Computers, Materials & Continua CMC, vol.65, no.3, pp.2543-2555, 2020

Research on Intelligent Mobile Commerce Transaction Security Mechanisms Based on Mobile Agent

Weijin Jiang[1, 2, 3], Wei Liu[2, *], Haolong Xia[1], Yuhui Xu[2], Dongbo Cao[1] and Guo Liang[4]

Abstract: In networked mobile commerce network transactions, trust is the prerequisite and key to a smooth transaction. The measurement of trust between entities involves factors such as transaction amount, transaction time, personal income of consumer entities and their risk attitude towards trust, etc., so it is difficult to accurately calculate quantitatively. In order to find out the essential characteristics of this trust relationship, based on the research background of mobile commerce in the mobile network environment, a dynamic trust mechanism is proposed through the research of trust in the mobile network environment, trust influencing factors and trust mechanism. The calculation model of mobile interactive services based on mobile service business transactions. The model calculates feedback credibility through feedback deviation and feedback robustness, and combines transaction context factors and trust mapping mechanism to judge the seller's credibility. This model better reflects the degree of influence of subjective factors such as personal preferences and risk attitudes on trust calculations, And the sensitivity of trust algorithms and transaction attributes has been greatly improved. After a large number of experiments and theoretical analysis, this mechanism provides an effective explanation for solving the problem of network trust computing. and provides valuable new ideas for the study of secure transactions in the mobile Internet environment.

Keywords: Mobile Internet, mobile commerce, dynamic trust model, reputation management, Mobile Agent System (MAS).

[1] College of Computer and Information Engineering, Hunan University of Technology and Business, Changsha, 410205, China.

[2] Institute of Big Data and Internet Innovation, Mobile E-business Collaborative Innovation Center of Hunan Province, Hunan University of Technology and Business, Changsha, 410205, China.

[3] Key Laboratory of Hunan Province for New Retail Virtual Reality Technology, Hunan University of Technology and Business, Changsha, 410205, China.

[4] School of Bioinformatics, University of Minnesota, Twin Cities, USA.

[*] Corresponding Author: Liu Wei. Email: 17762574410@163.com.

Received: 09 May 2020; Accepted: 08 June 2020.

1 Introduction

With the rapid development of mobile Internet (MI) technology. Moreover, mobile internet has promoted the sharing of consumption patterns, the intelligence of equipment and the diversification of scenarios. In recent years, most of the traditional e-commerce has been far outpaced by the growth rate of e-commerce. According to the 41st China Internet Development Statistical Analysis Report, the number of Internet users in China has reached an unprecedented level. Traditional e-commerce security protection methods focus on the confidentiality and integrity of information. These methods are based on identification, integrity verification, authentication, encryption, and access control. Therefore, there is an urgent need for a new method to solve this problem. It can be seen that integrity runs through the entire transaction process, which is the key to the smooth transactions. At the same time, this is also the most effective way to solve this problems [Chen, Sun and Liu (2012)].

Regarding the above shortcomings, based on long-term research on trust management, we have developed a mobile business transaction trust calculation model that can overcome these shortcomings. And transaction context factors are integrated with trust mapping. A mechanism for evaluating seller trust.

2 Related work

The trust relationship is a common social relationship that cannot be fully serviced. Its existence is not only abstract but also difficult to quantify. If there is no trust, it will be difficult for social groups to have a sense of trust with each other. At the same time, there will be variability and a lot of uncertainty before the trust relationship, which makes it more difficult to establish a model for quantification. And maintaining trust is very difficult [Gu, Yang and Yin (2018); Gan, Zeng, Ma et al. (2015); Gan, Ding, Li et al. (2011); Gan, Zeng, Li et al. (2012)]. The main task of establishing trust is to quantify the trust relationship and rely on this relationship to build a calculation model.

