Computers, Materials & Continua
DOI: 10.32604/cmc.2023.033798
Article

Tech Science Press

A Transaction Frequency Based Trust for E-Commerce

Dong Huang[1,*] **and Sean Xu**[2]

[1]School of Applied Foreign Languages, Zhejiang Yuexiu University, Shaoxing, 312000, China
[2]Anzina PTY Ltd., Sydney, NSW, 2118, Australia
*Corresponding Author: Dong Huang. Email: 563741855@qq.com

Received: 28 June 2022; Accepted: 26 September 2022

Abstract: Most traditional trust computing models in E-commerce do not take the transaction frequency among participating entities into consideration, which makes it easy for one party of the transaction to obtain a high trust value in a short time, and brings many disadvantages, uncertainties and even attacks. To solve this problem, a transaction frequency based trust is proposed in this study. The proposed method is composed of two parts. The first part is built on the classic Bayes analysis based trust models which are ease of computing for the E-commerce system. The second part is the transaction frequency module which can mitigate the potential insecurity caused by one participating entity gaining trust in a short time. Simulations show that the proposed method can effectively mitigate the self-promoting attacks so as to maintain the function of E-commerce system.

Keywords: Transaction frequency; trust; Bayes analysis; E-commerce

1 Introduction

With the rapid development of the Internet and big data, E-commerce is booming. The E-commerce platform has changed the traditional marketing mode and achieved explosive development. The E-commerce platform is convenient, efficient and open. It has broad prospects for development and huge room for growth. However, due to the openness of the Internet, anyone can trade goods on the E-commerce platform at any time and any place. In addition, the particularities of E-commerce platform transactions, such as being unable to access physical goods and real enterprises, have increased transaction uncertainty and risk, and related problems have become more and more prominent. E-commerce brings convenience to people, but it also inevitably brings risks. Therefore, the trust and security of E-commerce have become a crucial issue restricting the further development of E-commerce. At present, due to the imperfect trust mechanism of E-commerce platform, it is particularly necessary to establish or enhance the trust among the participating parties of E-commerce transactions in order to promote the sustainable, rapid and healthy development of E-commerce. Trust management is a very important research field, which involves sociology, psychology, artificial intelligence, management and many other aspects. Trust has become one of the key problems to be solved urgently in the development of E-commerce. In order to reduce the risk, a safe and effective E-commerce trust mechanism should be established.

However, most traditional trust computing models do not take the transaction frequency among participating entities into consideration, it brings many disadvantages, uncertainties and even attacks and frauds. The main contribution of this study is that a transaction frequency based trust for E-commerce is proposed to address the trust problems. The proposed method is composed of two parts. The first part is built on the classic Bayes analysis based trust models which are ease of understanding and computing. But one problem is that these traditional trust methods cannot prevent malicious entities from gaining higher trust in a short time. The second part is the transaction frequency module which can effectively deal with the problem. Simulations show that our proposed method can effectively alleviate the self-promoting attacks so as to maintain the function of E-commerce system.

The organization of this research is as follows. In Section 2, we give a relatively comprehensive overview of the current trust study in E-commerce. In Sections 3 and 4, we study and analyze the classic trust computing model based on Bayes analysis including the essential components, main functions, and related mechanisms. Our proposed transaction frequency based trust and the related simulations are presented in Sections 5 and 6 respectively, and Section 7 concludes this work.

2 Related Works

To develop E-commerce, it is critical to establish e-trust and ensure information security. Most existing literatures mainly focus on two aspects: one is the theoretical research on how trust and information security can promote the development of E-commerce; the other is the technical research on the effective realization of trust and information security, including models, algorithms, mechanism designs, etc.

