IJICTR
International Journal of Information & Communication Technology Research

Volume 11- Number 2 – Spring 2019 (62 -69)

Proposing a New Algorithm for Predicting Short-Term and Long-Term Trust-ability in Cloud Computing

Samiyeh Khosravi
Department of Computer Engineering, Faculty of Engineering, University of Birjand, Birjand, Iran
skhosravi@birjand.ac.ir

Received: 9 September 2018 - Accepted: 5 February 2019

Abstract: **Despite the huge use of cloud computing, due to its large dimensions and availability for all users, this type of network is weak and vulnerable to malicious attacks. Therefore, as a useful complement to existing security methods, trust management plays a crucial role in discovering suspicious behaviors in the cloud computing network. The critical question is, how can we find ideally and effectively users with suspicious behaviors in these complex environments. In this paper, the Markov chain model has been used to calculate the short-term reliability of users in the cloud network, and the trust management system has been proposed to mitigate the effects of complex environments to calculate the user's status. Furthermore, a new computational model has been introduced with relevant, practical factors for calculating the long-term trust that reduces the effect of changing environmental parameters in the calculations. In the Markov chain, in each time unit the transition occurs from one state to another, the number of these states can be counted. In this paper, two modes of normal (faultless) and having a risk (damaged, and having a fault) are considered for users. The simulation results show that the proposed algorithm, Markov chain trust management can more effectively detect suspicious behaviors of users in the cloud computing network, and in a meaningful way, provide a better rate of delivery of packets compared to their counterparts, and ultimately provide better security in the cloud computing network. To assess the effectiveness of the introduced Markov chain model, we compared it with two TBID and RFSN models. We have used MATLAB software to compare the performance of the cloud network.**

Keywords: Estimation and prediction, Cloud environment, Intrusion detection.

1. Introduction

Security and trust are two closely related concepts, which are used on a large number of occasions instead. The main difference between them is complexity and high level of overhead in security. Traditional security mechanisms, such as authentication and cryptography, cannot protect this type of network against external attacks by hosted users. For example, surveillance can send the wrong information to the network through users who have been conquered or distort the results they have achieved. These incorrect data are sent across the cloud network and can lead to false interpretation and decisions by users. Traditional and old mechanisms cannot detect the difference between the surveillance users with the primary users and the authenticity of these users are recognized correctly, and thus the wrong data easily is entered to the cloud network. To reduce these problems, trust and security issues have been widely discussed as a tool for providing more protection in the cloud computing network. In addition, in recent years, there have been several solutions proposed based on trust.

Trust measuring is initially a topic of interest to researchers in the social and sociological sciences, to identify the level of trust in humans. Then to examine its effects on business transactions, and in this regard, somewhat of a kind of reputation is posed instead of accuracy [1].

Since the last decade various ways for trust management in computer networks have been proposed to identify unreliable users, and much progress has been made in this regard, but existing trust management systems still find it difficult to identify reliable and unreliable users accurately because network users are inherently unpredictable and are in the midst of a mess of false information and hostile behaviors.

Unconstrained users can enter false or misleading data to the network, to invalidate the correct data or increase the system error rate, so that the network performance becomes unacceptable [2].

The main issue is how we can achieve the ideal detection rate of surveillance users in complex environments. This question is a critical issue in trust management in the cloud network.

Trust management, offers a practical idea to determine and evaluate the reliability of network users, which brings the reliable and faultless operation of computer networks. This idea applies to various routing, data accumulation, and attack exploitation activities. Because adding or deleting users from the network is based on the predicted trust of the users, to eliminate or alternate unreliable users from the network [3].

In this paper, in the first section, we have an introduction, which explains about trust and necessity of existing this factor in the cloud network. The second section will be a literature review, which will present a complete investigation of past researches regarding this issue. After that, in the third section, we will discuss trust in cloud computing, and why we need such criteria in this network. The fourth section will be a Markov chain and trust management in short-run. In this section, we will discuss how can we use the Markov chain to predict trust and reliability in short-run. The fifth section will be measuring long-term trust value with the use of the Markov chain model. Section sixth will be explained Markov chain trust management algorithm gradually and explain how such an algorithm will be used to predict the trust. Section seventh will show the simulation results, and finally, we will have a conclusion in section eighth.

