer-based assessment values are determined for the bottom evaluation sequence and the index weights. The combination of AHP and GST aims to obtain systematic and structured well-defined procedures that are based on step-by-step processes. The AHP and GST methods are applied successfully to handle any risk assessment problem of the CSP. Furthermore, substantial challenges are encountered in determining the CSP's response time and identifying the most suitable solution out of a specified series of solutions. This issue has been handled using two additive features: the response time and the grey incidence. The final risk values are calculated and can be used for prediction by utilizing the enhanced grey model (EGM) (1,1), which reduces the prediction error by providing direct forecast to avoid the iterative prediction shortcoming of standard GM (1,1). Thus, EGM (1,1) helps maintain the reliability on a larger scale despite utilizing more prediction periods. Based on the experimental results, we evaluate the validity, accuracy, and response time of the proposed approach. The simulation experiments were conducted to validate the suitability of the proposed model. The simulation results demonstrate that our risk assessment model contributes to reducing deviation to support CSPs with the three adopted models.

INDEX TERMS Analytic hierarchy process, cloud service provider, deviation reduction, grey model, risk assessment.

I. INTRODUCTION

Cloud computing is becoming a business trend and an investment in many applications. Information technology (IT) and telecommunications in businesses enable organizations to increase their profits [1]. These many companies adopt cloud computing in their businesses to maximize their profits. However, this causes a trust crisis in the industry [2] and creates a trade-off between gains and data privacy/security, which implies that companies that adopt the cloud computing paradigm do not have complete control over the computing resources on which they rely [3]. Therefore, most business-people expect that the CSP they choose will provide a reliable and safe cloud environment, which ensures that businesses can avoid severe data losses due to potential vulnerabilities and security threats in cloud computing [4], [5]. To identify a feasible approach to address the problem, this paper focuses on reliable models that can be used to perform a comprehensive risk assessment for the CSPs. Recently, a substantial amount of research has been conducted on risk assessment [6]

The associate editor coordinating the review of this manuscript and approving it for publication was Kashif Munir.

in cloud computing; however, most of these studies have limitations. A study on the business risk assessment model of city commercial banks that is based on grey system theory [7] applies the factor analysis method to determine the index weight at a micro-level. In the same context, the authors in [8] did not fully utilize grey system theory to determine the bottom evaluation sequence and failed to evaluate the judgment matrix consistency. Motivated by these challenges, the contributions of this paper are summarized as follows:

- Integration of GST and AHP models to determine the risk levels of a CSP, which helps reduce data deviations, and the inclusion of two additive features, namely response time and grey incidence, to facilitate the decision-making process. This contribution has a broader impact because the integration of GST and AHP yields an effective combination of the probability and the security of the risk. Prediction based on AHP-GST methods can be used to control the risk of CSP.
- EGM (1,1) is adopted to overcome the prediction error in GM (1,1). If the prediction horizon size increases, then the prediction error of GM (1,1) increases. Thus, EGM (1,1) not only produces a more reliable short-term prediction of CSP but also yields a reliable long-term prediction, which helps customers choose a more reliable CSP company.
- Additive features (the response time and the grey incidence) are incorporated to help determine the response time and to find a suitable solution among the specified solutions for the CSP when risk is encountered.

As many applications of cloud computing technology are increasingly used, security becomes critical. The major problem is to find a secure and stable CSP so that businesses can be less vulnerable to security attacks. However, at present, there is a lack of structured risk assessment approaches for realizing this objective. The traditional technical methods of risk assessment utilize subjective evaluations, which are easily affected by human factors; hence, the data tend to experience deviations. The bottom index evaluation, which is a first data item in the AHP model, is of high significance for obtaining the risk level and the index weight. The index weight is used as part of the objective assessment of CSPs.

To realize objective and comprehensive risk assessment of CSPs, the following should be considered: (a) how to classify risk elements, (b) how to determine the bottom index evaluation, and (c) how to determine the index weight. We find the answers to these questions and utilize them in our experimental results to make predictions regarding the best available CSPs. The remainder of the paper is organized as follows. Section II briefly analyzes the state-of-the-art related work. In Section III, the motivation behind the integration of GST-AHP models and EGM (1,1) is presented. Section IV presents the proposed GST, AHP, and EGM (1,1). Section V presents experimental results and a detailed evaluation of the performance of the proposed scheme and compares the results of EGM (1, 1) with other contending models. In Section VI, a security risk project which includes the result of the discussion is introduced. Finally, the conclusions of the paper are presented in Section VII.

II. RELATED WORK

In this section, the salient characteristics of existing approaches are discussed. A qualitative analysis model is proposed for making qualitative judgments on commercial banks' risks [9]. The proposed method is based on expert scoring and the Delphi methods, which contribute to quantitative estimates in the absence of sufficient statistical and raw data. However, the proposed method has limitations since it is based on a subjective model that leads to data fluctuation; therefore, the results are inaccurate, unreliable, and the model does not have typical adaptability. Hence, it cannot be applied in most cases. Ren *et al.* [10] proposed a new evaluation system that uses grey relational clustering to determine the index weight. The innovation of the new evaluation system lies in two aspects. First, some high indicators can be deleted with the help of the grey relational clustering. Second, factor analysis is applied to determine weights among layers. The use of grey system theory as a model facilitates the determination of the values of the solution layer accurately. However, the main disadvantage of the new evaluation system is that the factor analysis that is used to determine the index weight is typically conducted at a micro-level.

He [11] uses AHP as part of the proposed scheme to perform risk assessment efficiently. Using the proposed method, the relative weights of elements that are related to the information security risk could be calculated. Then, the optimal indicators, which provide a strong basis for taking relevant measures, could be selected by sorting the weights of the elements to reduce the number of indicators. However, the method that is proposed in his paper is limited. The result is likely to exhibit deviations since, in the model, the experimental data are not used to perform a consistency test.

Mahmod and Watanabe [12] introduced a modified grey model (MGM) for identifying the best input trend of the model with suitable values of the input parameters for adequately fitting the observations. The MGM helped reduce the calculation time. However, MGM cannot determine the risk value efficiently. Huiru and Guo [13] proposed a hybrid optimized grey model that uses the rolling mechanism and the ant lion optimizer R-ALO-GM (1, 1). The parameters of GM (1, 1) were identified by using the ant lion optimizer, which is a novel nature-inspired algorithm. The rolling mechanism was integrated for predicting the accuracy improvement. Two cases were selected for evaluating the efficiency and viability of the proposed Rolling-ALO-GM (1, 1) for annual power load forecasting. The empirical results demonstrate the performance of the proposed R-ALO-GM (1, 1) model. It has been claimed that the proposed model could substantially improve load prediction accuracy. Tien [14] proposed the first-entry grey model (FGM (1,1)) for overcoming the limitations of GM (1,1). The proposed FGM (1,1) proved that the first entry of the original series in GM (1,1) was unproductive for prediction. Hence, to handle this issue, arbitrary values were inserted before the original series. Xuan *et al.* [15] introduced the improved analytic hierarchy process (IAHP) for determining and controlling an index weight and evaluating the two theories' outcomes. The proposed approach attempted to determine weight accuracy. After extensive study of existing approaches, we determined that the prevailing proposed approaches are of substantial significance. All these approaches try to improve accuracy; however, our approach not only improves the accuracy but also reduces the risk and the deviation.

III. MOTIVATION BEHIND THE INTEGRATION OF GST-AHP MODELS AND EGM (1,1)

Most cloud computing problems cannot be predicted by precise attribute values but can be articulated using fuzzy values. Therefore, in cloud services, it is essential to extend the white numbers to grey numbers for real-time systems. Thus, GST deals with inadequate and imperfect information to increase the restrictions of using old-fashioned statistical methods. It can determine quantitative and qualitative relationships among complex dynamics with insufficient information. In contrast, the AHP method identifies the weights of CSP's evaluation criteria. It assigns values that are based on the actual conditions and uses a similar judgment process, a decomposition process, and a complete rational model for decision-making. Thus, AHP is an essential tool for system investigation [16]. AHP and GST are useful and practical; however, neither method can systematically handle the scenario of several elements performing together. As a result, the accuracy remains poor. To advance the accuracy, objectivity, and efficiency of the system, GST and AHP evaluate and estimate the scoring value.

The motivations behind the use of the hybrid method are to obtain systematic and structured results via well-defined and step-by-step procedures, to realize transparency of the computation process, and to ensure rational and logical results with an adequate mathematical foundation. The AHP and GST methods can also be applied to handle successfully any risk assessment problem of cloud computing. The integration of the two approaches, along with the addition of two additive features, namely, grey incidence and response time, can solve the risk assessment problems of cloud computing, including commercial and business applications, effectively. The existing GM (1,1) only applies the prediction values to obtain the predicted values for the next time. In the case of increasing prediction horizon, prediction values cannot be acquired based on the previously observed values after a while. This leads to the prediction error in the assessment model. Thus, EGM (1,1) provides grey direct prediction by resolving the issue of GM (1,1). Furthermore, it uses the period's prediction values $'Pr_v'$, which is based on the previous period's real observation values $'P_{ov}'$, in the grey direct prediction.

IV. PROPOSED GST, AHP, AND EGM (1,1)

A. MODEL CONSTRUCTION

We propose a new risk assessment scheme for CSP that is based on the GST, AHP, and EGM (1,1) models, as illustrated in Fig. 1. EGM (1,1) is an extension of standard GM (1,1) [17], [18]. GST is used to determine the bottom evaluation sequence, whereas AHP is used to determine the index weight. through these two schemes, we obtain values that indicate the risk level of a CSP by multiplying the bottom evaluation sequence with the index weight. The features of GST and AHP are combined and added with EGM (1,1). Additionally, the additive features (response time and grey incidence) are incorporated to support EGM (1,1). Finally, the risk assessment can be predicted based on the collected data.

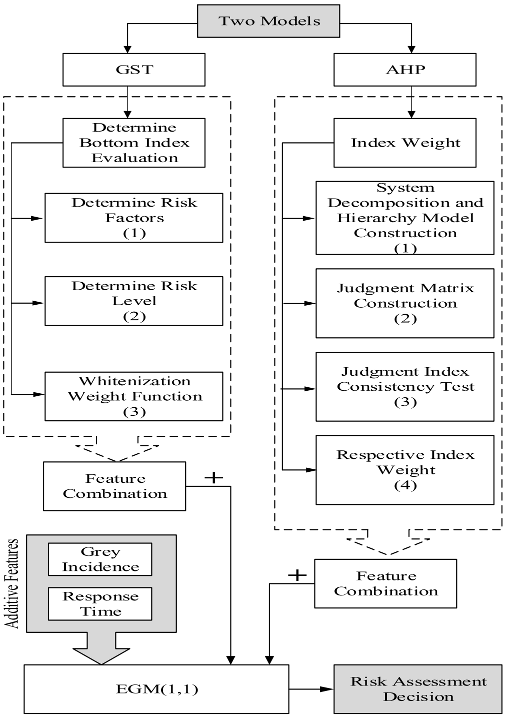
Two Models
GST
AHP
Determine Bottom Index Evaluation
Determine Risk Factors (1)
Determine Risk Level (2)
Whitenization Weight Function (3)
Index Weight
System Decomposition and Hierarchy Model Construction (1)
Judgment Matrix Construction (2)
Judgment Index Consistency Test (3)
Respective Index Weight (4)
Feature Combination
+
Additive Features
Grey Incidence
Response Time
Feature Combination
+
EGM(1,1)
Risk Assessment Decision

FIGURE 1. Models for risk assessment.

