Hindawi
Security and Communication Networks
Volume 2020, Article ID 7816925, 12 pages
https://doi.org/10.1155/2020/7816925

*Research Article*

# Risk Situation Assessment Model Based on Interdomain Interaction in Cloud Computing Environment

**Gaocai Wang and Ning Yu**

*School of Computer and Electronics and Information, Guangxi University, Nanning, China*

Correspondence should be addressed to Gaocai Wang; wanggcgx@163.com

Received 20 January 2020; Revised 20 March 2020; Accepted 12 May 2020; Published 25 August 2020

Academic Editor: Leandros Maglaras



With the widespread application of cloud computing sharing technology, the demand for cross-domain interaction is also increasing. However, due to the uncertainty of interaction behaviour and the difference of network service quality, the risk of cross-domain interaction cannot be accurately evaluated. Therefore, this paper proposes a risk situation evaluation model based on interdomain interactions. The model collects interactive credentials such as the frequency, credibility, and time-effectiveness of the user-submitted evaluations. At the same time, it collects the evaluation of quality of service provided by the network security domain. Then, we set up a risk evaluation equation based on the interaction credentials to implement the risk evaluation of cross-domain interaction behaviour. Finally, we apply MATLAB platform to simulate the evolution process of evaluation. The experimental results show that, compared with other models, the evaluation method proposed in this paper improves the accuracy of the evaluation results and meets the security requirements of multidomain interaction.

## 1. Introduction

With the development of cloud computing sharing technology and the increasing demand for users to request services, the interaction requirements between users and resources have gradually evolved from a single domain to multidomain interactions. Therefore, in order to meet the needs of users' cross-domain interaction, a series of cross-domain access control models have been proposed, such as multilevel network security framework based on cross-domain access [1], a cross-domain trust model based on content delivery [2], and an access control model based on risk assessment [3]. These cross-domain access control models judge the credibility of users' cross-domain interactions by calculating the trust value between users and security domains. However, due to the diversity and dynamics of interactive entities in the cloud environment, the trust relationship between users and security domains becomes difficult to evaluate. Therefore, in order to make the cross-domain access control model more robust, more and more researchers pay more attention to evaluating the risk in the process of cross-domain interaction, not just the results of the interaction. The traditional evaluation model rarely considers the interdomain operation factors, which leads to problems such as excessive calculation of trust, high system overhead, slow operating efficiency, and low practical value. Therefore, how to evaluate the risks of cross-domain interactions is a problem we need to solve.

The current approach to evaluating the risks of cross-domain interactions is to establish a trust mechanism, that is, establishing a trust framework and specifying some variables to measure trust to determine whether cross-domain interactions are in a safe state or a risk state. The comprehensive evaluation value in the trust mechanism consists of direct and indirect trust values. The direct trust value is obtained through the result of user interaction; the indirect trust value is obtained through a third-party recommendation. However, from an economic point of view, there are potential risks in each interaction process. The security of the model cannot be determined simply by calculating the results of user interaction.

Therefore, this paper proposes an evaluation model based on cross-domain interaction for cloud computing multidomain environments (RP-ECDM). One is based on the credibility, time-effectiveness, and interaction satisfaction of the user-submitted evaluation. The other is the feedback evaluation submitted by the security domain based on the frequency of user access and the importance of accessing resources. The proposed evaluation method can be evaluated from both the user and the security domain, which improves the accuracy of the evaluation results.

The remainder of this paper is organized as follows. Related work is discussed in Section 2. In Section 3, the evaluation model based on cross-domain access is described. In Section 4, the evaluation principle of cross-domain access evaluation model is introduced. Simulation experiments and results analysis are presented in Section 5. Finally, this paper is concluded in Section 6.

## 2. Related Work

At present, many scholars have researched the risk of interaction behaviour. According to different mathematical theories, considering the different characteristics of interaction behaviour, a series of classic trust-based and risk-based security assessment models have been proposed.

The trust-based security evaluation model mainly evaluates the security of the model based on the user's trust credentials. Most trust evaluation methods only focus on the trust calculation process by using mathematical analysis [4]. Shaikh et al. [5] proposed the concept of trust security. It is pointed out that the trust value of cloud providers is composed of static trust based on security parameters and dynamic trust based on user feedback. However, the parameters to be evaluated need to be different according to the type of service. Ye et al. [6] proposed an effective wireless network dynamic trust evaluation model (DTEM). The DTEM model achieves accurate and efficient trust evaluation by dynamically adjusting the weights of direct trust and indirect trust. However, indirect trust is recommended by trusted recommendations from third parties. This method has certain errors. Zhang et al. [7] proposed a trust-based access control mechanism, which can respond to the malicious entity's access behaviour. In order to solve the problem of node trust evaluation energy consumption and the subjectivity and objectivity of trust, Liu et al. [8] combined periodic event detection with trigger detection to propose a low energy consumption trust evaluation model based on node behaviour detection. The proposed model can quickly avoid malicious nodes and reduce energy consumption in the process of trust calculation. Song et al. [9, 10] proposed a multifactor based dynamic trust evaluation method. In the context of Huffing's probability inequality, the trust of nodes is measured by dynamic combination. Moreover, the classification criteria and dynamic weight allocation involved depend on the interaction time between nodes. Feng et al. [11] proposed a reliable Bayesian-based trust management scheme (BTMS), which consists of direct and indirect trust. Direct trust is calculated using an improved Bayesian equation with a penalty factor and is updated using a sliding window with an adaptive forgetting factor. But the indirect trust calculation is called from a third party. Manuel introduced a trust model based on the credentials of cloud resource providers [12]. The trust value is calculated based on four credential attributes such as availability, reliability, turnaround efficiency, and data integrity. However, this method does not consider the feedback information submitted with cloud users and only relies on the quantitative analysis of QoS monitoring, which reduces the authenticity of the evaluation results. Shin [13] proposed a service quality evaluation model based on the mobile cloud service environment. Cloud service quality evaluation is mainly performed from four aspects: functionality, reliability, usability, and efficiency. However, the quality indicators in the model are measured quantitatively on the system side, which lacks the flexibility of evaluation. It can be seen that the model based on trust evaluation mainly evaluates the credibility of the service quality of various services in the cloud computing environment.

In order to further adapt to the cloud environment, scholars began to apply the idea of risk management control model in economics to the evaluation model. The risk-based assessment model mainly evaluates cross-domain interactive behaviour. Risk evaluation is the most basic information for risk management and an important credential for system analysis. Bouchami et al. [14] proposed quantifying the user's historical behaviour information and system security status into risk assessment indicators and then calculating the risk value of the current interaction, but the study did not give specific implementation plans. Wang and Chen [15] used the method of defining risk levels to observe whether there is interaction risk between network nodes and then evaluated the risk of dynamic information according to the discrete static evaluation model. However, this evaluation method lacks the risk of considering human factors. Zhang and Li et al. [16] proposed a risk assessment method for risk assessment problems with multiple associated risks. However, when setting the risk correlation matrix, the weight of the risk factor is determined by the expert, leading to a certain error in the evaluation results. Sendi and Cheriet [17] proposed a framework for evaluating the security risks of cloud computing platforms. By adopting iterative and incremental methods, both cloud customers and cloud service providers can submit an evaluation value to reduce risk and achieve an acceptable level of security. Santos et al. [3] proposed a risk access control model based on cloud computing environment. This model develops a scalable risk assessment framework for implementing XACML-extended risk strategies. Wang and Fan [18] proposed a dynamic Bayesian network model based on the risk assessment process. This model calculates the risk probability of interaction based on Bayesian theory and inference process by analyzing the information system. Assessors can take measures to reduce the probability of risk occurrence, thereby verifying the accuracy of the dynamic evaluation model. However, the parameters in this model are specified by experts, and the influence of subjective factors is relatively large.