Novelty and contribution of our proposed system:

In this paper, it is assumed that the trust level can be estimated for the current state of each user and a TMS model is proposed to mitigate the effects of complex environments, on the calculation of the user's status in the short and long term. This Markov chain-based model can provide users with a degree of trust-ability in short-run according to their current behaviors. This method is used to determine the status of users and to determine whether users are reliable or not. The predicted value only reflects the degree of assurance and accuracy in the short-run. We assume that the process of changing the status of users in this model follows the Markov chain.

Unlike the existing systems which have very high computational loads – like the RFSN system, which uses the Bayesian model for each user to predict the future behavior of other users, our system is not cause lots of computational loads for the system and doesnot reduce the performance of the system.

2. Literature Review

Researches about cloud security have started with particular attention to the issue of information trust management, and various models have been presented in this regard [4].

In the RFSN (Reputation-based Framework for Sensor Network), using the Bayesian model, a model has been developed in which each user has the criteria for the reputation of other users and can predict their future behaviors. Using a mathematical tool to calculate and update the values of fame and being well known, they used them to determine the trust of users [5].

Subsequently, with a small change in the above framework, a quantitative framework was proposed to measure its reliability and distribution of it to counter attacks. In 2009 to reduce the amount of computing and less use of communications and storage space, a slight model of TMS was proposed, in which the idea of grouping was used. Its complementary research focused on regional block groupings [6].

The first model can calculate the trust-ability of users in the RFSN complement model. In this model, a distributed framework for the accuracy of information was presented, which was based on the selection of trust-ability of the gateways. In this way, each user has a reliability table that sends the trust-ability of its adjacent users to the gateways.

In recent models, a new method for locating and determining a weak area, based on trust management was presented. Following, a protocol called TIBFIT for managing information reliability, for the security of combined data was presented. Finally, a hierarchical structure of the TBID for the trust management of information was introduced, that used intrusive detection methods [7].

Fuzzy logic can be used to deal with inappropriate descriptions of intrusions [8]. Although it has better flexibility, for some uncertain issues, its accuracy of detection is less than the neural network. To reduce the training time of the neural network, we can use fuzzy logic with the neural network to quickly detect unknown attacks in the cloud computing network.

In [9], they used IDS based on neural network and fuzzy clustering. At first, a dataset is divided into training and validation sets. Then by applying clustering method on the training set, a new different training set is generated. For each different training subsets, different training neural network is used. At this step, to solve the errors of each neural network, the fuzzy aggregation model is used to combine the results of various neural networks. The True-Negative Criterion, which determines the number of attacks that have been appropriately detected, has not been conducted. If the number of training samples increases, the training time will be increased.

In [10], the authors used (Fuzzy Clustering-Artificial Neural Network) FC-ANN, which is presented in [10], and have come up with multi-layered IDS. In this model, the input and output data packets receive the UDP, IP, ICMP, and TCP values, and send to a shared queue for analysis. Then packet analysis is performed, and through efficient matching, surveillance packages will be detected by generating an alarm.

In [11], an over-observer detector system was designed by using the adaptive neuro-fuzzy algorithm. For the implementation, they used Cloudsim simulator. This detector monitors the performances of virtual machines. The ANFIS (Adaptive Network-based Fuzzy Inference System) model uses a Sugeno Fuzzy inference system and using a network analysis model, which trained in 150 rounds and at an error rate of about 2% was stopped as the best detection rate [25–31].

3. Trust in Cloud Computing

In this section, we describe the current and existing mechanisms of building trust in the cloud network including:

-Trust based on reputation

-Trust based on SLA

After creating primary trust and using the cloud service, the user must reassess and reassure their trust. The SLA (Service License Agreement) is a legal contract among cloud users and cloud service providers. Therefore, monitoring Quality of Service (QoS) and validating SLA in trust management of cloud computing is very important. But there are two problems in this regard [1-6]:

-SLA focuses on apparent elements of cloud performance and does not express intangible components, such as security and privacy [30].

-Many users cannot merely monitor quality.

For this purpose, we can use the help of a third party specialist company. In a private cloud, this is done by a trusted cloud agent or trusted scrutineer (such as the CTA that is being surveyed in the transparency cloud mechanisms section). In a hyper-cloud or among several clouds, there may not be much dependence on trust scrutineer. In the public cloud, individual users and some enterprise users may use a trusted agent (a cloud entity that is a specialist in business) [26, 27].

