

Trust evaluation in online social networks for secured user interactions

Anitha Yarava, C. Shoba Bindu

Department of CSE, JNTUA College of Engineering, Ananthapuramu, India

Article Info

Article history:

Received Jul 10, 2024

Revised Dec 28, 2024

Accepted Feb 28, 2025

Keywords:

Beta distribution

Followed factor

Follower factor

Fuzzy logic

Online social networks

Trust

Twitter

ABSTRACT

Online social network is a good platform, where users can share their opinions, ideas, products, and reviews with known (friends and relatives) and unknown users. The growing fame and its easy accesses of new users sometimes lead to security and privacy issues. Many methods are reported so far to address these issues but usage of high complex cryptographic algorithms creating new set of performance related challenges to the mobile users. In this paper, light weight soft security (trust) method is proposed. The proposed method "Trust evaluation in online social networks for secured user interactions-TEOSN" uses user social activities in estimation of his trustworthiness. Each user is observed in terms of followed factor- f_d (his interactions with others) and follower factor- f_r (others interaction with him). The factors f_d and f_r are estimated using fuzzy logic and user trust- τ is estimated using beta distribution. The performance of TEOSN is verified theoretically and practically. In experimental results, TEOSN is verified against different number of users; especially it outperformed existing methods in trust computation of target users at 2 to 4-hop distances.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Anitha Yarava

Department of CSE, JNTUA College of Engineering

Ananthapuramu, Andhra Pradesh, India

Email: y.anitha125@gmail.com

1. INTRODUCTION

Online social networks (OSN) web-based applications, those facilitates good platforms for the likeminded people to exchange their feelings, activities, interests and reviews [1]. Mobile technology increased the easiness in accessing of social networks like Facebook, Twitter, LinkedIn, and Google+ in a survey conducted by comScore [2] in America, users spending 86% of their time twitter through mobile services and this figure is 90% for Instagram. Usually, people interested to share their personal information like photos, videos, achievements, and sometimes financial matters. Social networks even allow people to express their reviews on products and government policies. On the other hand, people propagate the misinformation to mislead the users. In the coronavirus disease 2019 (COVID-19) pandemic season, lot of misinformation had been circulated regarding cause of disease, ways of speeding and death toll, which created lot of panic in people.

In social networks so many cyber law violations and crimes are reported by the untrustworthy users like misusing of others personal data and financial crimes [3]. Hence social network demands a strong social review system in classifying the posts as fake or genuine. But it is not a trivial task to do the news classification, since in OSNs gigabytes of information is generated with the user's daily activities. With these limitations, social network is becoming an attractive research area, where so many securities and privacy provision methods have to be proposed. Many methods or reported for this purpose, but they are lack of

accuracy and used complex encryption algorithms. So, people search is for a light weight soft security method usually referred as trust management methods.

Many solutions are reported in the literature survey to compute the user trust in social networks to increase the effective and efficiency of the applications. Trust can be estimated in different ways such as fuzzy model [4], Bayesian trust model, game theory model subjective trust, weighted based, Markov chain model and Beta distribution [5]. Many trust methods model the OSN as a trust network $G(V, E)$, where V is the set of users and E is the set of interactions among the users [6]. In OSN, trust is broadly classified into two types such as direct and indirect [7]. User do the direct trust assessment of other with whom they are interaction directly based on good and bad interactions they had. If the target user is not in direct communication, then he is assessed indirectly through mutual friends. In OSN, the indirect trust is evaluated like transitive trust rule [8]. If user- i trust on user- j is t_{ij} and user- j trust value on user- k is t_{jk} then user- i trust value on user- k is $t_{ik} = t_{ij} \times t_{jk}$. Social network is huge and complex one, there are multiple paths to reach target user/node [9]. Finding the most trustworthy route while suppressing biased recommendation of intermediate users is a challenging and still it is an open issue. Liu *et al.* [10] mentioned, a trust model three valued subjective logic (3VSL) is proposed, where OSN is configured as a arbitrary graphs. Here user trust is the combination of three different opinions like uncertainty, trustworthy and untrustworthy. Nasir and Kim [11] mentioned, the trust is estimated for the pair of unknown users, which is a continuous and real value. Here co-citation-based trust is computed and propagated as a trust transpose form. For a pair of users, trust is estimated as a average of their trust on each other and other users trust on them. Wu *et al.* [12] states, trust method is proposed for identification of trustworthy service provider in e-commerce applications. Where each customer's order demands finding high trustworthy service provider.