In a multidomain network environment, the behaviour of cross-domain interaction has become a regular operation. However, due to the uncertainty of cross-domain interaction behaviour and the difference in network service quality, security issues have become more serious. Therefore, in order to avoid high-risk interactions, it is very important to perform risk evaluation on the behaviour of multidomain interactions. At present, researchers have built a multidomain interaction trust evaluation model by constructing the Bayesian equation. However, most of the research methods only rely on the results of multidomain interactions and the credibility of the evaluator, without considering the dynamics of interaction behaviour and the network environment of the security domain. Therefore, this paper establishes a risk evaluation model based on interdomain interactions in a multidomain interaction network scenario. This model is based on the Bayesian equation and proposes an equation for risk evaluation. By analyzing the process of user cross-domain interaction, we found the risk factor of security domain interaction based on the risk factor of user interaction. Compared with other evaluation models, the accuracy of evaluation results is improved.

## 3. Description of the Evaluation Model

At present, the access technology adopted in a multidomain environment is a cross-domain access control model based on trust interaction under the condition of Role-Based Access Control (RBAC) [19]. This article also conducts a risk evaluation of the behaviour of cross-domain interactions based on trust interactions. The traditional cross-domain access control model decides whether to agree to the user's interaction request based on the user's credibility. But it ignores the user's risk evaluation in the interaction process. Therefore, in order to make the evaluation model more objective and authentic, we established a cross-domain access evaluation model (RP-ECDM) based on the risk factors found. From [13–16], we can know that as long as cross-domain interactions occur, there will be certain risks, and these risks are mainly composed of the requester and the requested party. The research background of this article is as follows: under the condition that the user submits the request interaction to the security domain, the risk of this interaction behaviour is evaluated. Therefore, this paper mainly conducts risk evaluation from the user side and the security domain, as shown in Figure 1. In a cloud computing multidomain environment, due to the sharing of resources, cloud users need to perform cross-domain interaction operations. Then, users are provided with dynamic access policies based on cross-domain access rules. After the user's cross-domain access is completed, the evaluations submitted by the user and the security domain are collected to calculate the risk value in the cross-domain interaction. Among them, the factors that affect user submission of feedback values include user credibility, user activity, and interaction satisfaction. The factors that affect the feedback evaluation of security domains are mainly the value of resources, the length of user interaction, and the ability of identifying malicious users.

Different from traditional evaluation models, the evaluation model proposed in this paper integrates the feedback evaluation of the user and the security domain, so that the evaluation model can be more convincing. We refer to [20] and give relevant definitions of the cross-domain access evaluation model (RP-ECDM).

*Definition 1.* User package ($U\_B$): this represents a packet carried by a user requesting cross-domain access, mainly includeing user credibility ($T\_U$), access time ($V\_T$), access frequency ($V\_AL$), and interaction satisfaction ($V\_O$).

*Definition 2.* Security domain information flow ($D\_S$): this represents a collection of security realms accessible to users.

*Definition 3.* Accessed resource object ($V\_R$): this represents the resource that the request interacts with. When users access resources, the corresponding values of different resources are also different, and risk levels are classified according to resources of different values. With reference to the method proposed by Guo [21], the risk value of the resource is taken as a discrete value, and the measurement of the value of the resource is based on the points system. The value set of the specified integral value is $C_1$, $C_1 = \{W_1, W_2, \ldots, W_m\}$, where $W_k$ ($k = 1, 2, \ldots, m$) is the value of the corresponding discrete integral set. In this paper, the set of risk levels corresponding to the value of resources is defined as $RF$, $RF = \{r_1, r_2, \ldots, r_m\}$, and the risk factor coefficient $W_k$ corresponding to each integral value $r_k$ is

$$r_k = \frac{W_k - \min W_k}{\max W_k - \min W_k}. \tag{1}$$

*Definition 4.* RP-ECDM model containing risk five-tuple information: $fm = \{u, d, Vt, Vh, E\}$. Among them, $u$ represents the user requesting access; $d$ represents the security domain of the requested access; $Vt$ represents the time when the user requested the access; $Vh$ represents the historical interaction information of the user; it includes user credibility, the frequency of the user-submitted evaluations, and user interaction time; $E$ indicates the satisfaction of users submitting this interaction.

*Definition 5.* $\cup_{k=1}^{n} T_k[0, +\infty)$: this is a collection of time intervals representing user cross-domain interactions.

*Definition 6.* Risk assessment level: this evaluates the risk level of cross-domain access interactions. The higher the risk level is, the less secure the cross-domain access control model is. $FT$ is the set of risk levels, $FT = \{Ft_1, Ft_2, ..., Ft_n\}$.

*Definition 7.* Mapping structure between user and security domain $ud$: suppose there are $x$ users: $u_1$, $u_2$, ..., $u_i$, ..., $u_x$. There are $y$ security domains: $d_1$, $d_2$, ... $d_j$, ..., $d_y$. It is assumed here that the user does not participate in the mapping of the ontology security domain. We borrow the idea of the role mapping matrix in [22] and use the matrix $ud_{x \times y}$ to represent the mapping relationship between users and security

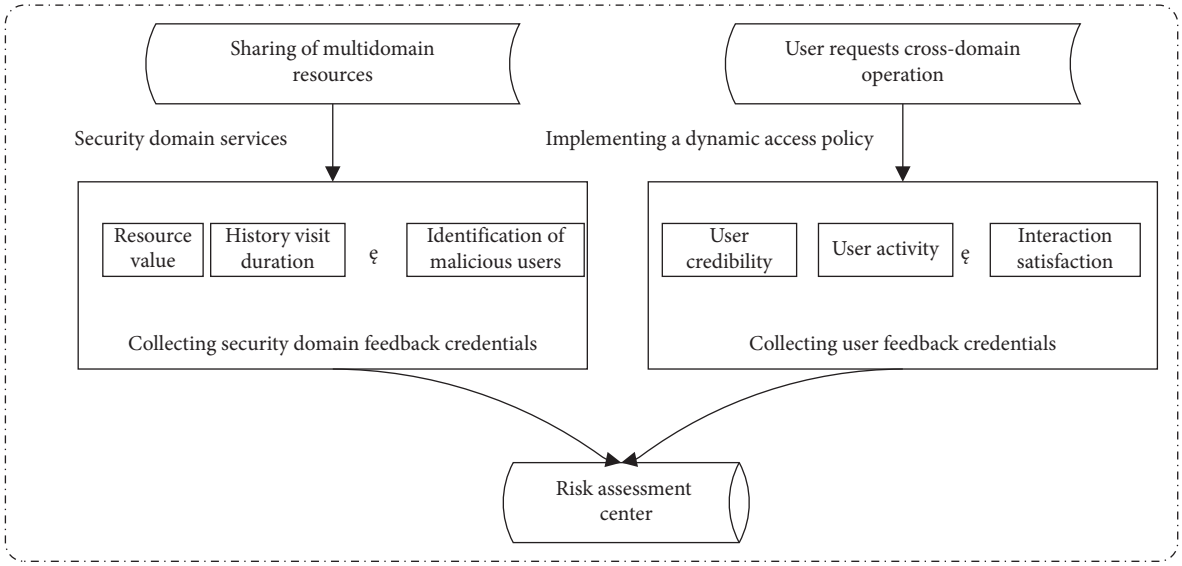


Figure 1: RP-ECDM evaluation model.

