IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received October 29, 2017, accepted November 23, 2017, date of publication December 4, 2017, date of current version March 16, 2018.

Digital Object Identifier 10.1109/ACCESS.2017.2779599

A New BRB Model for Cloud Security-State Prediction Based on the Large-Scale Monitoring Data

HANG WEI [1], GUAN-YU HU [2], XIAOXIA HAN [3], PEILI QIAO [1], ZHIGUO ZHOU [4], ZHI-CHAO FENG [3], AND XIAO-JING YIN [5]

[1]School of Computer Science and Technology, Harbin University of Science and Technology, Harbin 150080, China
[2]School of Information Science and Technology, Hainan Normal University, Haikou 570100, China
[3]High-Tech Institute of Xi'an, Xi'an 710025, China
[4]The University of Texas Southwestern Medical Center, Department of Radiation Oncology, Dallas, TX 75235, USA
[5]School of Mechatronic Engineering, Changchun University of Technology, Changchun 130012, China

Corresponding author: Peili Qiao (qiaopl@hrbust.edu.cn)

This work was supported in part by the Natural Science Foundation of China under Grant 61773388, Grant 61374138, Grant 61370031, and Grant 61702142, in part by the Postdoctoral Science Foundation of China under Grant 2015M570847 and Grant 2016T90938, and in part by the Natural Science Foundation of Hainan Province under Grant 617120.

ABSTRACT Considering the reliability of the cloud computing system, this paper aims to predict the security state with multiple large-scale attributes in cloud computing system. A double-layer method for predicting the security state of cloud computing system based on the belief rule-base model is proposed, where the evidential reasoning (ER) algorithm is employed to fuse the multiple system indicators of actual cloud system and make a reasonable assessment to describe the cloud security state. This method can utilize quantitative and qualitative information simultaneously. By using the ER algorithm to integrate multiple indicators whose attributes contain much uncertain information, the security state of the cloud computing system can be predicted accurately. Moreover, due to the initial parameters of the proposed models are given by experts that might cause imprecise results, the constraint CMA-ES algorithm is employed as the optimization tool to obtain the optimal parameters. A practical study about the cloud security-state prediction is verified to indicate the potential applications about the proposed prediction model in a cloud computing platform.

INDEX TERMS Belief rule base (BRB), cloud computing, multi-attributes integration, security-state prediction.

I. INTRODUCTION

Cloud computing as the interact-based network, provides a convenient service for users to access their resources. The cloud platform has huge capability in computing and management. It can distribute computing resources in real time to satisfy the user's various requirements. The wide applications of cloud computing have been recognized by the IT industry, and become a new generation of Internet services.

Currently, the surveys posted by the Cloud Security Alliance (CSA) and Institute of Electrical and Electronics Engineers (IEEE) indicate that most internet organization and company are eager to use cloud computing technology for producing. However, the attention of the security of cloud environment is much higher than the actual scale expansion of cloud system. Cloud computing can be regarded as a complex system, while its complex structures and components aggravate the impact of the reliability and security risk of the cloud system. It is not only faced with the security problems of hardware and software in traditional information system, but encountered other kinds of service quality problems, such as response quality and performance quality [1]. Therefore, the cloud security state is the significant security information to ensure system reliability [2], where it can fully reflect the security state of the cloud environment. It is important for providers to establish the completed active security monitoring system [3], [4], such as SLA-based monitoring services [5] and QoS-based

virtualized services [6]. However, these approaches only make sense when the threat have already happened, which cannot prevent the attack in advance. The prediction technology could make an early awareness of the security state. More importantly, it provides a theoretical basis for decision makers to take measures for avoiding losses.

To construct the prediction model of cloud security state, two methods can be consisted: the statistical model-based method and the data-driven method. The statistical model-based method is to determine the parameters and states that can reflect the behavior of a system according to the mathematical models. The early prediction techniques most employed by using kinds of filters and statistical models, such as Kalman filter [7], particle filter [8], KPI approach [9] and PLS approach [10]. These methods can be used to predict and analyze according to the system characteristics and noise. However, for a complex cloud computing system, a reasonable mathematical model is usually difficult to obtain. Thus, it is hard to achieve a reasonable and accurate result for cloud security state. The data-driven method has been widely employed recently, and there are three type models including qualitative knowledge-based model, quantitative information-based model and semi-quantitative information-based model. The qualitative knowledge-based model generally uses expert experience and subjective description for prediction, such as expert system [11], [12] and Petri net-based model [13]. These methods use the known qualitative knowledge for prediction. But considering the cloud computing systems which contain much uncertainty information are too complex, it is difficult to construct an accurate prediction model with single qualitative knowledge. Nevertheless, large amounts of the indicators might increase the computational complexity that affects the efficiency of the calculation. Relatively, the quantitative information-based models are widely applied, such as artificial neural network model (ANN) [14], grey theory-based model [15] and support-vector-machines-based model (SVM) [16]. When the prediction model is established, the parameters of the model are trained according to the quantitative data of the system. However, since the limitation of prior expert's experience and training samples, the quantitative information methods calculated with small-scale samples usually obtain inaccuracy prediction results. The semi-quantitative information model could employ both qualitative and quantitative knowledge for training, such as hidden Markov model (HMM) [17], [18], dynamic Bayesian networks (DBN) [19] and Fuzzy Neural Network [20]. These methods can set initial parameters through expert's experience, and then the observation data is used to optimize the initial parameters. It can obtain better prediction results with small-scale samples.

As mentioned above, it can be concluded that the prediction model based on semi-quantitative information has the advantages in predicting the cloud security state. However, the existing methods also have some shortcomings, which have limitations in dealing with uncertain information [21]. For example, hidden Markov model and Bayesian network model can deal with probabilistic uncertain information, but cannot settle fuzzy uncertain information. The fuzzy neural network model can solve the fuzzy uncertain information, but it cannot solve the probabilistic uncertainty information. The cloud environment is too complex to settle the uncertainty which have both probabilistic and fuzzy information. The probabilistic uncertainty information is generally due to the lack of a complete causality description of the system, whereas the fuzzy uncertain information is often due to the lack of the law of excluded middle description [22]. Thus, it is necessary to establish a prediction model that can both deal with the probabilistic and fuzzy information, which is more suitable for the practical situation in cloud computing environment.

In this paper, a new belief rule base (BRB) model with large-scale observable data is proposed to predict the cloud computing security state. The BRB model was presented by Yang *et al.* [23] in 2006. This model improved the traditional ''IF-THEN'' rule based on expert system, and then introduced the description of belief degree for the result, where the ER algorithm is employed for fusing the belief rules [24]. Zhou *et al.* [25] proposed a BRB prediction model in 2010 and applied it in the fault diagnosis technology. BRB prediction model can fully make use of the semi-quantitative information, and also can address the uncertainty information, such as probabilistic and fuzzy [26]. By defining of the belief degree, the actual situation of the system can be described more comprehensively and accurately. Compared with the traditional Bayesian probability, it can be seen as a more generalized probability, which means that it can describe a more special situation that the Bayesian probability theory cannot describe. Using BRB model can describe the security state of cloud system more objectively, and then obtain more accurate prediction results.

Furthermore, because of the subjectivity of experts' knowledge, the values of the initial parameters are not accurate, which may cause imprecise prediction results. To obtain more accurate predicting results, an optimization algorithm is used to train the proposed BRB model. This paper cites the CMA-ES algorithm for training the initial parameters [27], where leaky bucket mechanism is introduced to process the constraint conditions. Therefore, the prediction results of cloud security states can be obtained precisely.

The organization of this paper is shown as below. In section II, the problem about cloud security state is formulated. In section III, the inference of BRB prediction model and the parameter training using CMA-ES algorithm are introduced. In section IV, a practical case study for a real cloud computing platform is proposed and the simulation results are analyzed. Finally, the conclusion is concluded in section V.

II. PROBLEM FORMULATION

In this section, the assessment framework for describing the security state of system is constructed, and the BRB prediction model is established.