3.1. Clarify Mechanism in the cloud

3.1.1. STAR: To increase cloud clarity, the Cloud Security Association (CSA), has provided STAR program with the ability to self-assess security controls for cloud providers, either in the form of an initial accounts assessment matrix or in the form of a cloud control matrix. STAR is a useful resource for users when searching for cloud services. Although cloud providers provide self-assessment information, users can use the evaluations of independent expert organizations as third-party companies [1, 7].

3.1.2. CTP: The cloud trust scrutineer is introduced as one of the cloud services, and so-called Trust-as-a-Service (TaaS). The cloud trust scrutineer includes:

-Identification service

-Ability to log in to multiple cloud provider systems separately

-A profile acceptance service that enables the user to view the security profile of several cloud providers, according to standard criteria's.

However, as with STAR, the main disadvantage of CTP is that the cloud provider gives the information [1-8].

4. Markov Chain and Trust Measurement in Short-run

In the Markov chain, in each time unit the transition occurs from one state to another, the number of these states can be counted. In this paper, two modes of normal (faultless) and having a risk (damaged, and having a fault) are considered for users. The Markov chain is also a random memoryless process, which means that the conditional probability distribution of the next state depends only on the current state and does not depend on previous events [1, 9].

In this paper, it is assumed that the trust level can be estimated for the current state of each user and a TMS model is proposed to mitigate the effects of complex environments, on the calculation of the user's status in the short and long term. This Markov chain-based model can provide users with a degree of trust-ability in short-run according to their current behaviors. This method is used to determine the status of users and to determine whether users are reliable or not. The predicted value only reflects the degree of assurance and accuracy in the short-run. We assume that the process of changing the status of users in this model follows the Markov chain. Therefore, estimating the reliability of users can be modeled as a Markov model with the following five elements [10].

$$\Omega = (R, V, Q, \Lambda, \pi) \quad (1)$$

Where: $R = \{r_1, r_2, \dots, r_N\}$ is the set of normal statuses. $V = \{v_1, v_2, \dots, v_N\}$ is the set of having fault and uncertain situations. $Q = \{q_v\}$ is transition matrix of situations, which is a $k * k$ matrix. q_v represents transition rate from i to j: $i, j \in R \cup V$System parameters $\lambda_1, \lambda_2, \lambda_3, \lambda_4$ that λ_i represents the parameter of the distribution index, in which the status of each user is between R and V.$\pi = \{\pi_1, \pi_2, \dots, \pi_{N+M}\}$ represents the initial value or status of distributed confidence [28, 29].

$$\begin{gathered} \pi_i = P_0\{X(t) = r_i\}, \quad 1 \le i \le N \\ \pi_j = P_0\{X(t) = r_j\}, \quad N+1 \le j \le N+M \\ \sum_{i=1}^{N+M} \pi_i = 1 \end{gathered} \quad (2)$$

where $X(t)$ is known as user status at the time t. λ_1, λ_2, λ_3 and λ_4 are distributed index parameter from R to R, R to V, V to V, and V to R status respectively. T_i is the time that the user operates in λ_i status. As the status change from λ_1 to λ_4 the Λ will change and as a result, the users status will change accordingly [1-11].

4.1. Hypothesis

To formulate the above Markov chain, we must consider the following assumptions:

-In all $N+M$ existing conditions, the probability of changing the user status is in their own range. That is, the status of each node cannot be out of $N+M$ bounds.

-The Markov chain presented in this paper is time-independent, ergodic, irreducible, and non-periodic [1, 5, 12].

4.2. Formulation

To calculate the final amount of confidence, first of all, we should form the $Q\ matrix$. To do this, consider a positive and a small enough number of τ. Then we calculate the transition probability over the time interval of $[t, t+\tau]$.

$$P_{i,j}(z) = P\{X(t+\tau) = j \mid X(t) = i\} =$$
$$P\{T_k \le \tau\} = \int_0^{\tau} \lambda e^{-\lambda_k t} dt = 1 - e^{-\lambda_k \tau} =$$
$$\lambda_k \tau + O(\tau), \quad i,j \in R, \quad i \ne j \qquad (3)$$
$$P1 - (N-1)\lambda_1 \tau - M\lambda_2 \tau + O(\tau) \quad i,j \in R, \quad i = j$$
$$1 - (M-1)\lambda_3 \tau - M\lambda_4 \tau + O(\tau) \quad i,j \in V, \quad i = j$$

Then we can calculate the conversion rate of $q_{i,j}$ transformation and obtain the $Q\ matrix$ at the end.