Guidi [13] states, block chain technology is introduced to Online Social Networks. Here OSN platforms are proposed based on blockchain, where each user's social activity is validated and maintained in terms of block chain. Wang *et al.* [14] explained, trust model is proposed for competitive social network, where similar items compete with each other to spread their influence to users. Here the trust model is devised to find the top k -most positive and negative influencers. Yan *et al.* [15], decentralized trust model (social-chain) based on block chain technology is proposed. In online social networks, most of the users are participating with mobile devices. Here the light weight consensus algorithm using proof of trust helps the mobile users to use social network features effectively over the long period. The notable issues in social networks are preventing spam propagation, identification of fake news, evaluation of trustworthiness of user posted content, bot recognition. All these issues and solutions to them are reviewed comprehensively in [16]. Xiao *et al.* [17] explained, the proposed trust model focused mainly on misinformation especially related to COVID-19 and its impact. Jiang *et al.* [18] explained, community detection methods are proposed for social networks. Rathee *et al.* [19] states, a hypothetical trust model is proposed ensure the secure communication among the social network users. Liu *et al.* [20] mentioned, a novel trust propagation operator based on knowledge coverage is proposed to measure the trust of two end users on each other. Wu *et al.* [21] explained, two-fold personalized feedback system is proposed. It is to achieve common agreement among the group members. It considers the personal and group consensus to ensure secure environment. Ghafari *et al.* [22], pair wise trust prediction is proposed for pair of unknown users to classify them based on similarities and contrast in their activities. He *et al.* [23] states, a 3C (computing, caching, and communication) based deep learning method is proposed. The deep learning-based reinforcement method take the optimal decision of allocation mobile resources based on the current network condition.

Research gaps identified and contribution: the analysis of above existing methods is revealing the gaps in trust estimation methods such as unable to suppress the impact of biased trust recommendations and lagging in consideration of each and every activity in assessment of user trustworthiness. Many trust methods reported so far in literature proposed discrete trust values of a target user. But it takes real and continuous values. In OSN, user activities are inhomogeneous with different range of intervals; hence we proposed the fuzzy logic to aggregate them. In the proposed method –TEOSN (trust evaluation in online social networks for secured user interactions), each and every user activity is captured and estimated in terms of user trustworthiness.

Merits of TEOSN over existing methods: the proposed method consists of the following qualities.

- i) The method could achieve the good accuracy in user trust computation, since it uses the continuous probability distribution function (Beta) to consider each and every activity of user over the period of time.
- ii) The uncertainty in user activities is handled efficiently by using fuzzy inference model.
- iii) The proposed model is scalable and adoptable to other social networks.

In this paper, the trust model is applied to the twitter social network data set called “Influencers in social networks” [24] with 11,000 user's social activities. Further sections are organized such as. In section 2, the proposed method TEOSN is described. In section 3, the performance of TEOSN estimated. And the work is concluded in section 4 with future research directions.

2. METHOD

Here the user direct trust is computed based on his social activities. Each user is assessed as he is interacting with other (followed_count - f_d) and how others are treating him (follower_count- f_r). Fuzzy logic is applied over user activities like follower_count, retweets_received, and mentions_received to compute f_r . f_d is computed by considering followed_count, retweets_sent, and mentions_sent. Here direct trust- τ is treated as a continues random variable over f_r and f_d and computed using Bayesian conditional probability and beta distribution. The end-to-end work flow of TEOSN is described in the Figure 1.