B. DETERMINE THE RISK FACTORS OF CLOUD SERVICE PROVIDERS (CSPs)

To perform a risk assessment for CSPs, we conduct thorough research to identify the most relevant risk factors [19]–[27]. The CSP risks are classified into three categories: management risks, law risks, and technical risks. A CSP is affected by a combination of risks, which involve various configurable computing resources such as networks [28]–[32], servers, storage, services, and applications, which facilitate the provision of convenient and on-demand access to the cloud by users [33]–[35].

The goal is to ensure the security of the CSP. The factors are represented in three levels: The first level factors are F_1, F_2, F_3. The second-level factors are $F_{11}, F_{12}, F_{21}, F_{31}, F_{32}$. The third-level factors are $F_{111}, F_{112}, F_{113}, F_{121}, F_{122}, F_{123}, F_{211}, F_{212}, F_{213}, F_{311}, F_{312}, F_{313}, F_{314}, F_{321}, F_{322}, F_{323}$. These three levels of security factors are shown in Fig. 2.

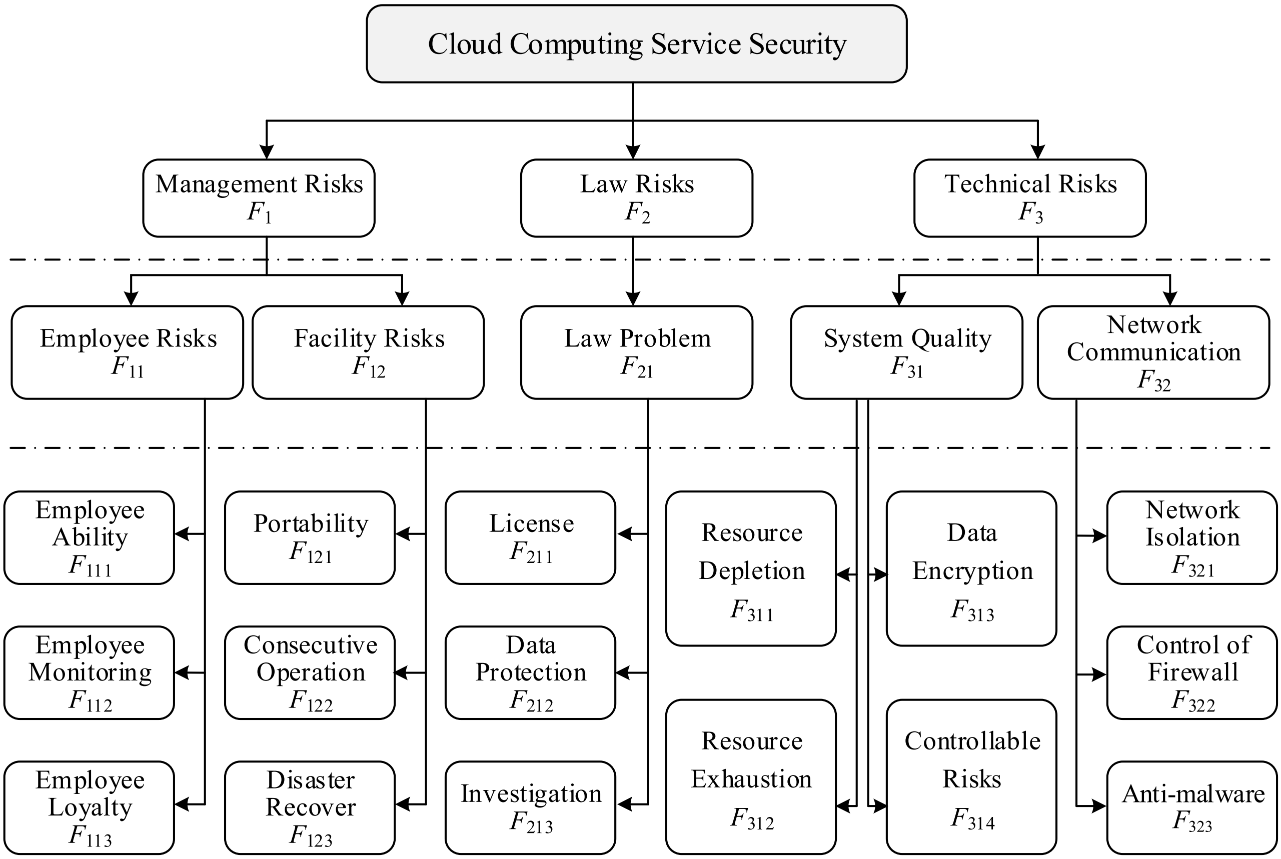
Cloud Computing Service Security
Management Risks F_1
Law Risks F_2
Technical Risks F_3
Employee Risks F_{11}
Facility Risks F_{12}
Law Problem F_{21}
System Quality F_{31}
Network Communication F_{32}
Employee Ability F_{111}
Employee Monitoring F_{112}
Employee Loyalty F_{113}
Portability F_{121}
Consecutive Operation F_{122}
Disaster Recover F_{123}
License F_{211}
Data Protection F_{212}
Investigation F_{213}
Resource Depletion F_{311}
Resource Exhaustion F_{312}
Data Encryption F_{313}
Controllable Risks F_{314}
Network Isolation F_{321}
Control of Firewall F_{322}
Anti-malware F_{323}

FIGURE 2. Risk factors for CSP.

TABLE 1. Criteria of risk rank.

Level	Characteristic	Description
5	Very high	Once it happens it will cause significant damage to the economy and society.
4	High	Once it happens, it will cause superior damage to the economy and society.
3	Medium	Once it happens, it will cause damage to the economy and society, but the damage degree is not huge.
2	Low	Once it happens, it can be handled in a short time, and the damage degree is small.
1	Very low	Once it happens, there can hardly be any influence or can be handled with simple solutions.

C. DETERMINE RISK LEVELS

Table 1 is based on "GB/T 20984-2007 Information security technology – Risk assessment specification for information security" [36]. According to Table 1, the risk assessment can be divided into five levels [37], as shown.

D. BUILDING THE GREY SYSTEM MODEL (GSM)

1) BOTTOM INDEX EVALUATION

To establish the relationships between the risk levels and grey clustering, our objective is to create a "whitenization" weight function that is based on the grey number and to use that information to transform the data that are provided by experts into a weight vector of the evaluation indices. Using this vector, we can determine the risk level of assessing indices.

- Bottom Evaluation sequence can be defined as:

$$F_{111}, F_{112}, F_{113}, F_{121}, F_{122}, F_{123}, F_{211}, F_{212}, F_{213}, F_{311}, F_{312}, F_{313}, F_{314}, F_{321}, F_{322}, F_{323}$$

- Evaluation Experts $'i'$ can be defined as: $i = 1, 2, 3 \ldots, \mathrm{m}$. where m is the total number of evaluation experts
  In grey intervals, each value of x has different weights. We use f(x) to represent the weights which belong to x and use $\otimes(x) = h$ to represent the value of x. The Whitenization weight function is defined as [38]:

$$f(x) = \begin{cases} x/h, & x \in [0, 6-h] \\ (5-x)/(h-1), & x \in [6-h, 5] \\ 0, & x \notin [0, 5] \end{cases} \quad (1)$$

where h is the grey clustering. The maximum return value from the function is 1, and the minimum is 0.

According to Table 1, it is concerned with the risk levels classification, the grey clustering: h = {1,2,3,4,5}. The five functions mentioned below are used to help determine the grey clustering sum in the later computations. The first grey clustering ($h = 1$) represents the very high-risk level. The domain is, therefore, ⊗_1 ∈ [0,5 ∞]. When we substitute $h = 1$ into (1), we get:

$$\mathrm{f}_1(\mathrm{x}_{\mathrm{ij}}) = \begin{cases} \mathrm{x}_{\mathrm{ij}}/5, & \mathrm{x}_{\mathrm{ij}} \in [0, 5] \\ 1, & \mathrm{x}_{\mathrm{ij}} \in [5, \infty) \\ 0, & \mathrm{x}_{\mathrm{ij}} \notin [0, \infty) \end{cases} \tag{2}$$

The first grey clustering ($h = 2$) represents the high-risk level. The domain is $\otimes_1 \in [0, 4, 5]$. When we substitute $h = 2$ into (1), we get:

$$\mathrm{f}_2(\mathrm{x}_{\mathrm{ij}}) = \begin{cases} \mathrm{x}_{\mathrm{ij}}/4, & \mathrm{x}_{\mathrm{ij}} \in [0, 4] \\ 5 - \mathrm{x}_{\mathrm{ij}}, & \mathrm{x}_{\mathrm{ij}} \in [4, 5] \\ 0, & \mathrm{x}_{\mathrm{ij}} \notin [0, 5] \end{cases} \tag{3}$$

The first grey clustering ($h = 3$): it represents the medium risk level. The domain is $\otimes_1 \in [0, 3, 5]$. When we substitute $h = 3$ into (1), we get:

$$\mathrm{f}_3(\mathrm{x}_{\mathrm{ij}}) = \begin{cases} \mathrm{x}_{\mathrm{ij}}/3, & \mathrm{x}_{\mathrm{ij}} \in [0, 3] \\ (5-\mathrm{x}_{\mathrm{ij}})/2, & \mathrm{x}_{\mathrm{ij}} \in [3, 5] \\ 0, & \mathrm{x}_{\mathrm{ij}} \notin [0, 5] \end{cases} \tag{4}$$

The first grey clustering ($\mathrm{h} = 4$): it represents the low-risk level. The domain is $\otimes_1 \in [0, 2, 5]$. When we substitute into Equation (1), we get:

$$\mathrm{f}_4(\mathrm{x}_{\mathrm{ij}}) = \begin{cases} \mathrm{x}_{\mathrm{ij}}/2, & \mathrm{x}_{\mathrm{ij}} \in [0, 2] \\ (5-\mathrm{x}_{\mathrm{ij}})/3, & \mathrm{x}_{\mathrm{ij}} \in [2, 5] \\ 0, & \mathrm{x}_{\mathrm{ij}} \notin [0, 5] \end{cases} \tag{5}$$

The first grey clustering ($\mathrm{h} = 5$): it represents a very low-risk level. The domain is $\otimes_1 \in [0, 1, 5]$. Substitute $h = 5$ into (1), we get:

$$\mathrm{f}_5(\mathrm{x}_{\mathrm{ij}}) = \begin{cases} 1, & \mathrm{x}_{\mathrm{ij}} \in [0, 1] \\ (5-\mathrm{x}_{\mathrm{ij}})/4, & \mathrm{x}_{\mathrm{ij}} \in [1, 5] \\ 0, & \mathrm{x}_{\mathrm{ij}} \notin [0, 5] \end{cases} \tag{6}$$

In the further calculation of the bottom indexes, we make a table which has i rows and j columns. Then the sample matrix x_{ij} is taken from Table 1.

