Digital Innovations & Contemporary Research in SCIENCE, ENGINEERING & TECHNOLOGY
Vol. 11. No. 1, 2023

Article Citation Format
Aderibigbe, O.S. & Okunade, T.A. (2023): Performance Assessment of Collaborative Trust Models .. Journal of Digital Innovations & Contemporary Research in Science, Engineering & Technology. Vol. 11, No. 1. Pp 65-77
DOI: dx.doi.org/10.22624/AIMS/DIGITAL/V11N1P5

Article Progress Time Stamps
Article Type: Research Article
Manuscript Received:18th January, 2023
Review Type: Blind Peer
Final Acceptance: 10th March, 2023

Performance Assessment of Collaborative Trust Models

Aderibigbe, O.S. & Okunade, T.A.
Department of Computer Sciences
Lagos State University of Science and Technology
Ikorodu, Lagos State, Nigeria.
E-mail: aderibigbe.os@lasustech.edu.ng

ABSTRACT

This study assessed existing Collaborative Models for trust awareness to ensure effective friend-to-friend collaboration in an overlay network for better control of private data towards a robust social media interaction. The result obtained showed that the Trust-Aware Model (T-AM) demonstrated significant reliability regarding recommendation accuracy and convergence. This was because benchmarking the result from assessing the T-AM with the result from that of assessing existing collaborative models, showed that the T-AM had an accuracy of 0.875, and that of the existing collaborative model was 0.750. While the T-AM had a convergence value of 0.125, that of the existing collaborative model was 0.250. The existing model had an effectiveness value of 0.1875, while the T-AM had an effectiveness value of 0.1094. This implies that the T-AM provided improved recommendation accuracy considering the standard scale of 0 to 1, and convergence (in terms of time) on a scale of 0 to 1. The implication of this is that the T-AM's ability to make recommendations is very significant since its accuracy value was 0.875 as compared to 0.750 of the existing collaborative models. For convergence, based on the scale rating provided above, it means that the T-AM provided accurate recommendations in a convergence of time of 0.125 as compared to 0.250 for the existing collaborative model. However, in terms of effectiveness, the T-AM performed less with an effectiveness value of 0.1094 as compared to the effectiveness value of 0.1875 of the existing collaborative models. The study concluded that trust data was effectively managed using the distributed hash table and symmetric replication methods, with significant improvement in reputational accuracy and convergence without compromising on scalability and secured online collaboration.

Keywords: Trust Awareness, Effectiveness, Convergence, Accuracy, Collaborative Model

1. INTRODUCTION

Social Networks (SNs) hold a lot of user data. These data grow steadily on a daily basis as a result of the myriads of interactions that go on between peers on the network (Krishnamurthy and Will, 2009). In the hands of the corporation(s) who owns the SNs, these data are exposed and open to misuse.

This is because owners of the SNs have direct access to the data. Interestingly, they are not bound by any law not to either sell or use the data to their own advantage. There have also been questions of data ownership when users discovered that their profile information still exist on the online social networking websites even after they had cancelled their account (Buchegger *et al.,* 2009). Moreover, every social network medium remains a potential for big data. The centralised nature of user data repositories that can be used for data mining and targeted advertising by the service providers also raise concerns (Buchegger *et al.,* 2009). These data are valuable information which ought to be at the exclusive reserve of the user. Users should have the right to determine what happens to their data. Based on the argument presented so far, the need to protect user data is overarching.

Firstly, users should know what is possible with the lots of data that accrue from their activities on the network. Secondly, this usual practice of having exclusive right to user data by social network owners needs to be reconsidered. This is because the practice puts users' confidentiality at the risk of infringement (Steel and Vascellaro, 2010; Greenwald and MacAskill, 2013; Opsahl, 2010). However, for users to have some measure of control over their data, the issue of ensuring trust becomes critical. Though, social trust holds a lot of promise in resolving this, there is a dearth of models to implement it for friend-to-friend collaboration. This research work filled this gap using the leverage of the P2P collaborative paradigm.

2. LITERATURE REVIEW

This work was inspired by a large amount of previous works on peer-to-peer network, trust models, friend-to-friend network and collaborative systems. The Turtle model developed by Popescu et al. (2006) relates to this current work in that it was developed for the safe sharing of sensitive information in a P2P network. The model was used to guarantee privacy, by organising data sharing as an overlay on top of a pre-existing user trust relationship. However, the theoretics of the mutable nature of trust was not considered. The belief in this current work is that trust is mutable. The trustworthiness of peers should be upheld as a priority. In this study, trustworthiness was modelled to be updated after each collaboration. In a similar study, Galuba (2009) developed a friend-to-friend collaborative model that allowed users' information sharing groups to build their own ad-hoc network and collaborate without requiring the service of a server or third-party service. As a result, the control of data was transferred to the users, however the concept of social trust was not incorporated into the model.