Reference [1] employed a logit model to identify and estimate determinants promoting E-commerce and e-trust, which included digital skills, online literacy, internet accessibility, data protection, etc. It emphasized the importance of trust for the development of E-commerce. Besides, equality education helps to boost E-commerce and e-trust. In turn, the building of electronic trust promotes the use of more digital resources. Reference [2] introduced a basic framework and method of trust measurement in E-commerce, including secret key, digital signature, evidence theory, probability analysis, path algebra, Bayesian network, etc. It described representative trust models in different categories, and then summarized the definition, purpose, measurement, algorithm and other aspects of these models. Reference [3] summarized trust mode and trust influence factors of E-commerce from the view of transaction mode and transaction process. It sorted out trust algorithms, summarized the trust mechanism constructed from the process of E-commerce transaction, and integrated trust mechanism using blockchain into interpersonal network. Reference [4] examined the complicated effects of trust and distrust on a buyer's purchase intentions. It found that trust can transfer from an intermediary to its seller, distrust in an intermediary can negatively influence his or her purchase intentions, and credible guarantee and good website quality of an intermediary give a positive impact on buyer's trust in the intermediary.

Reference [5] applied trust transfer theory, perceived risk, and alternative website quality to study repurchase intention. The results show that perceived risk (customer duty risk, confiscation risk, delivery risk, financial risk, and privacy risk), trust in provider, and trust in website affect repurchase intention significantly, where trust in website plays a critical role. Reference [6] evaluated the correlation between the Alexa rank (ranking) and the formal measure of trust in the electronic space by the Moore trust method, connection function (Copula function), etc. Their findings indicate that the trust in the websites is highly correlated with their reputation. Therefore, people can trust in the reputation of the E-commerce websites, and make a deal with them. Reference [7] examined the impact of changing the user interface on user trust through cross-sectional analysis and empirical research, indicating that the trust is very dependent on the user interface in E-commerce. Reference [8] analyzed 311 respondents data from Online to Offline, or O2O E-commerce users in Greater Jakarta Area with Structural Equation Modeling (SEM) to probe into factors affecting the loyalty of E-commerce customers. The results show that multi-channel integration and trust have a significant impact on customer loyalty both online and offline, which will greatly drive customer repurchase intention.

Reference [9] established a purchase intention model of Cross-Border E-commerce (CBEC) to study the influence of consumer trust on purchase. It used a questionnaire survey to collect data for simulation. And the regression results show that, five dimensions (trust, third-party authentication, website reputation, perceived security protection and privacy protection, perceived information quality) have significant impact on purchase intentions. However, this paper does not consider the demographic characteristics of consumers in issues, which has certain limitations in explaining specific consumption intentions. Reference [10] gave a formal description model of trust network, proposed a set of construction methods and optimization algorithm of trust network, defined a trust network description language, and developed a trust network visualization system. It laid foundation for the trust communication mechanism. Reference [11] established a trust evaluation index system combining the basic enterprise information and specific transaction information, constructed a Business to Business (B2B) trust evaluation model based on multi-agent, and conducted simulation experiments on the model. This research has certain significance for enterprises to choose appropriate partners in E-commerce and solve the trust problem in cooperation.

Reference [12] proposed a slope one algorithm (soa) based on fusion of trusted data and user similarity. Similarity is added to the weight factor of the improved slope one algorithm for multiple recommendation systems, the new soa is more accurate than traditional one. Reference [13] proposed a trust computation model based on various influencing factors, such as transaction amount, transaction completion time, and the credence of transaction object itself. In addition, the guarantee mechanism, reward and punishment mechanism are used to overcome the unfairness of the current trust management system to new users and the existing "free rider phenomenon". Reference [14] further divided the trust into direct trust and propagation of trust.

Reference [15] constructed a trust model based on reputation mechanism, including trade behavior analysis of identity nodes, design of partial and global reputation measurement models, and factors of influence. The model can accurately describe the influence of honest judgment on service mechanism in Peer to Peer, or P2P E-commerce. Reference [16] computed the direct trustworthiness of the buyer to the seller by transaction experience between them, then computed the reference trustworthiness from the buyer's friends in trust network, and finally acquired trust of the buyer to the seller through the integration of direct trustworthiness and reference trustworthiness with the trust adjusting factors. Reference [17] proposed a collaborative filtering algorithm based on the enhanced similarity and implicit trust. It introduced an enhanced similarity based on user preference, incorporated the user's interaction experience into the computation of direct trust, and fused users enhance similarity with trust. The new algorithm improved recommendation quality significantly. Reference [18] studied the statistical characteristics of shilling attacks user in recommendation scenarios containing trust information, and proposed an algorithm to detect them in trust networks. The algorithm can identify shilling attacks user accurately and enhance the robustness of the system.