According to the f_k concluded by evaluation index j which is evaluated by an expert i and sample x_{ij}, we can compute the weight vector for evaluation index j, which belonged to the Grey clustering h (where $h = 1,2,3,4,5$).

$$r_{jh} \sum_{i=1}^{m} f_{h}(x_{ij}) \tag{7}$$

Equation (7) represents the sum of the evaluation values that each expert gives, and the dependent variable is x_{ij}; x_{ij} taken from the sample matrix $X = \mathrm{x}_{\mathrm{ij}}$; where m is the total number of expert *i.*

$$r_j \sum_{h=1}^{5} r_{jh} \tag{8}$$

Equation (8) represents the Grey clustering sum of *j* columns, which consists on adding up n_{jh} calculated in (8).

$$\xi_{\mathrm{jh}} = \frac{\mathrm{r}_{\mathrm{jh}}}{\mathrm{r}_{\mathrm{j}}} \tag{9}$$

Equation (9) represents the statistics of the evaluation index *j,* which is belonged to the Grey clustering *h*, that is the quotient of (8) and (9). Similarly, $\xi_j = (\xi_{j1}\ \xi_{j2}\ \xi_{j3}\ \xi_{j4}\ \xi_{j5})$ represents the weight vector of the evaluation index *j,* and it is made up of the value from (9). U = (5, 4, 3, 2, 1) represents the numeric vector of each evaluation grey clustering level. The vector is decided from Table 1 to represent the risk level ranking in the descending order. Taking this into account, we get a comprehensive evaluation value which could be expressed as follows:

$$V = \sigma \times U^{T} \tag{10}$$

Equation (10) represents the comprehensive evaluation value of the evaluation index.

E. DEVELOPING THE ANALYTICAL HIERARCHY PROCESS MODEL

To organize and analyze complicated decisions, the AHP is a relatively structured management technique. It was developed by Thomas L. Saaty in the 1970s and has been extensively researched. In the subsequent sections, we will discuss the steps of this method.

1) DECOMPOSITION OF THE SYSTEM AND THE CONSTRUCTION OF THE HIERARCHY MODEL

This model consists of three layers, namely, the target layer, the criterion layer, and the solution layer, as illustrated in Fig. 3.

2) CONSTRUCTION OF THE JUDGEMENT MATRIX

The judgment matrix is constructed by comparing an element in its target layer with all elements that are related to it. For example, for criterion *H* in the criterion layer, *n* elements are related to it in the solution layer. Therefore, the judgment matrix is expressed as:

$$\mathrm{A} = \begin{bmatrix} a_{11} & a_{12} & a_{13} & \ldots\ldots a_{1j} \\ a_{21} & a_{22} & a_{23} & \ldots\ldots a_{2j} \\ a_{31} & a_{32} & a_{33} & \ldots\ldots a_{3j} \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots \\ a\quad_{i1} & a\quad_{i2} & a\quad_{i3} & \ldots\ldots a\ _{ij} \end{bmatrix}$$
$$(\mathrm{i} = 1, 2, 3 \ldots\ldots \mathrm{n};\ \mathrm{ji} = 1, 2, 3 \ldots\ldots \mathrm{n}) \tag{11}$$

In the matrix above (11), a_{ij} refers to the ratio of the importance of element i and element j in terms of the criterion H and satisfies $a_{ji} = \frac{1}{a_{ij}}$, where a_{ij} represents the scale between factor u_i and factor u_j. In the analytic hierarchy process, the comparison of the two elements can become quantitative according to Saaty's 1-9 scale method [36], as shown in Table 2.

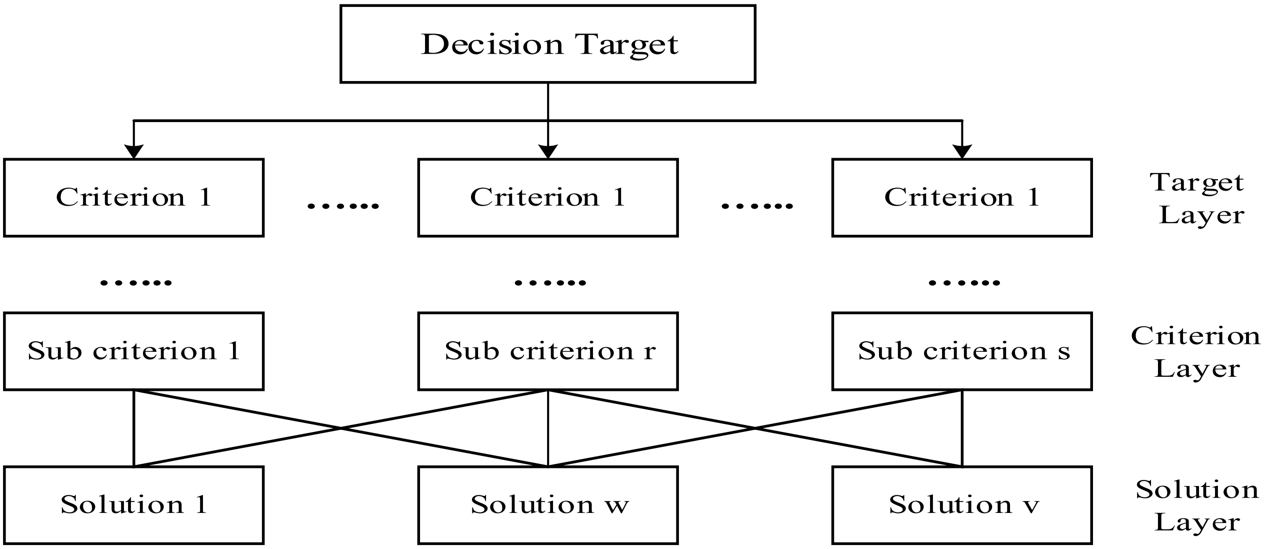

FIGURE 3. Construction of the hierarchy model.

TABLE 2. Saaty's 1-9 scale method.

Scale	Meaning (the comparison of the two elements)
1	The two elements are of equal importance
3	One element is slightly more important than another element
5	One element is more important than another element
7	One element is strongly more important than another element
9	One element is extremely more important than another element
2,4,6,8	Median of the two adjacent judgments above
Reciprocal of the number above	The importance ratio of the element i and element j are $\boldsymbol{a_{ij}}$, so the importance ratio of the element j and the element i is $\boldsymbol{a_{ji}} = \frac{\mathbf{1}}{\boldsymbol{a_{ij}}}$

TABLE 3. Values of RI [16].

N	1	2	3	4	5	6	7	8	9
RI	0	0	0.58	0.90	1.12	1.24	1.32	1.41	1.45

3) JUDGMENT MATRIX CONSISTENCY TEST

Once we obtain the judgment matrix, the relative weights are computed with the greatest characteristic root which is used for getting consistency index (*CI*). The equation for computing greatest characteristic root is expressed as follows:

$$\lambda_{max} = \frac{1}{n}\sum_{i=1}^{n}\frac{(Aw)_i}{w_i} \tag{12}$$

where λ_{max}: Greatest Characteristic Root; *A*: the judgment matrix; *w*: weight vector; *n*: order of the judgment matrix; $(Aw)_i$: the number *i* element of *Aw*.

Consistency Index (*CI*):

$$\mathrm{CI} = \frac{\lambda_{max} - n}{n-1} \tag{13}$$

where *n* is the order of the judgment matrix.

Consistency Ratio (*CR*):

$$\mathrm{CR} = \frac{CI}{RI} \tag{14}$$

where *RI* is given by Saaty and the table of the value is given in Table 3. Satty has also given the values of *RI,* as shown in Table 3. When *CR*<0.10. The judgment matrix meets the consistency index. The corresponding weight is the one we need. If *CR* does not satisfy the requirement, the judgment matrix needs to be adjusted to meet the consistency expectation (i.e., CR < 0.1)

4) COMPUTATION OF THE RESPECTIVE INDEX WEIGHTS

To determine the weights of indices for the risk assessment of CSPs, we invited experts who are working on cloud computing research to score the evaluation indices. The objective is to compare the indices at the same level in pairs and to provide promotional scale fractions according to the relative importance of the indices. The results of this exercise will be used in the judgment matrices.

a: COMPUTATION OF THE RESPECTIVE INDEX WEIGHTS

In this sub-section, we discuss the computation of weights used in the judgment matrices. The fundamental computation equation can be expressed as:

$$4\ \mathrm{A}= \begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{1n} \\ a_{21} & a_{22} & a_{23} & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}$$

(n is the number of the compared elements) *a) Use Root Method to Compute the Feature Vector:*

$$\overline{w_i} = \sqrt[n]{\prod_{j=1}^{n} \mathrm{a}_{ij}} \quad (i = 1, 2 \ldots, \mathrm{n}; \quad \text{where n is the order of the judgment matrix}) \quad (15)$$

So, the vector $v = (\overline{w_1}, \overline{w_2}, \ldots, \overline{w_n})^T$ can be obtained by using $\frac{\overline{w_i}}{\sum_{j=1}^{n} \overline{w_j}}$ (i = 1, 2,…,n) to normalize the vector v, The vector $v = (w_1, w_2, \ldots, w_n)^T$ is the needed feature vector. The most significant characteristic root can be obtained as shown in (12).

b) Judgment Matrix Consistency Test: In the judgment matrix consistency test, if $CR < 0.10$, the result is accepted. Then, second-level and third-level indices can be computed. Otherwise, the judgment matrix must be modified until it meets the standard ($CR < 0.1$).

b: EXPERT SCORING METHOD

Facilitated by the expert scoring method, the elementary scores for the indices are obtained [41].