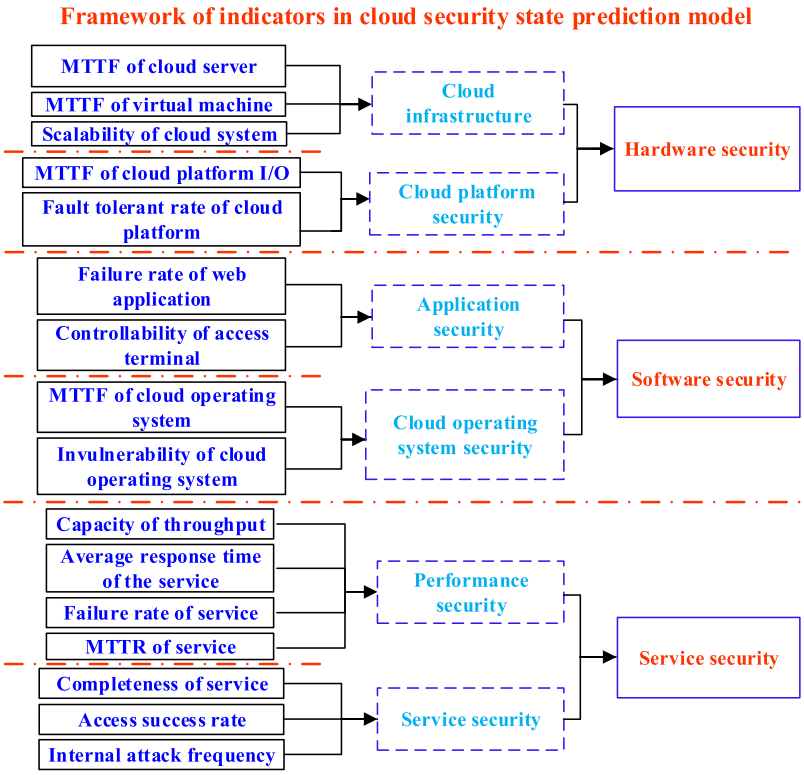

FIGURE 1. The formulation of BRB based cloud security-state prediction model.

A. THE ESTABLISHMENT OF THE ASSESSMENT INDICATORS FOR CLOUD COMPUTING SYSTEM

Before predicting of the security state of cloud computing system, it is necessary to make a comprehensive assessment based on the current indicators. According to the system characteristic of cloud computing, a multi-level indicators structure for the assessment of cloud computing security system is established with the security threat of actual system [28].

It is assumed that Y is the set of the whole indicators for reflecting the actual cloud system, which is defined as $Y = [y_1(t), \ldots, y_P(t)]^T$. In the practical system, according to the physical characteristic of system, the assessment framework is divided into three levels, including hardware security, software security and service security. When taking the significance of the whole related characteristic, the set of y as the screened characteristic selected from the set of Y, denoted as $\mathbf{y} = \left[y^1(t), \ldots, y^L(t)\right]^T$. L denotes the reordered number of the rescreened indicators, and notes that $L \leq P$. $y(t)$ means the monitoring data at the time instant t. The remained indicators are not taken into account considering for reducing the effort scale of the proposed model.

From the above definition, the selected indicators consist of three features in accordance with experience. In the level of the hardware security, the scalability of cloud system means that the load capacity to guarantee the normal operation of the system. The fault tolerant rate of cloud platform means the unstable probability that the system will reduce some factor or the normal operation of the system. These indicators are generally hard to be observed by the monitor accurately and the real value to be obtained needs experience as an assist. In the level of the software security, the indicators of controllability of access terminal and invulnerability of cloud operating system can be classified as qualitative knowledge, which means that it cannot be observed by the observation and obtained real data. Service security is one of the important indicators that assess customer satisfaction in cloud computing system, and its assessment is also needs the experts' experience. The change of its index acts a decisive role in assessing the cloud security state of the system. Evidential Reasoning (ER) algorithm can well dealing with the attribute that contains qualitative and quantitative knowledge. Considering this advantage, the ER algorithm is used to integrate the multiple indicators, and then the overall and accurate security state of system can be obtained. This proposed assessment framework can be analyzed from many aspects of system security, and it can be organized in Fig.1.

From the above description, it can be intuitively concluded that the system structure is too complex with large security indicators compared to other information systems. These indicators are both contained the quantitative data and qualitative knowledge, and also their information is full of many uncertainties. Thus, the Evidential Reasoning (ER) algorithm is employed to fuse the indicators of the system so that it can make a comprehensive assessment of cloud security state. The ER algorithm is a multi-criteria decision

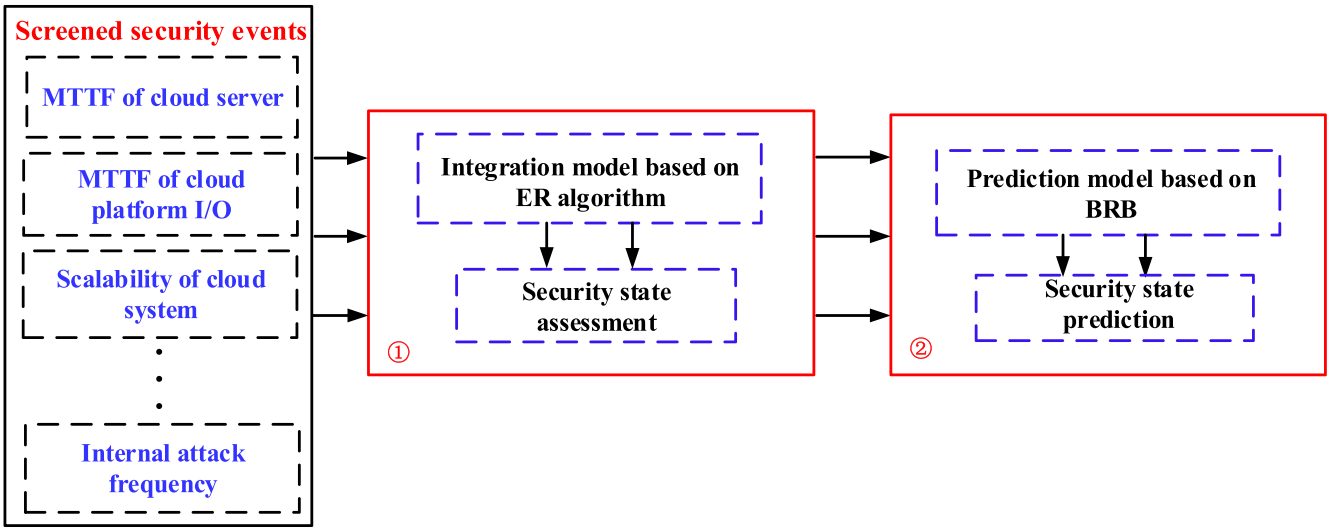

FIGURE 2. The process of the ER-BRB model.

analysis method (MCDA) based on reliability decision and D-S theory [29]. It can deal with conflicting evidence indicators very well, and has an advantage to address different types of information in the complex cloud computing system.

After all the screened indicators are integrated, the output assessment value is obtained, of which the range is 0 to 1. The physical definition of the data can be summarized as follows:

a. The assessment value of the cloud security state is quantized in the real number interval of [0, 1].

b. The higher of the assessment value is, the more security threats received on cloud platform.

c. When the security state exceeds the threshold range, the appropriate solutions is needed to make sure that the cloud system continually works properly.

When the assessment of the security state is completed using ER algorithm, next section is to construct the BRB prediction model. In the actual cloud computing system, the operation in the normal practice is rarely encountered the attack about security threats because of the complete security policy in every node and transmission mechanism. However, the vulnerability of cloud system is objective existing in engineering practice. In order to grab it and then establish a simulation environment to test the attack, it inevitably causes much difficulty and cost. Therefore, it is necessary to crawl the observation data with security indicators and then establishes a reasonable predicting model. Considering the testing data of cloud computing system is complex, it is hard to obtain the precise data in advance for training the prediction model. However, some knowledge of the indicators can be obtained directly by the monitor, as well as some other knowledge which act as qualitative forms or partial historical information may be given by expert experience. This knowledge indicated above can be well expressed in belief rules and then employed them to construct BRB prediction model to predict the behaviors [30].

The detail formulation of the two parts of ER-BRB based security-state prediction model is shown in Fig. 2, where the cloud states based on the security events can be predicted.

B. THE ESTABLISHMENT OF BRB PREDICTION MODEL FOR CLOUD SECURITY STATE

It is assumed that $x(t)$ is the assessed whole cloud security state at time instant t and exists $x(t) = E(\mathbf{y}(t))$, where function $E(\bullet)$ is a ER integration function. And then, the formulation at time instant t to $t+1$ based on BRB prediction model is described as follow [23]:

$$\begin{aligned} &R_k\text{: If } x(t) \text{ is } \mathrm{S}_k, \\ &\quad \text{Then } x(t+1) \text{ is } \left\{\left(S_1, \beta_{1,k}\right), \ldots, \left(S_N, \beta_{N,k}\right), \left(S, \beta_{S,k}\right)\right\} \\ &\quad \text{With rule weight } \theta_k \text{ and attribute weights } \delta = 1 \end{aligned} \tag{1}$$

where, R_k is the kth rule of the BRB prediction model. S_k represents the set of consequents, and the referential points consist of Excellent (E), Good (G), Medium (M) and Bad (B), and exists $S_k \in S(S = \{\mathrm{G}, \mathrm{M}, \mathrm{D}, \mathrm{VD}\})$. $\beta_{i,k}$ $(N = 1, \ldots, i, j, N; k = 1, \ldots, L)$ represents the belief degree of ith result for S_i in kth rule, N denotes the total number of the belief rule. $\beta_{S,k}$ is the remaining belief degree which means the unassigned to any consequent due to the lack of prior knowledge. This parameter reflects the completeness description of the BRB prediction model. θ_k can be defined as the weight of the kth rule, and δ can be defined as the weight located in the antecedent attribute, and their initial values are assumed that $\delta = 1$.