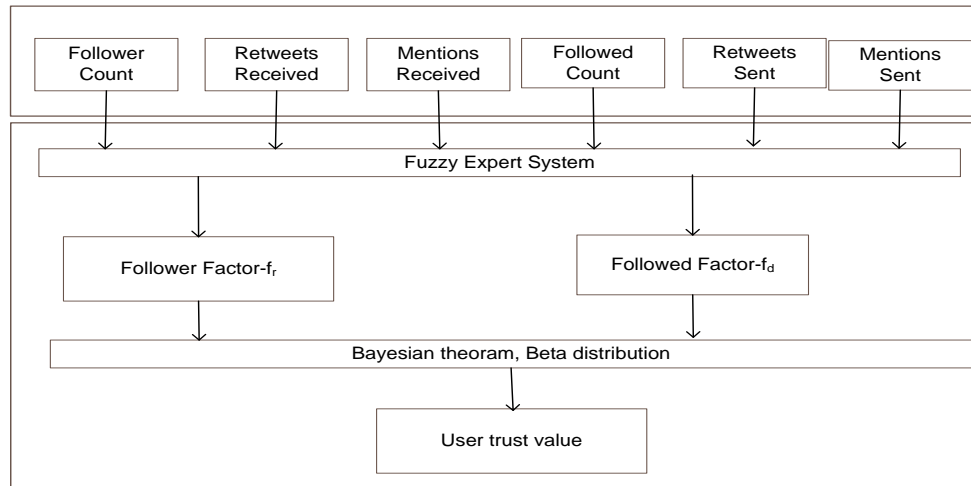


Figure 1. Frame work of proposed TEOSN

2.1. Social activity fuzzy sets

User social activities are inhomogeneous and cannot be aggregated directly to assess the trust value. Hence fuzzy logic is applied for aggregation of social activities and then trusts computation. Here fuzzy logic is applied separately on two sets of activities (input parameters) such as {follower_count, retweets_received, mentions_received} and {followed_count, retweets_sent, mentions_sent} to compute f_r and f_d (output parameters) respectively. In Tables 1 and 2, each of the social activities are divided into 4 fuzzy sets based on their interval values such as low, medium, high, and very high

Table 1. Follower_factor fuzzy sets intervals

Parameters	Fuzzy sets			
	Low	Medium	High	Very high
Follower count	1-10,000	98,000-300,000	296,000-5,000,000	4,900,000-36,543,194
Mentions received	0-100	90-1,000	990-100,000	99,900-1,145,218
Retweets received	0-50	48-100	95-1,000	980-52,349
Follower factor	0-0.25	0.23-0.40	0.38-0.70	0.68-1.0

Table 2. Followed_factor fuzzy sets intervals

Parameters	Fuzzy sets			
	Low	Medium	High	Very high
Followed count	1-10,000	9,800-300,000	290,000-700,000	690,000-1,165,830
Retweets sent	0-4	3-8	7-12	11-16
Mentions sent	0-19	17-38	36-58	56-76
Followed factor	0-0.25	0.23-0.40	0.38-0.70	0.68-1.0

2.2. Social activity fuzzy rule base

In fuzzy rule base each rule is in the form of IF-THEN. Where IF part is having input fuzzy sets and Then part consist of output variable fuzzy sets. In Tables 3 and 4 some of the fuzzy rules of f_r and f_d are described. In fuzzy logic fuzzification and defuzzification phases are implemented based on fuzzy rule base. A domain expert prepares the fuzzy rules based on his experience and observations. Here the rule base is prepared based on observation of data distribution in social networks.

Table 3. Follower rule base

Mentions received	Retweets received	Follower count	Follower factor
Low	High	Very high	High
Medium	Low	Low	Low
High	Very high	High	Very high
High	Low	Medium	Medium
Very high	Medium	High	High
Medium	Very high	Low	Medium

Table 4. Followed rule base

Mentions sent	Retweets sent	Followed count	Followed factor
High	High	Low	Medium
Medium	Medium	Low	Low
Low	High	Medium	Medium
Medium	High	High	High
High	Medium	Low	Low
Low	Low	High	Medium

2.3. Direct trust computation

TEOSN computes the user trust- τ as a real number which gets influenced and takes continuous values in the range of [0, 1]. Here user trust gets influenced by two factors, i.e how others are behaving with him (follower factor- f_r) and how he is behaving with others (followed factor- f_d). Hence in the data set the social activities are separated as two sets. After applying fuzzy logic as described in sections 2.1 and 2.2, f_r and f_d are calculated.

$$f_d = \mu[\text{following count, retweets sent, mentions sent}] \tag{1}$$

$$f_r = \mu[\text{follower count, retweets received, mentions received}] \tag{2}$$

Trust is a degree of belief and is considered as a random variable as $0 \leq \tau \leq 1$. Using baye’s theorem, user τ is computed as:

$$f(\tau, f_r/f_d) = \prod \frac{P(f_d/\tau, f_r)f(\tau, f_r)}{\int_0^1 P(f_d/\tau, f_r)f(\tau, f_r)d\tau} \tag{3}$$

Here $P(f_d/\tau, f_r)$ represents Likelihood probability and can be shown as a binomial distribution.

$$P(f_d/\tau, f_r) = \binom{f_r}{f_d} \tau^{f_d}(1 - \tau)^{f_r-f_d} \tag{4}$$

$f(\tau, f_r)$ represents prior probability and can be shown as a beta distribution with:

$$\text{Beta}(\tau; \alpha, \beta) = \frac{\tau^{\alpha-1}(1-\tau)^{\beta-1}}{\int_0^1 \tau^{\alpha-1}(1-\tau)^{\beta-1}d\tau} \tag{5}$$

where $\alpha > 0, \beta > 0$. Then,

$$f(\tau, f_r|f_d) = \frac{\binom{f_r}{f_d} \tau^{\alpha+f_d-1}(1-\tau)^{\beta+f_r-f_d-1}}{\left(\int_0^1 P(f_d/\tau, f_r)f(\tau, f_r)d\tau\right)\left(\int_0^1 \tau^{\alpha-1}(1-\tau)^{\beta-1}d\tau\right)} \tag{6}$$