F. ADDITIVE FEATURES

A grey prediction model can help determine whether the following additive features should be incorporated into the model or not:

- Response Time;
- Grey Incidence

1) RESPONSE TIME

The response time is the intervening time between a probe on the system and the response to the inquiry. Shorter response time improves the performance and reduces the critical risk. Based on differential values, let us assume that if a development coefficient value $'c'$ lies in the specific range, then the relationship between the risk and the inflation rate $\frac{\Delta p}{p}$ can be expressed as

$$\frac{\Delta p}{p} = c + \beta \frac{1}{y} \quad (16)$$

Thus, the basic grey model can be expressed as

$$y^{(0)}(k) + dz^{(1)}(k) = \beta \quad (17)$$

The shadow of the grey model is

$$\frac{dy^{(1)}}{dt} + cy^{(1)} = \beta \quad (18)$$

Equation (17) can be substituted by a differential equation. Thus, the response time of $EGM(1, 1)$ for CSP can be calculated via equation (19) and this response time can be used in the risk prediction process.

$$\hat{\mathrm{y}}^{(1)}(k+1) = \left(y^{(0)}(1) - \frac{\beta}{c}\right) e^{-ck} + \frac{c}{\beta}, \quad k= 1, 2, \ldots, n \quad (19)$$

where β denotes the grey model, $\hat{\mathrm{y}}$ the risk response time, and k the number of cloud users.

2) GREY INCIDENCE

The grey incidence facilitates the provision of methods for identifying the most suitable solution among a specified series of solutions for a real-world problem. The grey incidence is based on nearness and similarity.

Definition 1: Grey incidence degree

Let A_i, with $i \in M_2^+$, denote two orders of similar length that describe the sum of the risks between two successive time instants as follows:

$$G_i = \int_1^n (A_i - a_i(1))\, dt \; i \in M_2^+ \quad (20)$$

$$G_1 - G_2 = \int_1^n \{(A_1 - a_1(1)) - (A_2 - a_2(1))\, dt \quad (21)$$

$$\gamma_{12} = \frac{1 + |G_1| + |G_2|}{1 + |G_1| + |G_2| + |G_1 - G_2|} \quad (22)$$

This is referred to as the grey incidence between A_1 and A_2. This model can be used to determine whether the obtained risks should be treated differently. Assume that $'n'$ predicted risks $'i'$ are clustered into $'s'$ grey classes based on $'m'$ criteria. The predicted value of risk $'i'$ in terms of criterion $'j'$ is denoted as a_{ij}, with $i \in M_m^+$ and j $\in M_n^+$. The risk $'i'$ should be analyzed and identified on a_{ij} effectively.

G. EGM (1,1)

Through the GST and AHP models, the risk data that are used to assess the risk levels of the CSP in a specified year can be generated. This approach, the values for other years are obtained. Then, with these values and the EGM (1,1) model, the security levels in the coming years can be predicted. The process of the EGM (1,1) model will be discussed in the subsequent section.

1) DETERMINATION OF EGM (1,1)

The GM (1,1) model has been widely applied in several fields. It is a type of homogeneous exponential growth model that is based on the accumulation generation sequence and the least square method. GM (1,1) does not require prior information, but it can be used with limited input data. Thus, enhancement of the basic GM (1,1) is necessary for obtaining a more accurate prediction. GM (1,1) suffers from limited performance because it uses only predicted values to calculate the next period's prediction value for a short period. As the prediction horizon size increases, GM (1,1) produces larger prediction error. EGM (1,1) is adopted to handle the prediction error issue in GM (1,1). Thus, EGM (1,1) yields not only more reliable short-term predictions of CSP but also more reliable long-term predictions, which facilitates the selection of a more reliable CSP company by customers. If equations are available for $Pr_v > k$, new prediction values are not acquired using the previous observation values $'P_{ov}'$ after a specified period. Thus, EGM (1,1) is applied both iteratively and indirectly if the number of predicted periods is sufficiently large. The working process of EGM (1,1) is illustrated in Fig. 4.

Where G_l denotes the grey Length and γ the number of observations in the modeling set.

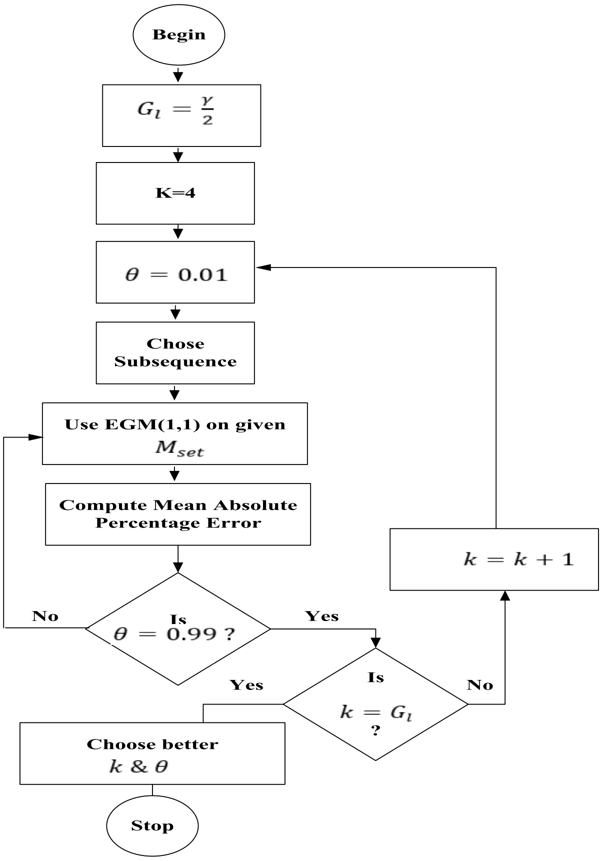

FIGURE 4. **Proposed EGM (1,1).**

Thus, EGM (1,1) provides grey direct prediction by resolving the issue that is encountered with GM (1,1). Furthermore, it uses the period's prediction values $'Pr_v'$ that are based on the previous period's real observation values $'P_{ov}'$ in the grey direct prediction. The complete derivations of EGM (1,1) are available.

(i) Suppose an original data sequence $X^{(0)}$ is given by:

$$X^{(0)} = \left(x^{(0)}(1), x^{(0)}(2), \ldots, x^{(0)}(n)\right) \quad \text{where } x^{(0)}(i) > 0, \; i = 1, 2, \ldots, n.$$

(ii) Accumulate the sequence: $\mathrm{x}^{(1)}(\mathrm{k}) = \sum_{\mathrm{i}=1}^{\mathrm{k}} \mathrm{x}^{(0)}(\mathrm{i})$

(iii) Generate the accumulation sequence:

$$X^{(1)} = \left(x^{(1)}(1), x^{(1)}(2), \ldots, x^{(1)}(n)\right)$$

$$\text{where } x^{(1)}(1) = x^{(0)}(1), x^{(1)}(k) = \sum_{i=1}^{k} x^{(0)}(i) \quad (k = 1, 2, \ldots, n).$$

(iv) Through the first-order accumulative generation sequence $X^{(1)}$, EGM (1, 1) model is established; a first-order differential equation can be generated as follows:

$$\frac{d_{x^{(1)}}}{d_t} + bx^{(1)} = m \qquad (23)$$

where b is the development Grey number and m is the endogenous control Grey number. The discretization yields the Equation (25) as follows:

$$\Delta^{(1)}[x^{(1)}(k+1)] + az^{(1)}(x(k+1)) = m \qquad (24)$$

where the $\Delta^{(1)}[x^{(1)}(k+1)]$ represents the consequence produced by $x^{(1)}$ With the method of IAGO at the time of $(k+1)$. Further derivations yield (25) and (26) as follows:

$$x^{(0)}(k+1) = b - \frac{1}{2}[x^{(1)}(k) + x^{(1)}(k+1)]\} + m \qquad (25)$$

Expanding (25) yields:

$$\left[\mathrm{x}^{(0)}(2)\,\mathrm{x}^{(0)}(3)\ldots\mathrm{x}^{(0)}(\mathrm{n})\right]^{\mathrm{T}} = \begin{bmatrix} -\frac{1}{2}[x^{(1)}(1) + x^{(1)}(2) & 1 \\ -\frac{1}{2}[x^{(1)}(2) + x^{(1)}(3) & 1 \\ \ldots & \ldots \\ -\frac{1}{2}[x^{(1)}(n-1) + x^{(1)}(n) & 1 \end{bmatrix} [\begin{smallmatrix} b \\ m \end{smallmatrix}] \qquad (26)$$

Equation (25) can be simplified and substituted in (26) to produce the following relationship:

$$Y = B\phi \qquad (27)$$

where: $Y = \left[x^{(0)}(2)\,x^{(0)}(3)\ldots x^{(0)}(n)\right]^T$ and $B = \begin{bmatrix} -\frac{1}{2}[x^{(1)}(1) + x^{(1)}(2) & 1 \\ -\frac{1}{2}[x^{(1)}(2) + x^{(1)}(3) & 1 \\ \ldots & \ldots \\ -\frac{1}{2}[x^{(1)}(n-1) + x^{(1)}(n) & 1 \end{bmatrix}$ and $\phi = [bm]^T$.

(vii) Least square method: The parameter vector ϕ can be computed by the least square method.

$$\phi = [\hat{b}\hat{m}]^T = (B^T B)^{-1} B^T Y \qquad (28)$$

(viii) Substitute the result into (28) and compute the discrete solution using the following:

$$\hat{x}^{(1)}(k+1) = [x^{(1)}(1) - \frac{\hat{m}}{\hat{b}}]e^{-\hat{b}k} + \frac{\hat{m}}{\hat{b}} \qquad (29)$$

Restoring to the raw data produces Equation (30) which is expressed as follows:

$$\begin{aligned} \hat{x}^{(0)}(\mathrm{k}+1) &= \hat{x}^{(1)}(\mathrm{k}+1) - \hat{x}^{(1)}(\mathrm{k}) \\ &= (1 - \mathrm{e}^{-\hat{a}})\left[\mathrm{x}^{(1)}(1) - \frac{\hat{m}}{\hat{b}}\right] * \mathrm{e}^{-\hat{b}\mathrm{k}} \end{aligned} \qquad (30)$$

Equations (29) and (30) express the time-dependent function model of EGM (1,1). They are the concrete computation formulas of enhanced grey prediction.

According to (31-34), the prediction of EGM (1,1) depends on the use of previous real observations. It helps select the previous observation values $'P_{ov}'$ after a specified period. Let us assume that if P_{ov}= 2, then the proposed EGM (1,1) applies subsequence $\{X_t, X_t - 2, X_t - 4, \ldots, X_t - 2k + 2\}$ for the next two-period prediction. To predict future periods, the previous observation values P_{ov} are chosen from the current time to k in every P_{ov} periods. Thus, subsequence $\{X_t, X_t - P_{ov}, X_t - 2P_{ov}, \ldots, -P_{ov}(k) + P_{ov}\}$ can be used to predict $\dot{\mathrm{X}}_{t+P_{ov}}$. GM(1,1) uses $k = 4$ and $\theta = 0.5$; however,

TABLE 4. Notation of parameters.