At the end of the twentieth century, the concept of online trust was just proposed. It was first proposed by the swamp. In the question of trust in this topic, the trust degree can be expressed by some symbols. According to the linear equation to solve the trust algorithm, the model is built to lay the foundation of the computer field [Hu and Tan (2018)]. Subsequently, Jiang et al. [Jiang, Wang, Jiang et al. (2020)] put forward trust management is an important direction of system security research. The important theory of trust management is proposed, which explains the relationship between trust behavior and trust. They use some symbols to define trust-related attributes in the theme. It lays a solid foundation for better application in computer-related fields, and proposes a dynamic analysis model for trust [Jiang, Xu, Guo et al. (2014); Liu, Wang, Lin et al. (2016); Li Duan and Cao (2018); Shao, Luo, Mei et al. (2012)]. The model uses a step-by-step method to filter recommended trust information. It uses the normal distribution function for modeling, so the dynamic model has greater immunity to interference and can avoid some deliberate destructive behavior.

Although REGRET is immature, the direction is accurate. Shen et al. [Shen, Zhang and Wang (2010)] constructed a formal model of a trust network based on a multi-agent system, but this model only considers the relationship between nodes and ignores trust.

Wang et al. [Wang, Gu and Liu (2019)] further studied the trust relationship between transaction entities in the e-commerce environment, and established a tool to automatically visualize the trust network. This model reduces the complexity of the trust measurement algorithm by optimizing the trust network. Wu et al. [Wu, Xiao, Qin et al. (2015); Xu, Zhong and Zheng (2015)] also consider adding reputation to the calculation method of trust, which injects many subjective factors into the evaluation of trust services.

In summary, in order to build a credit environment and promote the smooth operation of online transactions, it is urgent to continue to analyze the factors that the current trust model does not take into account. We establish a dynamic trust model to make it suitable for the mobile network environment. The trust model should have the following conditions.

For some of the above questions, this article draws on some of the research results published today, and combines the author's classic research results with the literature [Xu (2017); Xu, Si and Yang (2013); Yin, Ding and Wang (2019); You, Shang, Jing et al. (2017)], We implanted some attributes of social trust in the virtual e-commerce environment, and introduced a collaborative computing theory [Zhang and Xu (2013); Zhong, Chen and Sun (2018)], and a dynamic trust model based on MAS cooperation is proposed. The main contributions are as described in the introduction.

3 Online mobile transaction based on MAS trust model

In order to realize the above-mentioned trust calculation model and solve the credibility problem in the online transaction mechanism of the mobile internet, a dynamic trust calculation model of mobile agent e-commerce in a complex mobile network environment is proposed. This article also established a mobile business credit system and a secure transaction mechanism to ensure the normal order of mobile network transactions. The results of the relying party will be transmitted through public opinion, which will affect the behavior of others [Zhang and Xu (2013)]. Affected by self-motivation and other individuals, personal trust and trust-related behavior choices are uncertain and easy to change. The unique technical advantages of mobile agents such as intelligence, mobility, adaptability, initiative, and collaboration are very suitable for the development of mobile Internet and its business application systems [Zhang, Ma and Xi (2016)]. Therefore, we use it as a technical theory. The foundation of dynamic trust modeling.

3.1 Mobile transaction based on dynamic trust computing model

The definition of trust and reputation is explained as follows:

Definition 1 (trust) In the full text about mobile trust commerce, trusted user agents can infer agent judgments based on some relevant experience. which are also known as direct trust. Trust is usually the trustee's judgment of the trustee's ability and reliability. Agent partners are based on trust relationships. Therefore, the best way to choose a partner is to establish a good trust relationship.

Definition 2 (Reputation) Under the large-scale mobile commerce, reputation is never controlled by personal opinions, it is always obtained through the trust of other people on the phone.

Definition 3 (trust degree) We can quantify the credibility of the business through the degree of trust in customers.

Definition 4 (Trust Management) The main point of this concept is that there is an irreplaceable role in the entire trust and surplus. The process of user processing can be protected through the Internet, and it can also be interoperable.

The model is an extension and optimization of our model in the literature, but the model does not give the calculation method of the distance between nodes and the evaluation method of special attributes. To address the issue, we have extended the definition of trust. The significance of expansion lies in the establishment of a stable trust relationship between mobile nodes.

