2019

Fuzzy-GRA trust model for cloud risk management

Abdul Razaque

Muder Almiani

Meer Jaro Khan

See next page for additional authors

Authors

Abdul Razaque, Muder Almiani, Meer Jaro Khan, Basel Magableh, Ayman Al-Dmour, and Amer Al-Rahayfeh

2019 Sixth International Conference on Software Defined Systems (SDS)

Fuzzy-GRA Trust Model for Cloud Risk Management

Abdul Razaque
Department of Computer Science
New York Institute of Technology
arazaque@nyit.edu

Muder Almiani
College of Information Technology
Al-Hussein Bin Talal University
Ma'an, Jordan
malmiani@my.bridgeport.edu

Meer Jaro Khan
Department of Computer Science
National University of Modern Language, Pakistan
meerjk@publicist.com

Basel Magableh
School of Computer Science,
Technological University
Dublin, Ireland
basel.magableh@dit.ie

Ayman Al-Dmour
Department of Computer Science
Applied Science University
Manama, Bahrain
Ayman70jo@yahoo.com

Amer Al-Rahayfeh
College of Information Technology
Al-Hussein Bin Talal University
Ma'an, Jordan
amer.a.al-rahayfeh@ahu.edu.jo

***Abstract* - Cloud computing is not adequately secure due to the currently used traditional trust methods such as global trust model and local trust model. These are prone to security vulnerabilities. This paper introduces a trust model based on the fuzzy mathematics and gray relational theory. Fuzzy mathematics and gray relational analysis (Fuzzy-GRA) aims to improve the poor dynamic adaptability of cloud computing. Fuzzy-GRA platform is used to test and validate the behavior of the model. Furthermore, our proposed model is compared to other known models. Based on the experimental results, we prove that our model has the edge over other existing models.**

Index Terms –cloud safety, trust model, fuzzy mathematics.

I. INTRODUCTION

With the development of computer technology, Cloud Computing has received considerable attention [1]. It leverages the transmission capabilities of the internet and moves the analysis and computational tasks from the original client to be executed on a remote server [2]. Due to this significant advantage, it is evident that cloud computing is the future of Information Technology (IT) [3]. However, its security vulnerabilities hinder its development and widespread adoption. With the development of distributed control networks, software changes from static to dynamic, users can access it at random [4,5]. These characteristics allow users to grasp more information, which leads to more security threats. The improvement to the safety of Cloud Computing has become a problem to be solved [6]. It is expected that more people will benefit from a "safer cloud," due to this the development of safer cloud security technology will have a significant impact [7]. This research aims to establish an effective mechanism based on fuzzy mathematics and gray relational theory for ensuring the security of the cloud platform.

In our study, we plan to analyze the risk that Cloud Computing faces and identify the issue of existing trust model (global trust model and local trust model). Those models have solved some problems, but they do not address poor dynamic adaptability and lack an effective evaluation model [8]. Our model uses a specific algorithm Fuzzy-GRA that helps improve dynamic behavior. Furthermore, we conduct several tests to determine the effectiveness of this model.

The model proposed in this paper, Fuzzy-GRA, utilizes the computing power and storage capacity of the cloud platform to let it obtain the user's behavior factors. It then calculates and then builds the trust level module, so that it can restrain the nodes. Then it evaluates the user's trust vector to restrict the user's rights and gives customers different operating authority, minimizing destructiveness.

This paper undertakes the following objectives:

i.We establish an effective mechanism based on fuzzy mathematics and gray relational theory.

ii.We propose definitions and algorithms to build a trust model.

iii.The mechanism will evaluate users' trust level and give them corresponding access rights to ensure cloud security.

We organize our paper as follows:

Section I: Highlight problem identification and significance. Section II: Discuss the existing approaches in the related work. Section III: Describe the proposed approach Fuzzy-GRA. Section IV: Implement the approach. Section V: Analysis of experimental results.Section VI: Give the project a conclusion.

II. PROBLEM IDENTIFICATION AND SIGNIFICANCE

978-1-7281-0722-6/19/$31.00 ©2019 IEEE

We analyze two typical models utilized to deal with trust mechanisms in the aspect of trust management in cloud computing. The global trust model analyzes all transaction feedbacks in the network and establishes unique confidence for each node [9]. The calculation is based on the weighted average method after the penalty mechanism is adopted. However, it does not consider the factors of ambiguity and uncertainty.