In the area of collaborative models, Forster's *et al.* (2012) Collaborative Business Process Modelling used the Cheetah experimental platform to investigate how a business model can be collaboratively created. The research presented a collaborative method for creating business models and analysed the modelling process within a collaborative environment setting. This was with a view to using obtained data to improve collaborative modelling editors. The tool allowed users to synchronously work on the same model and do editing, while the users are separated using communication channel. The issue of trust is paramount in the scenario. This is because of the fact that the quality and sanctity of any editing can only be guaranteed by trust, which was clearly absent in the collaborative model. Varlamis *et al.* (2013) in their work used social network metrics to generate personalized user recommendations. They suggested that the impact of measures in recognizing trustworthy actors in a social network can be recommended to specific users. Such measures include: opinion/trust of the actor for other actors, the opinion/trust of the actor's network of trust, and the overall ranking of all actors.

This category of metrics falls into the category of local and global metrics, which were applied to manipulate and tackle any shortcomings, thereby improving the quality of recommendations. This study took a cue from Varlamis *et al.* (2013), by ensuring that only local metric (from personal trust conception) is not considered for trust quantification. In this work, both local metric (from personal trust), and global metric (from reputational/recommendation trust) were therefore drawn on. Chen and Pan (2014) in their research work considered and developed the open-source software collaborative user model based on social network and tag similarity. The model was used to detect contact and collaborative relationship between collaborators from their contact and work information.

It also constructs a social network model to reflect the social relationships that exist between collaborators. The goal was to be able to recommend accurate collaborators. The model uses a statistical and decision support accuracy procedure to evaluate the performance of recommendation. Experimental results showed that the model was effective in improving measurement of accuracy of relationship between collaborators, detecting a collaborator's role in a work team and detecting work teams in social network. However, the entrants of a new participants were not considered with respect to trust in the work. The trust-awareness concept has been highlighted as a resourceful solution to the traditional problem of recommender systems.

Collaborative Filtering (CF) is widely used as techniques for Recommender Systems (RS). Based on CF, RS as it does not require explicit content description, but rely on user's opinion. The traditional problem orchestrated by the CF is the blind searching for similar users and the using of the rating of the user to predict items that are recommended to users (Massa and Avesani, 2004). This blind searching undermines the level of trust between similar users that are searched. There is therefore, the need for a trust mechanism like the one provided in this work to determine the trust value of similar users. In Haydar et al. (2012), the hybridising collaborative filtering was introduced. It was to take advantage of the trust-awareness concept in order to side step the blind searching for similar users.

Thus, both opinion and trust similarity were hybridized. The goal was to improve on their similarity since they have been considered as different entities. The achieved trust level was commendable, except that the issue of distrust was not considered. Unlike the work of Massa and Avesani (2004) and Haydar et al. (2012), the work handled the issue of distrust by incorporating the trust manager. The trust manager computes the trust of all peers-nodes in the network at every opportunity and also updates same. This contribution solves the problem of distrust by isolating nodes without continual trust as distrust nodes

3. METHODOLOGY

The first model to be assessed was the Trust-aware Recommender Systems (TaRS); the system uses the collaborative filtering model for its recommendations. This model employs the techniques of collaborative filtering (Massa and Avesani, 2007). However, the system is faced with some challenges, including: (i) the inability to find similar users, (ii) the creation of ad-hoc user profiles, which are supposedly similar to the target user but make TaRS vulnerable to attacks by intruders, and (iii) the inability of TaRS to handle the cold start problem - new users in the network. To assess the TaRS model in this research work, its global nature - which considers global trust as a type of reputational trust - was considered. Similarly, similarity, which is one of its mechanisms for recommendation, was therefore considered as a metric for TaRS assessment.

In Varlamis et al. (2013), the application of social network metrics to assess the Trust-aware Collaborative Model (TaCM) was presented. Varlamis *et al.* (2013) examined the impact of measures in recognizing trustworthy actors in a social network that can be recommended to specific users. The measures considered include the opinion/trust of the actor for other actors, the opinion/trust of the actor's network of trust, and the overall ranking of all actors.

These were computed based on their position and interconnections in graphical form. In the work, both local and global metrics were applied, since global trust metrics were easily manipulated. However, local trust metrics were observed to be more resistant to attacks. Interestingly, conceptualizing both local and global trust metrics helped in the assessment of TaCM, with the belief that a better understanding of the metrics is needed to improve the quality of recommendations.

The Trust Singular Value Decomposition (TrustSVD) Collaborative Filtering model developed by Guo *et al.* (2015) was also considered for assessment. This is because TrustSVD uses the explicit influence of user trust and item ratings to resolve the problems of data sparsity and cold start associated with collaborative filtering. Both implicit and explicit influences of rated items were conceptualized and leveraged for the assessment of the TrustSVD collaborative model. TrustSVD is an extension of SVD++ (Koren, 2008), drawing on the concept of social trust information. However, the influence of trusters and trustees was not considered. In this research work, social trust information with a focus on harnessing the influence of trusters and trustees was leveraged. This was conceived based on the claim of Young *et al.* (2013) that incorporating trust, whether from a trustor's or trustee's perspective (or both), into collaborative systems can significantly improve their recommender's potential.