The trust level of user u at the specified time t can be calculated by Eq. (1):

$$\tau_t(\mathrm{u}) = \begin{cases} \alpha\tau_{t-1}(\mathrm{u}) + \beta \cdot \bar{f}(\mathrm{x},\mathrm{u}) \cdot \mathrm{e}^{\sum_{k\in N(\mathrm{u})} w[\mathrm{p(x,u)}]\cdot \mathrm{Cr}[\tau_{t-1}(\mathrm{x})]\cdot\rho(\mathrm{t}_x,\mathrm{t})} & , N(\mathrm{u}) \neq 0 \\ \tau_{t-1}(\mathrm{u}), & N(\mathrm{u}) = 0 \end{cases}. \tag{1}$$

In the interval [t-1, t], N(u) is mainly represented as the transaction set of user u. At t-1, $\tau_{t-1}(u)$ can be expressed as the degree of trust the user has at this moment. $\forall x \in N(u)$ Similarly, the degree of trust expressed as $\tau_{t-1}(x)$. $W[p(x,u)]$ refers to the weight function implied in value buying and selling. $Cr[\tau_{t-1}(x)]$ represents the weight value of x, and represents the credibility of x. $t_x \in [t-1,t]$ represents the time when users x and u conduct a trading transaction. $p(t_x,t)$ is expressed as a time value rate function, which only represents the proportion of reputation to time in the evaluation. When t_x is close to t, the user will show a high score because of the high weight of the reputation feedback evaluation.

$\rho(t_x,t) = \rho^{t-t_x}$, $0 < \rho < 1$, (where ρ is the time weighting factor) (2)

For transactions, we can use the symbols x and u to represent the agents and their reputation feedback. (3)

$$\bar{f}(x,u) = \frac{\sum_{i=1}^{|C|} \omega_{ci} f_{ci}(x,u)}{\sum_{i=1}^{|C|} \omega_{c_i}} c_i \tag{3}$$

Under the credit feedback evaluation of the agent $f_{c1}(x,u)$, we can evaluate c_i by the number of factors $f(x,u)=(f_{c1}(x,u),f_{c2}(x,u),\cdots\cdots,f_{cn}(x,u))$ of $c_1,c_2,\cdots\cdots c_n$, and under the conditions have an n-dimensional vector, that is to say, f(x,u) can be after the transaction between x and u Feedback between them on the degree of credit, which can represent the weight value of c_i.

3.2 Dynamic setting method of initial trust degree

In the era of the development of the mobile Internet, the influence of the degree of

credibility is a difficult problem to solve. The influence on the degree of trust of users is very important and necessary. In this article, we discussed two situations. The first one is that when the user's trust level value is particularly high, that is, when the user's trust level is much greater than the initial value, the user can use the original information. The second reason is trust. When the degree is low, it is lower than the initial value.

3.3 The method of trust punishment

From the perspective of environmental safety trust, there are many types of users, and they may fail with some bad intentions. For such situations, we will impose certain penalties. According to research, the punishment system implements the increase and decrease of trust value as a punishment process. The details are described below.

$$\tau_t(\mathrm{i}) = \tau_0 - (\mathrm{R}_i^{\max} - \mathrm{R}_i^{\min}) \times (1 - \frac{\sigma}{10}) \tag{4}$$

Regarding the penalty of trust value and the amount of purchase and sale, we can express it by the symbols τ_0, τ_t and σ. According to formula (5), we can divide the attribute into multiple levels to determine the $R_i^{\min}$ and $R_i^{\max}$ values. The formula for interval evaluation can be expressed as:

$$\sigma = \mathrm{R}_i^{\min} + \theta \times (\mathrm{R}_i^{\max} - \mathrm{R}_i^{\min}) \tag{5}$$

In formula (5), we can see that when i is above w/2, θ is higher than the horizontal line of i. When i is less than w/2, θ is much smaller than the weighted percentage.