Reference [19] proposed a fine-grained trust model for P2P E-commerce system, integrated time, transaction amount with other influencing factors, and measured the trust degree of nodes. The computation method of initial trust given by the model accelerated the speed of nodes approaching the real value. After that, they further expanded the model to consider the impact of different relationships between domains on recommendation reliability, they also used updated methods of Bayesian network and domain model to effectively curb the malicious behavior of nodes [20]. Reference [21] formulated effective trust management and attack defense measures for a variety of network attacks by making use of the technical advantages of software-defined networking, or SDN. By jointly utilizing the security resources of the perception layer, the forwarding layer and the control layer, the security functions such as trust management, DDoS (Distributed Denial of Service) attack detection, DDoS attack trace back and attack mitigation are realized from the bottom to the top. Reference [22] proposed a seller selection strategy for individual consumers. This strategy integrated trust and distrust, users' credibility and incredibility in social networks, updated a whitelist and a blacklist, and it was more robust than other defensing strategies.

3 Trust Mechanism

In social activities, trust intention or trust behavior consists of the following parts: trusted belief, system trust, situational trust and intentional trust [23–26]. Trust belief refers to the belief that one party believes that the other party is willing and able to act according to the wishes of others; system trust refers to the use of appropriate non-human organization structure to ensure reliable behavior in the future; intentional trust refers to the general trust expectation of other entities gradually established along with the evolution of the entity's life cycle; situational trust is applicable to trust. The benefit of trust behavior is greater than the negative impact of credible behavior. In the above, only trust belief and system trust are related to the concept of trust in computer networks, and the most suitable one to describe the concept of computer network trust is belief, that is, one entity believes that another entity's actions will be carried out in a certain way or that the network that constitutes the entity will operate in a certain way [27–30].

According to [31], trust is a belief in the aspects of reliability, integrity, and ability of an entity, while reputation is the evaluation of direct or indirect knowledge and experience derived from the past contact with an entity, and reputation is an evaluation of the degree of entity trust. The definition of trust value usually adopts certain policies and credentials. Therefore, if the behavior of an entity meets the requirements of the established policy system, it will have a higher trust value, otherwise, the opposite is true [32,33].

Generally, a standard trust system consists of five parts [34]: information collection, information evaluation, entity selection, transaction execution and reward and punishment mechanism shown in Fig. 1.

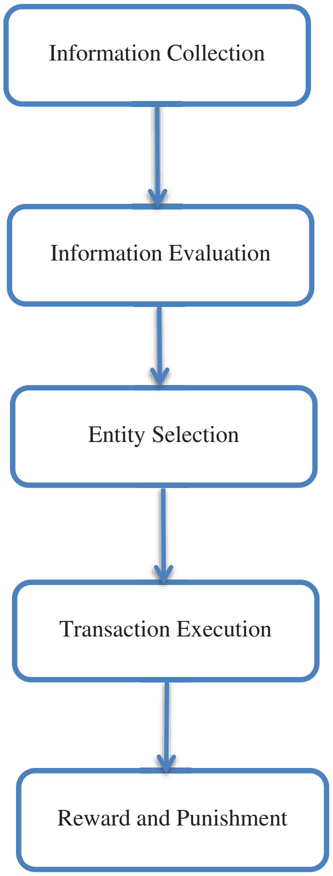

Figure 1: Trust system in [34]

4 Trust Computing

Trust is a relationship between two entities, namely, the trustor believes, expects and accepts that the trusted party will perform or intend to perform good behavior [35]. Trust relationship describes a kind of mutual relationship, which is established by two entities in the process of completing a given transaction. For example, in a service providing transaction, when the service is successfully provided, the service provider is considered to be with good behavior, and its trust value will be increased; on the contrary, when providing no service or unqualified service, the provider will lose its trust value. In this mechanism, trust will greatly improve the security of the system. In fact, trust mechanism provides a necessary reliability for point-to-point information exchange [35].