Parameters	Description
$\boldsymbol{F}_{(numbers)}$	The name of indexes
h	Grey clustering
$\boldsymbol{r_{jh}}$	The sum of the evaluation values
$\boldsymbol{r_j}$	The grey clustering sum of j columns
U	Numeric vector for grey clustering and U = (5 4 3 2 1)
V	The comprehensive evaluation
$\boldsymbol{\xi}$	Evaluation sequence
F(numbers)	The name of judgment matrixes
$\boldsymbol{\lambda_{max}}$	The greatest characteristic root
CR	Consistency ratio
v	Index weight vector

the values of both of these factors can affect the prediction of EGM(1,1). Thus, the values of both factors can be increased to improve the risk assessment performance.

$$[X_{t+1} = EGM(1,1)\{X_t, X_{t-1}, \ldots, X_t - k+1\}] \quad (31)$$

$$\left[X_{t+2} = EGM(1,1)\left\{X_t, X_{t-2}, X_{t-4}, \ldots, X_t - 2k+2\right\}\right] \quad (32)$$

$$\left[X_{t+3} = EGM(1,1)\left\{X_t, X_{t-3}, X_{t-6}, \ldots, X_t - 3k+3\right\}\right] \quad (33)$$

$$\left[\dot{X}_{t+P_{ov}} = EGM(1,1)\left\{X_t, X_{t-P_{ov}}, X_{t-2P_{ov}}, \ldots, X_t - P_{ov}k + P_{ov}\right\}\right] \quad (34)$$

V. EXPERIMENTAL EVALUATION

To evaluate the performance of the proposed model, we calculate the evaluation values and determine the risk level for the year 2017. The calculation of the index weights and the evaluation values and the prediction of EGM are conducted in Matlab2016 on a computer with the Windows 8 operating system. We consider four scores for every third-level index and calculate the bottom evaluation sequences. After conducting the consistency test in MATLAB, we calculate the evaluation values for second-level and first-level indices. Then, we determine the comprehensive values for the past nine years and make predictions in the next step. The parameters are listed in Table 4.

A. EXPERT SCORING

To determine an expert score for the CSP risk, various risk detection studies have been conducted [27], [33], [42]–[45], which serve as guides for expert data collection. To realize this objective, a web questionnaire was constructed and a total of 80 participants were invited to participate to obtain the expert data. From Enterprise Resource Planning China, NetSuite, SYSPRO, and ERPAG (ERP cloud service), 35, 22, 9, and 14 participants, respectively, are chosen. The average collected data are listed in Table 5. According to Table 5, the risk assessment can be divided into five levels: very high, high, medium, low, and very low. The values are assigned as 5, 4, 3, 2, and 1.

Then we can draw a graph to show the data in Table 5, and show it in Fig. 5:

TABLE 5. Expert scoring for the cloud service provider.

	Expert 1	Expert 2	Expert 3	Expert 4
Employee ability $\boldsymbol{F_{111}}$	3	3.5	2.5	3
Employee monitoring $\boldsymbol{F_{112}}$	2.5	3	2	2.5
Employee loyalty $\boldsymbol{F_{113}}$	1	1.5	1	1.5
Portability $\boldsymbol{F_{121}}$	4.5	4.5	4	3.5
Consecutive operation $\boldsymbol{F_{122}}$	2.5	3	3	3
Disaster recover $\boldsymbol{F_{123}}$	2	1.5	2	2
License $\boldsymbol{F_{211}}$	2.5	3	3	3
Data protection $\boldsymbol{F_{212}}$	3	2.5	2.5	2
Investigation $\boldsymbol{F_{213}}$	2	2	2.5	2
Resource depletion $\boldsymbol{F_{311}}$	3	3.5	3.5	4
Resource exhaustion $\boldsymbol{F_{312}}$	1	0.5	0.5	1
Controllable risks $\boldsymbol{F_{313}}$	2	1.5	2	2
Data encryption $\boldsymbol{F_{314}}$	4.5	4	4.5	4
Network isolation $\boldsymbol{F_{321}}$	0.5	1	0.5	0.5
Control of firewall $\boldsymbol{F_{322}}$	1	0.5	0.5	1
Anti-malware $\boldsymbol{F_{323}}$	2.5	3	3.5	3

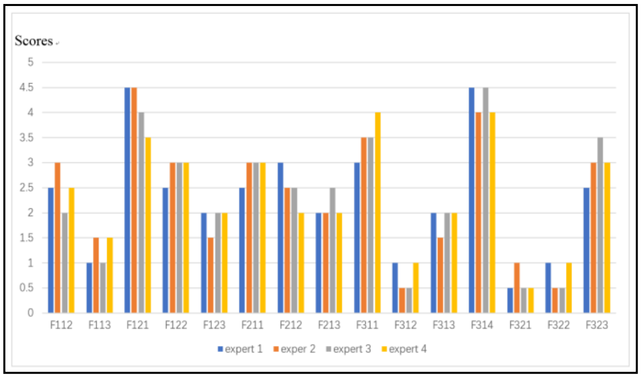

FIGURE 5. The data for expert scoring.

B. EXPERT SCORING BOTTOM SEQUENCE EVALUATIONS

The steps have been described explicitly in previous section. For instance, consider F_{111}(factor of employability) as an example and calculate its bottom evaluation sequence.

Step 1: According to Whitenization weight function and formula 2,3,4,5,6,7

When $h = 1, r_{11} = \sum_{i=1}^{4} f_1(x_{i1}) = f_1(3) + f_1(3.5) + f_1(2.5) + f_1(3) = 2.4.$

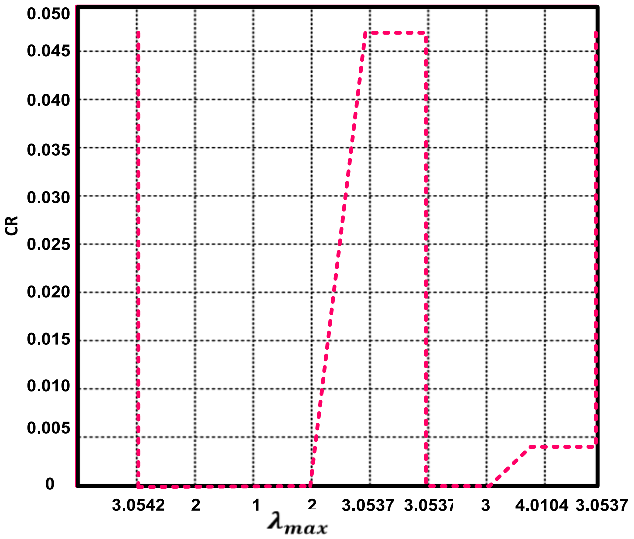

FIGURE 6. The calculation results of λ_*max* and CR.

When $h = 2, r_{12} = \sum_{i=1}^{4} f_2(x_{i1}) = f_2(3) + f_2(3.5)+f_2(2.5) +f_2(3) = 3$.

When $h = 3, r_{13} = \sum_{i=1}^{4} f_3(x_{i1}) = f_3(3)+f_3(3.5)+f_3(2.5) +f_3(3) = 3.58$.

When $h = 4, r_{14} = \sum_{i=1}^{4} f_4(x_{i1}) = f_4(3)+f_4(3.5)+f_4(2.5) +f_4(3) = 2.67$.

When $h = 5, r_{15} = \sum_{i=1}^{4} f_5(x_{i1}) = f_5(3)+f_5(3.5)+f_5(2.5) +f_5(3) = 2$.

Step 2: From equation (8), we get as

$$r_1 = \sum_{h=1}^{5} r_{1h} = 13.65$$

Step 3: From Equation (9): we can compute: $\xi_{111} = (0.18, 0.22, 0.26, 0.20, 0.15)$.

Step 4: Risk Level: Recall that the Grey clustering is defined as $h = (1, 2, 3, 4, 5)$ and $U = (5, 4, 3, 2, 1)$. Using Equation (10), the Grey evaluation value is V $= \xi_{111} \times U^T = 3.11$. Therefore, the Grey class is 3 with the risk level of medium. In the same method, we can get the bottom evaluation sequence, as shown in Table 6.

C. WEIGHT VECTOR AND CONSISTENCY TEST

According to the formulae in section IV.E.4, the index weight vectors of each layer are calculated. In the judgment matrix consistency test, the consistency ratios are all smaller than 0.10; hence, their bottom evaluation sequences pass the test and can be utilized. Therefore, the index weight vector of each level is determined, as listed in Table 7.

TABLE 6. Bottom sequence evaluation.

Third-Level	Bottom Evaluation Sequence	Statistics	Risk Level
F_{111}	ξ_{111}= (0.18, 0.22, 0.26, 0.20, 0.15)	3.11	Medium
F_{112}	ξ_{112}= (0.15,0.18,0.24,0.16,0.18)	2.69	Medium
F_{113}	ξ_{113}= (0.10, 0.12, 0.16, 0.25, 0.37)	2.33	Low
F_{121}	ξ_{121}= (0.33, 0.29, 0.18, 0.12, 0.09)	3.68	High
F_{122}	ξ_{122}= (0.16, 0.20, 0.26, 0.19, 0.20)	2.96	Medium
F_{123}	ξ_{123}= (0.12, 0.15, 0.20, 0.29, 0.25)	2.63	Medium
F_{211}	ξ_{211}= (0.16, 0.20, 0.26, 0.19, 0.20)	2.96	Medium
F_{212}	ξ_{212}= (0.15, 0.18, 0.24, 0.24, 0.18)	2.85	Medium
F_{213}	ξ_{213}= (0.11, 0.14, 0.19, 0.32, 0.24)	2.56	Medium
F_{311}	ξ_{311}= (0.22, 0.27, 0.23, 0.16, 0.12)	3.31	Medium
F_{312}	ξ_{312}= (0.08, 0.10, 0.13, 0.19, 0.51)	2.08	Low
F_{313}	ξ_{313}= (0.12, 0.15, 0.20, 0.29, 0.25)	2.63	Medium
F_{314}	ξ_{314}= (0.35, 0.31, 0.16, 0.10, 0.08)	3.75	High
F_{321}	ξ_{321}= (0.07, 0.09, 0.12, 0.17, 0.56)	1.97	Low
F_{322}	ξ_{322}= (0.08, 0.10, 0.13, 0.19, 0.51)	2.08	Low
F_{323}	ξ_{323}= (0.20, 0.33, 0.25 0.22, 0)	3.51	High

We show the trend to show the result of $\boldsymbol{\lambda}_{\mathbf{max}}$ and *CR* from Table 7 and show it in Fig. 6:

D. LAYERED EVALUATIONS

According to the results in Table 6 and Table 7, the risk levels for second-level indices and first-level indices is calculated. The process consists of several steps, which are described as follows.