In (6), $f(\tau, f_r|f_d)$ follows a beta distribution such as,

$$f(\tau, f_r|f_d) \cong \text{Beta}(\alpha + f_d, \beta + f_r - f_d) \tag{7}$$

The expectation of beta distribution is:

$$E[\tau] = \frac{\alpha}{\alpha+\beta} \tag{8}$$

In (8), the beta parameters are evaluated recursively as:

$$\alpha_n = \alpha_{n-1} + f_d \quad (9)$$

$$\beta_n = \beta_{n-1} + f_{r_{n-1}} - f_d \quad (10)$$

Initially, a new user is with no observations and expectations. Hence $\alpha_0 = \beta_0 = 1$ and his trust is 0.5, but over the period of time his trustworthiness is changed and rated as in (11) iteratively.

$$E_n[\tau] = \frac{\alpha_n}{\alpha_n + \beta_n} \quad (11)$$

2.4. User indirect trust computation

If a user is not in direct observation, then his trustworthiness is computed through common friends. But common friend's recommendations are not considered directly, they may give biased recommendations. Using trust transitive rule, a user indirect trust is computed. τ_{ij} is the user – i trust on user – j and τ_{jk} is the user – j trust on user – k then user – i trust on user – k is computed as:

$$\tau_{ik} = \tau_{ij} \times \tau_{jk} \quad (12)$$

2.5. Working of TEOSN

In Algorithm 1, first the pair of users i.e. (u_i, u_j) are verified, whether they are direct users or not. If they are direct users, direct trust is computed from step 1 to 9. Else indirect trust is computed in step 10. In step 3 and 4, the fuzzy values of user activities are computed. In step 6, likely wood is computed using binomial distribution. In step 7, prior distribution follower's beta distribution. In step 9, direct trust is computed as an expectation of beta distribution. In step 10, user indirect trust is computed.

Algorithm 1. Algorithm_ TEOSN (τ)

```

{
// $\tau$  is the  $u_i$ 's trust of user  $u_j$ 
If ( direct( $u_i, u_j$ ) )
{
// if  $u_i, u_j$  are in direct interaction, then compute  $\tau$  as a direct trust
1.  $u_i$ , observes  $u_j$  in terms of his activities like Follower count ( $f_r$ ), retweets received ( $tr$ ), Mentions received ( $ms$ ), followed count ( $f_d$ ), retweets sent ( $ts$ ) and mentions sent ( $ms$ ) and Computes trust
2.  $u_i$  Quantifies the  $u_j$ 's trust values as two parameters like follower factor  $f_r$ , followed factor  $f_d$  using fuzzy logic.
3.  $\mu(f_r) = \min\{\mu(fr_c), \mu(tr), \mu(ms)\}$ 
4.  $\mu(f_d) = \min\{\mu(fd_c), \mu(ts), \mu(ms)\}$ 
5. Computes the trust as a Bayesian conditional probability  $f(\tau, f_r | f_d)$  as a combination of likely Wood  $P(f_d / \tau, f_r)$  and prior probability  $f(\tau, f_r)$ 
6. Where  $P(f_d / \tau, f_r)$  follows binomial distribution
7.  $f(\tau, f_r)$  Follows beta distribution
8. Hence  $f(\tau, f_r | f_d)$  also follows a beta distribution with parameters  $\alpha + f_d$  and  $\beta + f_r - f_d$ 
9. Here expectation of beta distribution  $E_n[\tau]$  represents  $u_i$  direct trust on  $u_j$ .
}
else
{
// compute  $\tau$  as a in direct trust using trust transitive rule
10. If  $\tau_{ik}$  is a user-i trust on user-k and  $\tau_{kj}$  is the user-k trust on user-j then a user-i trust on user-j is computed as  $\tau = \tau_{ik} \times \tau_{kj}$ 
}
}

```

3. RESULTS AND DISCUSSION

The proposed method TEOSN is run on Twitter data set by considering its six features among its 11 features. The data set consist of 5,500 user's social activities. Here user direct and indirect trust is evaluated against the increased network sizes from [0.5k, 5.5k] users. The performance of the TEOSN is compared over the existing methods such as mole [25] and tidal [26]. For direct trust assessment, accuracy

and pearson correlation coefficient (PCC) methods are used. For indirect trust assessment, RMSE (root mean square error) metric is used.