Trust is very sensitive. For this feature, the model established in the paper can quickly reflect those malicious deceptions. However, there is another situation in which the punishment mechanism is necessary for some malicious users. T_0 is the length of the unit time, and each time the $|t_0|$ time is passed, τ_t attenuates one time. If the time for agentc to join the trust transaction network is initial, the time for trust evaluation of agentp is t. Here, t> initial, this interval spans a time window. Let the start time of the time window i (i=1, 2, ..., k) be tinitial_i and the end time is tend_i. Agentc trusts agentp in tinitial_itime as $\tau_{tinitial\_i}$ When the trust at tinitial_i time is $\tau_{tinitial\_i}$, then the time-sensitive function can be defined as:

$$sensitive(\tau_i) = \tau_{end\_i} \left(1 + \frac{\sum_{i=1}^{k} \tau_{end\_i} - \tau_{initial\_i} \Big/ \tau_{initial\_i}}{k} \right), \quad k = \left\lfloor \frac{t - t_{initial}}{t_0} \right\rfloor \tag{6}$$

4 Simulation experiments and performance analysis

4.1 Simulation environment and experimental steps

We estimate that the probability can be used to measure the performance of the trust model and the effectiveness of the model through the variance method. For example, the

pi of 41 merchants is uniformly distributed in the interval [0, 1], and pi can be set to multiple probability values, respectively [0, 0.025, 0.05, ..., 0.975, 1].

$$\Phi = \frac{1}{N_p}\sum_{i=1}^{N_p}(\mathrm{P}_i - \hat{P}_i)^2 \tag{7}$$

The execution steps of the simulation system are as follows.

(1) In the system, we chose a pair of $agent_e$ and $agent_p$ to conduct interactions between users and merchants. A total of 8200 times were generated, which means that each user and merchant must interact at least 20 times and generate users Existing historical information, the initial loop variable of $agent_p$ will start from i=1.

(2) Each scorer $agent_c$ will generate an evaluation based on the behavior of $agent_p$, and submit the evaluation result to the user $agent_c$.

(3) The user $agent_c$ will construct a message based on the exchange information between the merchant $agent_p$ and them that can be used to feed back to the $agent_c$ for querying information.

(4) User agents can respond to malicious behaviors based on the feedback they receive, and then use preventive methods to estimate the reputation of each $agent_p$.

(5) In this paper, we obtain the average variance error Φi which can be judged by Eq. (7).

(6) During the interaction between $agent_c$ and $agent_p$, we will let i++ sequentially according to the number of interactions.

The laboratory will be divided into two situations. The first situation is because in harsh environments, whether the system's defense performance can achieve optimistic results. The second is when all scoring users $agent_e$ have bad reputation, $agent_c$ will appropriately add its own experience when calculating the reputation of the merchant. This situation is also to compare the reliability and robustness of the model under special circumstances.

4.2 When the credit environment is at a level, the system's behavioral performance test checks

In the first case, the number of scoring user $agent_e$ in each experiment is set as shown in Tab. 1.

Table 1: Number of users per experimental $agent_e$

The type of Rating user $Agent_e$	Number of rating users $Agent_e$				
	1	2	3	4	5
fair	1	5	5	5	5
lying	0	5	0	0	0
noisy	0	0	5	0	0
Bad mouthing	0	0	0	5	0
bragging	0	0	0	0	5

After comparing Figs. 1 and 2, we demonstrate the filtering and prevention effects of user types. From the figure we can see that the biggest difference comes from the system. For example, when we encounter malicious attacks, it will cause Affect the reputation evaluation of the model system. In this paper, we have established a trust computing model, which has the same practicality as travos and E-FIRE.