III. INFERENCE OF BRB PREDICTION MODEL AND TRAINING USING CMA-ES ALGORITHM

In this section, the inference of the introduced BRB prediction model and ER algorithm is proposed. Due to the initial

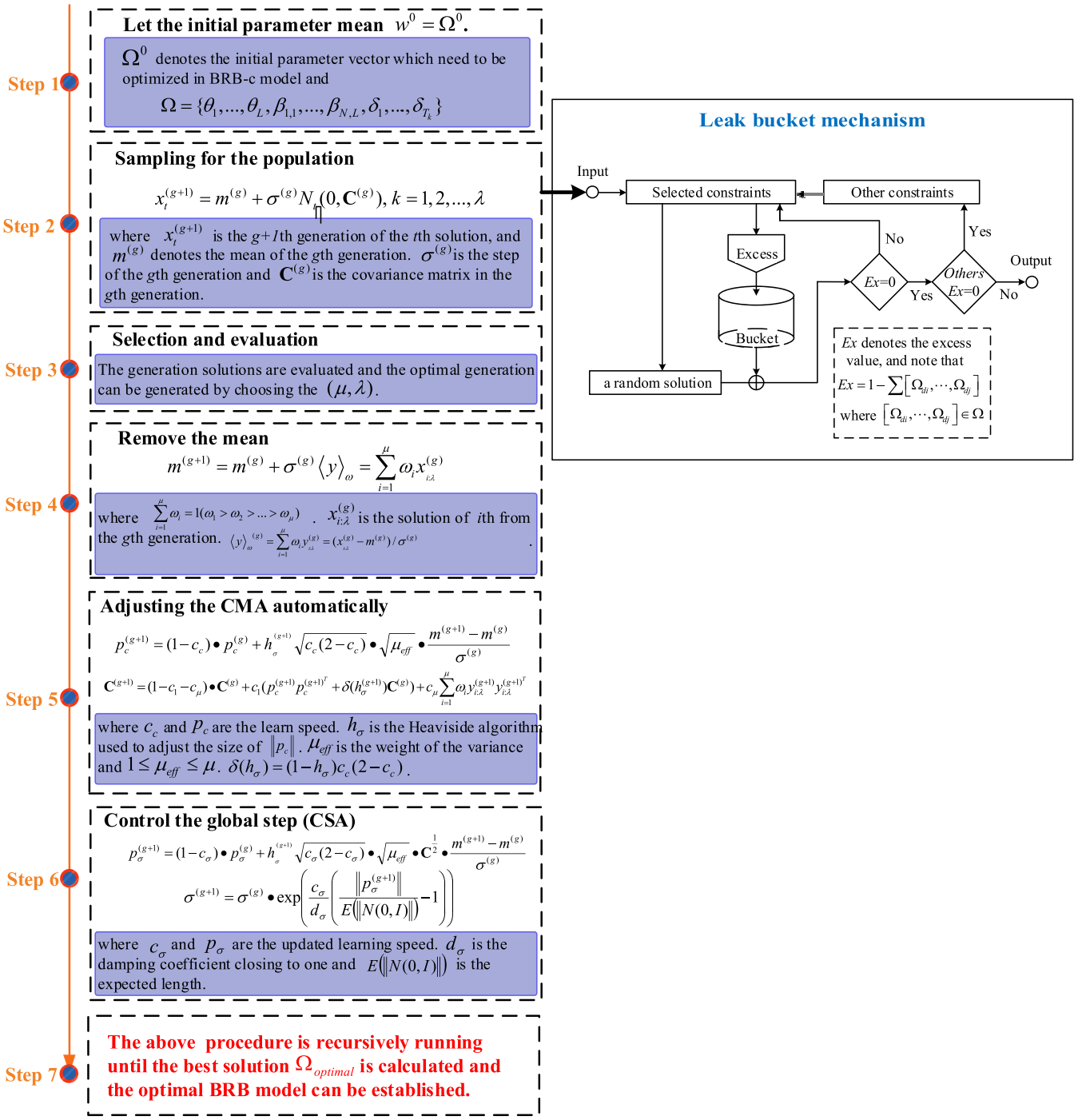

FIGURE 3. The process of CMA-ES optimization algorithm.

parameters in the process of training are given by the experts' experience that inevitably occurs to be inaccurate, The CMA-ES algorithm is employed to be optimized and the precise trained parameters are obtained.

A. INFERENCE FOR INTEGRATING MULTIPLE ATTRIBUTES USING ER ALGORITHM

To obtain the overall security state with multiple attributes in cloud computing platform, ER algorithm is introduced to integrate the security factors of system, and then obtain the assessment security state result $x(t)$. ER algorithm has an excellent performance in integrating different kinds of information, such as qualitative knowledge and quantitative data. It can deal with various types of features with uncertainties, and these features in the cloud computing environment have different types of information needed to be integrated that just the advantage of ER algorithm. The integrating process of ER can be introduced below:

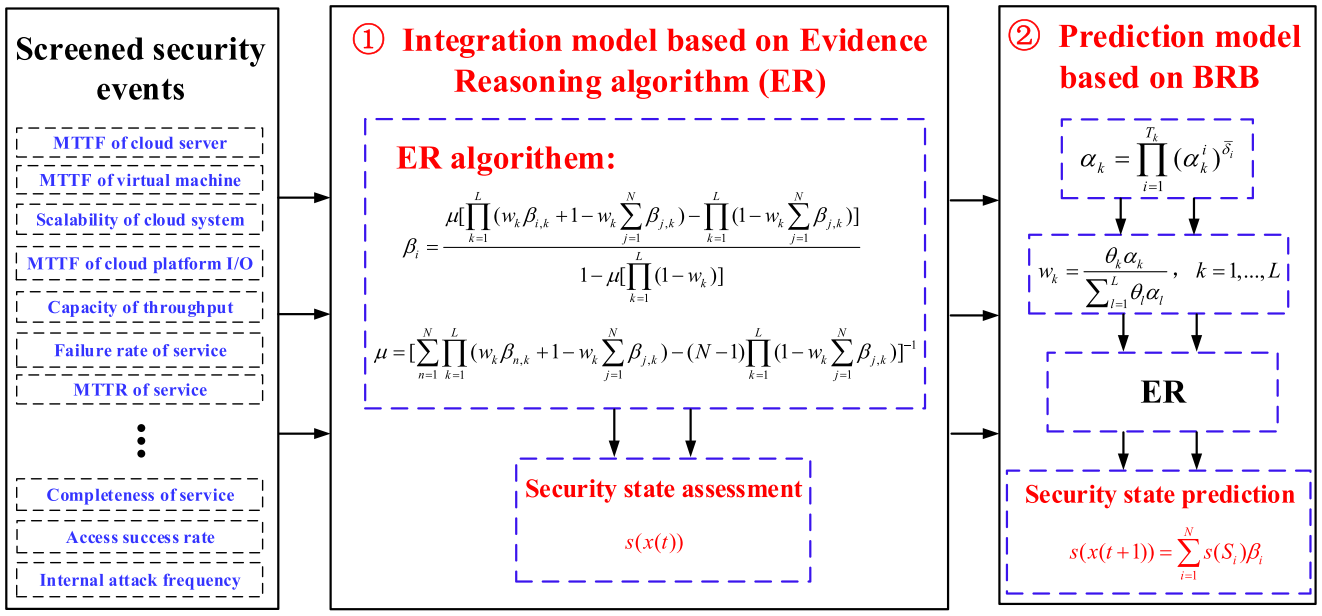

FIGURE 4. The formulation of BRB based cloud security-state prediction model.