$$Q_{i,j} = \lim_{r \to 0^+} \frac{P_{i,j}(z) - P_{i,j}(Q)}{\tau} \qquad (4)$$

$$if (i = j) \rightarrow P_{i,j}(0) = 0\ else\ P_{i,j}(0) = 1$$

According to the above formulas, we can obtain the $k * k$ transition matrix of Q in:

$$Q = \begin{bmatrix} q_{r_1 r_1} & \cdots & q_{r_1 v_M} \\ \vdots & \ddots & \vdots \\ q_{r_M r_1} & \cdots & q_{r_M r_M} \end{bmatrix} \qquad (5)$$

Also, we can use the Fokker-Planck equation and use the current probability distribution for predicting the absolute probability of user mode in the next phase. The resolution process is as follows [12, 20]:

$$\left(P'_{r_1}(t) \cdots P'_{V_M}(t)\right) = \left(P_{r_1}(t) \dots P_{V_M}(t)\right) * Q$$
$$\left(P_{r_1}(0) \dots P_{V_M}(0)\right) = \pi \qquad (6)$$
$$\pi_i = 1, \quad 1 \le i \le N+M$$

By the formulas mentioned above, we can calculate the probability of any statuses. Furthermore, users trust can be measured from the following equation [25]:

$$T = \sum_{i=1}^{N} P_{r_i}(t) = \qquad (7)$$
$$\frac{N\lambda_4}{M\lambda_2 + N\lambda_4}\left[1 - e^{-(M\lambda_2 + N\lambda_4)t}\right]$$

where T predicts the amount of the desired trust, which, of course, is only related to the state of the next step. In this paper, we have defined T as the amount of trust in the short-run, but the exact level of user's trust-ability is valuable over the long run. Following, we will discuss the idea of long-run authentication [1, 13].

5. Measuring Long-term Trust Value

This section discusses the idea of how to recognize and measure the reliability of cloud users in the long run. This idea can more accurately identify reliable users from unreliable users and can provide more security in the cloud network [13-20].

5.1. Computing User Status

In different environments, the probability, which shows that users in the normal state will be under attack, is not constant. It is assumed that users have only two situations: the standard and risky case or tricky situation. Besides, users have a specific and specific performance in different circumstances [1].

In this paper, the actual state of the users is calculated in four situations: status, actual status, short-term reliability, and long-term reliability.

For example, assume that one user in short-term has T_1 reliability, and in a next time slot a risky behavior will occur for that. This user is still in the normal state, but due to bad and undesired behaviors, its reliability decreases in the long run. From this idea, the real status and amount of reliability could be calculated for each user.

5.2. Computing Reliability in Long-term

In one of the previous papers, a framework for determining the long-term reliability of user based on dynamic memory factor is presented. In this paper, to describe a newer model, at first, we define the following formula:

$$Trust\_1^{new} = \beta_1 trust\_1^{t} + \beta_2 trust\_s \qquad (8)$$

$trust\_1^{t}$: the amount of long-run reliability at time t.

$trust\_s$: the amount of short-run reliability in $[t, t+1]$ interval.

$Trust\_1^{new}$: The amount of long-run reliability at $t+1$.

β_1, β_2: are inconstant memory norms that can be set dynamically [1].

Using Equ. 8, we can easily understand the disadvantages of this idea. If the reliability is too low for a user in a long-run, then the long term reliability of that user will show lousy behavior at the current time, while the user was working well. Therefore, this method cannot accurately determine abnormal behavior.

Therefore, we will propose a new method for identifying hostile users and calculating the long-run reliability, which formulates as follows:

$$trust\_1^{new} = \beta_1 trust\_1^n + \beta_2 trust\_f : \ i,j \in R, \ trust\_1^n \geq trust\_f$$

$$trust\_1^{new} = \beta_2 trust\_1^n + \beta_1 trust\_f : \ i,j \in R, \ trust\_1^n < trust\_f$$

$$trust\_1^{new} = \beta_1 trust\_1^n + \beta_2 trust\_f : \ i \in R, j \in V, \ trust\_1^n \geq trust\_f \quad (9)$$

$$trust\_1^{new} = \beta_2 trust\_1^n + \beta_1 trust\_f : \ i \in R, j \in V, \ trust\_1^n < trust\_f$$

$$trust\_1^{new} = \beta_1 trust\_1^n + \beta_2 trust\_f : \ j \in R, i \in V, \ trust\_1^n \geq trust\_f$$

$$trust\_1^{new} = \beta_2 trust\_1^n + \beta_1 trust\_f : j \in R, i \in V, \ trust\_1^n < trust\_f$$

i: Current status of the user.

j: Next status of the user.