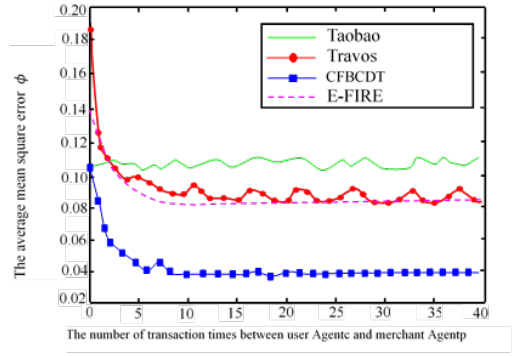

Figure 1: 50% of raters Agent$_e$ behavior prevention performance comparison

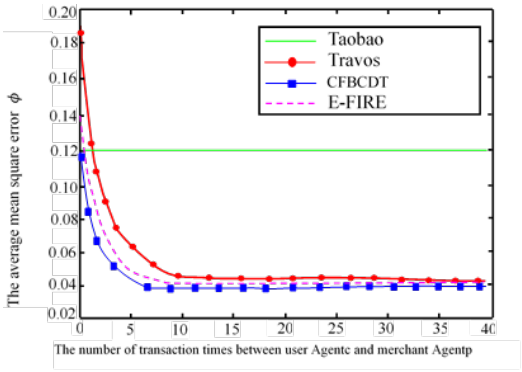

Figure 2: When the Agent$_e$ score is only 50, it will take action to prevent performance comparison

As time goes by, merchants and users spend more and more time interacting with each other, and the number of times has gradually increased, and Taobao's variance has gradually become lower than travos. For online transactions, this is also very good, because the number of times users buy things in the store in the physical store is less and less, so it is more willing to accept.

4.3 Experiments on reputation system preventive performance when introducing user agent's direct experience to all agents which are malicious behaviors

In the second case of the experiment, all agent$_e$ are malicious behaviors, Agent$_c$ will indirectly increase its own experience when calculating the reputation value of agent$_p$. This situation mainly compares the robust performance of the reputation system when the user agent$_c$ is in a very harsh environment. In each experiment, the number of agent$_e$ is shown in Tab. 2. The experimental results are shown in Figs. 3 and 4.

Table 2: The number of scoring users ($Agent_e$) in each experiment in the second case

Malicious $Agent_e$ type	Number of $Agent_e$			
	1	2	3	4
lying	10	0	0	0
noisy	0	10	0	0
badmouthing	0	0	10	0
bragging	0	0	0	10

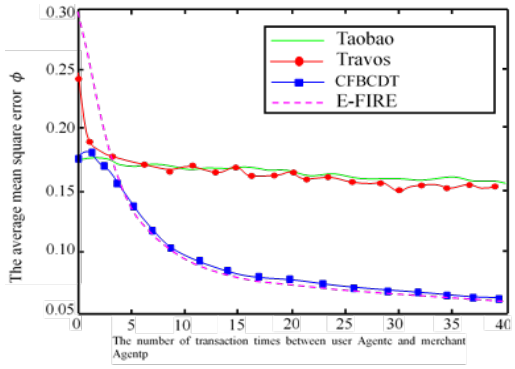

Figure 3: The direct experience of $Agent_c$ and the evaluation results of 10 noisy $Agent_e$

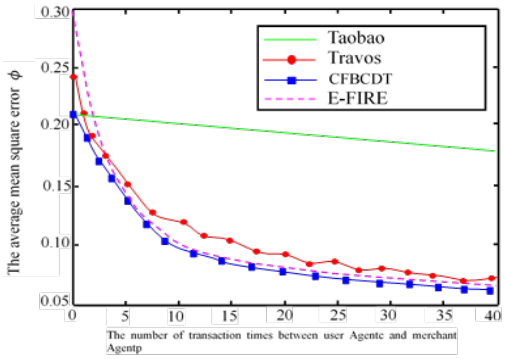

Figure 4: the direct experience of $Agent_c$ and the evaluation results of 10 badmouthing $Agent_e$

It can be seen from Figs. 3 to 4 that even if $agent_e$ next to $agent_c$ is a malicious behavior user, the filtering method and prevention technology can be applied to greatly reduce the influence of non-honesty malicious evaluation. The travos and E-FIRE models also produce errors that cannot be eliminated. Second, in response to badmouthing and bragging bad attacks, the calculation effect of the trust model of the paper has a situation in which all trading users are in a friendly environment. Third, When the number of interactions between the merchant $agent_p$ and the user $agent_c$ is relatively small, the

performance of the model is not much different from that of travos and E-FIRE models. In a very malicious situation, the overall effect of travos trust system is slightly better.