Firstly, the output belief degrees are transformed into the basic probability masses by

$$m_{j,k} = \omega_k \beta_{j,k} \tag{2}$$

$$m_{S,k} = 1 - \omega_k \sum_{j=1}^{N} \beta_{j,k} \tag{3}$$

$$\bar{m}_{S,k} = 1 - \omega_k \tag{4}$$

$$\tilde{m}_{S,k} = \omega_k \left(1 - \sum_{j=1}^{N} \beta_{j,k}\right) \tag{5}$$

where $m_{j,k}$ denotes the basic probability install for the jth consequent S_j. $m_{S,k}$ represents the basic probability install for the collection $S = \{S_1, \ldots, S_N\}$ and it also represents the basic probability install which is not distributed to any consequents S_j. w_k denotes activation weight in the kth rule. Note that $m_{S,k} = \bar{m}_{S,k} + \tilde{m}_{S,k}$. $\bar{m}_{S,k}$ is caused by the activation weight of the kth rule and if the kth rule is important totally, $\omega_k = 1$ and $\bar{m}_{S,k} = 0$. $\tilde{m}_{S,k}$ is produced by the incompleteness of the estimated output of the kth rule. If the kth rule is complete, $1 - \sum_{j=1}^{N} \beta_{j,k} = 0$ and $\tilde{m}_{S,k} = 0$.

Secondly, the L rules are integrated and the belief degrees of the consequents S_j $(j = 1, \ldots, N)$ are obtained. $m_{j,I(k)}$ is used to represent the basic probability install of the consequent after the first k rules are integrated by the Dempster rule and $m_{S,I(k)} = 1 - \sum_{j=1}^{N} m_{j,I(k)}$. Note also that $m_{j,I(k)} = m_{j,1}$ and $m_{S,I(1)} = m_{S,1}$. The first k rules are integrated by the following formulates:

$$m_{j,I(k+1)} = K_{I(k+1)} \left[m_{j,I(k)} m_{j,k+1} + m_{j,I(k)} m_{S,k+1} + m_{S,I(k)} m_{j,k+1} \right] \tag{6}$$

$$m_{S,I(k)} = \bar{m}_{S,I(k)} + \tilde{m}_{S,I(k)} \tag{7}$$

$$\tilde{m}_{S,I(k+1)} = K_{I(k+1)} \left[\tilde{m}_{S,I(k)} \tilde{m}_{S,k+1} + \tilde{m}_{S,I(k)} \bar{m}_{S,k+1} + \bar{m}_{S,I(k)} \tilde{m}_{S,k+1} \right] \tag{8}$$

$$\bar{m}_{S,I(k+1)} = K_{I(k+1)} \left[\bar{m}_{S,I(k)} \bar{m}_{S,k+1} \right] \tag{9}$$

$$K_{I(k+1)} = \left[1 - \sum_{j=1}^{N} \sum_{\substack{t=1 \\ t \neq j}}^{N} m_{j,I(k)} m_{t,k+1} \right]^{-1}, \quad k = 1, \ldots, L-1 \tag{10}$$

$$\hat{\beta}_j = \frac{m_{j,I(L)}}{1 - \bar{m}_{S,I(L)}}, \quad j = 1, \ldots, N \tag{11}$$

$$\hat{\beta}_S = \frac{\tilde{m}_{S,I(L)}}{1 - \bar{m}_{S,I(L)}} \tag{12}$$

where $\hat{\beta}_j$ is the belief degree in the jth consequent of S_j and $\hat{\beta}_S$ represents the remaining degree which is not distributed any consequents.

The output belief degree can also be calculated by the analytic form of ER algorithm which can be shown as follows:

$$\beta_i = \frac{\mu\left[\prod_{k=1}^{L} (w_k \beta_{i,k} + 1 - w_k \sum_{j=1}^{N} \beta_{j,k}) - \prod_{k=1}^{L} (1 - w_k \sum_{j=1}^{N} \beta_{j,k})\right]}{1 - \mu\left[\prod_{k=1}^{L} (1 - w_k)\right]} \tag{13}$$

$$\mu = \left[\sum_{n=1}^{N} \prod_{k=1}^{L} (w_k \beta_{n,k} + 1 - w_k \sum_{j=1}^{N} \beta_{j,k}) - (N-1) \prod_{k=1}^{L} (1 - w_k \sum_{j=1}^{N} \beta_{j,k})\right]^{-1} \tag{14}$$

where β_i is a belief degree in the ith consequent of S_i. N is the amount of the consequent in a belief rule. Note also that$0 \leq \beta_i \leq 1$ and $\sum_{i=1}^{N} \beta_i = 1$.

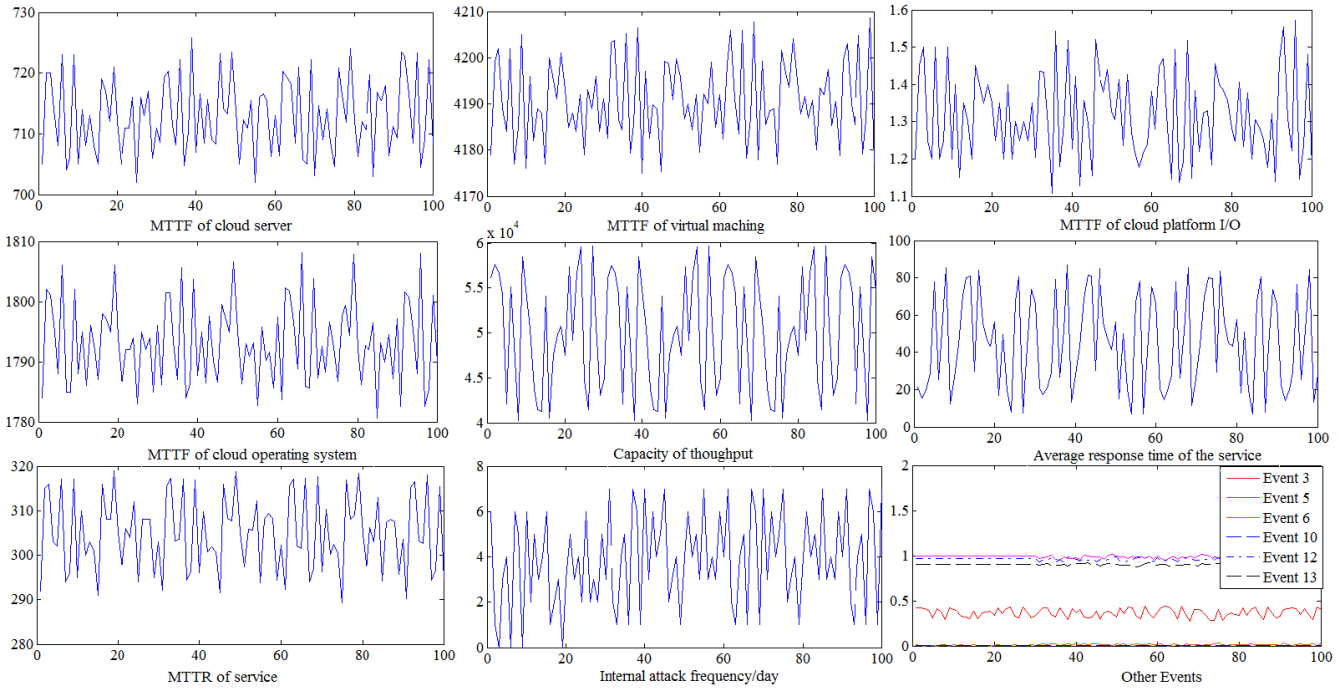

FIGURE 5. **Observation data during 100 days.**

Assume that there are L basic indicators, and note that $\{r_1, r_2, \cdots r_i, \cdots, r_L\}$, and $\{w_1, w_2, \cdots, w_i, \cdots, w_L\}$ is the weights of the basic indicators, exists $0 \leq w_i \leq 1$. There are M assessment grades $S_i\,(i = 1, \cdots, M)$, and then the overall assessment result is represented as $(S_1 : \beta_1, S_2 : \beta_2, \ldots, S_M : \beta_M)$ by the analytic ER algorithm [31]. $x\,(t)$ is obtained by

$$x\,(t) = \sum_{i=1}^{M} (U\,(S_i) \times \beta_i) \tag{15}$$

where $U\,(S_i)$ is the evaluated degrade of S_i.