$trust\_1^n$: The amount of long-run reliability at the current time.

$trust\_f$: The amount of predicted reliability from the current time to the next time slot.

From Equ. (9), we can quickly and accurately obtain new long-term reliability. For example, at time t, if the current state of the node is normal (it belongs to the set of normal states), and the next state of the node is from a set of uncertain nodes, then we will have: $i \in R, j \in V$.

For more explanation about this:

$$\beta_1 = 0.35, \beta_2 = 0.65, trust\_f = 0.45, trust\_1^n = 0.85$$
$$\rightarrow trust\_1^{new} = \beta_1 trust\_1^n + \beta_2 trust\_f \quad (10)$$
$$= 0.35 * 0.85 + 0.65 * 0.45 = 0.59$$

Although the method mentioned above still has some weak points, it has been able to effectively mitigate the shortcomings of previous methods as well as the impact of the environment.

6. Markov Chain based Trust Management (MCTM) Algorithm

In Markov chain algorithm, in each time step the transition occurs from one state to another, the number of these states can be counted. In this article, two modes of normal (faultless) and having a risk (damaged, and having a fault) are considered for users. The Markov chain is also a random memoryless process, which means that the conditional probability distribution of the next state depends only on the current state and does not depend on previous events [1, 9].

In this paper, it is assumed that the trust level can be estimated for the current state of each user and a TMS model is proposed to mitigate the effects of complex environments, on the calculation of the user's status in the short and long term. This Markov chain-based model can provide users with a degree of trust-ability in short-run according to their current behaviors. This method is used to determine the status of users and to determine whether users are reliable or not. The predicted value only reflects the degree of assurance and accuracy in the short-run. We assume that the process of changing the status of users in this model follows the Markov chain [24].

The step of the suggested algorithm is as follows:

1. First, the initial trust amount and status of the users are allocating them.
2. The primary values of $\lambda_1, \lambda_2, \lambda_3, \lambda_4$ parameters are given.
3. After that, the following loop will be repeated.
4. For each node, we calculate the rate of change ($q_{i,j}$) by the (3), (4) equations.
5. Using the (5), (6), and (7) formulas, we will calculate short-run trust.
6. Consider the amount of $trust\_f$ (predicting trust from current time to the next time slot) and $trust\_1^n$ amount of long-run trust at the current time.
7. After a certain period, each user monitors the other users in it's neighboring, to obtain their status.
8. The new value of the long-run trust ($trust\_1^{new}$), can be calculated by use of the Equ. (9).
9. If the network condition is changed, the Λ related parameters should be recalculated $\{\lambda_1, \lambda_2, \lambda_3, \lambda_4\}$.
10. $trust\_1^n = trust\_1^{new}$
11. The amount of $trust\_1^n$ will be entered again to the algorithm.
12. We start a new loop.

7. Simulation Results

To evaluate the efficiency of the introduced Markov chain model, we compared it with two TBID and RFSN models. We have used MATLAB software to compare the performance of the cloud network. Figure 1, shows the simulation of the reliability of the regular users by increasing the time. The above figure shows the effectiveness and feasibility of the new MCTM algorithm.

In different environments, the probability, which shows that users in the normal state will be under attack, is not constant. It is assumed that users have only two situations: the standard and risky case or tricky situation. Besides, users have a specific performance in different circumstances [1].

In this paper, the actual state of the users is calculated in four situations: status, actual status, short-term reliability, and long-term reliability [22, 23].

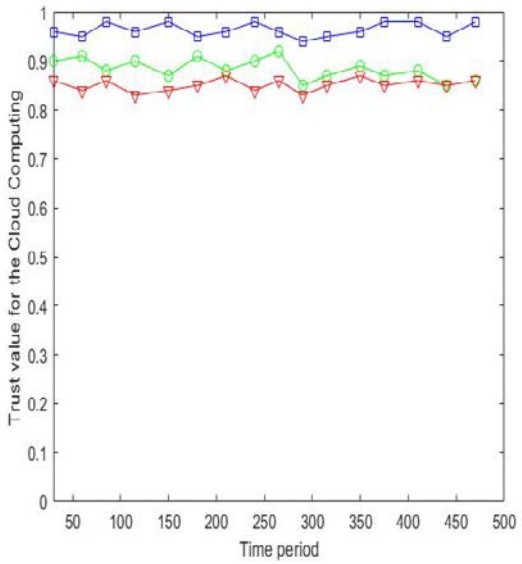

Fig. 1. *Comparison of the accuracy measurement percentages for normal users. Our proposed algorithm (blue line) is compared with the TBID (green line) and RFSN (red line) models, in terms of the trust values for the cloud computing.*