In this research work, the Trust-aware collaborative model for friend-to-friend networks (T-AM) presented was able to handle cold start. This was a major difference between T-AM and the collaborative models - TaRS, TaCM, and TrustSVD that were assessed. T-AM, as a collaborative model, was engineered so that trusted members of the F2F network can recommend a new entrant into the network. This implies that the continuous collaboration of a new entrant into the network will affect the entrant's trust rating of the recommender positively or negatively. It is interesting to note that based on the foregoing review, it was observed that local trust and global trust, or personal and reputational trust, either implicitly or explicitly, were a common trait. These conceptions were therefore operationalized towards raising the metrics needed to assess TaRS, TaCM, TrustSVD, and T-AM. Based on the philosophy and theory supporting this research work, trustworthiness becomes the nexus metric theme. Knowing that reputational trust (global metrics, since its rating is based on the recommendation of other peers) better influences personal trust (which is localized), reputational trust is adapted to assess trustworthiness.

This approach was considered plausible since (as earlier mentioned), the challenge of cold start was handled by the T-AM collaborative model, unlike the others - TaRS, TaCM, and TrustSVD. So, their assessment, therefore, adopts reputational accuracy, convergence, and effectiveness to be able to assess the influence of similarity and proximity of users towards recommending trusted peers.

The practice is consistent with the practice in Lagesse (2012), where similarity metrics were conceptualized and used. In Table 4.1, the actual trust metrics used and the weight attached to depict the effect of the metrics on the trustworthiness of recommendation are presented. Since it is easier to trust people with whom one has had a previous trust relationship than someone recommended, personal trust was assigned 2 points.

Trust relationships are a very important aspect of social information, and we are more likely to accept viewpoints from people that we trust (Sinha and Swearingen, 2001; Ziegler and Lausen, 2004). Trust also increases rapidly with higher recommendation (Netrvalova and Safarik, 2011); therefore, reputation was assigned 2 points, similarity 2 points, and proximity 2 points to be consistent with literature as presented in Figures 4.1 and 4.2. The models for the assessment are presented in equations 3.1, 3.2, and 3.3.

$$\alpha = \frac{\sum_{i=0}^{n-1} \left| R_p^i - R_\beta^i \right|}{n} \tag{3.1}$$

$$\chi^{(t)} = \frac{\left| R_p(t) - R_p(\infty) \right|}{R_p(\infty)} \tag{3.2}$$