B. INFERENCE OF THE BRB PREDICTION MODEL

When the input attributes are available, its matching degree of the *nth* attribute in the *kth* rule is obtained by

$$\alpha_k^n = \begin{cases} \dfrac{A_{n(j+1)} - x_n^*}{A_{n(j+1)} - A_{nj}} & k = j \text{ if } A_{nj} \leq x_n^* \leq A_{n(j+1)} \\ \dfrac{x_n^* - A_{nj}}{A_{n(j+1)} - A_{nj}} & k = j+1 \\ 0 & k = 1, 2, \ldots |x_n|,\ k \neq j, j+1 \end{cases} \tag{16}$$

where x_n^* can be regarded as the input of the *nth* attribute and $|x_n|$ is the amount of the belief rules containing *nth* attribute. A_{nj} and $A_{n(j+1)}$ are two reference values in the *jth* and $j+1$*th* rule including the *nth* attribute. Note that, α_k^n is the matching degree for the *nth* attribute located in the *kth* rule. The total matching degree of the input data for the *kth* rule α_k can be calculated as follow

$$\bar{\delta}_n = \frac{\delta_n}{\max\limits_{n=1,\ldots,T_k} \{\delta_n\}}, \quad 0 \leq \bar{\delta}_n \leq 1 \tag{17}$$

$$\alpha_k = \prod_{n=1}^{T_k} (\alpha_k^n)^{\bar{\delta}_n} \tag{18}$$

where T_k is the amount of attribute in *kth* rule. δ_n denotes the weight of *nth* attribute and $\bar{\delta}_n$ is its relative weight that represents the relative significance comparing with other attributes in the *kth* rule. Note that $0 \leq \alpha_k \leq 1$.

When the input attributes are available, the belief rules are activated and their activation weights are calculated by

$$w_k = \frac{\theta_k \alpha_k}{\sum_{l=1}^{L} \theta_l \alpha_l}, \quad k = 1, \ldots, L \tag{19}$$

where θ_k and w_k denote the relative weight and activation weight in *kth* rule, respectively. L is defined as the amount of the rule in BRB model. There are $0 \leq w_k \leq 1$ and $\sum\limits_{k=1}^{L} w_k = 1$. If the *kth* rule is fully activated, note that $w_k = 1$, otherwise, $w_k \leq 1$.

After certain rules have been activated, their output can be integrated by the (13) and (14). The utility of the *tth* consequent is assumed to $s(S_t)$ and the excepted utility of BRB model is calculated by

$$s(x^*) = \sum_{t=1}^{N} s(S_t)\beta_t \tag{20}$$

TABLE 1. The screened security events of cloud computing platform.

1st Level	2nd Level	3rd Level	Reference levels			
			VH(0)	H(0.3)	M(0.6)	L(1)
Hardware Security (0.3)	Cloud infrastructure Security (0.5)	Mean Time to Failures (MTTF) of cloud server (0.4)	1000	500	200	0
		MTTF of virtual machine (0.3)	8000	4000	3000	0
		Scalability of cloud system (0.3)	100%	70%	35%	0%
	Cloud platform Security (0.5)	MTTF of cloud platform I/O (0.5)	2	1	0.5	0
		Fault tolerant rate of cloud platform (0.5)	100%	90%	50%	0%
Software Security (0.3)	Application Security (0.5)	Failure rate of web application (0.5)	100%	20%	5%	0%
		Controllability of access terminal (0.5)	qualitative index			
	Cloud operating system Security (0.5)	MTTF of cloud operating system (0.5)	5000	3000	2000	0
		Invulnerability of cloud operating system (0.5)	qualitative index			
Service Security (0.4)	Performance Security (0.4)	Capacity of throughput (0.25)	60000	35000	20000	0
		Average response time of the service (0.25)	0	30	60	100
		Failure rate of service (0.25)	0%	10%	50%	100%
		Mean Time to Repair (MTTR) of service (0.25)	0	200	5000	10000
	Service Security (0.6)	Completeness of service (0.25)	100%	80%	40%	0%
		Access success rate (0.25)	100%	85%	40%	0%
		Internal attack frequency/day (0.5)	0	10	15	30

where $s(x^*)$ is the final output of BRB. x^* denotes the input of BRB.

C. OPTIMIZATION FOR THE SECURITY-STATE PREDICTION MODEL

For this predictive model, its initial parameters are given by experts. Because of the boundedness of the expert knowledge, the initial parameters may not appropriate the engineering practice. Therefore, an optimization model is needed for improving the precision about BRB prediction model. In this paper, the covariance matrix adaption evolution strategy (CMA-ES) is introduced in this paper [32]. Especially, the leak bucket mechanism is introduced to update the operators in population. Due to the inaccurate input parameters, parts of the operators are not satisfied with the constraints. It may impact the efficiency of the optimization. By iteratively calculating the excess value between the equality constraints till it equals to 0, the modified operators are obtained. The process of the CMA-ES optimization algorithm the can be introduced in Fig. 3.

There are three parameters are needed to be optimized in BRB model, including rule weights, attribute weights and belief degrees, which can be shown as follows:

a. The belief rule weights denote the relative significance of each rule and it should meet the following constraint:

$$0 \leq \theta_k \leq 1, \quad k = 1, 2, \ldots L \tag{21}$$

b. The constraint of attribute weights. An attribute weight is normalized and its value must between the interval from zero and one.

$$0 \leq \delta_n \leq 1, \quad n = 1, \ldots, T_k \tag{22}$$

c. The constraint of belief degrees. A belief degree in the rule is normalized and should between the interval from zero and one, i.e.

$$0 \leq \beta_{i,k} \leq 1, \quad k = 1, 2, \ldots L \tag{23}$$

d. The belief degrees denote the possibility of consequents of the *kth* rule. If the *kth* belief rule is completely processed, the sum of belief degrees is equal to one; otherwise, it should less than one, i.e.

$$\sum_{i=1}^{N} \beta_{i,k} \leq 1, \quad k = 1, 2, \ldots, L \tag{24}$$

The output of BRB prediction model can be expressed as

$$\text{output}_{estimated} = \sum_{n=1}^{N} s(S_i)\beta_i \tag{25}$$

where β_i represents a belief degree of *ith* consequent and $s(S_i)$ is the utility of the *ith* consequent of S_i.

The objective function is employed to train the parameters in BRB to decrease the value range of error between the assessed output and real output. The mean square error (MSE) between the estimated and real one is used to reflect the accuracy of the BRB model and it is calculated by

$$\text{MSE}(\theta_k, \beta_{i,k}, \delta_n) = \frac{1}{T} \sum_{i=1}^{T} (\text{output}_{estimated} - \text{output}_{actual})^2 \tag{26}$$

where output_{actual} is the actual output of BRB model gathered from monitoring data where T represents the size of dataset.

Therefore, the objective function is express as

$$\min \ MSE(\theta_k, \beta_{i,k}, \delta_n) \tag{27}$$

$$s.t. \ 0 \leq \theta_k \leq 1 \tag{28}$$

$$0 \leq \delta_n \leq 1, \quad n = 1, \ldots, T_k \tag{29}$$

TABLE 2. Referential points of cloud security states.

Referential points	Excellent (E)	Good (G)	Medium (M)	Bad (B)
Numerical values	0	0.35	0.65	1

TABLE 3. Initial weights and belief degrees of belief rules.

Number	Rule weights	*x(t)*	*x(t+1)* distribution $\{S_1, S_2, S_3, S_4\}$={E, G, M, B}
1	1	E	$\{(S_1, 1), (S_2,0), (S_3, 0), (S_4, 0), (S, 0)\}$
2	1	G	$\{(S_1, 0), (S_2,1), (S_3, 0), (S_4, 0), (S, 0)\}$
3	1	M	$\{(S_1, 0), (S_2,0), (S_3, 1), (S_4, 0), (S, 0)\}$
4	1	B	$\{(S_1, 0), (S_2,0), (S_3, 0), (S_4, 1), (S, 0)\}$

$$0 \le \beta_{i,k} \le 1, \quad i = 1, .., N, \ k = 1, 2, \ldots L \tag{30}$$

$$\sum_{i=1}^{N} \beta_{i,k} \le 1 \tag{31}$$

Remark 1: The time complexity of the CMA-ES algorithm is $O\left(n^3\right)$. When the constraints of the input attributes are calculated, the time complexity will fold increase according to the number of the belief rules. Nevertheless, due to the independently calculating operation for each sub-process, parallel computing can reduce the time complexity.

The framework of the process with formulations of this paper can be organized as Fig. 4. The screened security events are captured by the monitor, which are concerned the aspects of software security, hardware security and service security. ER algorithm is used to integrate these events and the assessment of the cloud security state denoted as $s(x\,(t))$ ranged from 0 to 1 is obtained. Finally, the BRB prediction model is constructed to predict the cloud security state, and the security state at instant $t+1$ denoted as $s(x\,(t+1))$ is finally calculated.

IV. CASE STUDY

To demonstrate the effectiveness of the proposed ER-BRB based prediction model applied in engineering, the assessment of security state in the actual cloud computing platform will be established by using 100 days monitoring logs. Moreover, the prediction model will be established and the comparative study is tested. In this study, it assumes that the testing data is reliable.