4.4 Algorithm convergence time and communication load evaluation analysis

4.4.1 Algorithm convergence time evaluation

In order to make the simulation experiment closer to the real mobile transaction scenario, and to make the node characteristics in the experiment closer to the characteristics of the nodes in the actual mobile transaction network, we set the nodes to enter and exit mobile transactions at will. This experiment compares and analyzes the convergence time of the trust models CMAIT, DDTM-TR and CFBCDT dynamic trust calculation. The experimental situation is shown in Fig. 6. The total number of agents increased from 99 to 9999, and 7 results were selected for comparative analysis during the experiment. It can be seen from Fig. 6. First, the convergence time of CMAIT is close to the convergence time of DDTM-TR, and the convergence time of DDTM-TR is shorter than that of CMAIT.

Second, the convergence time of CFBCDT is much lower than that of CMAIT and DDTM-TR third, the convergence time of the three models is proportional to the number of nodes participating in the transaction, and has a linear increasing characteristic. In the process of dynamic trust calculation, the most critical problem is convergence. The above experiments prove that CFBCDT effectively solves the convergence of dynamic trust calculation algorithms on mobile internet.

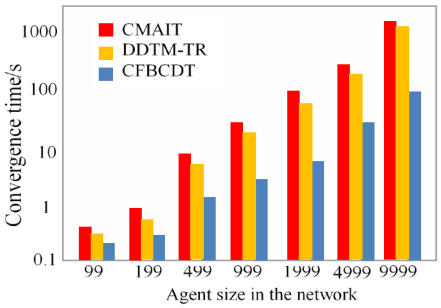

Figure 5: Comparison of convergence time

4.4.2 Dynamic trust calculation communication load analysis

The simulation experiment gives a comparison and analysis of the communication load required for the dynamic trust calculations of the trust models CMAIT, DDTM-TR, and CFBCDT. In the experimental process, the three models of trust computing are used to calculate the overall trust of five different mobile agents. The following two simulation experiments are done. In the first experiment, in order to calculate the overall trust of the mobile agent, the number of mobile agents n=999, the average transaction number of CMAIT, DDTM-TR and CFBCDT were 60.01, 31.97 and 29.98 respectively. The second experiment sets the number of mobile agent$_s$ n=9999. The experimental results are shown in Figs. 7 and 8. The average transaction number of CMAIT is 63012.01, DDTM-TR is 169987.06, and CFBCDT is 94699.13. This shows that (1) when n=999, the communication load of DDTM-TR and CFBCDT does not differ much from that of

CMAIT, which is lower than CMAIT; (2) When N=9999, the communication load of CFBCDT's overall trust calculation is much lower than CMAIT and DDTM-TR.

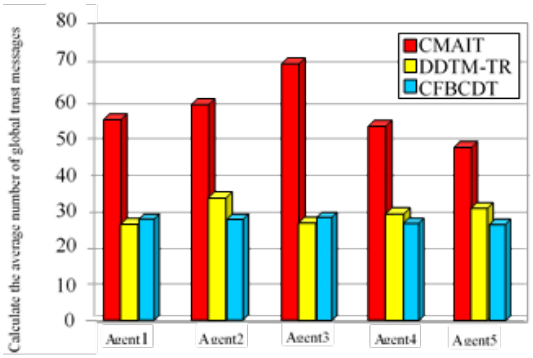

Figure 6: the average transaction number for calculating the overall trust degree at when N=999