$$\in = \frac{\alpha \times \chi}{\alpha_\sigma} \tag{3.3}$$

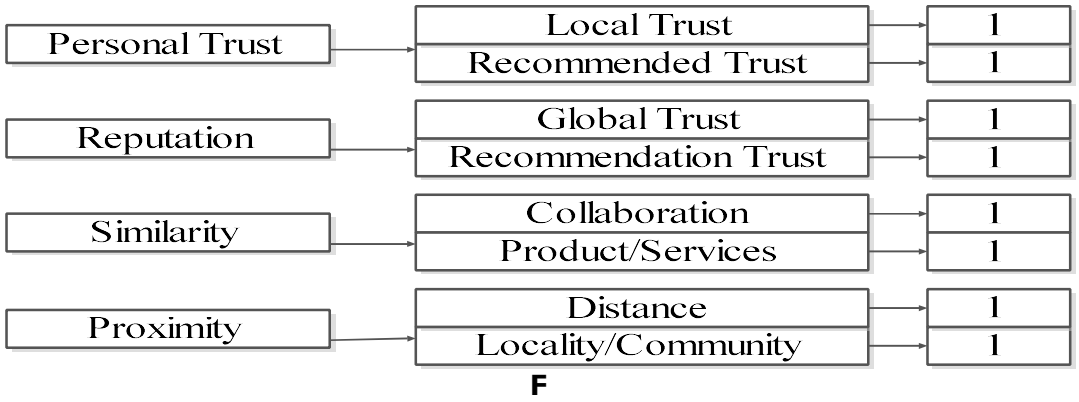

Figure 3.1: Trust Metrics and Weights

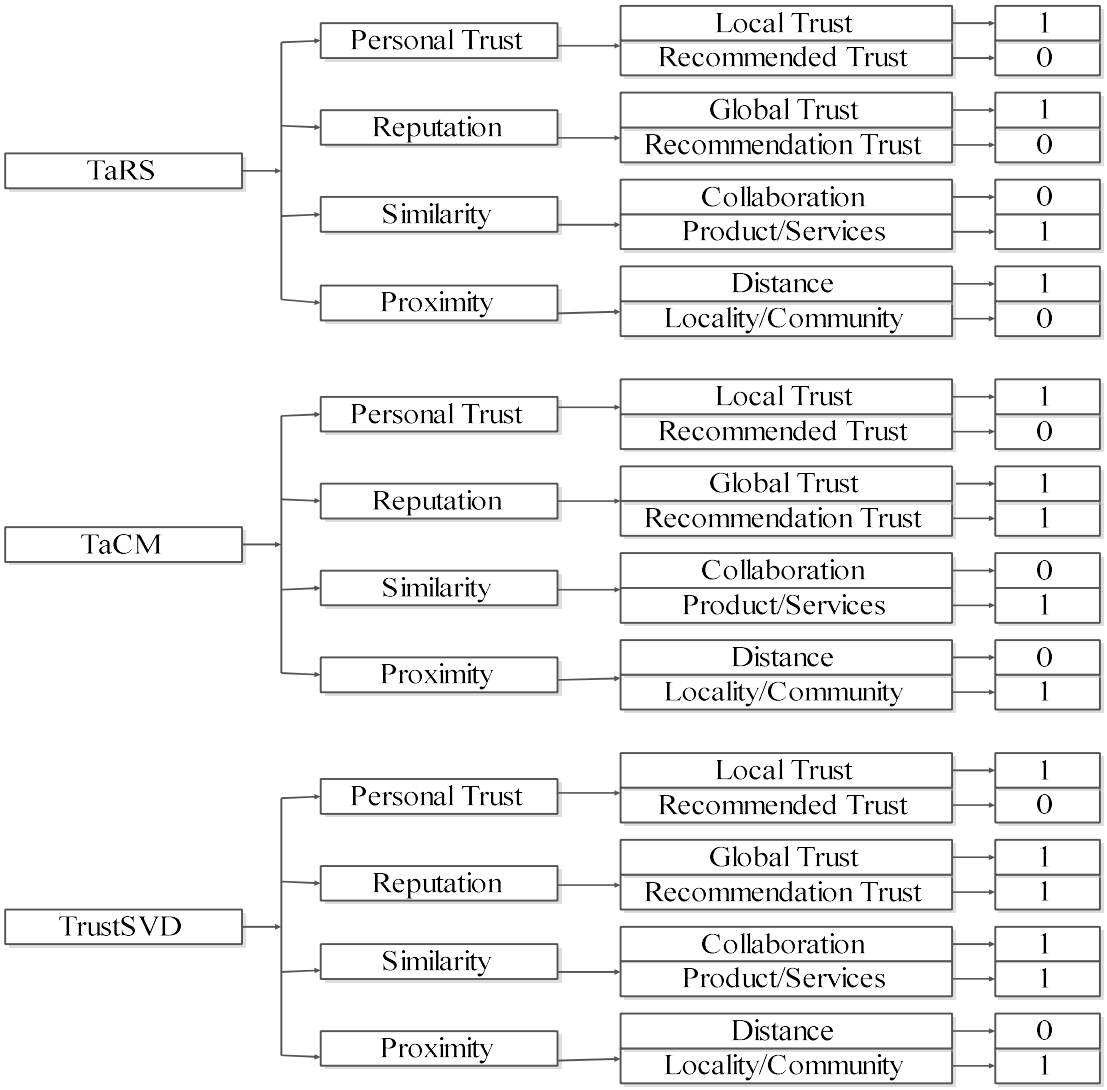

Figure 3.2: Collaborative Models Trust Metrics Weights

4. RESULTS AND DISCUSSIONS

This Section presents the result and its discussion with respect to the assessment of existing collaborative models for trust-awareness. Finally, the discussion of the result of the assessment and the prototype system's usability test are also presented. MATLAB 13.0 programming language was used to simulate the assessment of the three collaborative models and the T-AM using the parameters in Tables 4.1, 4.2, 4.3 and 5.4. The models have been discussed earlier in Section 3.6 of Chapter Three (3). The aforementioned models were simulated such that the models were evaluated for accuracy, convergence and effectiveness.

The assessment of three existing collaborative models (TaRS, TaCM and TrustSVD) using reputational accuracy, convergence and effectiveness as parameters as discussed in Section 3.0 provided information as regards the trust-awareness of each of the models. The trust metrics used for evaluation of the models were presented in Figure 3.2, the result of the model assessment for accuracy presented in Table 5.2 and Figure 5.1 show that TrustSVD reputational accuracy is 0.750, TaCM reputational accuracy is 0.625 and TaRS reputational accuracy is 0.50. The assessment of the existing models (TaRS, TaCM and TrustSVD) for reputational convergence were presented in Table 4.3 and Figure 4.2, the result show that TrustSVD had a convergent value of 0.250, TaCM convergence value is 0.375 and TaRS convergence value is 0.500. Assessment the existing models (TaRS, TaCM and TrustSVD) for reputational effectiveness were presented in Table 4.4 and Figure 4.3, the result showed that TrustSVD had a reputational effectiveness value of 0.187500, TaCM effectiveness value is 0.234375 and TaRS effectiveness value is 0.250000.