domains. The row of the $ud$ matrix represents the security domain, and the column represents the user. When $ud_{ij} = 1$, it indicates that the user $u_i$ requests access to the security domain $d_j$.

The main parameters and descriptions involved in the above are shown in Table 1.

## 4. Evaluation Principles of Cross-Domain Access Evaluation Model

This paper focuses on the risk of cross-domain access interactions, so cross-domain access rules are not described in detail here. The network scenario we simulated is based on the user's request for cross-domain interaction to complete the risk evaluation of cross-domain interaction behaviour. However, regarding the uncertainty of user interaction behaviour and the difference in network service quality, it is difficult to accurately evaluate the risk of cross-domain interaction. From Figure 1 in Section 3, we can see that we attribute the factors that affect interaction risks to the risks generated by users and the risks generated by security domains. Therefore, we evaluate the risk level of cross-domain interactions based on the collected risk factors, as shown in Figure 2. The following sections describe these risk attributes in detail.

*4.1. Assessing Interaction Risks.* Because the users have some malicious evaluations in cross-domain interactions, this paper uses the method of regression analysis in mathematical models to reasonably screen and analyze submitted evaluations. At the same time, the threshold for the number of user-submitted evaluations is set to $\tau$. If the number of user-submitted evaluations exceeds $\tau$ within $\Delta T$ time, it indicates that the user is at risk of malicious evaluation, and the user interaction request is frozen for a certain period of time. This also provides a guarantee for the RP-ECDM evaluation model and avoids some unreliable interaction requests.

Table 1: Main parameters and descriptions.

| Parameter | Description |
|---|---|
| $\theta_e$ $(u)$ | Multidomain interaction results submitted by users |
| $AL$ $(u)$ | Activity of user submitting multidomain interaction results |
| $G$ $(k)$ | User credibility decay function |
| $VT$ $(u)$ | Time of user cross-domain interaction |
| $\alpha$ $(u)$ | Credibility of user submission evaluation |
| $\Delta T$ | Time windows for cross-domain interactions |
| $e_k$ | Collection of user-submitted evaluation |
| T | Threshold of user activity within a specified time |
| $t_s$ | Time the user started the cross-domain interaction |
| $t_e$ | Time the user ended the cross-domain interaction |

Assume that each time user $u$ interacts with resources in security domain $d$ randomly (because this article mainly evaluates the risk of users' cross-domain access, it is specified here that user $u$ does not belong to the security domain $d$). After user $u$ completes interaction with security domain $d$, record the user interaction information.

(a) User feedback interaction result $\theta_e$ $(u)$: $\theta_e$ $(u)$ represents the user's evaluation of this cross-domain interactive service.

(b) Activity of user-submitted evaluation $AL$ $(u)$: the activity reflects whether some users give malicious evaluation in order to obtain higher authority operations.

(c) Time-effectiveness of user-submitted evaluation $g$ $(k)$: time-effectiveness reflects the dynamic nature of risk assessment. That is, the risk assessment value submitted by the user changes continuously with the different results of each interaction, which can improve the accuracy of the user submission evaluation to a certain extent.

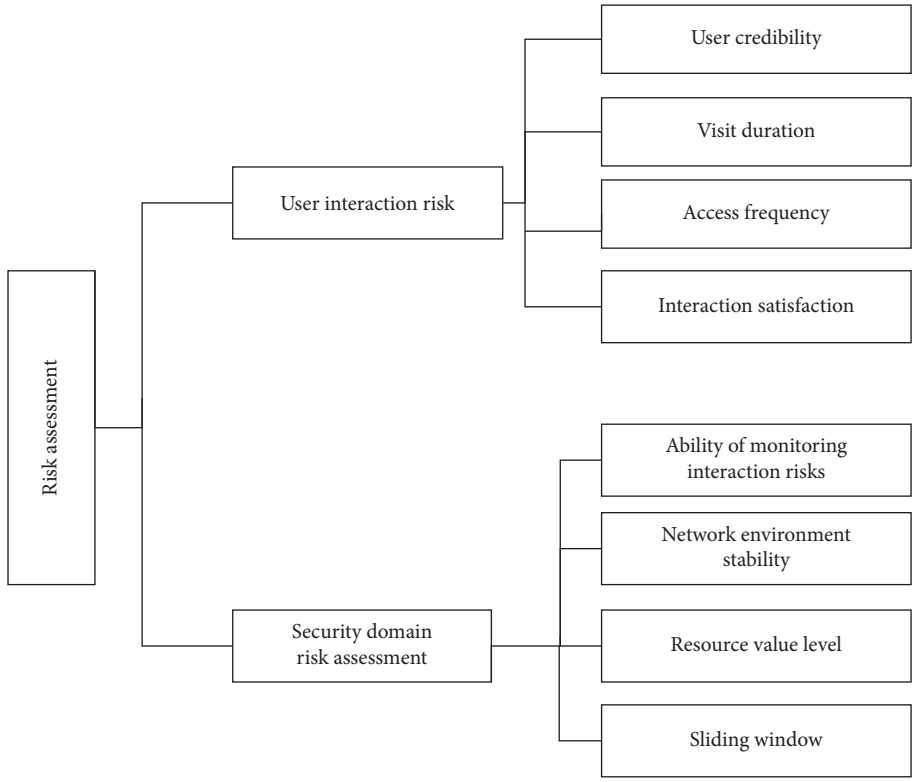


Figure 2: Network security risk assessment system.

(d) User interaction time $VT(u)$: this indicates that the longer the user interacts, the greater the risk is.

(e) The user's credibility $\alpha(u)$: the user's credibility means that the more reliable the evaluation submitted by the user with, the higher the credibility value.