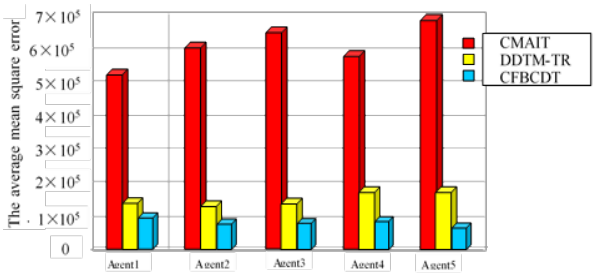

Figure 7: Average transaction count for trust calculation at N=9999

The above experiments show that CFBCDT can solve the communication load problem caused by mobile network dynamic trust calculation. With the increase in the number of participating transaction agents in the mobile network system, the communication load caused by CFBCDT is much smaller than that of CMAIT and DDTM-TR, indicating that CFBCDT can effectively handle large-scale mobile commerce interactive services.

5 Conclusion and next steps

In the business environment, the system mainly adopts the establishment of credibility between entities to solve the big data transaction problem for system evaluation. In this paper, there are various problems in current mobile transaction trust modeling and online transaction management. The main work and contributions of this paper are as follows. First, in the design of the trust calculation model, the time of scoring, the number of transactions, the transaction evaluation and the credibility of the scorer are introduced as the key factors to trust evaluation, thus solving the problem that the existing model can't accurately predict and judge the different behaviors of the participants. second, it solves the problem that many current models neglect to examine the credibility of transaction raters, and can effectively filter and eliminate the influence of malicious acts such as reputation squeezing and reputation defamation on transaction trust. Third, this paper solves the problem that the traditional reputation system cannot give the transaction users

a personalized evaluation by fully analyzing and applying the multi-dimensional characteristics of trust. Fourth, the paper improves the prevention and disciplinary measures against the bad behavior of traders, and changes the reliability and robustness of the trust model.

For the technology describing dynamic attributes and trust, we use cloud theory and mobile transaction methodology through the technical method of coordinated filtering, and establish a more powerful integrated computing method to make the whole world more capable of preventing risks, as well as node type identification And dynamic adjustment mechanism. A dynamic trust computing method and management technology are constructed.

Acknowledgment: The author is very grateful for the financial support of the new retail virtual reality technology (2017TP1026) of the key laboratory in Hunan Province.

Funding Statement: This work was supported by the National Natural Science Foundation of China (61772196; 61472136), the Key Social Science Fund of Hunan Provincial (2016ZDB006), the Social Science Achievement Review Committee Achievement Appraisal Research Project of Hunan Provincial (Hunan Social Assessment 2016JD05), the Key Social Science Achievement Review Committee of Hunan Provincial (XSP 19ZD1005), the Natural Science Foundation of Hunan Provincial (2020JJ4249), the Degree and Graduate Education Reform Research Project of Hunan Provincial (2020JGYB234), the Degree and Graduate Education Reform Project of Hunan University of Technology and Business (YJG2019YB13)), the Teaching Reform Project of Hunan University of Technology and Business (Xiaojiaozi [2020] No. 15) , and the Postgraduate Scientific Research Innovation Project of Hunan Province (CX20201074).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

Chen, H.; Sun, J. H.; Liu, C. (2012): A light-weight, secure and trusted virtual execution environment. *SCIENTIA SINICA Informationis*, vol. 42, no. 5, pp. 617-633.

Gu, K.; Yang, L. H.; Yin, B. (2018): Location data record privacy protection based on differential privacy mechanism. *Information Technology and Control*, vol. 47, no. 4, pp. 639-654.

Gan, Z. B.; Zeng, C.; Ma, Y.; Lu, H. W. (2015): C2c e-commerce trust algorithm based on trust network. *Ruan Jian Xue Bao/ Journal of Software*, vol. 26, no. 8, pp. 1946-1959.

Gan, Z. B.; Ding, Q.; Li, K.; Xiao, G. Q. (2011): Reputation-based multi-dimensional trust algorithm. *Journal of Software*, vol. 22, no. 10, pp. 2401-2411.

Gan, Z. B.; Zeng, C.; Li, K.; Han, J. J. (2012): Constrction and optimization of trust network in e-commerce environment. *Chinese Journal of Computers*, vol. 35, no. 1, pp. 27-37.