(i) Evaluation for the second-level risks: The matrices.

(i) Second level risk is used to evaluate the second-level index are made up of the third-level evaluation sequences which belong to the second-level indexes.

$$\begin{aligned} R_{F_{11}} &= [\xi_{111}\xi_{112}\xi_{113}]^T \\ &= \begin{bmatrix} \mathbf{0.18} & \mathbf{0.22} & \mathbf{0.26} & \mathbf{0.20} & \mathbf{0.15} \\ \mathbf{0.15} & \mathbf{0.18} & \mathbf{0.24} & \mathbf{0.16} & \mathbf{0.18} \\ \mathbf{0.10} & \mathbf{0.12} & \mathbf{0.16} & \mathbf{0.25} & \mathbf{0.37} \end{bmatrix} \end{aligned} \quad (35)$$

TABLE 7. Weight vector and consistency test.

Judgment Matrix	Indexes Weight Vector	$\boldsymbol{\lambda_{max}}$	CR
F	$\mathbf{(0.1822\ \ 0.1149\ \ 0.7028)^T}$	3.0542	0.0467
F1	$\mathbf{(0.2\ \ 0.8)^T}$	2	0
F2	$\mathbf{(1)^T}$	1	0
F3	$\mathbf{(0.25\ \ 0.75)^T}$	2	0
F11	$\mathbf{(0.3119\ \ 0.4905\ \ 0.1976)^T}$	3.0537	0.0463
F12	$\mathbf{(0.4905\ \ 0.3119\ \ 0.1976)^T}$	3.0537	0.0463
F21	$\mathbf{(0.1429\ \ 0.5714\ \ 0.2857)^T}$	3	0
F31	$\mathbf{(0.0999\ \ 0.3451\ \ 0.185\ \ 0.3701)^T}$	4.01	0.0038
F32	$\mathbf{(0.4905\ \ 0.1976\ \ 0.3119)^T}$	3.054	0.0463

TABLE 8. Second-level evaluation sequence.

Second-Level	Evaluation Sequence	Statistics	Risk Level
$\boldsymbol{F_{11}}$	ξ_{11}= (0.15, 0.18, 0.23, 0.19, 0.20)	2.74	Medium
$\boldsymbol{F_{12}}$	ξ_{12}= (0.24, 0.23, 0.21, 0.18, 0.16)	3.27	Medium
$\boldsymbol{F_{21}}$	ξ_{21}= (0.14, 0.17, 0.23, 0.26, 0.20)	2.79	Medium
$\boldsymbol{F_{31}}$	ξ_{31}= (0.2, 0.2, 0.16, 0.17, 0.26)	2.88	Medium
$\boldsymbol{F_{32}}$	ξ_{32}= (0.11, 0.17, 0.16, 0.19, 0.38)	2.47	Low

The second-level evaluation sequence of $\boldsymbol{F_{11}}$ is defined in (36):

$$\boldsymbol{\xi_{11}} = \mathbf{v}^{\mathbf{T}}_{\mathbf{F_{11}}} \times \mathbf{R_{F_{11}}} = \mathbf{(0.31190.49050.1976)} \times \begin{bmatrix} \mathbf{0.18} & \mathbf{0.22} & \mathbf{0.26} & \mathbf{0.20} & \mathbf{0.15} \\ \mathbf{0.15} & \mathbf{0.18} & \mathbf{0.24} & \mathbf{0.16} & \mathbf{0.18} \\ \mathbf{0.10} & \mathbf{0.12} & \mathbf{0.16} & \mathbf{0.25} & \mathbf{0.37} \end{bmatrix} = (0.15, 0.18, 0.23, 0.19, 0.2) \tag{36}$$

The evaluation value of F_{11} is given as:

$$\mathrm{V}_{\mathrm{F}_{11}} = \xi_{11} \times \mathrm{U}^{\mathrm{T}} = (0.15, 0.18, 0.23, 0.19, 0.20) \times (54321)^{\mathrm{T}} = 2.74 \tag{37}$$

In the same method, we can get the evaluation sequences and evaluation values of other second-level indexes. The results are shown in Table 8.

(i) *Evaluation for the First-Level Indexes:* The matrices which are used to evaluate the first-level index are made up of the second-level evaluation sequences, which belong to the first-level indexes. In the same method in (i), we can get the evaluation sequences and evaluation values of the other first-level indexes as shown in Table 9.

TABLE 9. First-level evaluation sequence.

First-Level	Evaluation Sequence	Statistics	Risk Level
$\boldsymbol{F_1}$	ξ_1= (0.22, 0.22, 0.21, 0.18, 0.17)	3.14	Medium
$\boldsymbol{F_2}$	ξ_2= (0.14, 0.17, 0.23, 0.26, 0.20)	2.79	Medium
$\boldsymbol{F_3}$	ξ_3= (0.13, 0.18, 0.16, 0.19, 0.35)	2.58	Medium

E. RESULTS EVALUATIONS

According to the hierarchy in our evaluation system, the evaluation matrix is made up of the first-level evaluation sequences. With the same method presented in the previous section (4.4), the evaluation value of index F *could be expressed* as follows:

$$\mathrm{V_F} = \xi_{\mathrm{F}} \times \mathrm{U}^{\mathrm{T}} = (0.150.190.180.200.30) \times (54321)^{\mathrm{T}} = 2.75$$

The evaluation value of the index F is approximated as 2.75 with the risk level medium. This shows that the CSP had a moderate risk.

VI. SECURITY RISK PROJECTION

A. PROJECTION OF RISK VALUES FROM 2009 TO 2018

In this experiment, the deviation is calculated for the CSP by using risk values that were directly collected via expert scoring and by using GST and AHP models. The data are plotted for the years 2009-2018 in Fig. 7. A peak is observed at 3.5 in 2013 and the lowest point is attained in 2011 when using collected data from expert scoring and the weight indices have not been considered. In contrast, a stable increase is observed for risk values that are calculated exclusively from

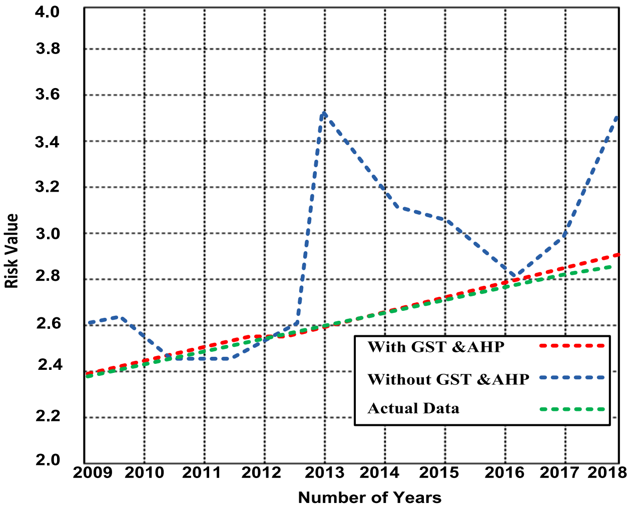

FIGURE 7. Comparison among GST and AHP, without GST and AHP and actual data.

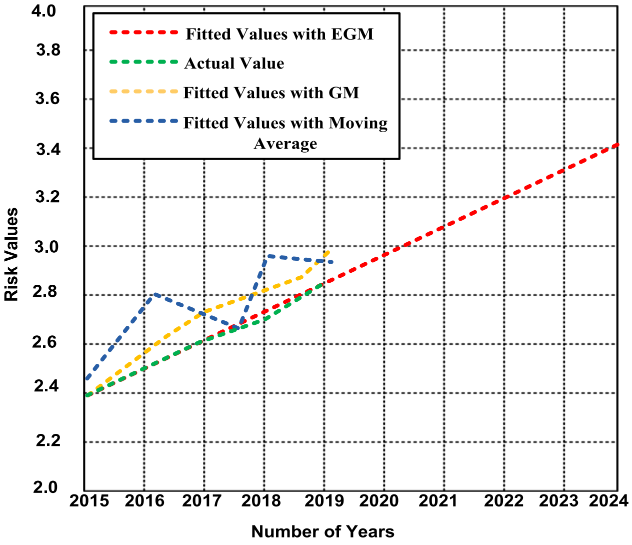

FIGURE 8. Comparison among EGM, GM, actual value and moving average.

2.4 to 2.75 by using the GST and AHP models. Furthermore, the actual data are plotted in Fig. 7 for comparison with the results of the AHP and GST models in terms of accuracy. Based on the data trend, we observed that the risk values that were not calculated by the GST and the AHP models show substantial deviations [39]. The maximum value exceeds the minimum value by a factor of two. In contrast, when applying the GST and the AHP models for risk assessments, the curves for the risk values become flat [40].

Our proposed models deal with extreme values in advance and determine the index weights among factors. Hence, our models are more suitable and accurate in real conditions because the GST model can determine quantitative and qualitative relationships among complex dynamics with inadequate information [46]. In addition, the AHP method identifies the weights of CSP's evaluation criteria accurately. Furthermore, AHP assigns the values based on the actual conditions and uses a comparative judgment process, a decomposition process, and a complete rational mode for decision-making. Thus, it is a vital tool for system investigation [47], [48]. The hybrid method facilitates the development of systematic and accurate well-defined and step-by-step procedures; ensures the transparency of the computation process; and utilizes a rational and logical approach that has an adequate mathematical foundation [49].

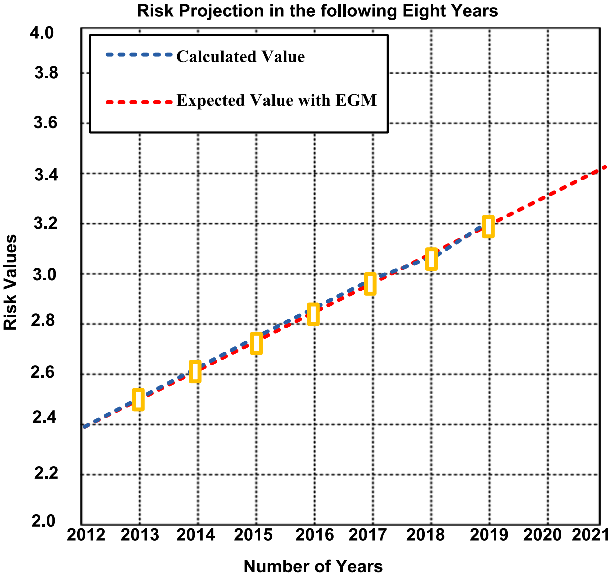

FIGURE 9. Risks projection in the following eight years with EGM (1,1).