A. PROBLEM FORMULATION

From above discussion, we indicate that the security state is mainly influence on the performance of actual cloud computing platform. Firstly, the real security events of indicators during 100 days are collected by the system Monitor in cloud computing platform. According to the assessment framework proposed above, some data of these indicators are obtained indirectly because of the specific factors that need experts knowledge beforehand. Also, some data is of the attributes with qualitative knowledge that cannot be directly measured. Thus, the original observation data that can be crawled directly is shown in Fig. 5.

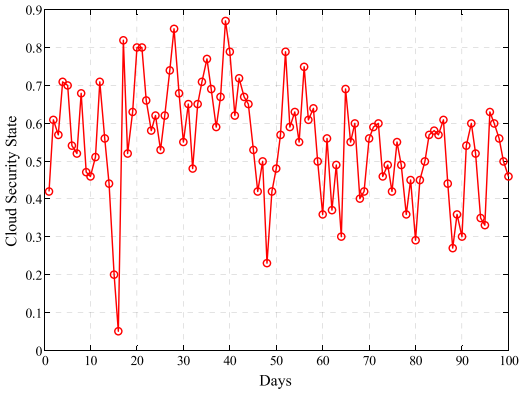

FIGURE 6. The cloud security states during 100 days.

Before assessing these large-scale indicators, the certain weights of each attributes need to be is set by the experts. The reference points of input parameters are set as Low (L), Medium (M), High (H), Very High (VH), and the boundary values of each level are demonstrated as Table 1.

Remark 2: The initial data set is supported by Mobike Technology Ltd. in China, whose system is running on the Tencent Cloud platform. A total of 100 days' logs of server security state were collected by monitor from the system event logs, which recorded the security related events.

B. CONSTRUCTING THE BRB-BASED SECURITY-STATE PREDICTION MODEL

In this case, the quantized security states of a cloud computing platform during 100 days are obtained by using the proposed method, as shown in Fig. 6. The values of these security states are normalized, and the greater value represents more dangerous state.

To predict the cloud security state, the BRB prediction model is established with a belief rule that is shown below:

$$\begin{aligned} R_k\text{: If } x\,(t) \text{ is } \mathrm{S}_k, \text{ Then } x\,(t+1) \\ \text{is } \left\{\left(E, \beta_{1,k}\right), \left(G, \beta_{2,k}\right), \left(M, \beta_{3,k}\right), \left(B, \beta_{4,k}\right), \left(S, \beta_{D,k}\right)\right\} \\ \text{With rule weight } \theta_k \end{aligned} \tag{32}$$

TABLE 4. The initial parameters of the forecasting models in comparative studies.

Comparative model	Initial parameters
Markov model	Initial probability vector = [0.25,0.25,0.25,0.25]; Initial probability transfer matrix = [1,0,0,0;0,1,0,0;0,0,1.0,0;0,0,0,1];
RBF model	Input neurons: 3; Output neurons: 1; Sliding window size: 3

TABLE 5. The initial parameters of CMA-ES for prediction models.

	Values of initial parameters
Initial parameters of CMA-ES	$m^0 = O^0$; $\sigma^0 = 0.5$; $\lambda = 13$;
	$\tau = 6$; $a_1 = 0.0031$;
	$a_\tau = 0.0066$; $p_\psi^0 = 0$;
	$a_\psi = 0.147$; $p_\sigma^0 = 0$;
	$a_\sigma = 0.1813$; $d_\sigma = 1.1813$;
	$e = 0.6$; Loop=100 ;

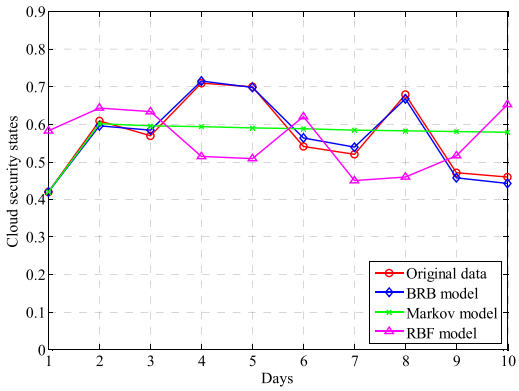

FIGURE 7. The comparative results in round 1.

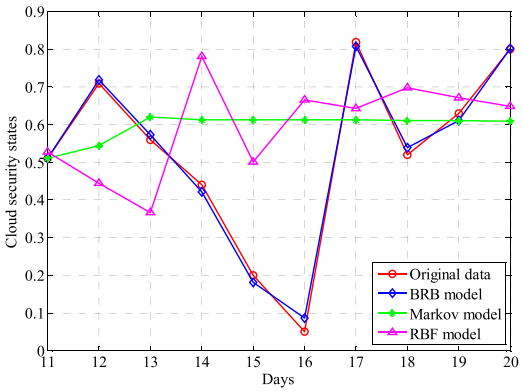

FIGURE 8. The comparative results in round 2.

where S_k denotes the assessment result from integrating the multiple attributes by using ER algorithm, and $A_k \in \{E, G, M, B\}$.

Ten-fold cross validation is used to make the predictive results more realistic and credible, and interval estimation is employed to verify the accuracy. Thus, the data-set of cloud security states in Fig. 6 is divided into 10 parts, where 9 parts are used as the training data, and 1 part is used as the testing data. Four referential points are assigned to the security states and the corresponding values are illustrated in Table 2.

C. THE INITIALIZATION OF COMPARATIVE EXPERIMENT

In this section, to prove the precision and advancement of the this prediction method, three forecasting models which include Markov forecasting model (MM), Neural Network forecasting model with Radical Basis Function (RBF) and BRB forecasting model are selected for comparative studies, where the proposed constrained CMA-ES optimizing algorithm is employed for each model respectively. RBF Neural Network model is one of the most popular quantitative information-based model employed recently, which has a high performance compared with other Neural Network. Markov forecasting model is the typical semi-quantitative model based on Bayesian probability. These two models are taken as the comparison is to prove the high efficiency and accuracy of the proposed BRB prediction model.

The initial weights of belief rule and belief degrees for proposed prediction model are illustrated in Table 3.

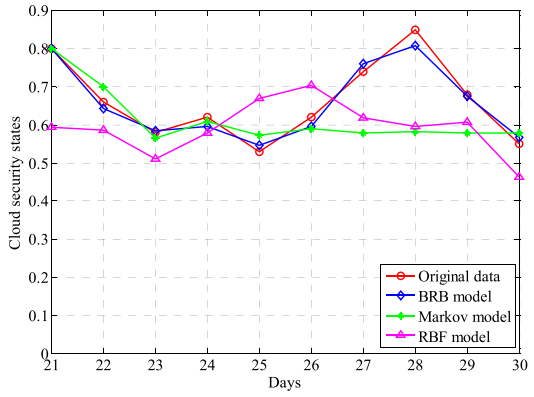

FIGURE 9. The comparative results in round 3.

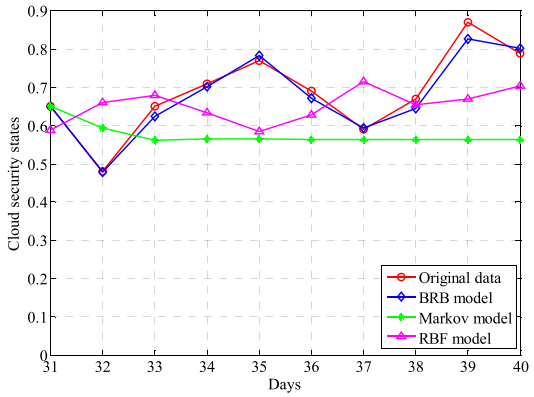

FIGURE 10. The comparative results in round 4.

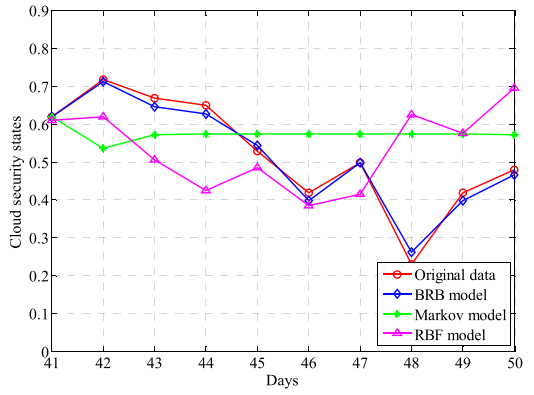

FIGURE 11. The comparative results in round 5.

