
ISSN: 2321-2152
IJMECE
International Journal of modern
electronics and communication engineering
E-Mail
editor.ijmece@gmail.com
editor@ijmece.com
www.ijmece.com

ISSN2321-2152

www.ijmece .com

Vol 12, Issue 2, 2024

Trustworthiness Assessment of Users in Social Reviewing Systems

[1]MR.CH SURESH,[2] KATTA BHAVYA

[1](Assistant Professor), MCA, Swarnandhra College

[2]MCA, scholar, Swarnandhra College

ABSTRACT

Social Networks represent a cornerstone of our daily life, where the so-called social reviewing systems (SRSs) play a key role in our daily lives and are used to access data typically in the form of reviews. Due to their importance, social networks must be trustworthy and secure, so that their shared information can be used by the people without any concerns, and must be protected against possible attacks and misuses. One of the most critical attacks against the reputation system is represented by mendacious reviews. As this kind of attacks can be conducted by legitimate users of the network, a particularly powerful solution is to exploit trust management, by assigning a trust degree to users, so that people can weigh the gathered data based on such trust degrees. Trust management within the context of SRSs is particularly challenging, as determining incorrect behaviors is subjective and hard to be fully automatized. Several attempts in the current literature have been proposed; however, such an issue is still far from been completely resolved. In this study, we propose a solution against mendacious reviews that combines fuzzy logic and the theory of evidence by modeling trust management as a multicriteria multi expert decision making and exploiting the novel concept of time-dependent and content-dependent crown consensus. We empirically proved that our approach outperforms the main related works approaches, also in dealing with sockpuppet attacks.

The framework employs a multi-faceted approach that integrates machine learning algorithms, natural language processing techniques, and social network analysis. Firstly, text analysis methods are utilized to

analyses the content of reviews, identifying linguistic patterns indicative of trustworthiness or deceit. Secondly, machine learning models are trained to detect anomalies in user behavior, such as suspicious review patterns or sudden spikes in activity. Thirdly, social network analysis is employed to examine the relationships between users, identifying potential collusion or fake review networks.

1.INTRODUCTION

Internet-enabled apps that facilitate the development of interpersonal relationships between users who have common interests or hobbies are sometimes referred to as online social networks. In addition to sharing media files like photos and videos, most of these apps let users discuss certain subjects in order to recommend things to check out (like Foursquare and TripAdvisor) or to create communities that can help with specific tasks (like LinkedIn for job searches, Research Gate for finding answers to research questions, Amazon for shopping, etc.). These social apps, which we'll call social reviewing systems (SRSs), have grown in popularity thanks to the widespread use of remark and opinion sharing, which is essential for people's day-to-day decision-making. Most of us, for instance, look up reviews and ratings on our preferred SRS before deciding on a restaurant or making a purchase. Advanced opinion modeling and analysis, capitalizing on the influence of neighbors on user preferences, and tackling the current information overload in SRS all attest to people's growing and mutually beneficial reliance on them. Because of this, the reliability of SRS is crucial for a community's opinion dynamics and the spread of trust among its members. Indeed, SRSs are vulnerable to deceitful communications and imposters who may fool people into thinking they're making the proper choice. Given the potential sharing and leakage of sensitive personal information within SRS, as well as the fact that users can adopt a false online persona or have software robots (or "Bots") act in a humanoid fashion, this could give rise to a number of privacy and security concerns. Data breaches, phishing attempts, information manipulation, and other risks in SRS never stop with a single social actor; rather, they propagate like an infection across the network, picking up victims among the friends of the infected players. That is why it is crucial for an SRS supplier to provide adequate security measures to ensure its reliability.

ISSN2321-2152
www.ijmece .com
Vol 12, Issue 2, 2024

Since the problem of message forgery is readily overcome by means of encryption, certain publications in the present literature, including, primarily address this issue. Still unresolved, however, is the second kind of malevolent conduct, which originates from imposter users. The issue of hidden or phony users has been the subject of many proposals during the last decade. To address the problem of providing privacy, access control measures have been implemented. In order to combat the forging of nodes, identities, and social relationships, authentication of users and their communications has been needed. While it is very difficult to resist bad actions by genuine SRS members, these methods often target outside attackers or outsiders. A simplistic approach to safeguarding against harmful persons would be for users to exercise caution when selecting romantic partners. Many different types of connections may exist between two social network users: Systems similar to Facebook allow users to designate other users as "friends," while systems similar to Instagram allow users to "follow" other users. On the other hand, users aren't always cautious when accepting joining requests, and it's usually rather tough to choose other users to be linked with (as bad actors are masters at hiding their identities, too). The majority of relationships in social networking sites (SNSs) are not based on direct knowledge of the people behind them, but rather on users' profiles. This is true even though relationships among SRS social actors should be based on direct knowledge of the people behind them, such as former classmates, colleagues, or members of the same family or group of friends. When it comes to protecting against these types of insider threats, trust management is a common choice. The process involves determining a user's "trust" worth by observing their actions or by observing the trust relationships between various social actors. With this goal in mind, we've developed a gentle security solution that suggests cutting links with low-trust actors or restricting them access to certain data and features in order to make them more difficult to work with. The primary SRS systems do not provide trust management directly because of problems with its automated calculation, even though it is a strong way of security.