This paper uses [23] to calculate the direct trust method to evaluate the risk of user interaction. We assume that there are $m$ interactions between the user and the security domain. The number of successful interactions between user $u$ and security domain $d$ is $S_{ud}$, and the number of user $u$ failures with security domain $d$ is $F_{ud}$. It can be known from [23] that the risk probability $\hat{\theta}_e$ of the interaction between the user and the security domain conforms to the Beta distribution in the probability distribution. The calculation method is as follows:

$$\begin{aligned}\mathrm{Beta}\left(\theta|S_{ud},F_{ud}\right) &= \frac{\Gamma\left(S_{ud}+F_{ud}+2\right)}{\Gamma\left(S_{ud}+1\right)\Gamma\left(F_{ud}+1\right)},\\ \hat{\theta}_e &= E\left(\mathrm{Beta}\left(\theta|S_{ud}+1,F_{ud}+1\right)\right)\\ &= \frac{F_{ud}+1}{S_{ud}+1+F_{ud}+1},\end{aligned} \tag{2}$$

where $0<\theta<1$ and $S_{ud}, F_{ud}>0$.

In practical applications, we need to calculate the credibility of formula 2 by interval estimation. Therefore, we use $(\hat{\theta}_e-\varepsilon, \hat{\theta}_e+\varepsilon)$to represent the confidence level $\varphi$ of $\theta_e$, $\varepsilon$represents the fault tolerance rate, and the calculation method of $\varphi$ is as follows:

$$\begin{aligned}\varphi &= P\left(\hat{\theta}_e-\varepsilon<\theta_e<\hat{\theta}_e+\varepsilon\right)\\ &= \frac{\int_{\hat{\theta}_e-\varepsilon}^{\hat{\theta}_e+\varepsilon}\theta^{S_{ud}-1}(1-\theta)^{F_{ud}-1}\mathrm{d}\theta}{\int_0^1\theta^{S_{ud}-1}(1-\theta)^{F_{ud}-1}\mathrm{d}\theta}\\ &= \frac{\Gamma\left(S_{ud}\right)\Gamma\left(F_{ud}\right)}{\Gamma\left(S_{ud}+F_{ud}\right)}\int_{\hat{\theta}_e-\varepsilon}^{\hat{\theta}_e+\varepsilon}\theta^{S_{ud}-1}(1-\theta)^{F_{ud}-1}\mathrm{d}\theta.\end{aligned} \tag{3}$$

The frequency of user-submitted feedback is denoted by $AL$. In order to prevent some users from submitting the evaluation value $UFE(u)$ too frequently within a certain time, it affects the authenticity of the submitted evaluation. Therefore, the credentials of the user's interaction are collected. That is, look at the user's historical access record and observe the frequency of the user in submitting evaluation within a period of $\Delta T$. Determine whether users frequently submit evaluation in their recent interaction records. Check the user's historical interaction record to determine the user's activity in submitting evaluations within $\Delta T$ time. If the user is highly active in submitting a review within the $\Delta T$, time, the user is at risk of hypocritical interaction. In this paper, the frequency of user interaction is calculated as follows:

$$AL = \frac{\mathrm{count}\left(UFE(u)\right)}{\Delta T}. \tag{4}$$

The time-effectiveness of user-submitted feedback is denoted by *UE*. In order to conveniently record the estimated risk value of the interaction between user $u$ and the security domain, the type of data table used in this paper is user × risk value for each interaction and is represented by the set $u = (u_{i1}, u_{i2}, u_{ik}, ..., u_{ij})$. When $i = 1, 2, \ldots, n$, it means that there are $n$ users; when $j = 1, 2, \ldots, m$, it means that the user has performed $m$ interactions. That is, each time the user provides a feedback value $u_{ij}$, the evaluation data table *UE* formed can be written as an $n \times m$ matrix, as shown in the following formula:

$$UE = \left(u_{ij}\right)_{n\times m} = \begin{bmatrix} e_1^{t_1} \\ \vdots \\ e_n^{t_k} \end{bmatrix}. \tag{5}$$

Among them, $e_k = (u_{i1}, u_{i2}, ..., u_{im})^T$, $t_k \in T$, and $T$ is the current time window, which represents the set of user-submitted evaluations in the time from $t_1$ to $t_k$. If the set time window is larger, it means that the proportion of historical evaluation is larger. In order to make the calculation result more reliable, it is necessary to consider the time-effectiveness of submitting the evaluation. It means that the users submit more evaluation, and it contains more information. At the same time, in order to improve the accuracy of evaluating the interaction risk, we added a credibility decay function when calculating the interaction evaluation submitted by the user. The meaning of $g(k)$ is that the reference value of the latest submission of the evaluation is larger, and the reference value of the previous submission of the evaluation is getting smaller and smaller. The calculation method is as follows:

$$g(k) = \begin{cases} 1 - \dfrac{1}{2m}, & k = m, \\ g(k-1) - \dfrac{1}{m}, & 1 \le k < m, \end{cases} \tag{6}$$

where $k$ represents the feedback evaluation value submitted by the user for $k$-th time.

Then, check the user's historical access record and calculate the credibility $\alpha(u)$ of the user's submitted evaluation:

$$\alpha(u) = \frac{1}{m}\sum_{k=1}^{m}\left(1 - \theta_e(u) \cdot g(k)\right). \tag{7}$$

In order to more accurately assess the risk of the user's interaction with the security domain, when collecting the interaction credentials between the user and the security domain, a data standardization process needs to be performed on the sample data. Therefore, we refer to the regression analysis method in the mathematical model to fit the sample data in this paper. We calculate the risk based on the interaction, establish the evaluation model equation based on the interaction risk, and calculate the feedback value *ufe* submitted by the user, as shown in the following formula:

$$ufe = \frac{1}{m}\sum_{k=1}^{m}\left(\theta_e(u) \times AL(u) \times VT(u) \times \alpha(u)\right), \tag{8}$$

where $VT(u)$ represents the time of user interaction: $VT = t_e - t_s$. Here, $t_e$ indicates the end time of the cross-domain interaction, and $t_s$ indicates the start time of the cross-domain interaction. Among the test samples, the variance matrix $S$ of the evaluation submitted by the user is as follows:

$$S = \left(s_{ij}\right)_{n\times m} = \frac{1}{n-1}\sum_{k=1}^{n}\left(e_k - UFE\right)\left(e_k - UFE\right)^T. \tag{9}$$

Among them,

$$s_{ij} = \frac{1}{n-1}\sum_{k=1}^{n}\left(u_{ki} - \frac{e_i}{n}\right)\left(u_{kj} - \frac{UE}{n}\right). \tag{10}$$

Therefore, the value of the *UFE* submitted by the user is as follows:

$$UFE = ufe - |S|. \tag{11}$$

Compared with other evaluation models, the evaluation method proposed in this paper not only collects the credentials of user interaction, but also collects the credentials of security domain interaction. There are two main factors that affect the security domain submission evaluation. One of them is the average length of each user's cross-domain access. If the length of each user's interaction takes a long time, it means that the user's interaction behaviour has caused certain risks to the security domain. Another factor is the stability of the quality of service *Cu* provided by the network environment in the security domain as shown in the following formula:

$$Cu = \frac{1}{m}\sum_{k=1}^{m} u_k\left(t_e - t_s\right) \cdot r_k \tag{12}$$

where $r_k$ is the resource value risk, $t_e$ indicates the end time of the multidomain interaction, and $t_s$ indicates the start time of the multidomain interaction. The above formula indicates that the longer the access time of a high-value resource, the greater the threat to the security of the resource.