Another method is the local trust model. This method considers various elements, such as time factor and historical factor. It can respond well to strong dynamic situations [9]. The disadvantage present is that the model does not solve the problem of cooperative spoofing. This is because highly trusted nodes may also provide false information, and its recommended that trust is limited to adjacent nodes, which cannot calculate global trust.

Weak security, high cost, and poor dynamic adaptability are the common problems of the trust model under the current mechanism [10]. Therefore, cloud computing research has become a hot topic in academia. In traditional distributed networks, the basic concept of trust management is incomplete; thus system security decisions require a trusted third party to provide additional security information. In addition, the large-scale distributed network system has transformed from a single software application into a dynamic system. It changes to a system with several software collaboration services and the closed, mutual understanding between users, to the open, publicly accessible dynamic cooperative service model. Moreover, in an open distributed network environment, to obtain primary information, there must be a specific authority of the central node. If it is not present, the requestor may also be deceptive or even cause damage to the author. This can result in a dynamic trust model management issue which needs to be resolved.

III. RELATED WORK

Rigid authentication mechanisms, such as Public Key Infrastructures (PKIs) or Kerberos [11] are introduced to deal with the authorities in centralized systems. These mechanisms have allowed this model to be extended to distributed systems within a few closely collaborating domains or within a single administrative domain. This is because, in centralized systems, security is typically based on the authenticated identity of external parties. However, during recent years, computer science has moved from centralized systems to distributed computing. The rigid authentication mechanisms are unable to perform well in distributed computing.

In [12], the problem of modeling trust is illustrated. Social scientists consider unqualified trust values as not transferable, but a more pragmatic approach would conclude that qualified trust judgments are transferred as far as decisions are taken considering others' opinion. These are better than the ones made in isolation. In [13], the authors researched the problem of trust transferability in distributed environments.

PTM is a trust model proposed in [14]. It manages the dynamic trust mechanism. The calculation of trust is evaluated by the weighted average method after adopting the penalty mechanism, which is an excellent way to reflect the dynamic. The ambiguity of trust and uncertainty are, however, not considered.

Eigen trust, a global trust model, proposed in [15], implements trust propagation based on iterative trusts among nodes, thus calculating the global confidence for each node. [16] Has proposed a dynamic model based on a fuzzy-trust model. It establishes the trust reasoning rule of opportunity via fuzzy logic and proposes two input factors: transaction success rate and self-defense ability. It introduces the decision-making process. It did not consider the update of the trust value and based on fuzzy logic reasoning makes the system overhead relatively large.

In [17], the peer trust model is introduced which provides a much more effective assessment of the trustworthiness of nodes. It describes various malicious behavior in the p2p network, not only as a measure of trust, but also taking into account the total number of transactions, feedback the level of trust, the context factor of the transaction, and the community context factor. The problem is that it cannot effectively prevent collusion, and the overhead in communication is substantial.

In [18], the Bayesian-based trust model is characterized by distinguishing the concept of trust and credibility. Trust refers to the ability of the node to provide excellent service. The credibility of the node is recommended through other nodes of credibility. The advantage of this model is that when two nodes in the network have different evaluation criteria for the same service, a flexible solution is proposed to produce a different degree of trustworthiness.

In [19], a fully distributed way is introduced to store the user's reputation information. Unlike other trust systems, in this system, the trust information stored by the node is the satisfactory feedback from other nodes to the service provided by it. So the node has the motivation to store the trust information, but the model does not use the exact method of calculating the trust and thus, cannot eliminate the impact of malicious recommendations.

IV. PROPOSED APPROACH FUZZY-GRA TRUST MODEL

In this section, we introduce a trust model based on fuzzy mathematics and gray relational theory in detail. Based on the former trust model, we propose definitions and structure of Fuzzy-GRA.

A. Trust model concept

I) Definition 1

Consider vector T as the trust evaluation that shows the behavior between cloud and users that is considered as trust vector. The trust vectors are divided into five levels to represent different characteristics for different users according to their credit history information. The characteristics are shown in Table 1.