In Figure 2, user direct trust is assessed. The accuracy of trust is verified over the number of users in social network. In the graph the direct trust is increased with the increased number of users. When the size of network is increased then user social activities are defined precisely and then his trust is estimated. The proposed method TEOSN with more evidence of user activities can judge him more accurately; hence the accuracy is increased with increased number of recommenders. In the Figure 3, user computed direct trust values are compared with the actual trust values. PCC is statistical metric used to measure the correlation between actual and computed user trust values. It is formulated as in (13).

$$pcc = \frac{\sum_{i=1}^n (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^n (x_i - \bar{x})^2} \sqrt{\sum_{i=1}^n (y_i - \bar{y})^2}} \tag{13}$$

Here x_i and y_i are *user – i* actual and computed trust values respectively. \bar{x} and \bar{y} are users actual and computed mean trust values respectively. PCC values are in the interval [-1 +1], where the values closer to +1 represents good correlation. In the Figure 3 PCC values are verified against number of users. When number of users is increased, TEOSN can derive the more accurate user trust value and hence can measure improved PCC values.

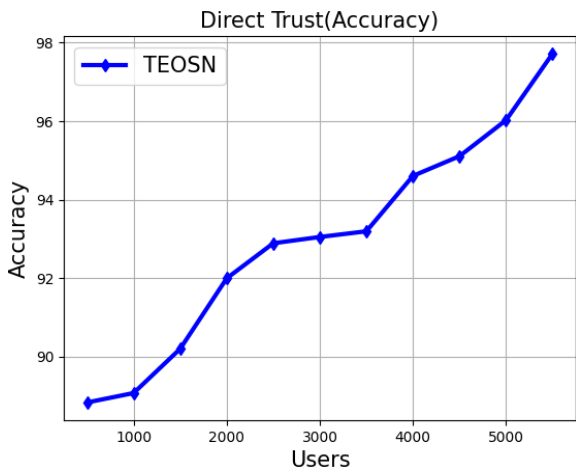


Figure 2. Number of users vs trust accuracy

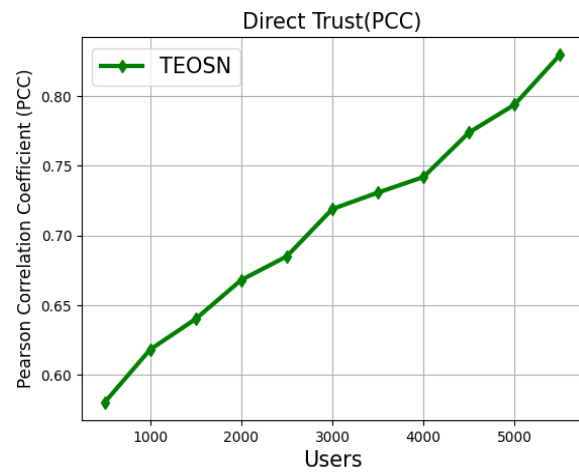


Figure 3. Number of users vs PCC

In Figure 4, the performance of trust methods is estimated with the parameter called the RMSE and is formulated as in (14).

$$RMSE = \sqrt{\frac{\sum_{i=1}^n (x_i - y_i)^2}{n}} \tag{14}$$

Here x_i and y_i are *user – i* actual and computed trust values respectively. In Figure 4, a user who is 3-hop away distance from evaluator is assessed. To assess him the evaluator has to consider the intermediate users i.e common friend’s recommendations towards the target user. But may provide biased recommendations hence accuracy is decreased with a greater number of users. The performance of the TEOSN is compared with other existing methods like mole and tidal trusts. The proposed method with the help of fuzzy logic, can consider all the network conditions and estimate the trust value, hence it could measure the less error increase over other methods.

In Figure 5, a user at 4-hop away distance is evaluated. Social networks are complex and huge with millions of users; hence a user can be reached through multiple trust paths with different trust levels. According to trust transitive rule, the accuracy loss is more when the user is at increased hops distances. In above graphs, the proposed method TEOSN can decrease this trust leakage along the path towards target user by monitoring mutual friend’s behavior time to time. Hence the proposed method could still measure better results than other methods for increased network sizes.