*4.2. Comprehensive Evaluation Value.* It can be known from Section 4.1 that the risk value of cross-domain interaction is composed of evaluations submitted by users and security domains, and the risk evaluation equation is obtained as follows:

$$TEC = \frac{1}{\gamma}\left(UFE + Cu\right). \tag{13}$$

Among them, $\gamma$ represents a normalization function to ensure that the value of TEC is between [0, 1].

The value of UFE, Cu, and TEC can be obtained in Algorithm 1, the core algorithm for assessing risk in this article.

**Input** *V*_User, *V_D*, *V*_Resource
**Output** UFE, Cu, TEC
**Begin**
(1) Initialize RP_ECDM = (*V*_User, *V_D*, *V*_Resource, *V*_Time)/*Initialize the cross-domain access control model*/
(2) Construct *u*, *d*/ ∗ Construct random interaction information between user and security domain*/
(3) Construct a matrix of interaction information between users and security domains
(4) Calculate the user and security domain ratings based on the interactive information, and see (9) and (10) for details.
(5) Finally, the comprehensive risk value of the RP-ECDM model is obtained
(6) Back *UFE*, *Cu*, TEC
**End**

Algorithm 1: Comprehensive algorithms for risk assessment.

## 5. Simulation Results and Analysis

The experiment mainly uses MATLAB experimental tools to complete the evaluation of the test model. The experiment is tested from two aspects of the evaluation submitted by the user and the security domain. The main parameter settings of the experiment are shown in Table 2, where *user* represents the number of users requesting cross-domain interaction, *D_Num* represents the number of security domains in a simulated cloud environment, *DA_Num* indicates the number of user cross-domain requests, *D_S* represents the number of resources in the security domain, *V_Time* indicates the length of the user's access, and the unit is calculated in minutes.

Table 2: Initialization parameters.

| Parameter | Parameter value |
|---|---|
| *User* | 10~300 |
| *D_Num* | 50 |
| *DA_Num* | 10~300 |
| *D_S* | 10~100 |
| *V_Time* | 1~90 |

*5.1. Explicit Euler Numerical Results.* In this section, the experiment mainly performs the following tasks.

(1) Testing the impact of user credibility on interaction behaviour is mainly illustrated by two sets of experimental data. The experimental results are shown in Figures 3 and 4.

Figure 3 shows the influence of test user credibility $\alpha$ ($u$) on the comprehensive evaluation of TEC values. When researching the risk of cross-domain interactions, we found that if the user's credibility is not considered, there may be some malicious users who provide some false evaluations. Therefore, this paper finds the influence factors of user credibility in cross-domain interaction. In this way, we can judge the authenticity of the submitted evaluation according to the user's credibility. We selected two sets of data for simulation experiments, and the experimental results are shown in the figure. The experimental results in Figure 3 show that when evaluating the risk of cross-domain interactions, the value of the comprehensive evaluation value TEC is low after adding credentials for user credibility. If the user's trusted value is not considered, some users with low trust value will submit some false evaluations. As a result, the RP-ECDM evaluation model cannot accurately evaluate the security of cross-domain interactions.

Figure 4 shows testing the user $\alpha$ ($u$) with three different trust values for 100 interactions and observing the changes in the comprehensive assessment of the risk value TEC. The purpose of this test is to determine the impact of users with different trust values on cross-domain interactions. In order to improve the accuracy of the evaluation results, we judge the credibility of the submitted evaluation according to the user's credibility value. That is, the evaluation submitted by a user with a high trust value is relatively real. If the user's trustworthiness is low, then we think that the reference value of the submitted evaluation is relatively low. In order to better observe the experimental results, we selected three groups of users with different credible values for simulation experiments. From the experimental results, after 100 user interactions with high trust values, the risk value TEC of cross-domain interaction is higher. This is because, after obtaining a user with a high trust value, it also has higher operation permissions. If these users interact illegally, it is more destructive than users with low trust.

(2) This group of experiments mainly tests the impact of user activity and resource value levels on the evaluation results. The experimental results are shown in Figures 5 and 6.

Figure 5 tests the impact of the frequency $AL$ ($u$) of user submissions on the comprehensive risk value TEC. We found in previous research that, in the early stage of cross-domain interactions, there were incidents of malicious attacks after multiple hypocritical interactions by some users. Therefore, when we evaluate interaction risk, we find risk factors for user activity. This article collects feedback information submitted by users, observes the number of times users submit evaluations within $\Delta T$ time, and determines whether users frequently submit evaluations. If a user submits evaluations too frequently, then we consider that

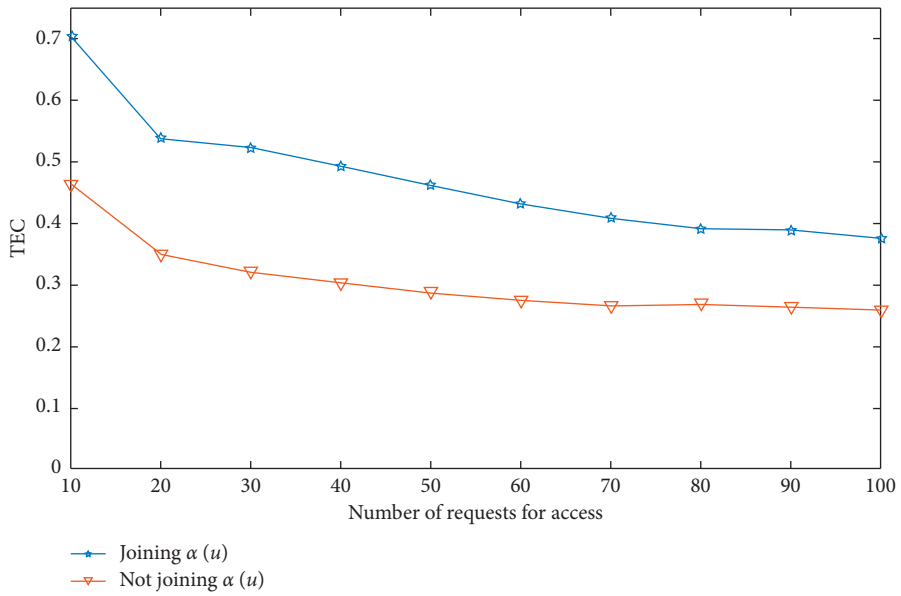


Figure 3: Impact of user trusted values.