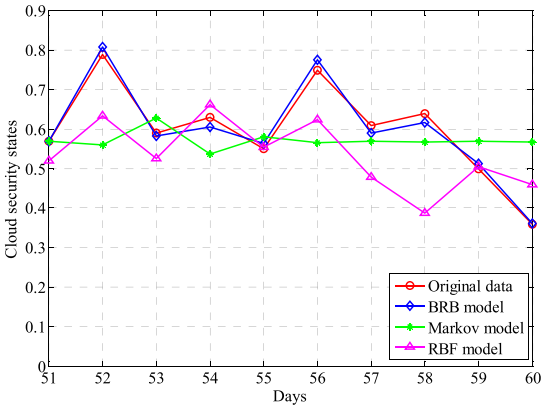

FIGURE 12. The comparative results in round 6.

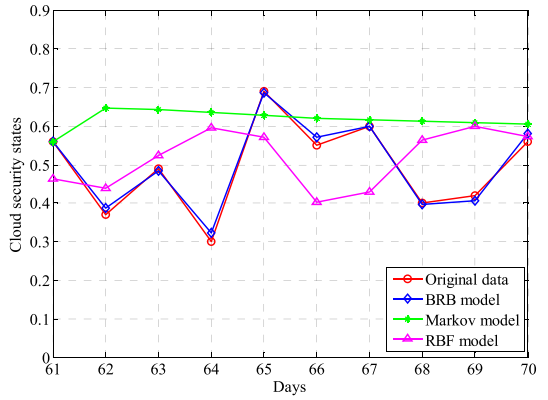

FIGURE 13. The comparative results in round 7.

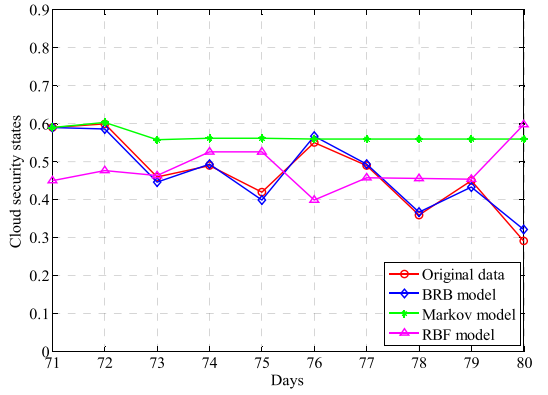

FIGURE 14. The comparative results in round 8.

The input parameters about other forecasting models are illustrated in Table 4. The initial input parameters of CMA-ES optimization algorithm are listed in Table 5.

D. COMPARARATIVE RESULTS

The 10-fold cross validation experiments are picked in 10 times, and prediction results generated by different models with same CMA-ES optimization algorithm are listed in Figs. 7 to 16. The mean square errors of these results are listed in Table 6.

The total MSE and the interval estimation of the mean with 95% probability of BRB prediction results in 10 rounds, and the comparative results are followed, which is listed in Table 7.

From above results, it concludes that the errors of the BRB model are better than that of MM and RBF models. Moreover, the interval of the error is limited in a narrow range, which is acceptable in an actual situation of cloud computing environment.

TABLE 6. The mean square error and of 10-fold cross-validation.

Round	1	2	3	4	5
BRB	1.60E-4	3.16E-4	3.90E-4	3.67E-4	3.27E-4
MM	5.40E-3	5.99E-2	1.12E-2	2.06E-2	2.23E-2
RBF	1.69E-2	7.60E-2	1.66E-2	1.38E-2	2.79E-2
Round	6	7	8	9	10
BRB	3.03E-4	1.47E-4	1.53E-4	1.85E-4	2.19E-4
MM	1.09E-2	3.02E-2	9.20E-3	1.87E-2	1.33E-2
RBF	1.29E-2	2.28E-2	8.00E-3	2.03E-2	3.65E-2

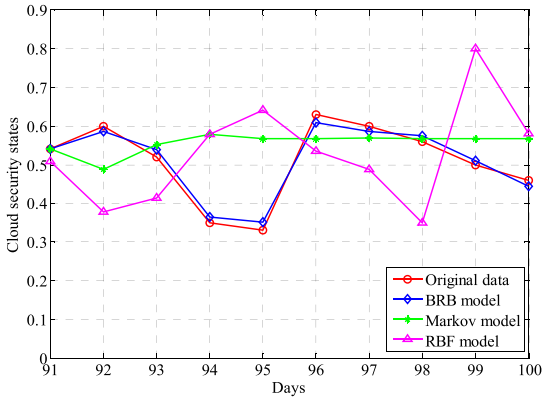

FIGURE 15. The comparative results in round 9.

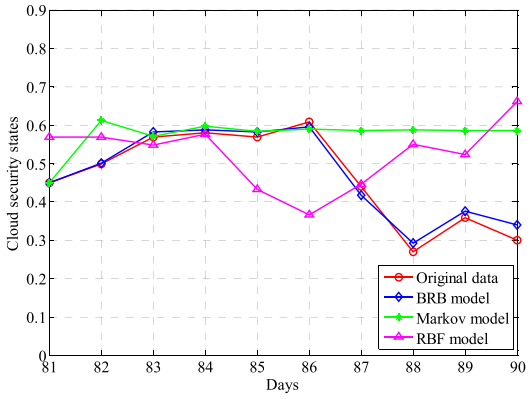

FIGURE 16. The comparative results in round 10.

TABLE 7. The total MSE and the interval estimation.

	Total MSE	Interval estimation
BRB	2.56E-4	[1.89E-4, 3.23E-4]
MM	2.02E-2	[8.90E-3, 3.15E-2]
RBF	2.52E-2	[1.35E-2, 3.58E-4]

V. CONCLUSIONS

In this paper, considering the multiple indicators with large-scale monitoring data in cloud computing system, a new BRB cloud security-state prediction model is proposed. A three-level assessment framework of the indicators is illustrated. ER algorithm is employed to fuse these indicators which can take the view of both cloud computing servers and users. ER algorithm has an excellent performance in multiple attributes decision making. It can well deal with the evidence containing high conflict and complete conflict so that the assessment result can be accurately obtained. Moreover, a BRB prediction model based on the assessment results is proposed to predict the cloud computing security state. To determine the optimal input parameters, the CMA-ES optimization algorithm is used in training process. Equipped with this optimal algorithm, the precise BRB based prediction model for cloud security state is finally constructed whose prediction results are obtained by using large-scale monitoring data and expert knowledge. A practical case study is presented to prove a high accuracy and efficiency in this proposed prediction model.

In this paper, the system events are the only considering factor for the cloud security state description. However, cloud computing environment is so complex that there are also other threats can impact the security state, such as network attack, data storage security and human error. Thus, more security factors should be taken into further works so that the actual cloud environment can be real described.

REFERENCES

[1] Y. Q. Zhang, X. F. Wang, X. F. Liu, and L. Liu, "Survey on cloud computing security," *J. Softw.*, vol. 27, no. 6, pp. 1328–1348, 2016.
[2] D. G. Rosado, D. Mellado, E. Fernandez, and M. Piattini, *Security Engineering for Cloud Computing: Approaches and Tools*. Hershey, PA, USA: IGI Global, 2012, pp. 1–19.
[3] A. Muñoz, J. Gonzalez, and A. Maña, "A performance-oriented monitoring system for security properties in cloud computing applications," *Comput. J.*, vol. 55, no. 8, pp. 979–994, 2012.
[4] S. Jonathan, "Monitoring cloud computing by layer, part 1," *IEEE Security Privacy*, vol. 9, no. 2, pp. 66–68, Apr. 2011.
[5] D. Petcu, "A taxonomy for SLA-based monitoring of cloud security," in *Proc. IEEE 38th Annu. Comput. Softw. Appl. Conf. (COMPSAC)*, Jul. 2014, pp. 640–641.
[6] K. Alhamazani, R. Ranjan, F. Rabhi, L. Wang, and K. Mitra, "Cloud monitoring for optimizing the QoS of hosted applications," in *Proc. IEEE 4th Int. Conf. Cloud Comput. Technol. Sci. (CloudCom)*, Dec. 2012, pp. 765–770.
[7] S. Vakilinia, B. Heidarpour and M. Cheriet, "Energy efficient resource allocation in cloud computing environments," *IEEE Access*, vol. 4, pp. 8544–8557, 2016.