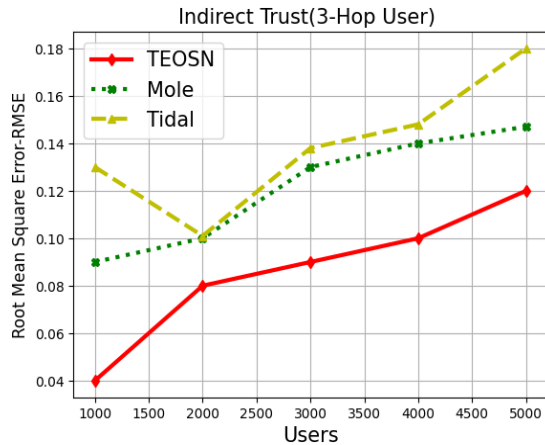


Figure 4. No. of users vs trust error for 3-hop users

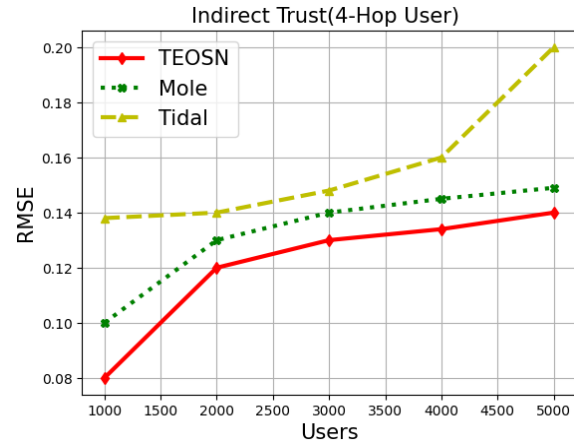


Figure 5. No. of users vs trust error for 4-hop users

In Figure 6, a user 5-hop level trust is estimated. The error is increased with increased hop count of target user. Here the challenges in trust assessment are like multiple paths, trust leakage and elimination of loop back paths towards target user. Hence the error magnitude is increased from 2-hop to 5-hops. The proposed method TEOSN, with the help of beta distribution can measure the impact of positive and negative attitude of each user along the target user. Hence comparatively TEOSN could sustain its performance over the existing methods. In Figure 7, trust information leak along the path towards target user is measured over the data set of 11,000 user records. When the path length (hop count) is increased, biased component in the intermediate user’s recommendations is also increased. TEOSN could minimize this information leak by applying proper set of fuzzy rules and beta distribution. Hence it outperformed the other trust methods.

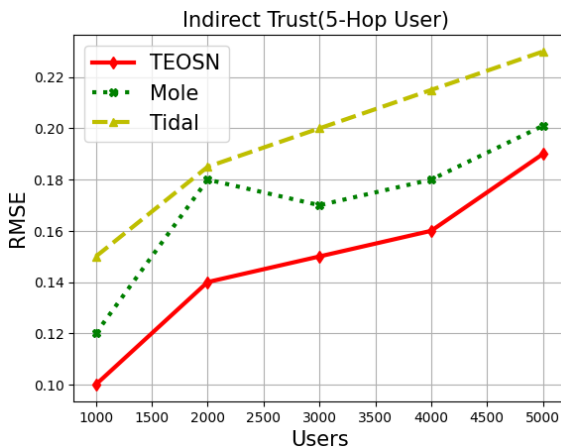


Figure 6. No. of users vs trust error for 5-hop users

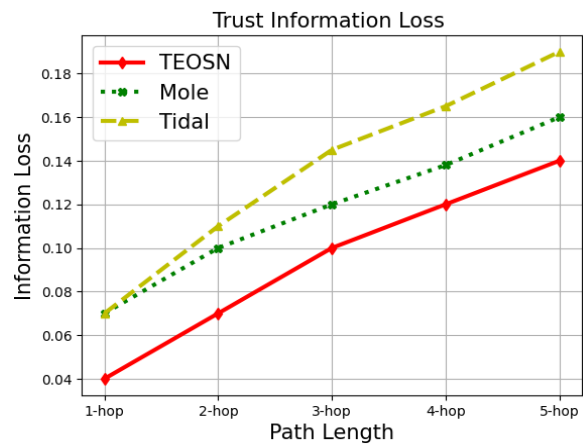


Figure 7. Path length of users vs trust information loss

4. CONCLUSION

Online social networks are very convenient platforms to the users to share their feelings, thoughts and information to other people. For the service providers, it is a good media to do publicity of their products and services. On the other hand, there is threat from unknown users through the propaganda of their false news and biased ratings. Hence assessing the unknown user before following his recommendations is very useful in OSNs. In this work, the proposed method TEOSN categories the user activities into two groups as follower factor and followed factor. These factors are computed by fuzzy logic and then with the help of Bayesian and beta distribution user trustworthiness is computed. Here twitter social network data set is used for modeling trust model. With the commonness of the social networks, the proposed TEOSN is also be scalable to other social networks such as Facebook and Instagram.