Hu, L. B.; Tan, L. (2018): Research on trusted virtual platform remote attestation method in cloud computing. *Journal of Software*, vol. 29, no. 9, pp. 2874-2895.

Jiang, W. J.; Wang Y.; Jiang Y. R.; Xu Y. H.; Chen J. H. et al. (2020): Mobile internet mobile agent system dynamic trust model for cloud computing. *Computers, Materials & Continua*, vol. 62, no. 1, pp. 123-136.

Jiang, W. J.; Xu, Y. S.; Guo, H.; Zhang, L. M. (2014): Multi agent system-based dynamic trust calculation model and credit management mechanism of online trading. *Science China: Information Science*, vol. 44, no. 9, pp. 1084-1101.

Liu, C. Y.; Wang, G. F.; Lin, J.; Fang, B. X. (2016): Practical construction and audit for trusted cloud execution environment. *Chinese Journal of Computers*, vol. 39, no. 2, pp. 339-350.

Li, J. Q.; Duan, P. Y.; Cao, J. D. (2018): A hybrid pareto-based tabu search for the distributed flexible job shop scheduling problem with e/t criteria. *IEEE Access*, vol. 1, no. 1, pp. 99-108.

Shao, K.; Luo, F.; Mei, N. X.; Liu, Z. T. (2012): Normal distribution based dynamical recommendation trust model. *Journal of Software*, vol. 23, no. 12, pp. 3130-3148.

Shen, C. X.; Zhang, H. G.; Wang, H. M. (2010): Research on trusted computing and its development. *Science China Information Sciences*, vol. 40, no. 2, pp. 139-166.

Wang, J.; Gu, X. J.; Liu, W.; Sangaiah, A. K.; Kim, H. J. et al. (2019): An empower hamilton loop based data collection algorithm with mobile agent for wsns. *Human-Centric Computing and Information Sciences*, vol. 9, no. 1, pp. 1-14.

Wu, T.; Xiao, J.; Qin, K.; Chen, Y. X. (2015): Cloud model-based method for range constrained thresholding. *Computers & Electrical Engineering*, vol. 42, no. 2, pp. 33-48.

Xu, J.; Zhong, Y. S.; Zheng, Y. F. (2015): A trust evaluation approach of multi-dimensional integrated intuitionistic fuzzy information. *Computer Engineering & Science*, vol. 37, no. 9, pp. 1777-1782.

Xu, J. (2017): Survey of trust model based on uncertainty theory. *Journal of Chinese Computer Systems*, vol. 38, no. 1, pp. 99-106.

Xu, J.; Si, G. N.; Yang, J. F. (2013): An internetware dependable entity model and trust measurement based on evaluation. *Sci Sin Inform*, vol. 43, no. 1, pp. 108-125.

Yin, C. Y.; Ding, S. L.; Wang, J. (2019): Mobile marketing recommendation method based on user location feedback. *Human-Centric Computing and Information Sciences*, vol. 9, no. 1, pp. 1-17.

You, J.; Shang, G.; Jing, L.; Xu, S. K. (2017): Distributed dynamic trust management model based on trust reliability. *Journal of Software*, vol. 28, no. 2, pp. 1-15.

Zhang, S. B.; Xu, C. X. (2013): Study on the trust evaluation approach based on cloud model. *Chinese Journal of Compute*, vol. 36, no. 2, pp. 422-431.

Zhong, X. Y.; Chen, G. Q.; Sun, L. L. (2018): Mining mobile information service patterns based on multi-view features fusion. *Systems Engineering-Theory & Practice*, vol. 38, no. 7, pp. 1853-1861.

Zhang, S. B.; Xu, C. X. (2013): Study on the trust evaluation approach based on cloud model. *Chinese Journal of Computes*, vol. 36, no. 2, pp. 422-431.

Zhang, T.; Ma, J. F.; Xi, N. (2016): Trust-based decentralized service composition approach in service-oriented mobile social networks. *Acta Electronica Sinica*, vol. 44, no. 2, pp. 258-267.