It can also be seen that the amount of oscillation in the calculations (with increasing time) has a noticeable improvement over the other models. The higher accuracy is due to the Markov chain to predict and to consider more parameters in the calculations.

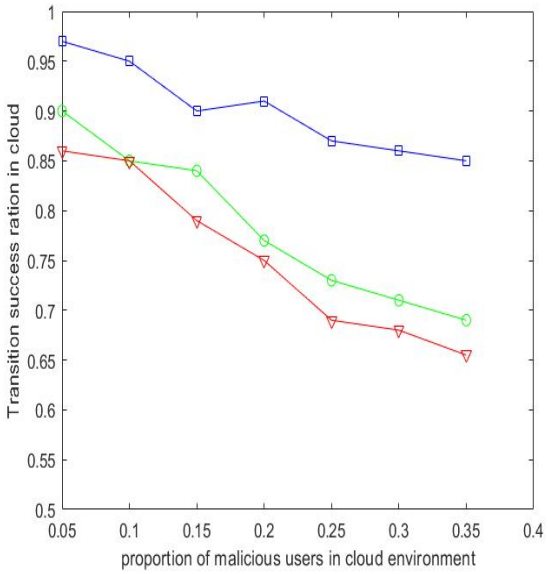

Fig. 2. *Our proposed algorithm (blue line) is compared with the TBID (green line) and RFSN (red line) models, in terms of the percentage of successful operations against malicious attacks with respect to increasing time*

Figure 2, shows the percentage amount of successful decisions when the network will be attacked, with the use of different methods. These attacks reduce the accuracy and trust of normal users, increase the credibility of the affected users, and increase the amount of incorrect information in the network. The figures show that, in all of the three algorithms selected for comparison and simulation, with increasing time and collecting more information about the adjacent users, a better situation than these attacks is found, but the stability of the MCTM algorithm is better than the two other algorithms.

Figure 3, shows the relationship between successful process rates, in increasing number of risky users. Of course, with an increase in the percentage of risky users, the transaction success rate is reduced. However, the slop and success rate in MCTM algorithm is better, which shows that due to the use of Markov chain, the detection rate of risky users has more accuracy than the other two algorithms, which prevents a significant reduction in the percentage of successful operation.

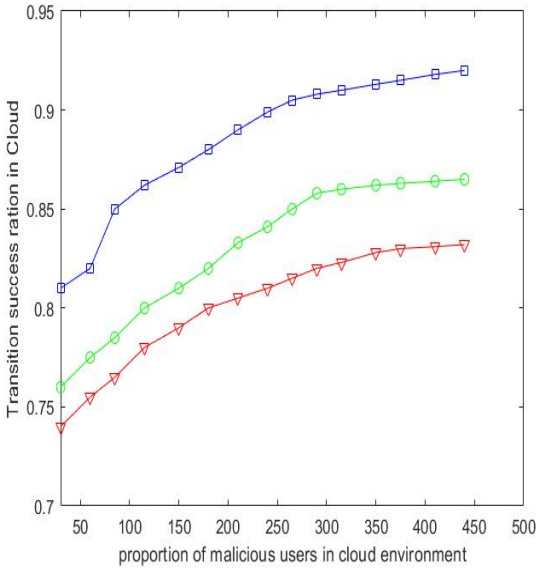

Fig. 3. *Our proposed algorithm (blue line) is compared with the TBID (green line) and RFSN (red line) models, in terms of the successful operation ratio with increasing the percentage of risky users*

Although the method mentioned above still has some weak points, it has been able to effectively mitigate the shortcomings of previous methods – like very high computational loads that they impose to the system and also very high amount of time that they need to do the process - as well as the impact of the environment. The previous systems cannot work in real-time and needs some time to detect any kind of attack or risk, the previous systems used the previous history of the network in order to acquire a pattern and then by use of that pattern they can recognize the reliable users from the risky users. Our proposed Markov chain-based model can provide users with a degree of trust-ability in short-run according to their current behaviors. This method is used to determine the status of users and to determine whether users are reliable or not. The predicted value only reflects the degree of assurance and accuracy in the short-run.