Among various trust computing methods for E-commerce, the Bayes analysis and the related Beta distribution and binomial distribution have received much attention due to their ease of understanding and computing. Suppose that x_1 and x_2 are two entities acting as a buyer and a seller in an E-commerce transaction, respectively. And let a and b denote the historical successful and unsuccessful transactions between the two entities. Before the next transaction, the trust value $T_{1,2}$ about x_2 kept by x_1 is defined by

$$T_{1,2} = E\left(Beta\left(\alpha, \beta\right)\right) = \frac{\alpha}{\alpha + \beta} \tag{1}$$

where the beta distribution with the shape parameters (α, β) can be expressed by using the gamma function as below.

$$f(\varphi) = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)}\varphi^{\alpha-1}(1-\varphi)^{\beta-1} \tag{2}$$

It can be noticed that the historical successful and unsuccessful transactions can be regarded as the two shape parameters in the Beta distribution. Therefore, Eq. (1) can be considered as the historical trust about x_2 held by x_1. Further, in Bayes analysis, the posterior distribution of binomial distribution is also Beta distribution. x_1 can refer to this trust value to decide whether or not to trade with x_2 next time. If it does, then the update of $T_{1,2}$ is defined by

$$T'_{1,2} = E(Beta(\alpha+1, \beta+1)) = \frac{\alpha+1}{\alpha+1+\beta+1} \tag{3}$$

where the beta distribution with the shape parameters can be expressed by using the gamma function as below.

$$f(\varphi') = \frac{\Gamma(\alpha+1+\beta+1)}{\Gamma(\alpha+1)\Gamma(\beta+1)}\varphi'^{\alpha}(1-\varphi')^{\beta} \tag{4}$$

More details about the Bayes trust computing are recommended to refer to [36].

In the practical E-commerce transactions, there are usually multi participants and the above trust computing is only for direct trust through direct observation. In fact, using only the direct trust obtained through direct observation may cause the result to be flawed with subjectivity, incomprehensibility, and not making full use of all available indirect trust information from the multi participants.

Dempster Shafer theory [37] is a classic method to deal with the indirect trust. It uses opinion to describe the credibility of a statement. The opinion is a triple (belief, disbelief, uncertainty), e.g., the opinion of entity X to Y is expressed as

$$O_Y^X = \left(b_Y^X, d_Y^X, u_Y^X\right),\ b+d+u=1 \tag{5}$$

Let $O_T^Y = \left(b_T^Y, d_T^Y, u_T^Y\right)$ denote Y's opinion on T, then X's opinion on T through Y is $O_T^{X:Y} = \left(b_T^{X:Y}, d_T^{X:Y}, u_T^{X:Y}\right)$ and according to [37], $b_T^{X:Y}, d_T^{X:Y}, u_T^{X:Y}$ satisfies

$$b_T^{X:Y} = b_Y^X b_T^Y,\ d_T^{X:Y} = d_Y^X d_T^Y,\ u_T^{X:Y} = d_Y^X + u_Y^X + b_Y^X u_T^Y \tag{6}$$

Map Eq. (6) to Beta distribution, we can get

$$b = \frac{\alpha}{\alpha+\beta+2},\ d = \frac{\beta}{\alpha+\beta+2},\ u = \frac{2}{\alpha+\beta+2} \tag{7}$$

And the indirect trust components can be obtained as follows.

$$\begin{cases} \alpha_{1,3}^2 = \alpha_{1,3} + \dfrac{2\alpha_{1,2}\alpha_{2,3}}{\left(\beta_{1,2}+2\right)\left(\alpha_{2,3}+\beta_{2,3}+2\right)+2\alpha_{1,2}} \\ \beta_{1,3}^2 = \beta_{1,3} + \dfrac{2\alpha_{1,2}\beta_{2,3}}{\left(\beta_{1,2}+2\right)\left(\alpha_{2,3}+\beta_{2,3}+2\right)+2\alpha_{1,2}} \end{cases} \tag{8}$$