TABLE 1：CHARACTERISTICS OF TRUST LEVELS

Ti (trust-level vector)	Characteristics
T1	Full trust. Successful trade, good quantity, and resource of service.
T2	General trust. Successful trade, relatively good quantity and resource of service.
T3	Neutral trust. Successful trade, average quantity and resource of service.
T4	Distrust. Failing trade, relatively bad quantity and resource of service.
T5	Full distrust. Failing trade, bad quantity, and resource of service.

II) Definition 2

As shown in Table 1, H represents different quantities of services according to trust vectors. For example, user A's trust level is T2, then the service it enjoys is H2. The authorities that the users can get according to their levels are shown in table 2

TABLE 2 : APPROPRIATE AUTHORITIES OF SERVICE

levels	Appropriate authorities
H1	User can do all the operations and maintain cloud facilities
H2	User can edit, download and use cloud facilities
H3	User can download and use cloud facilities
H4	User can download cloud facilities (read-only)
H5	Denial of service

III) Definition 3

'K' is the trust vector set that consisted of every index factor of the evaluation node. It concludes all attributes that form trust types. For example, node I trust factor set K= {service attitude, speed, IP transfer rate, loss tolerance}.

IV) Definition 4

'V' is the judgment set that is consistent with the total evaluation result to the evaluation node. The level of trust set is corresponding to the level of evaluation.

B. The structure of the trust model

We design the proposed Fuzzy-GRA trust model by using computing and storage the power of the cloud platform. It provides trust evaluation services for users. The main structure is shown in figure 1.

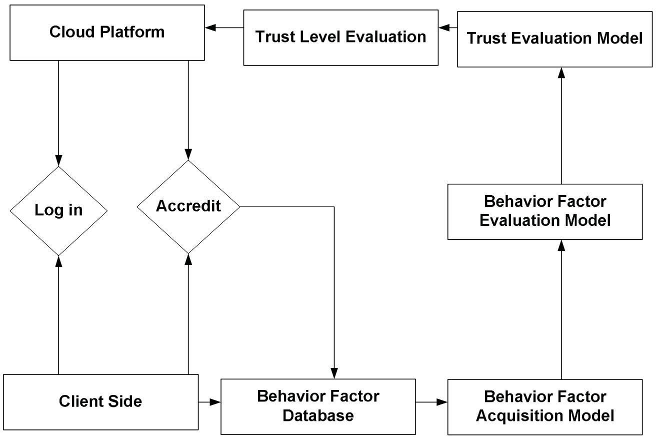

Figure 1: the structure of the trust model

The trust model structure is based on the following steps.

i) Users log in the cloud platform, and it inquires the user's behavior database.

ii) Cloud platform acquires user's behavior factor.

iii) Platform gets user's trust vector via calculating user's behavior factor.

iv) Trust level module evaluates user's trust vector to get user's level.

v) Cloud platform gives corresponding rights to users.

C. Trust Model design

The direct trust level of a node is the evaluated level that computed in the cloud computing platform according to the transaction of the node through assorted performance factors in this process. In this model, a fuzzy comprehensive evaluation is used to compute the trust level of nodes.

The specific process is in the following five steps:

i) Determine the factor set

The performance of node (i) should be evaluated from different aspects including their serving speed and the transmission rate of IP and loss Tolerance. The set of these factors is defined as U=(U1,U2,……Un).

ii) Determine the weight of the factor

The importance of factors in U are not the same, so it is necessary to attach a weight to each factor. The set W= (w1,w2,……wn) is defined to describe the weight. w1,w2,……wn represent the weight of each factor.

iii) Determine the evaluation set

According to the different evaluations of each factor, different levels can be formed. This passage divides trust into five levels; the evaluation set is in accordance with trust levels, also divided into five levels as V=(V1, V2, V3, V4, V5), which represents good, relatively good, average, relatively bad, bad.

iv) Determine the fuzzy relation judging matrix.

First, evaluate the single factors and after statistical analysis of each factors, for example, if service attitude has a set of evaluation, r11 is good, r2 is relatively good, r13 is average, r4 is relatively bad, r5 is bad, then the judging set is r1= $(r11, r12, r13, r14, r15)$.

Through this we can get the speed factor r2=(r21,r22,r23,r24,r25) and so on.