ACKNOWLEDGMENTS

The authors would like to thank the department of Computer Science and Engineering, JNTUA College of Engineering, Anantapuramu for supporting this work.

FUNDING INFORMATION

Authors state no funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Anitha Yarava	✓	✓	✓		✓	✓		✓	✓	✓	✓		✓	
C. Shoba Bindu		✓		✓			✓			✓		✓	✓	

C : **C**onceptualization
M : **M**ethodology
So : **S**oftware
Va : **V**alidation
Fo : **F**ormal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : **O**riting - **O**riginal Draft
E : **E**riting - **R**eview & **E**ditting
Vi : **V**isualization
Su : **S**upervision
P : **P**roject administration
Fu : **F**unding acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

INFORMED CONSENT

We have obtained informed consent from all individuals included in this study.

DATA AVAILABILITY

The data that support the findings of this study are openly available in Kaggle competitions at <https://www.kaggle.com/c/predict-who-is-more-influential-in-a-social-network/data>, reference number [24].




REFERENCES

- [1] J. Khan and S. Lee, "Implicit user trust modeling based on user attributes and behavior in online social networks," *IEEE Access*, vol. 7, pp. 142826–142842, 2019, doi: 10.1109/ACCESS.2019.2943877.
- [2] V. V. H. Pham, S. Yu, K. Sood, and L. Cui, "Privacy issues in social networks and analysis: a comprehensive survey," *IET Networks*, vol. 7, no. 2, pp. 74–84, Mar. 2018, doi: 10.1049/iet-net.2017.0137.
- [3] Y. Gao, X. Li, J. Li, Y. Gao, and P. S. Yu, "Info-trust: a multi-criteria and adaptive trustworthiness calculation mechanism for information sources," *IEEE Access*, vol. 7, pp. 13999–14012, 2019, doi: 10.1109/ACCESS.2019.2893657.
- [4] N. R. Sirisala and R. Bandi, "Fuzzy logic aware QoS multicasting in MANETs with load balance," *International Journal of Engineering & Technology*, vol. 7, no. 4.6, pp. 269–274, Sep. 2018, doi: 10.14419/ijet.v7i4.6.20488.
- [5] Z. Wei, H. Tang, F. R. Yu, M. Wang, and P. Mason, "Security enhancements for mobile ad hoc networks with trust management using uncertain reasoning," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 9, pp. 4647–4658, Nov. 2014, doi: 10.1109/TVT.2014.2313865.
- [6] N. Sirisala and C. Bindu, "A novel QoS trust computation in MANETs using fuzzy petri nets," *International Journal of Intelligent Engineering and Systems*, vol. 10, no. 3, pp. 116–125, Apr. 2017, doi: 10.22266/ijies2017.0430.13.
- [7] N. Sirisala and C. S. Bindu, "Recommendations based QoS trust aggregation and routing in mobile adhoc networks," *International Journal of Communication Networks and Information Security (IJCNIS)*, vol. 8, no. 3, pp. 215–220, Apr. 2022, doi: 10.17762/ijcnis.v8i3.2065.
- [8] N. Sirisala, A. Yarava, Y. C. A. P. Reddy, and V. Poola, "A novel trust recommendation model in online social networks using soft computing methods," *Concurrency and Computation: Practice and Experience*, vol. 34, no. 22, Oct. 2022, doi: 10.1002/cpe.7153.
- [9] S. Sirisala, N. Sirisala, and G. Rajeswarappa, "Eigen vector based trust model (EVTM) for ensuring quality of service (QoS) in mobile ad hoc networks," *International Journal of Computer Networks and Applications*, vol. 11, no. 3, pp. 351–362, Jun. 2024, doi: 10.22247/ijcna/2024/22.
- [10] G. Liu, Q. Yang, H. Wang, and A. X. Liu, "Trust assessment in online social networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 2, pp. 994–1007, Mar. 2021, doi: 10.1109/TDSC.2019.2916366.
- [11] S. U. Nasir and T.-H. Kim, "Trust computation in online social networks using co-citation and transpose trust propagation," *IEEE Access*, vol. 8, pp. 41362–41371, 2020, doi: 10.1109/ACCESS.2020.2975782.
- [12] J. Wu, N. Chen, C. Zhou, H. Che, C. Han, and Q. Liu, "Computing the number of loop-free k-hop paths of networks," *IEEE Transactions on Services Computing*, vol. 15, no. 4, pp. 2114–2128, Jul. 2022, doi: 10.1109/TSC.2020.3035706.