5 Transaction Frequency Based Trust

Generally, among the various E-commerce transactions, entity a may only have a limited number of transactions with entity b, and the number of transactions with entity c is much more than that with entity b. However, due to the limitations of the above trust computing model, the trust on entity b could be equal to or higher than that on entity c. The establishment of trust is a long-term interaction process between entities. Although a short-term successful transactions can improve the trust value of one party, this method will bring many disadvantages, uncertainties and even attacks and frauds. Although a long-term transactions may experience successful ones and unsuccessful ones between entities, the trust establishment could be slow but relative reliable. To address this problem, a trade-off must be made and a transaction frequency based trust is proposed in this study. The transaction frequency based trust is defined as

$$T_f = w_1 \frac{n_i}{\sum n_i} \left(\frac{\alpha + 1}{\alpha + 1 + \beta + 1} \right) + w_2 T_{indirect} \tag{9}$$

where $w_1 + w_2 = 1$ and they are weight values for the direct trust and indirect trust respectively, and n_i denote one of the participating entities that a given entity makes transactions with. Notice that the more the participating entity transacts with the given entity, the higher trust value it may obtain. With the transaction frequency based trust, several attacks such as self promoting can be effectively mitigated in the E-commence.

In self-promoting attacks, malicious entities seek to falsely increase their own trust. Essentially, such an attack is to take the advantage of the trust computing model, and to explore the weaknesses of the trust calculation. Self-promoting attacks can further be launched by a group of malicious entities to form colluding attacks, in which they work with each other to increase or usually decrease a third party so as to more effectively launch the attacks. E-commerce systems are vulnerable to such attacks due to the difficulty for them to tell real trust feedback from false one.

6 Simulations

In this section, our proposed method, namely transaction frequency based trust, or TFT is tested against the self-promoting attacks, and classic trust method in [36] is selected as the baseline for comparison. Test settings are as follows. Suppose that three kinds of participating entities coexist in a certain E-commerce transaction, i.e. normal, malicious and selfish. Normal entities participate in the transaction with others and provide positive trust feedback after the transaction, thus they keep constant high trust values all along. While malicious entities also take part in the transaction, but they constantly switch between providing false trust feedback and positive one after the transaction so that they can obtain decent trust values before launching the attack. After finishing the transactions, selfish entities might selectively provide trust feedback. Assume that there are 100 entities in the transaction and these three kinds of entities are evenly distributed. Among them, 70 are normal entities, 20 are malicious and 10 are selfish. It is also assumed that each entity has an initial trust of 0.5. Test results are presented in Figs. 2–4.

It can be seen from Fig. 2 that with the increasing number of transactions, the mean trust of the normal entities of the two methods increases, but the mean trust of the proposed method increases faster. For example, in the 60th transaction, the proposed method has about 0.76 and 0.71 respectively, while that of the comparison method is about 0.62. This is because in the comparison method, malicious entities often provide false feedback, and the normal entities trading with these entities are affected to a certain extent, resulting in the decline of the trust of some normal entities, thus affecting the mean trust of all normal entities. By contrast, due to the application of the transaction frequency based trust mechanism in the proposed method, malicious entities have less impact on normal ones. Notice that in Fig. 2, the proposed method provides two different sets of parameters, namely (w1 = 0.6, w2 = 0.4) and (w1 = 0.4, w2 = 0.6). From the test results, it can be seen that when there exist malicious entities such as 20%, giving a smaller weight to the direct trust and a larger weight to the indirect trust is conducive to restraining the negative impact of malicious entities on normal ones. Thus the main purpose of setting different w1 and w2 values is to adjust the weight of direct trust and indirect trust. When there are many malicious entities, a larger w2 value can be set to suppress their negative impact on the transactions.