B. PROJECTION OF RISK VALUES FROM 2015 TO 2024

In this experiment, we have obtained the risk values of the CSP for the past nine years with the GST and the AHP models. Next, we should apply the projection for the same service provider in the following five-year period to evaluate its reliability and service consistency for the future. We use the actual values, the moving average method, GM (1,1), and the proposed EGM (1,1) model for projection.

Based on the results, we observed in Fig. 8 that the moving average and GM value have higher fitting precision compared with the EGM for risk prediction. Fig. 9 shows that the EGM (1,1) model is more suitable for both short-term and long-term projections for the risk assessment of CSP. Our proposed model has high fitting precision relative to the actual values, as shown in Fig. 9.

C. ACCURACY PROBABILITY

GM (1,1) [17], R-ALO-GM (1,1) [13] and IAHP [15] are satisfactory methods for reducing the deviations of variables. In Fig. 10, we plot the prediction accuracies of GM, R-ALO-GM, and IAHP and compare them with the predictions of our proposed EGM. Based on the results, there is a linear decline in the prediction accuracy over the period of 2010 to 2019.

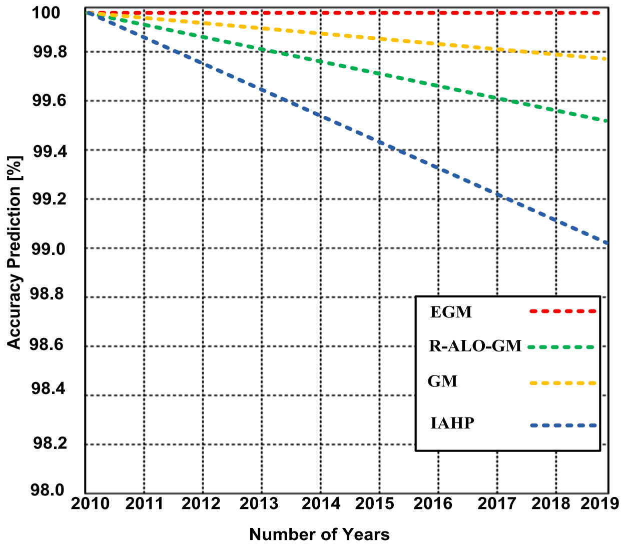

FIGURE 10. The accuracy prediction of GM, IAHP, R-ALO-GM, and EGM during 2010-2019.

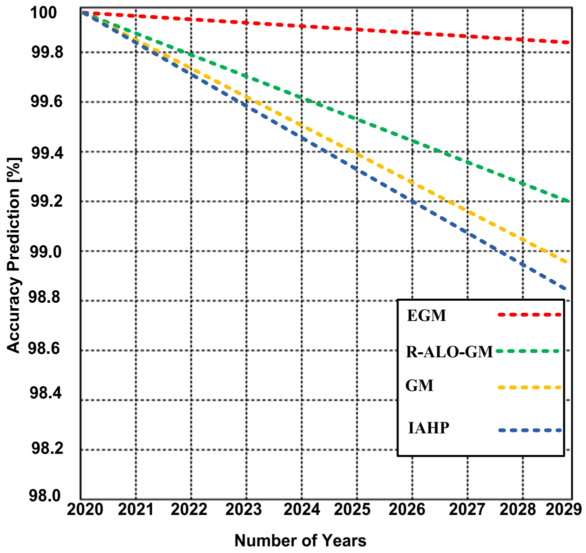

FIGURE 11. The accuracy prediction of GM, IAHP, R-ALO-GM, and EGM during 2020-2029.

However, the prediction accuracy of the EGM is higher than those of the other contending models.

In Fig. 11, according to the graphical trend, GM and IAHP experience sharp decreases in the period from 2022 to 2029, compared to a slight decrease in the EGM (1,1) prediction accuracy, which reaches approximately 99.99 to 99.82. This decrease is marginal and does not affect our proposed model's prediction. Hence, we conclude that EGM outperforms the other contending models in terms of prediction accuracy. We use the EGM due to its performance in reducing the deviations for risk assessment to support CSP.

D. DISCUSSION OF RESULT

The risk assessment for CSP is conducted using the GST, the AHP, and EGM (1,1) models. The GST model is used to determine the bottom sequence evaluation. Furthermore, GST handles the insufficient and flawed information to strengthen the restrictions of old-fashioned statistical methods. In addition, the AHP model recognizes the weights of CSP's assessment criteria. It allocates the values based on the actual scenario and uses a comparative judgment process, a complete rational mode for decision-making and a decomposition process. Thus, AHP is an effective tool for system analysis. EGM (1,1) reduces the prediction error based on a direct prediction feature to avoid the iterative prediction shortcoming of standard GM (1,1). Thus, EGM (1,1) helps maintain higher accuracy despite the larger number of predicted periods. According to Table 5, the risk level of the bottom sequence evaluation ranges from high to low and most of the values are distributed at the medium level. A hierarchy model of three layers is constructed based on a CSP's information system. All the index weights between layers, which are determined by the AHP model, pass the consistency test because their consistency ratios are all smaller than 0.01. The advantage of conducting a consistency test is that it reduces the error in the judgment matrix. Combing the GST and the AHP models, we could objectively obtain the risk values, which are listed in Table 9. According to our simulation results, the risk values show a slight increase over the past years. When analyzing the results of the R-ALO-GM, GM and the IAHP models, we clearly observed that the EGM contributes to the risk assessment successfully and produces less deviation compared to other contending models. However, our proposed EGM (1,1) has a slight limitation when determining the risk value for a one-year period. EGM (1,1) inherits few features from GM (1,1). For example, GM (1,1) represents the time series as a differential equation. Thus, the modeling values and predictions of EGM (1, 1) are independent due to the inclusion of a first entry in the original series. Therefore, the proposed EGM (1,1) encounters the same limitation. Thus, this limitation can be overcome by using a random number in the front of the original series to replace the data from the first entry.

VII. CONCLUSION

A risk assessment model that is based on GST, AHP, and EGM (1,1) has been introduced for CSPs. The proposed model is compared with previous models. Our proposed model eliminates human factors and reduces the deviation of the experimental results in the risk assessment. The GST model is used to calculate the weight vectors and the evaluation values of bottom indices. In this model, whitenization functions are applied to overcome poor samples. The judgment matrix in the AHP model has ensured the reliability of our calculations, which are primarily the risk values that are used to assess the risk level of a CSP based on the AHP. EGM (1,1) provides direct prediction values by overcoming the limitations of GM (1,1). In addition, EGM (1,1) facilitates successful risk assessment and reduces the deviations compared to other contending models. Our simulation results demonstrated an effective reduction in the data deviations when performing the risk assessment and prediction using the combined model (GST, AHP, and EGM) in terms of risk projection and accuracy.

REFERENCES

[1] A. Razaque, R. V. Nikhileshwara, N. Soni, and G. S. Janapati, "Task scheduling in cloud computing," in *2016 IEEE Long Island Syst., Appl. Technol. Conf. (LISAT)*, Nov. 2016, pp. 1–5.

[2] S. K. Madria, "Security and risk assessment in the cloud," *Computer*, vol. 49, no. 9, pp. 110–113, Sep. 2016.

[3] A. Razaque and S. S. Rizvi, "Privacy preserving model: A new scheme for auditing cloud stakeholders," *J. Cloud Comput.*, vol. 6, no. 1, p. 7, Dec. 2017.

[4] Z.-U. Rehman, O. K. Hussain, and F. K. Hussain, "User-side cloud service management: State-of-the-art and future directions," *J. Netw. Comput. Appl.*, vol. 55, pp. 108–122, Sep. 2015.

[5] R. Kumar and R. Goyal, "On cloud security requirements, threats, vulnerabilities and countermeasures: A survey," *Comput. Sci. Rev.*, vol. 33, pp. 1–48, Aug. 2019.

[6] S. K. Garg, S. Versteeg, and R. Buyya, "A framework for ranking of cloud computing services," *Future Gener. Comput. Syst.*, vol. 29, no. 4, pp. 1012–1023, Jun. 2013.

[7] G. Brunette and R. Mogull, "Security guidance for critical areas of focus in cloud computing v2.1," in *Proc. Cloud Secur. Alliance*, 2009, pp. 1–5. [Online]. Available: https://cloudsecurityalliance.org/csaguide.pdf

[8] R. C. Zoie, B. Alexandru, R. Delia Mihaela, and D. Mihail, "A decision making framework for weighting and ranking criteria for cloud provider selection," in *Proc. 20th Int. Conf. Syst. Theory, Control Comput. (ICSTCC)*, Oct. 2016, pp. 590–595.

[9] W. Kenton. *Delphi Method*. Accessed: Aug. 7, 2018. [Online]. Available: http://www.investopedia.com/terms/d/delphi-method.asp

[10] S. Ren, D. Wang, and H. Wang. "Research on business risk assessment model of city commercial banks based on grey system theory," Tech. Rep.

[11] M. He, "Information security risk assessment based on analytic hierarchy process," *Indonesian J. Elect. Eng. Comput. Sci.*, vol. 1, no. 3, pp. 656–664, Mar. 2016.

[12] W. E. Mahmod and K. Watanabe, "Modified grey model and its application to groundwater flow analysis with limited hydrogeological data: A case study of the Nubian sandstone, Kharga oasis, Egypt," *Environ. Monitor. Assessment*, vol. 186, no. 2, pp. 1063–1081, Feb. 2014.

[13] H. Zhao and S. Guo, "An optimized grey model for annual power load forecasting," *Energy*, vol. 107, pp. 272–286, Jul. 2016.

[14] T.-L. Tien, "A new grey prediction model FGM(1,1)," *Math. Comput. Model.*, vol. 49, nos. 7–8, pp. 1416–1426, Apr. 2009.

[15] X. Li, Y. Li, H. Liang, and H. Liu, "Research on evaluation of urban pumping station engineering aging based on AHP and IAHP," in *Proc. 4th Int. Conf. Inf. Sci. Control Eng. (ICISCE)*, Jul. 2017, pp. 585–589.

[16] S. Malakar and M. K. Maharana, "Network contingency ranking using analytic hierarchy process to calculate unequal importance factors for static severity indices," in *Proc. Michael Faraday IET Int. Summit*, 2015, pp. 249–255, doi: 10.1049/cp.2015.1639.

[17] Z.-X. Wang, Q. Li, and L.-L. Pei, "A seasonal GM(1,1) model for forecasting the electricity consumption of the primary economic sectors," *Energy*, vol. 154, pp. 522–534, Jul. 2018.

[18] C. Li, J. Qin, J. Li, and Q. Hou, "The accident early warning system for iron and steel enterprises based on combination weighting and grey prediction model GM (1,1)," *Saf. Sci.*, vol. 89, pp. 19–27, Nov. 2016.