Then we can get the fuzzy evaluation matrix like:

$$\begin{pmatrix} r11 & \cdots & r15 \\ \vdots & \ddots & \vdots \\ rm1 & \cdots & rm5 \end{pmatrix} \qquad (1)$$

v) Compute the trust vector

The computing formula of the trust vector is T=W*R

$$T= (w1,w2,\ldots\ldots wm)*\begin{pmatrix} r11 & \cdots & r15 \\ \vdots & \ddots & \vdots \\ rm1 & \cdots & rm5 \end{pmatrix} \qquad (2)$$

After computing this trust vector, we get the result that "full trust" is attached to T1, "general trust" is attached to T2 and so forth.

According to the principle of the maximum of membership, the trust value provided by the node is Max (Ti). Other data is not fully used, thus resulting in the inaccuracy of results or even great errors. Therefore, we introduce Grey Relational Analysis into our computing.

D. Use Grey Relational Analysis to analyze the trust vector

We define the reference vector to the trust vector as Tj. The process of it is:

i) Determine the reference vector Tj

Pick 5 reference vector Tj1,Tj2, Tj3, Tj4, Tj5 randomly,

Tj1=(0.5, 0.4,0.3,0.2, 0.1)
Tj2=(0.3, 0.5,0.4,0.2, 0.1)
Tj3=(0.2, 0.4,0.5,0.3, 0.1)
Tj4=(0.1, 0.2,0.4,0.5, 0.3)
Tj5=(0.1, 0.2,0.3,0.4, 0.5)

ii) Compute the relational degree coefficient

$$\xi ij(k) = \frac{\rho 1MMIN(j)+\rho 2MMAX(j)}{\Delta ij(k)+\rho 2MMAX(j)} \qquad (3)$$

In the formula, $MMIN(j) = {}^{min}_{k}|T_{ik} - T_{ik}|$ represent the minimum difference between Ti and Tj.

$MMAX(j) = {}^{max}_{k}|T_{ik} - T_{ik}|$ represent the maximum difference between Ti and Tj.

$\Delta ij(k) = {}^{min}_{k}|T_{ik} - T_{ik}|$ represent the absolute difference between Ti and Tj.

ρ represent the resolution ratio.

iii) Compute relational degree rij

$$rij = \frac{1}{5}\Sigma_{k=1}^{5}\xi ij(k) \qquad (4)$$

iv) Determine the trust level

After computing the relational degree, we compare the value of relational degree, Rs = max(ri1,ri2,…….,ri5), s =1,2,3,4,5, represents that node i has the maximum relation with Ts, so node i is attached to S, and owns its service.

E. Algorithm analysis of our trust model Fuzzy-GRA

Algoritm1. Fuzzy Mathematics and Grey Relation Analysis Algorithm **(Fuzzy-GRA)**

```
1. Initialization: W= (W1,W2,……Wm): weight of each factor;
V= (V 1, V2, ……, Vn): the evaluation set;
2. Input: U = (U1,U2,……Un): set of factors;
3. Output: T, trust level
4. Build the fuzzy relation judging matrix
5. Compute MatrixR (U, V);
6: Calculate trust vector: T=W*R;
7: Calculate the correlation coefficient: $\xi ij(k) = \frac{\rho 1MMIN(j)+\rho 2MMAX(j)}{\Delta ij(k)+\rho 2MMAX(j)}$;
8: Calculates relational degree rij: $rij = \frac{1}{5}\Sigma_{k=1}^{5}\xi ij(k)$;
9. Return T.
```

Line 1 shows that the 1st step is to initialize the weight of each factor and the evaluation set. Line 2 shows the input is the set of factors we gain from the nodes. Line 3 shows the output is trust level T. Then, in line 4, we build the fuzzy relation judging matrix and compute it by using the data from the input. In line 6, calculate the correlation coefficient. In line 7, calculate relational degree using correlation coefficient. At last, T is returned.

V. Analysis of experimental results

To show the efficiency of our trust model Fuzzy-GRA, we tested the various nodes. Based on the results, we compared the performance of our proposed model with other existing approaches: Inspection of Trust-Based Cloud(ITC) [20], Trust enforcement through Self-adapting cloud(TESC) [21], Neural network-based trust prediction(NNTP) [22], RecTrust[23], EigenTrus[24] and p2pTrust[25] As, similar scenarios have been generated for testing purposes and compared using same testing machine with exactly same parameters. Table 3 shows used parameters in experiments.