Table 4.1: Collaborative Models Rating Per Metrics

S/N	Trust Metrics	Weight	TaRS	TaCM	TrustSVD	T-AM
1	Personal Trust	2	1	1	1	2
2	Reputation	2	1	2	2	2
3	Similarity	2	1	1	2	2
4	Proximity	2	1	1	1	1

LEGEND

TaRS: Trust-aware Recommender System | TrustSVD: Trust Singular Value Decomposition

TaCM: Trust-aware Collaborative Model | T-AM:Trust-aware Collaborative Model for F2F Network

Table 4.2: Assessment of Existing Collaborative Models for Accuracy (α)

No. of Predictors	TaRS Accuracy (α)	TaCM Accuracy (α)	TrustSVD Accuracy (α)
1	0.125	0.125	0.125
2	0.250	0.375	0.375
3	0.375	0.500	0.625
4	0.500	0.625	0.750

LEGEND

TaRS: Trust-aware Recommender System | TrustSVD: Trust Singular Value Decomposition

TaCM: Trust-aware Collaborative Model

Table 4.3: Assessment of Existing Collaborative Models for Convergence (χ)

No. of Predictors	TaRS Convergence (χ)	TaCM Convergence (χ)	TrustSVD Convergence (χ)
1	0.875	0.875	0.875
2	0.750	0.625	0.625
3	0.625	0.500	0.375
4	0.500	0.375	0.250

LEGEND
TaRS: Trust-aware Recommender System
TaCM: Trust-aware Collaborative Model
TrustSVD: Trust Singular Value Decomposition

Table 4.4: Assessment of Existing Collaborative Models for Effectiveness ($\in$)

No. of Predictors	TaRS Effectiveness ($\in$)	TaCM Effectiveness ($\in$)	TrustSVD Effectiveness ($\in$)
1	0.109375	0.109375	0.109375
2	0.187500	0.234375	0.234375
3	0.234375	0.250000	0.234375
4	0.250000	0.234375	0.187500

LEGEND
TaRS: Trust-aware Recommender System
TaCM: Trust-aware Collaborative Model
TrustSVD: Trust Singular Value Decomposition