8. Conclusion

Cloud computing can be called a new paradigm in information technology, that has attracted the attention of many specialists and industry experts. Cloud computing, in addition to being a prominent phenomenon in the information technology market, is also considered as one of the most important sectors in the industry that has affected all of its ecosystems. However, there are still many concerns about the cloud. The most important of such concerns are security, privacy, and trust.

The simulation results show that the Markov chain reliability management algorithm more effectively detects and manages suspicious users in the cloud network. Besides, by increasing the percentage of good data, it provides a better delivery rate of packets than the other methods and can offer higher security rates in the cloud computing network.

9. References

1 Yousefi, M., Khorsandi, S.: 'Trust Management in WSN based on Markov Chain', Iranian Journal of Marine Science and Technology, 2015, 19, (75), pp. 50-57.

2 Sato, H., Kanai, A., & Tanimoto, S. (2010, July). A cloud trust model in a security aware cloud. In 2010 10th IEEE/IPSJ International Symposium on Applications and the Internet (pp. 121-124). IEEE.

3 Li, W., & Ping, L. (2009, December). Trust model to enhance security and interoperability of cloud environment. In IEEE International Conference on Cloud Computing (pp. 69-79). Springer, Berlin, Heidelberg.

4 Filippov, A. E., & Gorb, S. N. (2019). Methods of the pattern formation in numerical modeling of biological problems. Facta Universitatis, Series: Mechanical Engineering, 17(2), 217-242.

5 Dmitriev, A. I., Nikonov, A. Y., Österle, W., & Jim, B. C. (2019). VERIFICATION OF RABINOWICZ'CRITERION BY DIRECT MOLECULAR DYNAMICS MODELING. Facta Universitatis, Series: Mechanical Engineering, 17(2), 207-215.

6 Bashirov, A. E., & Norozpour, S. (2018). On an alternative view to complex calculus. Mathematical Methods in the Applied Sciences, 41(17), 7313-7324.

7 Filippov, A. E., & Gorb, S. N. (2019). Methods of the pattern formation in numerical modeling of biological problems. Facta Universitatis, Series: Mechanical Engineering, 17(2), 217-242.

8 Kassai, M., Poleczky, L., Al-Hyari, L., Kajtar, L., Nyers, J.Investigation of the energy recovery potentials in ventilation systems in different climates(2018) Facta Universitatis, Series: Mechanical Engineering, 16 (2), pp. 203-217

9 Tsukanov, A., Psakhie, S. Adhesion effects within the hard matter-soft matter interface: Molecular dynamics(2016) Facta Universitatis, Series: Mechanical Engineering, 14 (3), pp. 269-280.

10 Benad, J. (2018). Efficient calculation of the BEM integrals on arbitrary shapes with the FFT. Facta Universitatis, Series: Mechanical Engineering, 16(3), 405-417.

11 Li, X., & Du, J. (2013). Adaptive and attribute-based trust model for service-level agreement guarantee in cloud computing. IET Information Security, 7(1), 39-50.

12 Jozi, F.: 'Security, Trust, Privacy in Cloud Computing', MSc. Thesis, 2016, Al-Zahra University.

13 Akcay, M., Armutlu, H.: 'Distance education application architecture and cloud computing', IEEE 8th International Conference on Application of Information and Communication Technologies (AICT), 2014, pp. 1-5.

14 M. Darbandi; "Proposing New Intelligent System for Suggesting Better Service Providers in Cloud Computing based on Kalman Filtering"; Published by HCTL International Journal of Technology Innovations and Research, (ISSN: 2321-1814), Vol. 24, Issue 1, PP. 1-9, Mar. 2017, DOI: 10.5281/Zenodo.1034475.

15 Rukhsara, L., Aklam, F., Nawer, T., Chauhan, N.S., Islam, M.N.: 'A conceptual cloud-based model for developing e-commerce applications in context of Bangladesh', 5th International Conference on Informatics Electronics and Vision (ICIEV), 2016, pp. 117-121.

16 Bruce Berriman, G., Deelman, E., Groth, P., Juve, G.: 'The application of cloud computing to the creation of image mosaics and management of their provenance', Proceeding of SPIE 7740, Software and Cyberinfratsructure for Astronomy, 2010, 77401F.