TABLE 3：USED PARAMETERS IN EXPERIMENTS

Tools	Description
Programming platform	Java JDK 1.6
Integrated Development Environment	Eclipse 3.5
Risk Generating Model	spiral model
Experimental facility	2.8 GHz Lenovo Dual Core CPU
Test machine	8-bit version of Windows 10

Based on testing process, we obtain interesting results that are plotted and showing the effectiveness of proposed Fuzzy-GRA model and its comparison with contending trust models.

i Trust level of nodes between Fuzzy-GRA and maximum membership.
ii The rate of threat that the platform suffers.
iii Accuracy of trust models in number of the risks.

A. Trust level of nodes between Fuzzy-GRA and maximum membership.

The results of table 4 show the trust levels of nodes under different environment. Various nodes log in the cloud platform and ask service to the cloud. At the same time, cloud platform acquires user's behavior factor and gets the node's trust vector. According to the Figure 2, Use the principle of the maximum membership degree to determine the node's level ignores node's other membership vectors, the results are not accurate, and our model is more closed to the excepted results.

TABLE 4 : RESULTS OF EXPERIMENT 1

Node	Trust vector	Level of the maximum membership degree	Level in Fuzzy-GRA
A	TA=(0.40, 0.43,0.07,0.06,0.05)	2	1
B	TB=(0.32, 0.18,0.12,0.19,0.16)	1	2
C	TC=(0.24, 0.22,0.22,0.20,0.10)	4	3
D	TD=(0.06, 0.00,0.40,0.53,0.03)	4	4
E	TE=(0.08, 0.16,0.28,0.07,0.42)	5	5

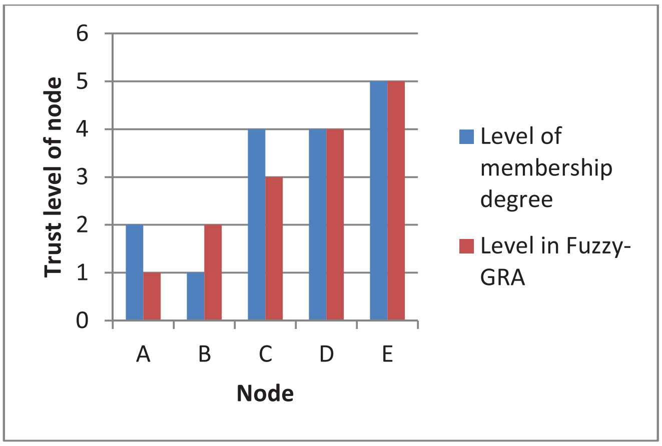

Figure 2: Trust level of nodes between fuzzy-GRA and maximum membership.

B. The rate of threat that the platform suffers when it has a trust model, and it does not.

100 nodes are generated at random, and 1000 transactions are stimulated. The trust levels of 100 notes are determined according to nodes' transaction behavior. They are compared to analyze the threat that the platform suffers when it has a trust model, and it does not.

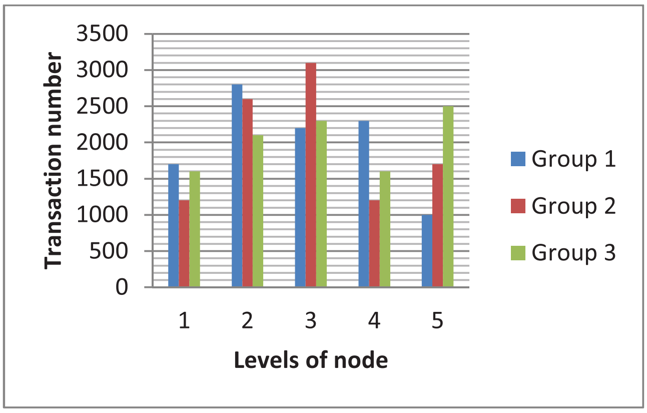

Figure 3: the transaction numbers of each group

Figure 3 shows three groups of data. Each group has its transaction distribution. For example, level 1 nodes in group 1 have 1647 transactions; level 2 has 2753 transactions, level 3 have 2178 transactions, level 4 have 2462 transactions, level 5 have 1018 transactions.