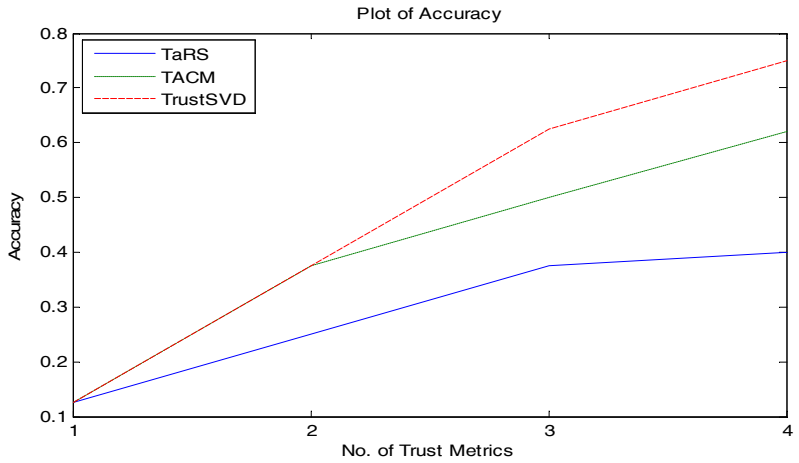

Figure 4.1: Collaborative Model Assessment for Accuracy

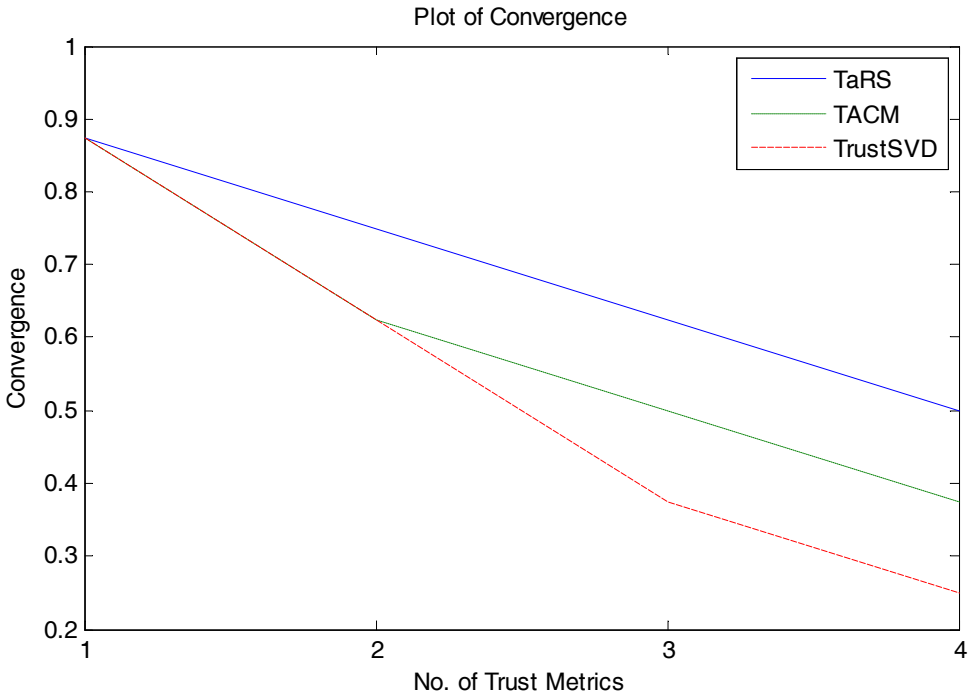

Figure 4.2: Collaborative Model Assessment for Convergence

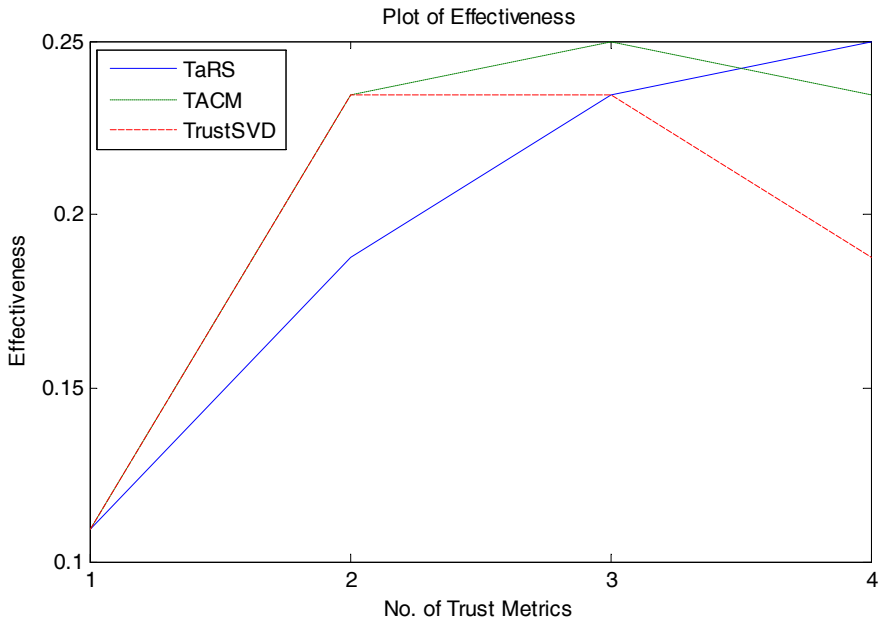

Figure 4.3: Collaborative Model Assessment for Effectiveness

The simulation result showed that TaRS out performed TaCM, while TrustSVD outperformed TaRS with respect to recommendation accuracy and convergence. This actually buttresses the fact that trust awareness improves the performance of collaborative systems like recommender system.

4.1 Result of the Assessment of TrustSVD and T-AM

In order to access the performance of T-AM, the performance of T-AM was benchmarked against the earlier result obtained from the assessment of the existing models that showed that TrustSVD performed better than the other models assessed as it had the highest reputational accuracy and converges faster than other collaborative models considered during the assessment. The goal was to evaluate its performance in recommending trustworthy collaborators. Table 4.5 and Figure 4.4, showed the result of the assessment of T-AM and TrustSVD for accuracy. From the result T-AM had a reputational accuracy of 0.875 compared to TrustSVD that had a reputational accuracy of 0.750. The assessment of T-AM and TrustSVD for reputational convergence was presented in Table 5.6 and Figure 4.5, the result showed that T-AM had a reputational convergence value of 0.125 while TrustSVD had a convergent value of 0.250. The implication of this result is that T-AM converges faster than TrustSVD. Assessing T-AM and TrustSVD for reputational effectiveness was presented in Table 4.7 and Figure 4.6, the result show that T-AM had a reputational effectiveness of 0.109375 while TrustSVD had a reputational effectiveness value of 0.187500.

Table 4.5 Assessment of TrustSVD and T-AM for Accuracy

No. of Predictors	TrustSVD Accuracy (α)	T-AM Accuracy (α)
1	0.125	0.250
2	0.375	0.500
3	0.625	0.750
4	0.750	0.875

Table 4.6 Assessment of TrustSVD and T-AM for Convergence

No. of Predictors	TrustSVD Convergence (χ)	T-AM Convergence (χ)
1	0.875	0.750
2	0.625	0.500
3	0.375	0.250
4	0.250	0.125

Table 4.7 Assessment of TrustSVD and T-AM for Effectiveness

No. of Predictors	TrustSVD Effectiveness ($\in$)	T-AM Effectiveness ($\in$)
1	0.109375	0.187500
2	0.234375	0.250000
3	0.234375	0.187500
4	0.187500	0.109375