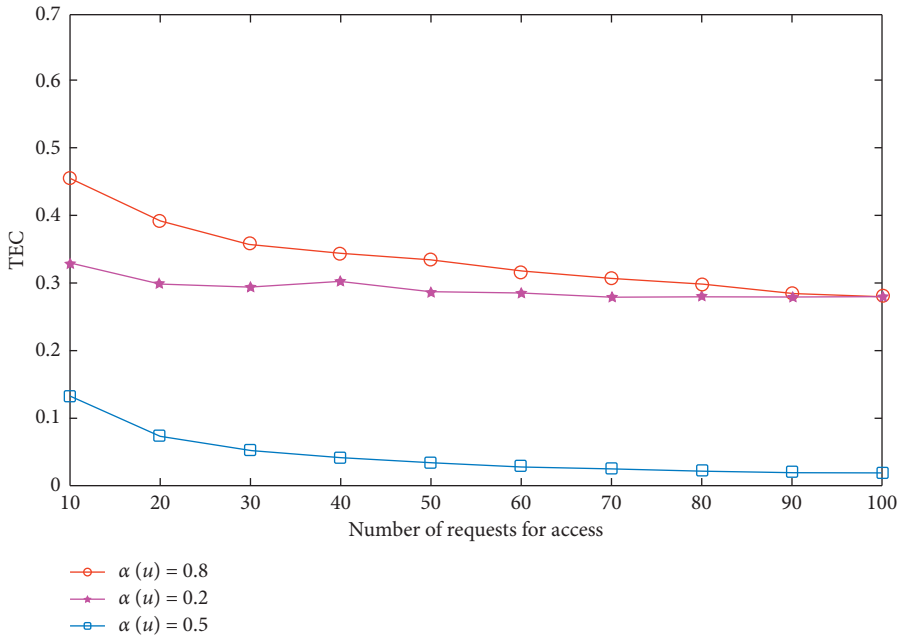


Figure 4: The impact of different trust value users.

user is at risk of malicious interaction. Therefore, we tested the impact of user activity on the evaluation results in the experiment. The experimental results are shown in Figure 5. It is known from the experimental results that, after the risk factor of user activity is added, the risk of cross-domain user interaction is low. Experiments show that our method can effectively circumvent some hypocritical users and improve the security of cross-domain interactions.

Figure 6 shows testing users' malicious access to resources of different values and observing the changes in the comprehensive assessment of TEC risk values. Because the value of each resource is different, the risk of interaction is also different. Therefore, compared with other evaluation models, we consider the factor of value resource level. In the experiment, we tested the user to interact with three different levels of resources. The experimental results are shown in Figure 4. It can be known from the experimental results that when a user accesses a high-value resource, the higher the comprehensive risk assessment TEC, the lower the value of the resource and the lower the risk value. This is because the security of high-value resources is higher. After multiple malicious interactions by users, the security of resources is

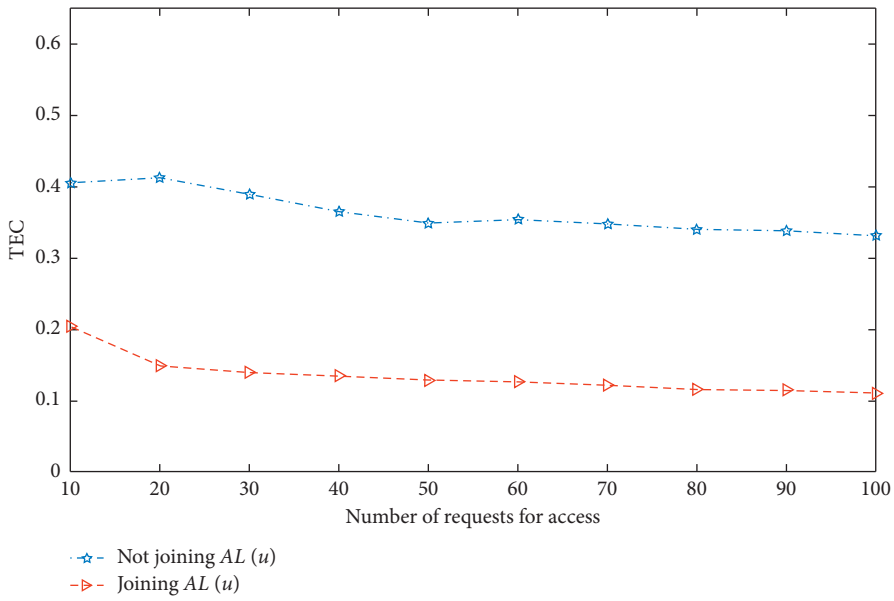


Figure 5: Impact of user activity.

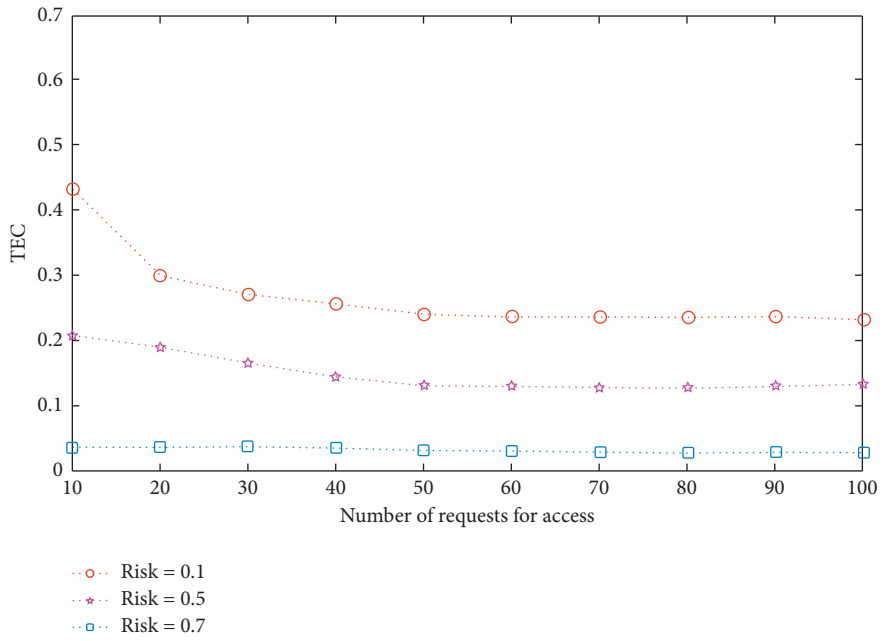


Figure 6: Impact of different value resources.

greatly reduced. It is more likely to cause more damage than lower value resources.

*5.2. Assessing the Performance of Security Domains.* In this section, the experiment mainly performs the following tasks.

(1) The accuracy of the evaluation of the security domain and the RP-ECDM evaluation model was tested. The experimental results are shown in Figures 7 and 8.