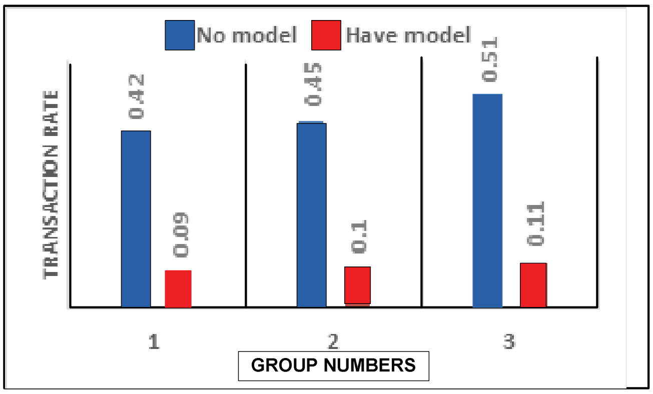

Figure 4: the threat rate of each group.

In Figure 4, the data in the first group has the threat rate of 0.42 in the situation of no trust model, and it has the threat rate of 0.09 in the situation of Fuzzy-GRA model. The threat rate drops by 0.33.

The data in the second group has the threat rate of 0.45 in the situation of no trust model, and it has the threat rate of 0.1 in the situation of Fuzzy-GRA model. The threat rate drops by 0.35.

The data in the third group has the threat rate of 0.51 in the situation of no trust model, and it has the threat rate of 0.011 in the situation of Fuzzy-GRA model. The threat rate drops by 0.40.

According to analysis, we can conclude that under the current trust model, the threat rate in the cloud platform has considerably decreased. Therefore, the trust mechanism can substantially maintain the safety of the platform.

C. Accuracy of Trust Models in number of risks

In this experiment, the performance of Fuzzy-GRA was tested and compared with contenting trust models from accuracy perspective: (ITC), (TESC), (NNTP), RecTrust, EigenTrus and p2pTrust. To measure the accuracy, the spiral model is used to determine the accuracy level of trust. In experiment, the number of the risks were artificially generated to determine the effectiveness of trust models. As, similar tools and parameters were used for conducting the experiment. Based on the results, it is observed that proposed Fuzzy-GRA found better trust model in detecting the artificially generated risks in the cloud. The accuracy rate of proposed model found 99.96%. On the other hand, the contending trust models reduced the accuracy rate. The worst trust model was ITC during the risk detecting process that shows the accuracy rate 97.92% with 45 risks. The EignTrust model that was also observed as better trust model whose risk-detecting capability was close to proposed Fuzzy-GRA model. However, its accuracy remained 99.45%. The results indicate that proposed Fuzzy-GRA trust model is the better candidate for detecting the risk in the cloud computing. As, the risk-detecting performance of the proposed Fuzzy-GRA and other contending trust models is depicted in Figure 5.

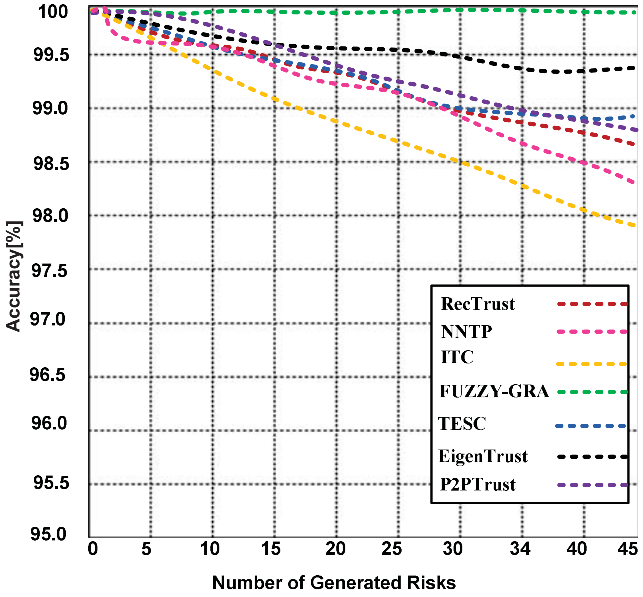

Figure 5: Accuracy of proposed GRA-Fuzzy and other contenting models in presence of generated risks