2.LITERATURE SURVEY

User trustworthiness in online social networks:

ISSN2321-2152
www.ijmece .com
Vol 12, Issue 2, 2024

A comprehensive analysis The overlay panel opens when clicking the author's links. There is a risk that anonymous individuals may be able to do harmful things on social media due to the platforms' increasing popularity and their willingness to accommodate new members. These systems have a lot of motivation to stop this from happening, but they can't handle the amount of data that needs processing. Another difficulty is that attackers often alter their tactics quickly in reaction to defensive measures. As a result, there have been a lot of fascinating studies done in recent years concerning user trustworthiness on social networks. The purpose of this study is to summarize the current situation of research in this area and to evaluate the studies that have attempted to solve this issue using different approaches and published between 2012 and 2020. There are a variety of proposed remedies in the literature; some concentrate on anti-spam measures, others on bot identification methods, and still others on identifying false news or grading the veracity of user-generated information. While several of these solutions do a good job in certain areas, none of them can guarantee complete safety from every conceivable kind of assault. Keeping an eye on this area of research is crucial, and by showcasing new studies that address the topic of online user trustworthiness, this review aims to help shed light on the notion.

Acquiring Knowledge about Social Internet of Things Trustworthiness Management: In an effort to create a social network of linked items, the next iteration of the Internet of Things (IoT) makes it easier to incorporate the idea of social networking into things, or smart objects. As a result of these developments, a new paradigm known as the Social Internet of Things (SIoT) has emerged, which has great promise. In this model, smart items serve as social objects and mimic human social behavior with intelligence. In order to find new services, these social objects may form connections with other nodes in the network and leverage those interactions. To establish the credibility and dependability of systems and to accomplish the shared objective of trustworthy cooperation and collaboration among objects, trust is crucial. In the context of the SIoT, an unreliable object has the potential to compromise the service's quality and dependability while also interfering with its core operation via the delivery of harmful messages. We provide a comprehensive analysis of SIoT trustworthiness management

ISSN2321-2152
www.ijmece .com
Vol 12, Issue 2, 2024

in this survey. Prior to delving into a comprehensive analysis of the trust management components in SIoT, we covered the fundamentals of trust across several fields. Moreover, we compare and analyze the trust management schemes by mainly classifying them into four groups according to their strengths, weaknesses, the trust management components used by each scheme, and the performance of these studies on various trust evaluation dimensions. We wrap off by talking about where the new paradigm of SIoT is taking research, specifically in the area of SIoT trustworthiness management.

3. EXISTING SYSTEM

Yu *et al.* described an approach for computing user trustworthiness by leveraging on the "familiarity" and "similarity" concepts and considering the influence of user actions on the trustworthiness computation. The aim of this methodology is to detect malicious users-based also on a security queue to record users' historical trust information. Afterward, Yu *et al.* proposed an approach based on deep learning techniques in conjunction with user trustworthiness characterization for configuring privacy settings for social image sharing. In addition, a two-phase trust-based approach based on deep learning techniques has also been proposed by Deng *et al.* for social network recommendation, so as to determine the users' interests and their trusted friends' interests together with the impact of community effect for recommendations.

Other related approaches exploit reviews' evaluation for detecting and/or characterizing spam in social media. Shehnepoor *et al.* proposed a framework named *NetSpam* that models reviews in online social media, as a case of heterogeneous networks, by using spam features for detection purposes. Ye *et al.* described an approach based on the temporal analysis by monitoring selected indicative signals of opinion spams.