Figure 7 mainly tests the impact of the evaluation submitted by $Cu$ ($d$) in the security domain on the RP-ECDM evaluation model. When studying cross-domain interaction behaviours, we found that, in addition to the interaction risks brought by user requesters, the quality of network services in the security domain is also a factor that affects interaction risks. Therefore, compared to other evaluation models, we collect not only the interactive evaluations submitted by users, but also the evaluation of service quality in the security domain. This is also an important feature of our evaluation method. The evaluation provided by the security domain is mainly based on the evaluation of the network service environment, service quality, and user interaction. The

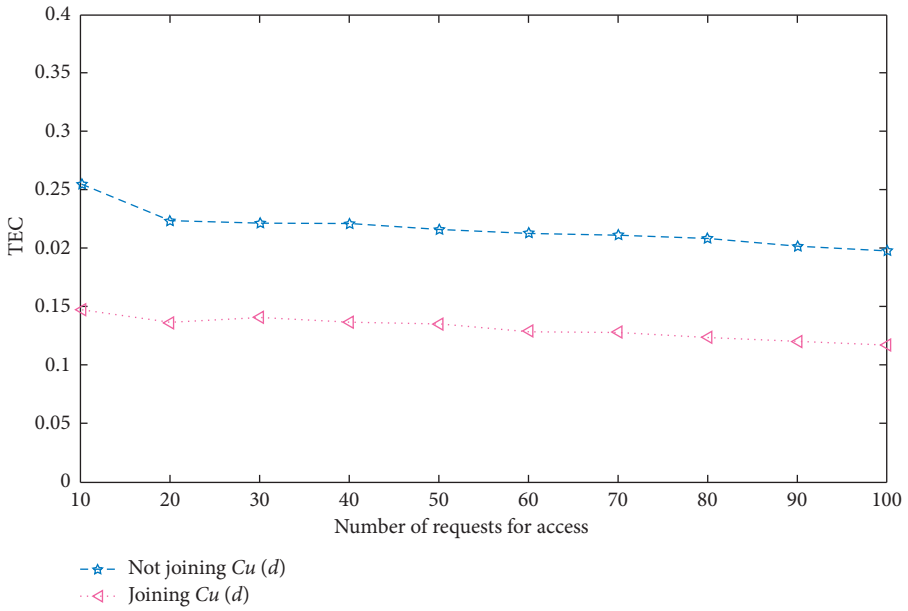


Figure 7: Impact of security domain assessment.

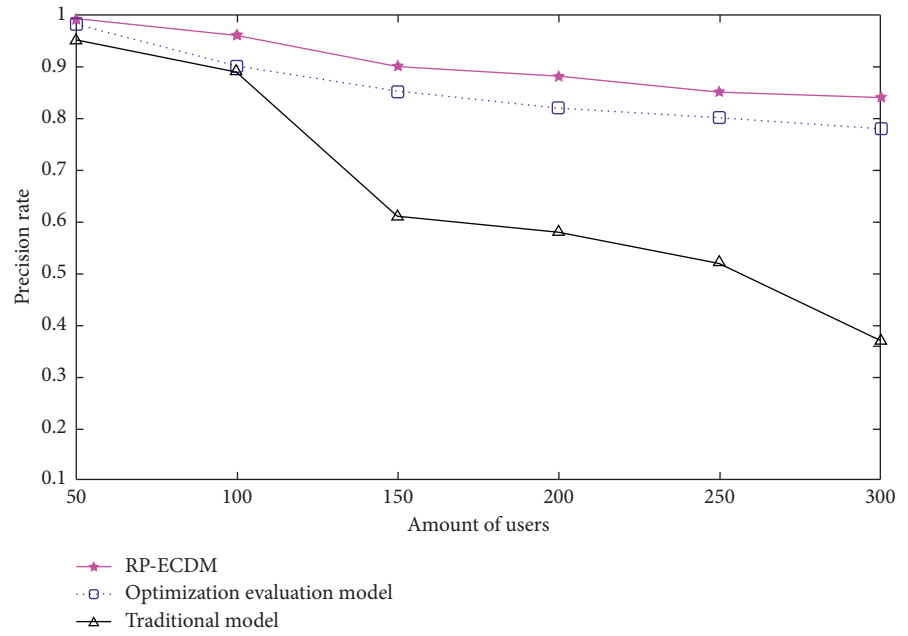


Figure 8: Precision rate.

purpose of this is to avoid the problem of false evaluations provided unilaterally by the user, so that the risk of cross-domain interactions cannot be accurately evaluate. The experimental results in Figure 7 show that if the evaluation provided by the security domain $Cu$ $(d)$ is not considered in the evaluation model, the risk of cross-domain interaction is also higher.

Figure 8 tests accuracy. Accuracy indicates the ratio between the actual malicious behaviour and the high-risk interaction behaviour detected by the RP-ECDM evaluation model. The higher the accuracy rate is, the more effective the evaluation method is. This is also an important indicator for detecting and evaluating whether the model has efficient performance. In order to further verify the effectiveness of the RP-ECDM evaluation model, the experiments in this group are mainly compared with the classification optimization model by Xi [24] (referred to here as optimization evaluation model) and traditional evaluation model proposed. The experimental results shown in Figure 8 show that, with the increase

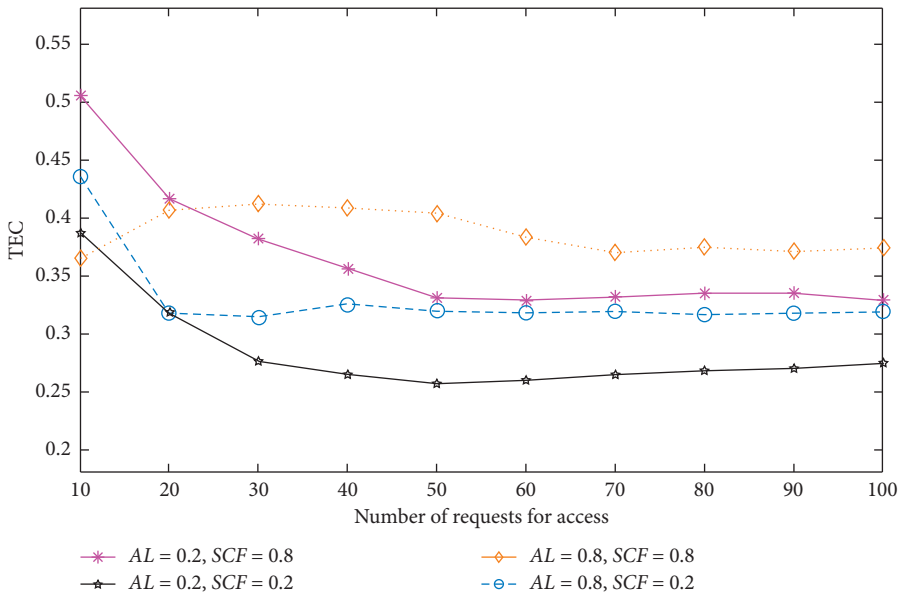


Figure 9: Impact of the network environment.

of the number of user interactions, the accuracy of the RP-ECDM evaluation model, optimization evaluation model, and traditional evaluation model are gradually decreasing. However, the precision of the RP-ECDM evaluation model proposed in this paper has always been better than the other two models, and the downward trend has gradually stabilized. This shows that the performance of the RP-ECDM evaluation model is better.

(2) Test the performance of the RP-ECDM evaluation model in different network environments. It consists of the following two indicators:

(a) The frequency $AL$ of the feedback provided by the user ($0 \le AL \le 1$): it indicates the busyness of resource occupation in a multidomain cloud computing environment. The larger the value of $AL$, the busier the network.