- [13] B. Guidi, "When blockchain meets online social networks," *Pervasive and Mobile Computing*, vol. 62, pp. 101–131, Feb. 2020, doi: 10.1016/j.pmcj.2020.101131.
- [14] F. Wang *et al.*, "Maximizing positive influence in competitive social networks: a trust-based solution," *Information Sciences*, vol. 546, pp. 559–572, Feb. 2021, doi: 10.1016/j.ins.2020.09.002.
- [15] Z. Yan, L. Peng, W. Feng, and L. T. Yang, "Social-chain: decentralized trust evaluation based on blockchain in pervasive social networking," *ACM Transactions on Internet Technology*, vol. 21, no. 1, pp. 1–28, Feb. 2021, doi: 10.1145/3419102.
- [16] M. Alkhamees, S. Alsaleem, M. Al-Qurishi, M. Al-Rubaian, and A. Hussain, "User trustworthiness in online social networks: a systematic review," *Applied Soft Computing*, vol. 103, pp. 107–159, May 2021, doi: 10.1016/j.asoc.2021.107159.
- [17] X. Xiao, P. Borah, and Y. Su, "The dangers of blind trust: examining the interplay among social media news use, misinformation identification, and news trust on conspiracy beliefs," *Public Understanding of Science*, vol. 30, no. 8, pp. 977–992, Nov. 2021, doi: 10.1177/0963662521998025.
- [18] L. Jiang, L. Shi, L. Liu, J. Yao, and M. E. Ali, "User interest community detection on social media using collaborative filtering," *Wireless Networks*, vol. 28, no. 3, pp. 1169–1175, Apr. 2022, doi: 10.1007/s11276-018-01913-4.
- [19] G. Rathee, S. Garg, G. Kaddoum, D. N. K. Jayakody, M. J. Piran, and G. Muhammad, "A trusted social network using hypothetical mathematical model and decision- based scheme," *IEEE Access*, vol. 9, pp. 4223–4232, 2021, doi: 10.1109/ACCESS.2020.3048077.
- [20] Y. Liu, C. Liang, F. Chiclana, and J. Wu, "A knowledge coverage-based trust propagation for recommendation mechanism in social network group decision making," *Applied Soft Computing*, vol. 101, p. 107005, Mar. 2021, doi: 10.1016/j.asoc.2020.107005.
- [21] J. Wu, S. Wang, F. Chiclana, and E. Herrera-Viedma, "Two-fold personalized feedback mechanism for social network consensus by uninorm interval trust propagation," *IEEE Transactions on Cybernetics*, vol. 52, no. 10, pp. 11081–11092, Oct. 2022, doi: 10.1109/TCYB.2021.3076420.
- [22] S. M. Ghafari *et al.*, "A survey on trust prediction in online social networks," *IEEE Access*, vol. 8, pp. 144292–144309, 2020, doi: 10.1109/ACCESS.2020.3009445.
- [23] Y. He, C. Liang, F. R. Yu, and Z. Han, "Trust-based social networks with computing, caching and communications: a deep reinforcement learning approach," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 1, pp. 66–79, Jan. 2020, doi: 10.1109/TNSE.2018.2865183.
- [24] "Influencers in social networks," *Kaggle.com*, 2013. <https://www.kaggle.com/c/predict-who-is-more-influential-in-a-social-network/data>.
- [25] P. Yue, R. Li, and B. Pang, "A light-weight mitigation scheme on the mole content poisoning attack in NDN," in *2020 21st Asia-Pacific Network Operations and Management Symposium (APNOMS)*, Sep. 2020, pp. 132–137, doi: 10.23919/APNOMS50412.2020.9236974.
- [26] M. Naderan, E. Namjoo, and S. Mohammadi, "Trust classification in social networks using combined machine learning algorithms and fuzzy logic," *Iranian Journal of Electrical and Electronic Engineering*, vol. 15, no. 3, pp. 294–309, 2019, doi: 10.22068/IJEEE.15.3.294.

BIOGRAPHIES OF AUTHORS



Anitha Yarava    received is a research scholar in CSE Department at Jawaharlal Nehru Technological University Anantapur, Ananthapuramu, Andhra Pradesh, and India. She holds a M.Tech degree in computer science and engineering. Her research areas are machine learning, algorithms and soft computing systems. She can be contacted at email: y.anitha125@gmail.com.



Prof. Dr. C. Shoba Bindu    received is working as a professor in Department of CSE at Jawaharlal Nehru Technological University Anantapur, Ananthapuramu, Andhra Pradesh, India. She holds a Ph.D. degree in computer science and engineering. Her research areas are machine learning, wireless networks, cloud computing, internet of things (IoT), algorithms, and soft computing systems. She can be contacted at email: shobabindu.cse@jntua.ac.in.