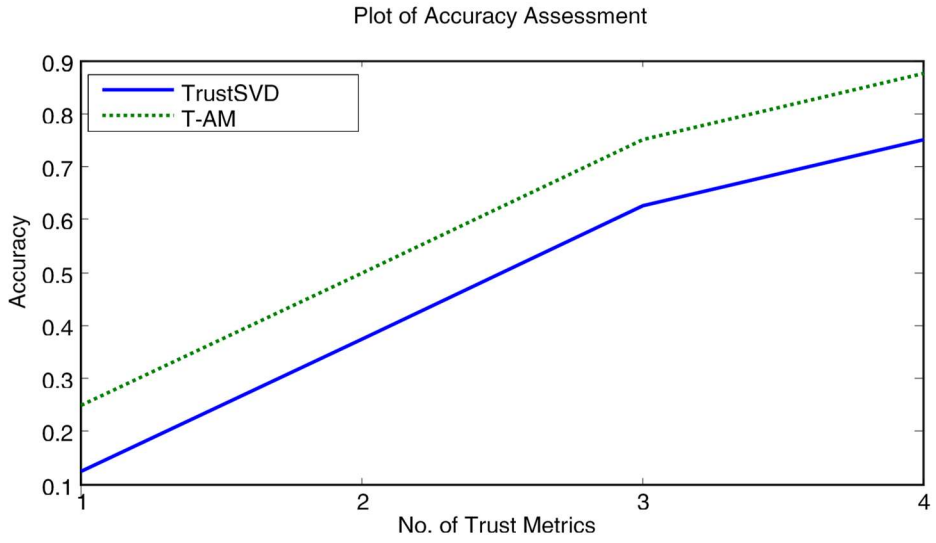

Figure 4.4: Assessment of TrustSVD and T-AM for Accuracy

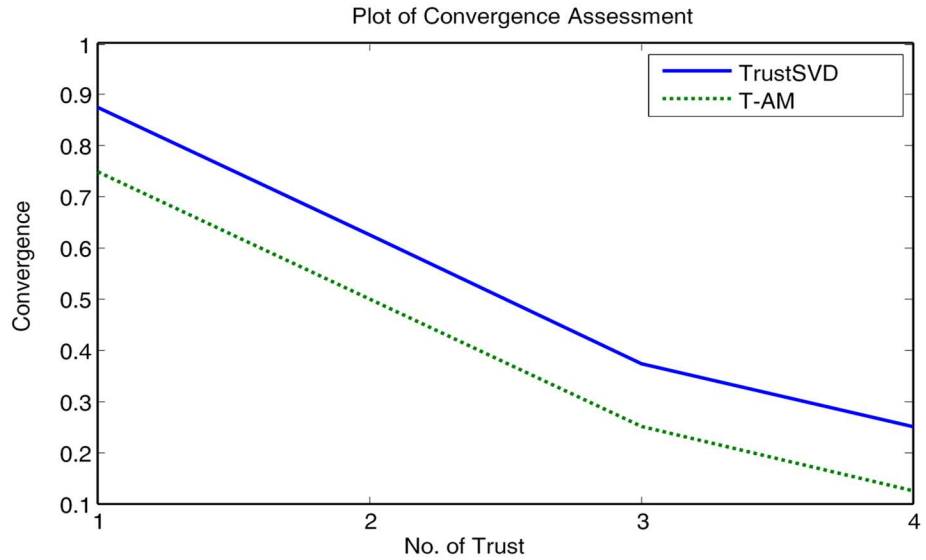

Figure 4.5: Assessment of TrustSVD and T-AM for Convergence

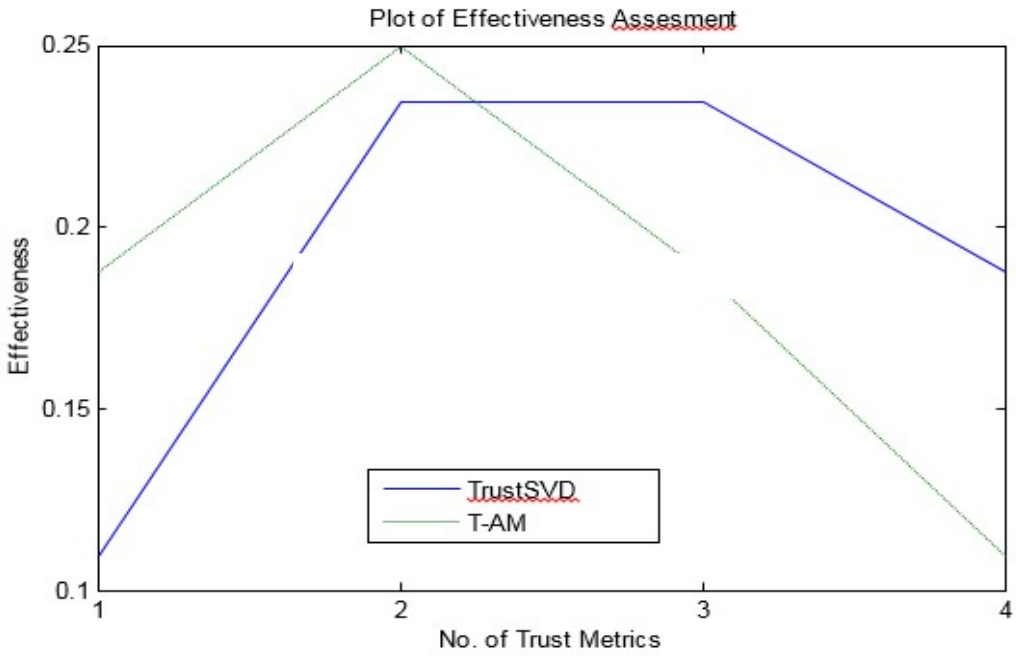

Figure 4.6 Assessment of TrustSVD and T-AM for Effectiveness

5. CONCLUSION

The results of the assessment of existing collaborative models show that reputational accuracy increases with increasing number of predictors and also converges faster as the number of predictor's increases, but the effectiveness of the model reduces as the number of predictors increases. Benchmarking T-AM with TrustSVD that performed better than TaCM and TaRS during the assessment of the existing models earlier presented in Section 4.2, result showed that T-AM have an edge over TrustSVD in the aspect of reputational accuracy and reputation convergence whereas, TrustSVD performance is better in effectiveness assessment. The T-AM's better performance was a function of the number of metrics that were considered in the model for trust evaluation.

REFERENCES

1. Buchegger, S., Schiloberg, D., Vu, L.H., and Datta, A (2009). PeerSoN: P2P Social Networking: Early Experiences and Insights. *In proceedings of the Second ACM EuroSys Workshop on Social Network Systems*, pp. 46-52.
2. Chen, X., and Pan, Y. H. (2014). The Study of Open Source Software Collaborative User Model Based On Social Network and Tag Similarity. *Journal of Electronic Commerce Research*, 15(1), 77.
3. Forster, S., Pinggera, J., and Weber, B. (2012). Collaborative Business Process Modelling. In EMISA. 206, 81-94.
4. Galuba, W. (2008). Friend-to-Friend computing: Building the social web at the internet edges (No. LSIR-REPORT-2009-003). Retrieved from http://lsirpeople.epfl.ch/galuba/ papers/ f2f.pdf on 15/10/2014 @ 7.06pm.
5. Greenwald, G. and MacAskill, E. (2013). NSA Prism Program Taps into User Data of Apple, Google and Others. 2013. Retrieved from http://www.guardian.co.uk/world/2013/Jun/06/ us-tech-giants-nsa-data on 08-07-2014 @ 8.00pm.
6. Guo, G., Zhang, J., and Yorke-Smith, N. (2015, January). TrustSVD: Collaborative Filtering with Both the Explicit and Implicit Influence of User Trust and of Item Ratings. In *AAAI*, pp. 123-129.