(b) Quality of Service $SCF$ ($0 \le SCF \le 1$): it indicates the average access time of all users in the security domain. The larger the $SCF$ value, the longer the average user access time, indicating that the service quality provided by the security domain is more unstable. And stipulate the calculation method as

$$SCF = \frac{\sum_{k=1}^{m} Cu_k}{m}. \tag{14}$$

Compared with other evaluation models, we also consider the impact of the network environment in the security domain on the evaluation results, as shown in Figure 9. We change in the evaluation value TEC for four different network environments that $AL$ is not busy and $SCF$ is unstable, $AL$ is not busy and $SCF$ is stable, $AL$ busy and $SCF$ unstable, and $AL$ busy and $SCF$ stable. The experimental results shown in Figure 9 show that when the security domain provides not busy and stable network environment, the risk value is lower, and, as the number of interactions increases, the TEC risk value fluctuations tend to stabilize. The risk value is higher when providing a busy and unstable network environment. Experiments show that the evaluation results are more accurate under the stable and idle network environment. A good network environment is also a factor affecting the RP-ECDM evaluation model.

## 6. Conclusion

As the demand for cross-domain interactions continues to increase, researchers have proposed a series of cross-domain access control models, but they have ignored the issue of risk in the interaction process. This paper analyzes and studies the trust-based cross-domain access control model and risk-based assessment model. And we proposed a risk situation assessment model based on interdomain interactions. Compared with other trusted evaluation models, this model has the service quality evaluation submitted by the security domain in addition to the evaluation submitted by the user. From the experimental results, we know that our proposed method avoids malicious users from submitting false evaluations after obtaining high trust values and improves the reliability of the evaluation results. However, the evaluation method proposed in this paper needs to improve the accuracy of the evaluation results when the network is busy. Therefore, our next work will focus on how to further improve the accuracy of the evaluation results in a busy network environment.

## Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

## Conflicts of Interest

The authors declare that they have no conflicts of interest.

## Acknowledgments

This study was supported by the National Natural Science Foundation of China under Grant no. 61562006 and in part by the Natural Science Foundation of Guangxi Province under Grant no. 2016GXNSFBA380181.

## References

[1] H. Zhang, J. Wang, and J. Chang, "A multi-level security access control framework for cross-domain networks," in *Proceedings of the 2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC)*, no. 2, pp. 316–319, Guangzhou, China, 2017.

[2] S. Li, I. Doh, and K. Chae, "Non-redundant indirect trust search algorithm based on a cross-domain trust model in content delivery network," in *Proceedings of the 2017 19th International Conference on Advanced Communications Technology*, IEEE, Pyeongchang, South Korea, pp. 72–77, 2017.

[3] D. R. D. Santos, R. Marinho, G. R. Schmitt et al., "A framework and risk assessment approaches for risk-based access control in the cloud," *Journal of Network and Computer Applications*, vol. 74, pp. 86–97, 2016.

[4] B. Zhao, J. He, N. Huang, Y. Zhang, S. Zhou, and J. Ji, "Designs and simulations of multi-factor in trust evaluation," *International Journal of Database Theory and Application*, vol. 8, no. 1, pp. 235–244, 2015.

[5] G. X. Zhan, W. S. Shi, and J. Deng, "TARF: a trust-aware routing framework for wireless sensor networks," in *Proceedings of the 2010 Wireless Sensor Networks, 7th European Conference, EWSN 2010*, Coimbra, Portugal, February 2010.

[6] R. Shaikh and M. Sasikumar, "Trust model for measuring security strength of cloud computing service," *Procedia Computer Science*, vol. 45, pp. 380–389, 2015.

[7] Z. Ye, T. Wen, Z. Liu, X. Song, and C. Fu, "An efficient dynamic trust evaluation model for wireless sensor networks," *Journal of Sensors*, vol. 2017, pp. 1–16, 2017.

[8] Y. Zhang, J. He, B. Zhao, Z. Huang, and R. Liu, "Towards more pro-active access control in computer systems and networks," *Computers & Security*, vol. 49, pp. 132–146, 2015.

[9] Y. B. Liu, X. H. Gong, and Y. F. Feng, "Trust system based on node behaviour detection in Internet of Things," *Journal on Communications*, vol. 35, no. 5, pp. 8–15, 2014.

[10] J. Song, X. Li, J. Hu et al., "Dynamic trust evaluation of wireless sensor networks based on multi-factor," in *Proceedings of the 2015 IEEE Trustcom/BigDataSE/ISPA*, pp. 33–40, Helsinki, Finland, 2015.

[11] R. Feng, X. Han, Q. Liu et al., "A credible Bayesian-based trust management scheme for wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2015, pp. 1–9, 2015.

[12] P. Manuel, "A trust model of cloud computing based on quality of service," *Annals of Operations Research*, vol. 233, no. 1, pp. 1–12, 2013.

[13] Y. R. Shin and E. N. Huh, "mCSQAM: service quality assessment model in mobile cloud services environment," *Mobile Information Systems*, vol. 2016, Article ID 2517052, 9 pages, 2016.

[14] A. Bouchami, E. Goettelmann, O. Perrin et al., "Enhancing access-control with risk-metrics for collaboration on social cloud-platforms," in *Proceedings of the 2015//IEEE Trustcom/BigDataSE/ISPA*, pp. 864–871, Helsinki, Finalnd, August 2015.

[15] S. Q. Wang and H. Y. Chen, "Research on information security risk assessment based on discrete dynamic Bayesian network," *Applied Mechanics and Materials*, vol. 608-609, pp. 295–299, 2014.

[16] Z. Zhang, K. Li, and L. Zhang, "Research on a risk assessment method considering risk association," *Mathematical Problems in Engineering*, 2016.

[17] A. S. Sendi and M. Cheriet, "Cloud computing: a risk assessment model," in *Proceedings of the 2014 IEEE International Conference on Cloud Engineering (IC2E)*, IEEE, Boston, MA, USA, pp. 147–152, March 2014.

[18] J. Wang, K. F. Fan, W. Mo et al., "A method for information security risk assessment based on the dynamic Bayesian network," in *Proceedings of the 2016 International Conference on Networking & Network Applications*, pp. 279–283, Hakodate, Japan, 2016.

[19] F. Zhang, J. Chen, H. Zhou et al., "A dynamic access control model for spatial data," in *Proceedings of the 2017 International Conference on Computational Intelligence & Security*, no. 1, pp. 547–550, Hakodate City, Japan, 2017.

[20] G. Q. Zhou and Q. K. Zeng, "Trust evaluation model based on role separation," *Journal of Software*, vol. 23, no. 12, pp. 3187–3197, 2012.

[21] Y. F. Guo, T. Li, and Y. C. Guo, "Trust management model based on value-at-risk evaluation with changing time in P2P network," *Computer Application*, no. 9, pp. 235–238, 2012.

[22] F. Wang, H. H. Shen, and X. Zhou, "Cross-domain role mapping method based on IRBAC," *Computer Application*, vol. 30, no. S1, pp. 106–108, 2010.

[23] L. Wang, X. Li, X. Yan, S. Qing, and Y. Chen, "Service dynamic trust evaluation model based on Bayesian network in distributed computing environment," *International Journal of Security and its Applications*, vol. 9, no. 5, pp. 31–42, 2015.

[24] H. L. Xi and Y. H. Zhang, "Simulation of classification optimization model in malicious network software behaviour assessment," *Computer Simulation*, vol. 32, no. 10, pp. 467–470, 2015.