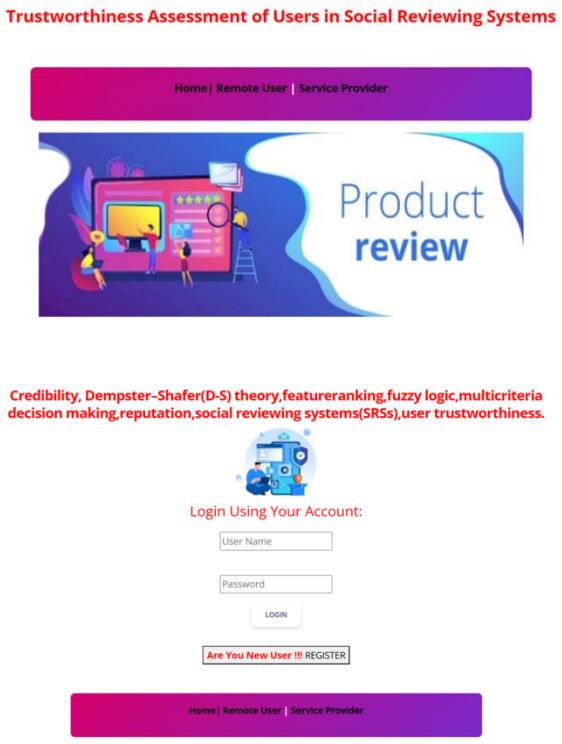
A system based on four integrated components, specifically: 1) a reputation-based component; 2) a credibility classifier engine; 3) a user experience component; and Furthermore, another framework, namely, *LiquidCrowd*, has been proposed by Castano trustworthiness techniques for managing the execution of collective tasks. Kumar *et al.* proposed a system, namely, *FairJudge*, to identify fraudulent users based on the mutually recursive definition of the following three metrics: 1) the user trustworthiness in

ISSN2321-2152
www.ijmece .com
Vol 12, Issue 2, 2024

rating products; 2) the rating reliability; and 3) the goodness of a product. For identifying fake reviews and Liu *et al.* [32] investigated the sockpuppet attacks on reviewing systems by proposing a fraud detection algorithm, called RTV, that introduces trusted users and also considers reviews left by verified users.

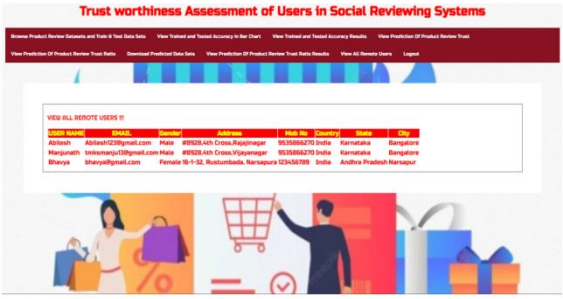
4. OUTPUT SCREENS

Home page



View profile page:

View Remote



User Login

Output

ISSN2321-2152
www.ijmece .com
Vol 12, Issue 2, 2024

5. CONCLUSION

When it comes to social networks, dealing with the subjectivity of malicious behavior detection and the need for objectivity in designing an automated process to assign trust degrees to users based on their activity is a major challenge. This study offered a solution to this problem. In order to achieve this goal, we have used fuzzy theory to tackle the subjective and nebulous nature of social network review analysis. We have used the philosophy of evidence to design an MCME-DM procedure that optimizes trust estimates by aggregating judgments from diverse viewpoints. Using the YELP and Amazon datasets, we conducted a realistic experimental campaign and shown that combining the results of several criteria improves the accuracy of identifying fraudulent reviews. We also demonstrated that our method achieved superior effectiveness by using 80% and 100% of the examined dataset by comparing it to the primary comparable research in the current literature.

We intend to study the privacy issues with recommendation systems in light of important legal frameworks like the EU General Data Protection Regulation (GDPR) and conduct more in-depth investigations into the impact of typical attacks on such systems in order to strengthen their security in future work. In addition, those who are against D-S aggregation primarily point out that method might combine inconsistent or incorrect information from different sources, leading to outcomes that don't make sense. Over the last 10 years, new ideas from D-S theory, such the evolutionary combination rule (ECR), and modified versions of the mass functions have been developed to enhance the identification of possible aggregation process problems. We have deferred investigating this method inside our work to a later stage.

6.REFERENCES

[1] M. Faloutsos, T. Karagiannis, and S. Moon, “Online social networks,” *IEEE Netw.*, vol. 24, no. 5, pp. 4–5, Sep/Oct. 2010.

[2] J. Castro, J. Lu, G. Zhang, Y. Dong, and L. Martinez, "Opinion dynamics-based group recommender systems," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 48, no. 12, pp. 2394–2406, Dec. 2018.

[3] F. Xiong, X. Wang, S. Pan, H. Yang, H. Wang, and C. Zhang, "Social recommendation with evolutionary opinion dynamics," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 50, no. 10, pp. 3804–3816, Oct. 2020.

[4] R. Ureña, G. Kou, Y. Dong, F. Chiclana, and E. Herrera-Viedma, "A review on trust propagation and opinion dynamics in social networks and group decision making frameworks," *Inf. Sci.*, vol. 478, pp. 461–475, Apr. 2019.

[5] Y. Xiang, E. Bertino, and M. Kutylowski, "Security and privacy in social networks," *Concurrency Comput. Practice Exp.*, vol. 29, no. 7, 2017, Art. no. e4093.