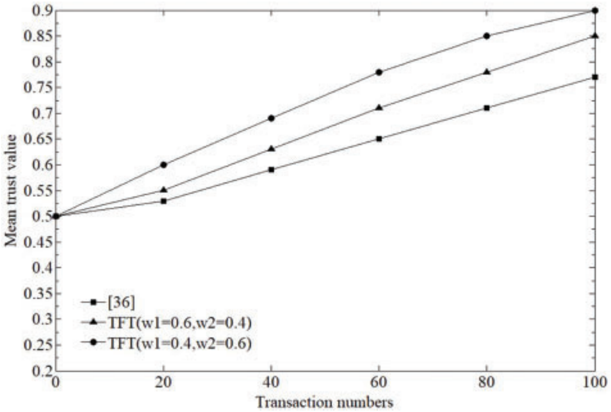

Figure 2: Mean trust value of normal entities

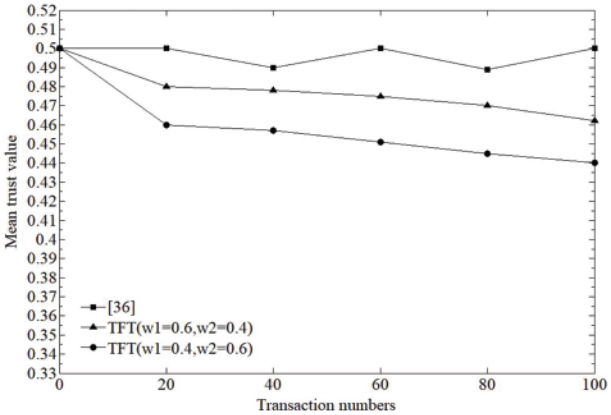

Figure 3: Mean trust value of selfish entities

As mentioned above, the selfish entities will selectively provide trust feedback. Because the evaluation of trust is mutual, this will not only affect the trust of the trading entities, but also affect the trust of the selfish entities themselves. In Fig. 3, the mean trust of the selfish entities in the comparison method always fluctuates around 0.5. In the proposed method, the less trust feedback the selfish entity provides, the more its trust will be affected. Therefore, in the proposed method, the mean trust of the selfish entity declines faster. Similar to Fig. 2, giving a smaller weight to direct trust also helps to degrade the trust of selfish entities faster. Further, in Fig. 4, malicious entities constantly switch between providing false trust feedback and positive one after the transaction, resulting in their mean trust fluctuation between 0.5 in the comparison method. While in the proposed method, because the transaction frequency mechanism, their negative impact on the normal entities is effectively alleviated, and their false feedback is also easier to be detected by the normal entities.

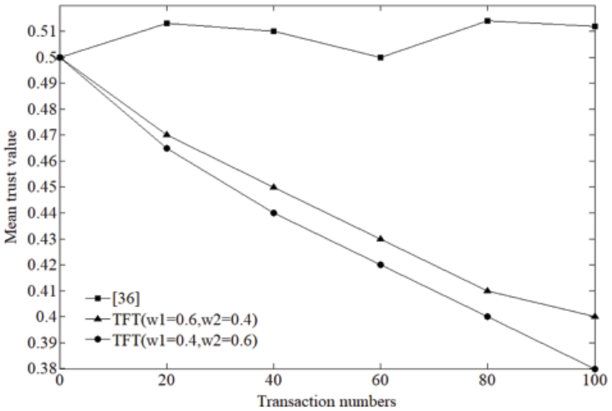

Figure 4: Mean trust value of malicious entities

7 Conclusion

The trust and security of E-commerce have become the key issues restricting the further development of E-commerce. However, most traditional trust computing models do not consider the transaction frequency between participating entities, which makes it easy for one party especially for malicious entities to obtain a high trust value in a short time. To solve this problem, this study proposes an E-commerce trust model based on transaction frequency, which is also further verified by the simulations. In addition, as is shown in the simulation section, different w1 and w2 values will mitigate the impact of malicious entities on the transactions to different levels, but how to select proper w1 and w2 values so that they can be of full benefit to the transactions are still worth studying which will be our future study direction.

Acknowledgement: The authors would like to thank the anonymous reviewers for the suggestion.

Funding Statement: The authors received no specific funding for this study.