[8] T. Boukra, "Identifying new prognostic features for remaining useful life prediction using particle filtering and neuro-fuzzy system predictor," in *Proc. IEEE 15th Int. Conf. Environ. Elect. Eng. (EEEIC)*, Jun. 2015, pp. 1533–1538.
[9] S. Yin, X. Xie, J. Lam, K. C. Cheung, and H. Gao, "An improved incremental learning approach for KPI prognosis of dynamic fuel cell system," *IEEE Trans. Cybern.*, vol. 46, no. 12, pp. 3135–3144, Dec. 2016.
[10] X. Xie, W. Sun, and K. C. Cheung, "An advanced PLS approach for key performance indicator-related prediction and diagnosis in case of outliers," *IEEE Trans. Ind. Electron.*, vol. 63, no. 4, pp. 2587–2594, Apr. 2016.
[11] P. R. Vundavilli, M. B. Parappagoudar, S. P. Kodali, and S. Benguluri, "Fuzzy logic-based expert system for prediction of depth of cut in abrasive water jet machining process," *Knowl.-Based Syst.*, vol. 27, pp. 456–464, Mar. 2012.
[12] X. Cheng and S. Lang, "Research on network security situation assessment and prediction," in *Proc. 4th Int. Conf., IEEE Comput. Inf. Sci. (ICCIS)*, Aug. 2012, pp. 864–867.
[13] A. Rogge-Solti and M. Weske, "Prediction of business process durations using non-Markovian stochastic Petri nets," *Inf. Syst.*, vol. 54, pp. 1–14, Dec. 2015.
[14] C. H. Wang, X. L. Zhang, and X. C. Liang, "Research on load forecasting strategy based on BP neural network under cloud computing architectures," *Electr. Power Inf. Commun. Technol.*, vol. 14, no. 11, pp. 46–50, 2016.
[15] Y. Jie and W. G. Weng, "Improved unbiased grey model for prediction of gas supplies," *J. Tsinghua Univ. (Sci. Technol.)*, vol. 54, no. 2, pp. 145–148, 2015.
[16] R. Hu, J. Jiang, G. Liu, and L. Wang, "Efficient resources provisioning based on load forecasting in cloud," *Sci. World J.*, vol. 2014, Feb. 2014, Art. no. 321231.
[17] W. Zhao, J. Wang, and H. Lu, "Combining forecasts of electricity consumption in China with time-varying weights updated by a high-order Markov chain model," *Omega*, vol. 45, pp. 80–91, Jun. 2014.
[18] A. R. M. Forkan, I. Khalil, Z. Tari, S. Foufou, and A. Bouras, "A context-aware approach for long-term behavioural change detection and abnormality prediction in ambient assisted living," *Pattern Recognit.*, vol. 48, no. 3, pp. 628–641, 2015.
[19] M. Frigault, L. Wang, A. Singhal, and S. Jajodia, "Measuring network security using dynamic Bayesian network," in *Proc. 4th ACM Workshop Quality Protection*, 2008, pp. 23–30.
[20] R. Dash and P. Dash, "Efficient stock price prediction using a self evolving recurrent neuro-fuzzy inference system optimized through a modified differential harmony search technique," *Expert Syst. Appl.*, vol. 52, pp. 75–90, Jun. 2016.
[21] Z.-J. Zhou, C.-H. Hu, B.-C. Zhang, D.-L. Xu, and Y.-W. Chen, "Hidden behavior prediction of complex systems based on hybrid information," *IEEE Trans. Cybern.*, vol. 43, no. 2, pp. 402–411, Apr. 2013.
[22] G. Li, Z. Zhou, C. Hu, L. Chang, Z. Zhou, and F. Zhao, "A new safety assessment model for complex system based on the conditional generalized minimum variance and the belief rule base," *Safety Sci.*, vol. 93, pp. 108–120, Mar. 2017.
[23] J.-B. Yang, J. Liu, J. Wang, H.-S. Sii, and H.-W. Wang, "Belief rule-base inference methodology using the evidential reasoning approach-RIMER," *IEEE Trans. Syst., Man, Cybern. A, Syst., Humans*, vol. 36, no. 2, pp. 266–285, Mar. 2006.
[24] F.-J. Zhao, Z.-J. Zhou, C.-H. Hu, L.-L. Chang, Z.-G. Zhou, and G.-L. Li, "A new evidential reasoning-based method for online safety assessment of complex systems," *IEEE Trans. Syst., Man, Cybern., Syst.*, to be published, doi: 10.1109/TSMC.2016.2630800.
[25] Z.-J. Zhou, L.-L. Chang, C.-H. Hu, X.-X. Han, and Z.-G. Zhou, "A new BRB-ER-based model for assessing the lives of products using both failure data and expert knowledge," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 46, no. 11, pp. 1529–1543, Nov. 2016.
[26] Z.-J. Zhou, C.-H. Hu, G.-Y. Hu, X.-X. Han, B.-C. Zhang, and Y.-W. Chen, "Hidden behavior prediction of complex systems under testing influence based on semiquantitative information and belief rule base," *IEEE Trans. Fuzzy Syst.*, vol. 23, no. 6, pp. 2371–2386, Dec. 2015.
[27] N. Hansen, "The CMA evolution strategy: A comparing review," in *Towards a New Evolutionary Computation* (Studies in Fuzziness and Soft Computing), vol. 192. Berlin, Germany: Springer, 2006, pp. 75–102.
[28] H. Wei and P. L. Qiao, "Reliability assessment of cloud computing platform based on semiquantitative information and evidential reasoning," *J. Control Sci. Eng.*, vol. 2016, Sep. 2016, Art. no. 2670210.
[29] Y. M. Wang, J. B. Yang, D. L. Xu, and K. S. Chin, "The evidential reasoning approach for multiple attribute decision analysis using interval belief degrees," *Eur. J. Oper. Res.*, vol. 175, no. 1, pp. 35–66, 2006.
[30] Z.-J. Zhou, G.-Y. Hu, B.-C. Zhang, C.-H. Hu, Z.-G. Zhou, and P.-L. Qiao, "A model for hidden behavior prediction of complex systems based on belief rule base and power set," *IEEE Trans. Syst., Man, Cybern., Syst.*, to be published, doi: 10.1109/TSMC.2017.2665880.
[31] J. B. Yang, "Rule and utility based evidential reasoning approach for multiattribute decision analysis under uncertainties," *Eur. J. Oper. Res.*, vol. 131., no. 1, pp. 31–61, 2001.
[32] G.-Y. Hu, Z.-J. Zhou, B.-C. Zhang, X.-J. Yin, Z. Gao, and Z.-G. Zhou, "A method for predicting the network security situation based on hidden BRB model and revised CMA-ES algorithm," *Appl. Soft Comput.*, vol. 48, pp. 404–418, Nov. 2016.

HANG WEI received the B.Eng. and M.Eng. degrees from the Harbin University of Science and Technology, Harbin, China, in 2011 and 2014, respectively, where he is currently pursuing the Ph.D. degree. His research interests include cloud computing, complex system reliability assessment, and information security.

GUAN-YU HU received the B.Eng. degree from the Harbin University of Science and Technology, Harbin, China, in 2005, the M.Eng. degree from the Changchun University of Technology, Changchun, China, in 2010, and the Ph.D. degree from the Harbin University of Science and Technology. He is currently an Associate Professor with the School of Information Science and Technology, Hainan Normal University, Haikou, China. His research interests include intelligent computing, optimization algorithm, network security, and belief rule base.

XIAOXIA HAN received the B.Eng. and M.Eng. degrees from the Xi'an University of Architecture and Technology, Xi'an, China, in 2001 and 2004, respectively. She is currently a Lecturer with the High-Tech Institute of Xi'an. Her current research interests include belief rule base and failure prognosis.

PEILI QIAO is currently a Professor with the Harbin University of Science and Technology, Harbin, China, and the Dean of the School of the Computer Science and Technology. He is also a Ph.D. Advisor. He has authored or co-authored approximately 100 papers. His research interests include information security and intelligent technology.

ZHIGUO ZHOU received the B.Eng. and Ph.D. degrees in computer science and technology from Xidian University, Xi'an, China, in 2008 and 2014, respectively. He was a Visiting Scholar with Leiden University, Leiden, The Netherlands, from 2013 to 2014. He is currently a Post-Doctoral Researcher with the Department of Radiation Oncology, The University of Texas Southwestern Medical Center, Dallas, TX, USA. He has authored or co-authored approximately eight papers. His current research interests include medical image processing, medical physics, medical informatics, pattern recognition, and machine learning.

ZHI-CHAO FENG received the B.Eng. degree in control science and management from the High-Tech Institute of Xi'an, Xi'an, China, in 2012, where he is currently pursuing the master's degree. His research interests include evidential reasoning, information fusion, safety assessment, and fault prognosis and optimal maintenance of dynamic systems.

XIAO-JING YIN received the B.Eng. degree from the Liren College, Yanshan University, Qinhuangdao, China, in 2011, and the M.Eng. degree from the School of Mechatronic Engineering, Changchun University of Technology, Changchun, China, in 2014, where she is currently pursuing the Ph.D. degree in mechanical engineering. Her research interests include complex system fault diagnosis and prediction, health estimation, and prognostics.