[6] D. Irani, S. Webb, K. Li, and C. Pu, "Modeling unintended personal information leakage from multiple online social networks," *IEEE Internet Comput.*, vol. 15, no. 3, pp. 13–19, May/Jun. 2011.

[7] A. Nosko, E. Wood, and S. Molema, "All about me: Disclosure in online social networking profiles: The case of Facebook," *Comput. Human Behav.*, vol. 26, no. 3, pp. 406–418, 2010.

[8] K. Krombholz, D. Merkl, and E. Weippl, "Fake identities in social media: A case study on the sustainability of the Facebook business model," *J. Service Sci. Res.*, vol. 4, no. 2, pp. 175–212, 2012.

[9] E. Ferrara, O. Varol, C. Davis, F. Menczer, and A. Flammini, "The rise of social bots," *Commun. ACM*, vol. 59, no. 7, pp. 96–104, 2016.

[10] X. Wang *et al.*, "Game theoretic suppression of forged messages in online social networks," *IEEE Trans. Syst., Man, Cybern., Syst.*, early access, Mar. 5, 2019, doi: 10.1109/TSMC.2019.2899626.

[11] M. A. Ferrag, L. Maglaras, and A. Ahmim, "Privacy-preserving schemes for ad hoc social networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 3015–3045, 4th Quart., 2017.

[12] I. Kayes and A. Iamnitchi, "Privacy and security in online social networks: A survey," *Online Soc. Netw. Media*, vols. 3–4, pp. 1–21, Oct. 2017.

[13] S. R. Sahoo and B. B. Gupta, "Classification of various attacks and their

defence mechanism in online social networks: A survey," *Enterprise Inf. Syst.*, vol. 13, no. 6, pp. 832–864, 2019.

[14] C. Zhang, J. Sun, X. Zhu, and Y. Fang, "Privacy and security for online social networks: Challenges and opportunities," *IEEE Netw.*, vol. 24, no. 4, pp. 13–18, Jul. 2010.

[15] H. Gao, J. Hu, T. Huang, J. Wang, and Y. Chen, "Security issues in online social networks," *IEEE Internet Comput.*, vol. 15, no. 4, pp. 56–63, Jul./Aug. 2011.

[16] F. Buccafurri, G. Lax, D. Migdal, S. Nicolazzo, A. Nocera, and C. Rosenberger, "Contrasting false identities in social networks by trust chains and biometric reinforcement," in *Proc. Int. Conf. Cyberworlds*, 2017, pp. 17–24.

[17] W. Sherchan, S. Nepal, and C. Paris, "A survey of trust in social networks," *ACM Comput. Surveys*, vol. 45, no. 4, p. 47, 2013.

[18] G. Liu *et al.*, "TOSI: A trust-oriented social influence evaluation method in contextual social networks," *Neurocomputing*, vol. 210, pp. 130–140, Oct. 2016.

[19] H. Xia, F. Xiao, S.-S. Zhang, X.-G. Cheng, and Z.-K. Pan, "A reputation based model for trust evaluation in social cyber-physical systems," *IEEE Trans. Netw. Sci. Eng.*, vol. 7, no. 2, pp. 792–804, Apr.–Jun. 2020.

[20] X. Niu, G. Liu, and Q. Yang, "Trustworthy website detection based on social hyperlink network analysis," *IEEE Trans. Netw. Sci. Eng.*, vol. 7, no. 1, pp. 54–65, Jan.–Mar. 2020.

[21] R. E. Bellman and L. A. Zadeh, "Decision-making in a fuzzy environment," *Manag. Sci.*, vol. 17, no. 4, pp. B141–B164, 1970.

[22] C. Esposito, A. Castiglione, and F. Palmieri, "Information theoretic based detection and removal of slander and/or false-praise attacks for robust trust management with Dempster–Shafer combination of linguistic fuzzy terms," *Concurrency Comput. Practice Exp.*, vol. 30, no. 3, 2018, Art. no. e4302.

[23] S. K. T. Lam, D. Frankowski, and J. Riedl, "Do you trust your recommendations? An exploration of security and privacy issues in recommender systems," in *Emerging Trends in Information and Communication Security*. Berlin, Germany: Springer, 2006, pp. 14–29.

[24] R. Katarya, "A systematic review of group recommender systems techniques,"

Proc. Int. Conf. Intell. Sustain. Syst. (ICISS), Dec. 2017, pp. 425–428.

[25] M. Casanovas and J. Merigó, "Fuzzy aggregation operators in decision making with Dempster–Shafer belief structure," *Expert Syst. Appl.*, vol. 39, no. 8, pp. 7138–7149, 2012.