7. Haydar, C., Boyer, A., and Roussanaly, A. (2012). Hybridising collaborative filtering and trust-aware recommender systems. In *8th International Conference on Web Information Systems and Technologies-WEBIST*'2012.
8. Krishnamurthy, B. and Wills, C. (2009). On The Leakage of Personally Identifiable Information via Online Social Networks. In *Proceedings of the Workshop of on Online Social Networks.* Retrieved from http:/www.research.att.com/~bala/papers/www09.pdf on 06/08/2014 @ 9.00pm.
9. Lagesse, B. (2012). Analytical Evaluation of P2P Reputation Systems', *International Journal of Communications Networks and Distributed Systems*, 9(1), 82-96.
10. Massa, P., and Avesani, P. (2004). Trust-aware collaborative filtering for recommender systems. In *On the Move to Meaningful Internet Systems 2004*: CoopIS, DOA, and ODBASE, pp. 492-508. Springer Berlin Heidelberg.
11. Opsahl, K. (2010). Facebook's Eroding Privacy Policy: A Timeline. Retrieved from https://www.eff.org/deeplinks/2010/04/facebook-timeline on 22/04/2014 @ 6.06pm.
12. Popescu, B.C., Crispo, B., and Tanenbaum, A.S. (2006). Safe and Private Data Sharing with Turtle: Friends Team-Up and Beat the System. In *Proceedings of Security Protocols*, Springer Berlin Heidelberg, pp. 221-230.
13. Sinha, R. R., and Swearingen, K. (2001). Comparing Recommendations Made by Online Systems and Friends. In *DELOS workshop: personalisation and recommender systems in digital libraries* (Vol. 106). 24/11/2015 @ 02:12pm.
14. Steel, E. and Vascellaro, J.E. (2010). Facebook, Myspace Confront Privacy Loophole, The wall Street Journal, May Edition.
15. Varlamis, I., Eirinaki, M., and Louta, M. (2013). Application of social network metrics to a trust-aware collaborative model for generating personalized user recommendations, *Springer Vienna*, pp. 49-74.

16. Ziegler, C.N., and Lausen, G. (2004). Analyzing correlation between trust and user similarity in online communities. *In International Conference on Trust Management,* Springer Berlin Heidelberg, pp. 251-265.
17. Netrvalova, A., and Safarik, J. (2011). Trust Model for Social Network. In *Proceedings of the 25th European Simulation and Modelling* Conference, October 24-26, Guimaraes, Portugal, pp. 102-107.