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

References

[1] F. F. Bonilla, C. Gijon and B. D. Vega, “E-commerce in Spain: Determining factors and the importance of the e-trust,” *Telecommunications Policy*, vol. 46, no. 1, pp. 1–12, 2022.

[2] Y. Zhang, H. J. Chen and X. H. Jiang, “A survey of trust management for E-commerce systems,” *Electronic Journal*, vol. 36, no. 10, pp. 2011–2020, 2008.

[3] L. Chen, “A survey of E-commerce trust,” *China’s Collective Economy*, vol. 23, no. 1, pp. 73–74, 2019.

[4] S. J. Lee, C. Ahn, K. M. Song and H. Ahn, “Trust and distrust in E-commerce,” *Sustainability*, vol. 10, no. 1, pp. 1–19, 2018.

[5] M. Jian, C. Yi and K. Kurcz, “Trust, risk and alternative website quality in B-buyer acceptance of cross-border E-commerce,” *Journal of Global Information Management*, vol. 28, no. 1, pp. 167–188, 2020.

[6] I. Najafi, M. Kamyar and A. Kamyar, "Investigation of the correlation between trust and reputation in B2C E-commerce using Alexa ranking," *IEEE Access*, vol. 5, no. 1, pp. 12286–12292, 2017.

[7] N. Yashmi, E. Momenzadeh and S. T. Anvari, "The effect of interface on user trust; user behavior in E-commerce products," in *Proc. Int. Design Conf.*, Croatia, pp. 1589–1596, 2020.

[8] I. D. Savila, R. N. Wathoni and A. S. Santoso, "The role of multichannel integration, trust and offline-to-online customer loyalty towards repurchase intention: an empirical study in online-to-offline (O2O) E-commerce," *Procedia Computer Science*, vol. 161, no. 1, pp. 859–866, 2019.

[9] Y. Sun and Y. R. Li, "The impact of risk-aware consumer trust on CB E-commerce platforms and purchase intention," *Journal of Global Information Management*, vol. 30, no. 3, pp. 1–13, 2021.

[10] Z. B. Gan, C. Zeng, K. Li and J. J. Han, "Construction and optimization of trust network in E-commerce environment," *Chinese Journa of Computers*, vol. 35, no. 1, pp. 27–37, 2012.

[11] H. M. Sun and W. N. Zou, "Research on the B2B trust evaluation model based on multi-agent under the E-commerce environment," *Operations Research and Management Science*, vol. 23, no. 5, pp. 231–236, 2014.

[12] L. L. Jiang, Y. T. Cheng, L. Yang and J. Li, "A trust-based collaborative filtering algorithm for E-commerce recommendation system," *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, no. 1, pp. 3023–3034, 2018.

[13] W. X. Hu and N. Z. Cheng, "The research of trust value calculating model in the electronic commerce," *E-commerce*, vol. 9, no. 1, pp. 61–65, 2007.

[14] S. Z. Zhang and H. D. Zhong, "Mining users trust from E-commerce reviews based on sentiment similarity analysis," *IEEE Access*, vol. 7, no. 1, pp. 13523–13535, 2019.

[15] J. L. Wang, "Trust model based on reputation mechanism in P2P E-commerce," *Business Economic Research*, vol. 7, pp. 77–80, 2018.

[16] Z. B. Gan, C. Zeng, Y. Ma and H. W. Lu, "C2C E-commerce trust algorithm based on trust network," *Journal of Software*, vol. 26, no. 8, pp. 1946–1959, 2015.

[17] Z. B. Gan, C. Zeng, Y. Ma, H. W. Lu, P. Zheng *et al.,* "C2C E-commerce trust algorithm based on trust network, Recommendation algorithms based on enhanced similarity and implicit trust," *Journal of Software*, vol. 26, no. 8, pp. 1946–1959, 2018.

[18] X. Zhang and G. Huang, "Trust-based shilling attacks user detection algorithm," *Applications and Software*, vol. 37, no. 11, pp. 286–291, 2020.

[19] J. F. Tian, R. Tian, L. D. Yang and C. Li, "The fine-grain trust model based on merchandise domain for P2P E-commerce systems," *High Technology Communication*, vol. 20, no. 4, pp. 371–378, 2010.