17 Mehdi Darbandi; "Proposing New Intelligence Algorithm for Suggesting Better Services to Cloud Users based on Kalman Filtering"; Published by Journal of Computer Sciences and Applications (ISSN: 2328-7268), Vol. 5, Issue 1, 2017; PP. 11-16; DOI: 10.12691/JCSA-5-1-2; USA.

18 Campbell, R., Gupta, I., Heath, M., Ko, S.Y., Kozuch, M., Kunze, M., Kwan, T., Lai, K., Lee, H. Y., Lyons, M., Milojicic, D., O'Hallaron, D., Soh, Y. C.: 'Open cirrus TM cloud computing testbed: federated data centers for open source systems and services research', Usenix HOTCloud'09 Conference, 2009.pp. 1-10.

19 Buyya, R., Yeo, C. S., Venugopal, Broberg, J., Brandic, I.: 'Cloud computing and Emerging IT platforms: Vision, Hype, and Reality for delivering computing as the 5th utility', Future Generation Computer Systems, 2009, 25, (06), pp. 599-616.

20 Menasce, D., Ngo, P.: 'Understanding cloud computing: experimentation and capacity planning', Proc. Computer Measurement Group Conf., 2009.

21 Ghazi, Z., Doust Mohammadi, A.: 'Cyber intrusion detection on critical infrastructures', Journal of Control, 2018, 12, (3), pp. 77-90.

22 Besharati, E.: 'Intrusion detection in cloud computing with use of combinational machine learning algorithms', MSc. Thesis Submitted to Engineering Faculty of Chamran University, 2016, Iran.

23 Ibrahim, F., Hemayed, E.: 'Trusted cloud computing architectures for infrastructure as a service: survey and systematic literature review', Computers & Security, 2019, 82, pp. 196-226.

24 Ruan, Y., Durresi, A.: 'A trust management framework for clouds', Computer Communications, 2019, 144, (15), pp. 124-131.

25 Chiregi, M., Navimipour, N.: 'Cloud computing and trust evaluation: a systematic literature review of the state-of-the-art mechanisms', Journal of Electrical Systems and Information Technology, 2018, 5, (3), pp. 608-622.

26 Prufer, J.: 'Trusting privacy in the cloud', Information Economics and Policy, 2018, 45, pp. 52-67.

27 Zhang, P., Zhou, M., Fortino, G.: 'Security and trust issues in fog computing: a survey', Future Generation Computer Systems, 2018, 88, pp. 16-27.

28 Benad, J. (2018). Efficient calculation of the BEM integrals on arbitrary shapes with the FFT. Facta Universitatis, Series: Mechanical Engineering, 16(3), 405-417.

29 S. Haghgoo, M. Hajiali, A. Khabir, "Prediction and Estimation of Next Demands of Cloud Users based on their Comments in CRM and Previous usages", International IEEE Conference on Communication, Computing & Internet of Things; Feb. 2018, Chennai. DOI: 10.1109/IC3IoT.2018.8668119.

30 Wang, W., Zeng, G., Tang, D., Yao, J.: 'Cloud-DLS: dynamic trusted scheduling for cloud computing', Expert Systems with Applications, 2012, 39, (3), pp. 2321-2329.1

31 Petrović, G., Mihajlović, J., Ćojbašić, Ž., Madić, M., Marinković, D.Comparison of three fuzzy MCDM methods for solving the supplier selection problem(2019) Facta Universitatis, Series: Mechanical Engineering, 17 (3), pp. 455-469.

32 Marinković, D., Rama, G., Zehn, M.Abaqus imlementation of a corotational piezoelectric 3-node shell element with drilling degree of freedom(2019) Facta Universitatis, Series: Mechanical Engineering, 17 (2), pp. 269-283.

33 MOMENZADEH, M., NOROZPOUR, S., & BASHIROV, A. E. On Fractional Differential Operator over biα-Calculus.
34 Momenzadeh, M., & Norouzpoor, S. (2019). Study of new class of q-fractional derivative and its properties. arXiv preprint arXiv:1905.11115.

Samiyeh Khosravi is a lecturer in the Computer Engineering Department, University of Birjand, Iran. She received her B.Sc. degree in computer engineering in 2006 and her M.Sc. degree in IT Management from Alzahra University . Her research interests include Data Mining, Cloud Computing and Trust management.