[19] S. Tanimoto, M. Hiramoto, M. Iwashita, H. Sato, and A. Kanai, "Risk management on the security problem in cloud computing," in *Proc. 1st ACIS/JNU Int. Conf. Comput., Netw., Syst. Ind. Eng.*, May 2011, pp. 147–152.

[20] Djemame, Karim, Django Armstrong, Mariam Kiran, and Ming Jiang, "A risk assessment framework and software toolkit for cloud service ecosystems," *Cloud Computing*, vol. 5, pp. 119–126, May 2011.

[21] B. Martens and F. Teuteberg, "Decision-making in cloud computing environments: A cost and risk based approach," *Inf. Syst. Frontiers*, vol. 14, no. 4, pp. 871–893, Sep. 2012.

[22] S. H. Albakri, B. Shanmugam, G. N. Samy, N. B. Idris, and A. Ahmed, "Security risk assessment framework for cloud computing environments," *Secur. Commun. Netw.*, vol. 7, no. 11, pp. 2114–2124, Nov. 2014.

[23] F. A. Alali and C.-L. Yeh, "Cloud computing: Overview and risk analysis," *J. Inf. Syst.*, vol. 26, no. 2, pp. 13–33, Nov. 2012.

[24] R. Latif, H. Abbas, S. Assar, and Q. Ali, "Cloud computing risk assessment: A systematic literature review," in *Future Information Technology*. Berlin, Germany: Springer, 2014, pp. 285–295.

[25] M. Lang, M. Wiesche, and H. Krcmar, "Criteria for selecting cloud service providers: A delphi study of Quality-of-Service attributes," *Inf. Manage.*, vol. 55, no. 6, pp. 746–758, Sep. 2018.

[26] I. Petri, O. F. Rana, G. C. Silaghi, and Y. Rezgui, "Risk assessment in service provider communities," *Future Gener. Comput. Syst.*, vol. 41, pp. 32–43, Jan. 2014.

[27] J. O. Fitó and J. Guitart, "Business-driven management of infrastructure-level risks in cloud providers," *Future Gener. Comput. Syst.*, vol. 32, pp. 41–53, Mar. 2014.

[28] I. Indu, P. M. R. Anand, and V. Bhaskar, "Identity and access management in cloud environment: Mechanisms and challenges," *Eng. Sci. Technol. Int. J.*, vol. 21, no. 4, pp. 574–588, Aug. 2018.

[29] E. D. Knapp and J. T. Langill, *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*. New York, NY, USA: Syngress, 2014.

[30] Z. Zhang and A. Meddahi. *Security in Network Functions Virtualization*. Amsterdam, The Netherlands: Elsevier, 2017.

[31] N. Subramanian and A. Jeyaraj, "Recent security challenges in cloud computing," *Comput. Electr. Eng.*, vol. 71, pp. 28–42, Oct. 2018.

[32] J. Moura and D. Hutchison, "Review and analysis of networking challenges in cloud computing," *J. Netw. Comput. Appl.*, vol. 60, pp. 113–129, Jan. 2016.

[33] D. Warren and L. Mathiassen, "Cloud-based business services innovation: A risk management model," *Int. J. Inf. Manage.*, vol. 6, no. 36, pp. 639–649, 2017.

[34] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," *Future Gener. Comput. Syst.*, vol. 28, no. 3, pp. 583–592, Mar. 2012.

[35] I. Sahu and U. S. Pandey, "Mobile cloud computing: Issues and challenges," in *Proc. Int. Conf. Adv. Comput., Commun. Control Netw. (ICACCCN)*, Oct. 2018, pp. 247–250.

[36] Z. Wei and M. Li, "Information security risk assessment model base on FSA and AHP," *Proc. Int. Conf. Mach. Learn. Cybern. (ICMLC)*, Qingdao, China, 2010, pp. 2252–2255.

[37] F. Sha, X. Yezhi, and S. Dan, "A gray multi-level integrated assessment method for information system risk assessment," *J. Mod. Inf.*, vol. 12, p. 11, Feb. 2012, doi: 10.3969/j.ssn.1008-0821.2012.12.010.

[38] B. Liu, X. Zhang, G. Zhang, "Information system vulnerability assessment method based on analytic hierarchy process," *Comput. Sci.*, vol. 33, no. 12, pp. 62–64, 2006.

[39] A. Taha, R. Trapero, J. Luna, and N. Suri, "AHP-based quantitative approach for assessing and comparing cloud security," in *Proc. IEEE 13th Int. Conf. Trust, Secur. Privacy Comput. Commun.*, Sep. 2014, pp. 634–641.

[40] Z. Feng, G. Yin, and H. Lin, "Comprehensive evaluation of CNC machine tools accuracy based on AHP," *TELKOMNIKA Indonesian J. Elect. Eng.*, vol. 12, no. 3, pp. 1658–1667, 2014.

[41] E. Cayirci, A. Garaga, A. Santana de Oliveira, and Y. Roudier, "A risk assessment model for selecting cloud service providers," *J. Cloud Comput.*, vol. 5, no. 1, p. 14, Dec. 2016.

[42] M. Keil, A. Tiwana, and A. Bush, "Reconciling user and project manager perceptions of IT project risk: A delphi study1," *Inf. Syst. J.*, vol. 12, no. 2, pp. 103–119, Apr. 2002.

[43] S. Liu, J. Zhang, M. Keil, and T. Chen, "Comparing senior executive and project manager perceptions of IT project risk: A chinese delphi study," *Inf. Syst. J.*, vol. 20, no. 4, pp. 319–355, 2020.

[44] S. Huang, I. Chang, S. Li, and M. Lin, "Assessing risk in ERP projects: Identify and prioritize the factors," *Ind. Manage. Data Syst.*, vol. 104, no. 8, pp. 681–688, Oct. 2004.

[45] S. Clarke, *Information Systems Strategic Management: An Integrated Approach*. Evanston, IL, USA: Routledge, 2012.

[46] P. Chand, J. J. Thakkar, and K. K. Ghosh, "Analysis of supply chain complexity drivers for indian mining equipment manufacturing companies combining SAP-LAP and AHP," *Resour. Policy*, vol. 59, pp. 389–410, Dec. 2018.

[47] "AHP-GST," vol. 11, no. 25, pp. 120–123, 2007.

[48] "AHP-GST," vol. 12, no. 28, pp. 72–75, 2006.

[49] X uihui, C. Yulin, and S. Dapeng, "Evaluation of the interchange shemes by AHP and GST based on security factor," *Mod. Transp. Technol.* p. 3, 2008.

ABDUL RAZAQUE (Member, IEEE) received the Ph.D. degree in computer science and engineering from the University of Bridgeport, USA, in 2015. He is currently an Associate Professor with the Department of Computer Engineering and Telecommunications, International Information Technology University. His research interests include the wireless sensor networks, cyber security, cloud computing security, design and development of mobile learning environments, and ambient intelligence. He has authored over 170 international academic publications, including journals, conferences, book chapters, and four books. He is the author of four books. He has served as the Editor-in-Chief for the *International Journal for Engineering and Technology* (IJET), Singapore, from 2012 to 2015. In addition, he is an Editor, an Associate Editor, and a member of Editorial Board of several international journals.

FATHI AMSAAD received the Ph.D. degree in engineering science from Toledo (UToledo), OH, USA. He is currently an Assistant Professor with the School of Information Security and Applied Computing (SISAC), Eastern Michigan University (EMU). He is also the Founder and the Director of the Cyber Security Laboratory, and the Co-Director of the Advanced Computing Research Laboratory. His research expertise include in the areas of cyber security and cyber-physical systems with special interests in hardware-oriented security and trust for device and system authentication, secure embedded architectures, VLSI/FPGA systems testing, fault tolerance hardware, detection and prevention of hardware trojans, network and mobile wireless security, and the security of IoT applications and smart systems. He is also an active IEEE/ACM member. He has served as a Project Adviser for several groups of senior undergraduate students and a Reviewer of high impact and peer-review conferences/journals. He was a recipient of the prestigious IEEE Best Graduate Student Award by IEEE Region 4 and the College of Engineering, UToledo. Additionally, he was the 2017 nominee for the best Ph.D. Dissertation Award. He holds MCP, MCSA, MCTS, and MCSE Professional Certificates from Microsoft Company.

SALIM HARIRI received the Ph.D. degree in computer engineering from the University of Southern California, in 1986. He is currently a Professor and the University of Arizona site Director of the NSF-Funded Center for Cloud and Autonomic Computing. He founded the IEEE/ACM International Symposium on High Performance Distributed Computing, or HPDC. He is also the co-founder of the IEEE/ACM International Conference on Cloud and Autonomic Computing. He has coauthored three books on autonomic computing, parallel and distributed computing, and edited Active Middleware Services, a collection of articles from the second annual AMS Workshop published by Kluwer, in 2000. He serves as the Editor-in-Chief for the scientific journal *Cluster Computing*, which presents research and applications in parallel processing, distributed computing systems, and computer networks.

MARWAH ALMASRI is currently a Computer Science Expert, a Researcher, and a Reviewer. She has more than twenty publications in international journals and conferences in the field of autonomous mobile robots, wireless sensor networks, computer networks, cloud computing, blockchain, the IoT, and data fusion. She also works as an Assistant Professor/Researcher and a Consultant to the Vice Rector of Graduate Studies and Scientific Research with Saudi Electronic University. She is also the Director of the Science and Technology Unit and a Supervisor of the administration of knowledge resources at the university. She has received many awards from various international honor societies, such as Upsilon Pi Epsilon and Phi Kappa Phi.

SYED S. RIZVI received the Ph.D. degree in modeling and simulation from the University of Bridgeport, in 2010. He is currently an Associate Professor of information sciences and technology with The Pennsylvania State University, Altoona. His research interests include intersection of computer networking, and information and wireless security. He has been working on security issues in cloud computing, the Internet of Things (IoT), big data, identity thefts, cognitive radios for wireless communications, and modeling and simulation of large-scale networks. He has authored or coauthored several technical refereed and non-refereed papers in various international conferences, journal articles, and book chapters in research and pedagogical techniques. His expertise includes the design, analysis, implementation, optimization, and comparisons of algorithms in the areas of wireless/multiuser communications, information security, and parallel/distributed systems. He is also a member of the IEEE Communications Society and the ACM.

MOHAMED BEN HAJ FREJ (Graduate Student Member, IEEE) is currently a Computer Networks Expert, a Researcher, and a Reviewer. He has more than twenty-five years of experience in securing and administering networks. He is also the IT Lead with the Research and Development facility of Airgas, Inc. He is also an Adjunct Instructor with numerous colleges and universities. He has authored or coauthored many technical refereed and non-refereed articles in the fields of cloud computing security, wireless sensor networks, and open source software. He currently serves as a Council Member with the Engineering Division, Council of Undergraduate Research (CUR), USA. He is also a member of the Editorial Board of many journals.