[20] J. Tian and R. Tian, "A fine-grain trust model based on domain and bayesian network for P2P E-commerce system," *Journal of Computer Research and Development*, vol. 48, no. 6, pp. 974–982, 2011.

[21] R. Wang, "Research on trust management and attack defense mechanisms for software-defined internet of things," Ph.D.dissertation, Shandong University, China, 2018.

[22] H. Ma, Y. Liang, S. Ji and D. Li, "A trust-distrust based reputation attacks defending strategy and its stability analysis," *Journal of Computer Research and Development*, vol. 55, no. 12, pp. 2685–2702, 2018.

[23] J. Cheng, J. Li, N. Xiong, M. Chen and H. Guo, "Lightweight mobile clients privacy protection using trusted execution environments for blockchain," *Computers, Materials & Continua*, vol. 65, no. 3, pp. 2247–2262, 2020.

[24] S. Kaur and V. K. Joshi, "Hybrid soft computing technique based trust evaluation protocol for wireless sensor networks," *Intelligent Automation & Soft Computing*, vol. 26, no. 2, pp. 217–226, 2020.

[25] L. Sun, Q. Yu, D. Peng, S. Subraman and X. Wang, "Fogmed: A fog-based framework for disease prognosis based medical sensor data streams," *Computers, Materials & Continua*, vol. 66, no. 1, pp. 603–619, 2021.

[26] V. Nivedita and N. Nandhagopal, "Trust management-based service recovery and attack prevention in manet," *Intelligent Automation & Soft Computing*, vol. 29, no. 3, pp. 771–786, 2021.

[27] T. M. Navmani and P. Yogesh, "Trust based secure reliable route discovery in wireless mesh networks," *KSII Transactions on Internet and Information Systems*, vol. 13, no. 7, pp. 3386–3411, 2019.

[28] X. Chen and L. Wang, "A cloud-based trust management framework for vehicular social networks," *IEEE Access*, vol. 5, pp. 2967–2980, 2017.

[29] J. Wu, Z. G. Chen and M. Zhao, "Effective information transmission based on socialization nodes in opportunistic networks," *Computer Networks*, vol. 129, no. 10, pp. 297–305, 2017.

[30] S. Haibo, Z. Kechen and Z. Hong, "A trust evaluation method for improving nodes utilization for wireless sensor networks," *KSII Transactions on Internet and Information Systems*, vol. 12, no. 3, pp. 1113–1135, 2018.

[31] A. Tajeddine, A. Kayssi, A. Chehab, I. Elhajj and W. Itani, "CENTERA: A centralized trust-based efficient routing protocol with authentication for wireless sensor networks," *Sensors*, vol. 15, no. 2, pp. 3299–3333, 2015.

[32] Z. Bankovic, J. C. Vallejo, D. Fraga and J. M. Moya, "Detecting bad-mouthing attacks on reputation systems using self-organizing maps," in *Lecture Notes in Computer Science: Computational Intelligence in Security for Information Systems*, Berlin: Springer, vol. 6694, pp. 9–16, 2011.

[33] I. Pinyol and J. Sabater-Mir, "Computational trust and reputation models for open multi-agent systems: A review," *Artificial Intelligence Review*, vol. 40, no. 1, pp. 1–25, 2013.

[34] F. G. Mármol and M. P. Gregorio, "Towards pre-standardization of trust and reputation models for distributed and heterogeneous systems," *Computer Standards & Interfaces*, vol. 32, no. 4, pp. 185–196, 2010.

[35] A. Boukerche and Y. Ren, "A trust-based security system for ubiquitous and pervasive computing environments," *Computer Communications*, vol. 31, no. 18, pp. 4343–4351, 2008.

[36] A. Jøsang and R. Ismail, "The beta reputation," in *15th Bled Electronic Commerce Conf. e-Reality: Construction the e-Economy*, Bled, Slovenia, pp. 324–327, 2002.

[37] G. Shafer, *A mathematical theory of evidence*. Princeton, NJ: Princeton University Press, 1976.