VI. DISCUSSION OF TRUST MODELS

The complexity of our model is O(n), which is simpler than another model. The contending models have higher complexity. As, EigenTrust has complexity of O(n*m), RecTrust has complexity of O(n^2), p2pTrust has complexity of O(n^2), ITC has complexity of O(n^2), NNPT has complexity O(n+n) and TESC has complexity O(log n+n). Hence, it is concluded that our model has less cost, which can consume less Internet resources. Also, the model proposed in this paper makes use of the cloud platform, which can calculate the node level with high efficiency. The time complexity of FUZZY-GRA and contending trust models is shown in Table 5.

TABLE 5: Time complexity of Trust models

Trust Models	FUZZY-GRA	Eigen Trust	RecTrust	p2ptrust	TESC	NNPT	ITC
Time Complexity	O(n)	O(n*m)	O(n^2)	O(n+n)	O(log n+n)	O(n+n)	O(n^2)

Malicious nodes refer to the malicious intention of some malicious node to sabotage platform facilities. Analysis of simulation results and trust model plays a significant role in restraining the behavior of the malicious nodes. Some malicious nodes in the network are difficult to destroy on the platform due to the limitation of authority. The facilities of the platform can play a critical protection factor. Experiments demonstrate that under the trust model of the approach proposed in this paper, the cloud platform has achieved a considerable level of restrictions on malicious nodes. When a malicious node makes a malevolent action on the cloud platform, the platform system gives it low operating privileges and minimizes the possibility of it causing unwanted actions.

VII. Conclusion

This paper proposes Cloud platform trust model (Fuzzy-GRA) based on fuzzy mathematics and gray relational theory. We combine other models, analyze and handle the evaluation of trust according to computing method of gray relational degree to make the results more specific. The results of experiments show that the nodes can be evaluated more specifically according to the gray relational degree algorithm. Our model restricts the user's right and gives customers different operating authority, minimizing the destructiveness of malicious nodes to address cloud safety. Furthermore, the performance of proposed Fuzzy-GRA has also been compared with contending trust models from curacy perspective: (ITC), (TESC), (NNTP), RecTrust, EigenTrus and p2pTrust. The testing results show the accuracy 99.96%. risk-detection capability of proposed Fuzzy-GRA that is much higher as compared with other contending trust models.

In future work, we may propose the real-time monitoring module based on the Fuzzy-GRA model; this model can be used to manage the behavior of irregular nodes in real time. With the development of computer technology, cloud computing has received much attention and is utilized by society in many aspects. It has become the developing direction of network information technology. Cloud safety is the basis of its development; only the security work done, can allow the system to be developed further. Therefore, the study of cloud safety has a significant impact on society as a whole.

REFERENCES

[1] Razaque, Abdul, and Syed S. Rizvi. "Privacy preserving model: a new scheme for auditing cloud stakeholders." *Journal of Cloud Computing* 6, no. 1 (2017): 7.

[2] Razaque, Abdul, Nikhileshwara Reddy Vennapusa, Nisargkumar Soni, and Guna Sree Janapati. "Task scheduling in cloud computing." In *2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*, pp. 1-5. IEEE, 2016.

[3] Rizvi, Syed, Abdul Razaque, and Katie Cover. "Cloud data integrity using a designated public verifier." In *2015 IEEE 17th International Conference on High Performance Computing and Communications, 2015 IEEE 7th International Symposium on Cyberspace Safety and Security, and 2015 IEEE 12th International Conference on Embedded Software and Systems*, pp. 1361-1366. IEEE, 2015.

[4] Yin C, Feng L, Ma L; An improved Hoeffding-ID data-stream classification algorithm; J. Supercomput., 72 (7) (2016), pp. 2670-2681.

[5] Guo, Liang, Pu Du, Abdul Razaque, Muder Almiani, and Amer Al Rahayfeh. "Energy saving and maximize utilization cloud resources allocation via online multi-dimensional vector bin packing." In *2018 Fifth International Conference on Software Defined Systems (SDS)*, pp. 160-165. IEEE, 2018.

[6] J. Li, X.L. Zheng, D.R. Chen, W.W. Song; Trust based service selection in service-oriented environment; Int. J. Web Serv. Res., 9 (3) (2012), pp. 23-42.

[7] K.K. Fletcher, X.F. Liu, M. Tang; Elastic personalized non-functional attribute preference and trade-off-based service selection; ACM Trans. Web, 9 (1) (2015), pp. 1-27.

[8] Hoogendoorn, M.; Jaffry, S.W.; Maanen, P.P. van & Treur, J. (2011). Modeling and Validation of Biased Human Trust. IEEE Computer Society Press, 2011.

[9] Dondio, Pierpaolo, and Luca Longo. "Trust-based techniques for collective intelligence in social search systems." In *Next generation data technologies for collective computational intelligence*, pp. 113-135. Springer, Berlin, Heidelberg, 2011.

[10] Sun, Dawei, Guiran Chang, Lina Sun, and Xingwei Wang. "Surveying and analyzing security, privacy and trust issues in cloud computing environments." *Procedia Engineering* 15 (2011): 2852-2856.

[11] Lagesse, Brent. "Analytical evaluation of P2P reputation systems." *International Journal of Communication Networks and Distributed Systems* 9, no. 1-2 (2012): 82-96.

[12] Liu, Sifeng, Yingjie Yang, and Jeffrey Forrest. *Grey data analysis*. Springer: Berlin, Germany, 2017.

[13] G Bin, S Victor; Incremental learning for V-support vector regression; Neural Netw, 67(4) (2015), pp.140-150.

[14] S.S. Yau, Y. Yin. QoS-based service ranking and selection for service-based systems, in: Proceedings of the International Conference on Services Computing, SCC, 2011.

[15] Noorian, Zeinab, Michael Fleming, and Stephen Marsh. "Preference-oriented QoS-based service discovery with dynamic trust and reputation management." In *Proceedings of the 27th Annual ACM Symposium on Applied Computing*, pp. 2014-2021. ACM, 2012.

[16] P Pantel.From frequency to meaning: Vector space models of semantics J. Artif. Intell. Res., 37 (1) (2010), pp. 141-188.

[17] Blade.(2013).Retrieved on 6th May, 2017: http://www.expreview.com/29009-all.html

[18] Molnar, David, and Stuart E. Schechter. "Self-Hosting vs. Cloud Hosting: Accounting for the Security Impact of Hosting in the Cloud." In *WEIS*. 2010.

[19] Lee, Wei-Po, and Chuan-Yuan Ma. "Enhancing collaborative recommendation performance by combining user preference and trust-distrust propagation in social networks." *Knowledge-Based Systems* 106 (2016): 125-134.

[20] Prasad, Vivek Kumar, Mrugesh Shah, Namrata Patel, and Madhuri Bhavsar. "Inspection of Trust Based Cloud Using Security and Capacity Management at an IaaS Level." *Procedia computer science* 132 (2018): 1280-1289.

[21] El-Kassabi, Hadeel T., M. Adel Serhani, Rachida Dssouli, and Alramzana N. Navaz. "Trust enforcement through self-adapting cloud workflow orchestration." *Future Generation Computer Systems* (2019).

[22] Somu, Nivethitha, Gauthama Raman MR, V. Kalpana, Kannan Kirthivasan, and Shankar Sriram VS. "An improved robust heteroscedastic probabilistic neural network based trust prediction approach for cloud service selection." *Neural Networks* 108 (2018): 339-354.

[23] Abrams, Zoë, Robert Mcgrew, and Serge Plotkin. "A non-manipulable trust system based on eigentrust." *ACM SIGecom Exchanges* 5, no. 4 (2005): 21-30.

[24] Xing, Xing, Weishi Zhang, Zhichun Jia, Xiuguo Zhang, and Nan Xu. "Trust-based Top-k Item Recommendation in Social Networks." *JOURNAL OF INFORMATION &COMPUTATIONAL SCIENCE* 10, no. 12 (2013): 3685-3696.

[25] Li, Xiaoyong, Feng Zhou, and Xudong Yang. "Scalable feedback aggregating (SFA) overlay for large-scale P2P trust management." *IEEE Transactions on Parallel and Distributed Systems* 23, no. 10 (2012): 1944-1957.