International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-6S3, September 2019

# Mining Social Media Content to Predict Peer Trust Level in Social Networks

**Sumithra M, Asha Abraham, M.Rajesh, N.Nithiyanandam**

***Abstract*: Paper Setup must be in A4 size with Margin: Top 0.7", Bottom 0.7", Left 0.65", 0.65", Gutter 0", and Gutter Position Top. Paper must be in two Columns after Authors Name with Width 8.27", height 11.69" Spacing 0.2". Whole paper must be with: Font Name Times New Roman, Font Size 10, Line Spacing 1.05 EXCEPT Abstract, Keywords (Index Term), Paper Tile, References, Author Profile (in the last page of the paper, maximum 400 words), All Headings, and Manuscript Details (First Page, Bottom, left side).Paper Title must be in Font Size 24, Bold, with Single Line Spacing. Authors Name must be in Font Size 11, Bold, Before Spacing 0, After Spacing 16, with Single Line Spacing. Please do not write Author e-mail or author address in the place of Authors name. Authors e-mail, and their Address details must be in the Manuscript details. Abstract and Keywords (Index Term) must be in Font Size 9, Bold, Italic with Single Line Spacing. All MAIN HEADING must be in Upper Case, Centre, and Roman Numbering (I, II, III…etc), Before Spacing 12, After Spacing 6, with single line spacing. All Sub Heading must be in Title Case, Left 0.25 cm, Italic, and Alphabet Numbering (A, B, C…etc), Before Spacing 6, After Spacing 4, with Single Line Spacing. Manuscript Details must be in Font Size 8, in the Bottom, First Page, and Left Side with Single Line Spacing. References must be in Font Size 8, Hanging 0.25 with single line spacing. Author Profile must be in Font Size 8, with single line spacing. Fore more details, please download TEMPLATE HELP FILE from the website.*

***Keywords* : About four key words or phrases in alphabetical order, separated by commas.**

## I. INTRODUCTION

Data analytics (DA) refers to qualitative and quantitative techniques with set of processes to examine the data sets to analyze data behaviors and to identify patterns enhance productivity and business gain in order to draw conclusions with the aid of specialized systems and software. The techniques and technologies are widely used in social networks to facilitate commercial industries and enterprises to make more-informed business decisions and by scientists and researchers to verify or disprove scientific models, theories and hypotheses. The Social networks are turning into an incredibly powerful wellspring of aggregate 0intelligence insight. There are 2.5 quintillion bytes of information made every day. In recent two years alone 90 percent of the information on the planet was created. More than 3.7 billion people utilize the web (that is a development rate of 7.5 percent more than 2016). Worldwide there are 5 billion inquiries per day. As per Domo's Information Never Dozes 5.0 report, these are numbers produced each moment of the day: Snapchat clients share 527,760 photographs, in excess of 120 experts join LinkedIn, clients watch 4,146,600 YouTube recordings, 456,000 tweets are sent on Twitter, Instagram clients post 46,740 photographs. With 2 billion dynamic clients Facebook is as yet the top most social media platform as sown in Fig.1. These PB of data can be utilized by commercial organizations through data analytics tools to identify useful patterns and trends. The knowledge gained from such big data are influenced in futuristic product design, election result prediction, stock market analysis, connecting friends and followers etc.,

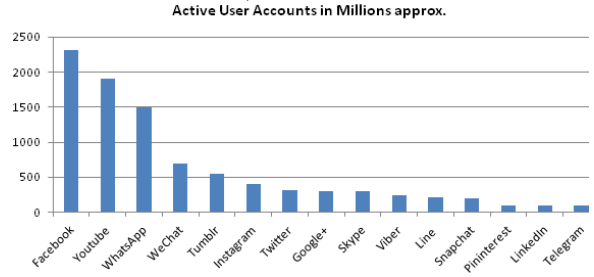


Fig.1 Active User Accounts in Social Media

Evolving data facilitates decision-making. For example, a social networking website gathers information identified with client interests and fragment it as per determined criteria related to user preferences, community interests and categorize based on demographics, age or gender. The business analysts can filter the user details and their trends to enhance the social network's to configure the layout, content and overall strategy. Data can be categorized as implicit data and explicit data. Utilizing the social data has some serious challenges like identifying fake data, applying mining techniques to infer the exact sense of the phrase. Users generate data in form of discussions, reviews and ratings are usually unstructured data and impossible to process it manually. It is mandatory to predict the meaning of the phrases, images, notations from the social media content to identify the implicit representation of the data. Those identified data can be used as a feature to make decision in correlating users as a cluster to make business related decisions. Identifying the related users and the level of trust can enable the OSN users to receive high quality recommendations. Moreover, trust is often employed to prevent spams and attacks [1] and thus improving the security of social networks. Sherchan et al. [2] has identified trust as a critical factor to the social capital of an online community.

**Manuscript published on 30 September 2019.**
***** Correspondence Author (s)
**Sumithra M,** Department of Computer Science and Engineering, Veltech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, Chennai, Tamil-Nadu, India
**Asha Abraham,** Department of Computer Science and Engineering, Veltech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, Chennai, Tamil-Nadu, India
**Rajesh M,** Dept of Computer Science and Engineering, KRS College of Engineering., RaGa Academic Solutions, Tamilnadu, India.
**N.Nithiyanandam**, Assistant Professor, Department of Computer Science and Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, Chennai, Tamilnadu, India

Ruan and Durresi [3] overviewed trust derivation and potential nearby trust related assaults in online social networks. Josang et al. [4] dissected inquires about on trust and notoriety frameworks for OSNs. In spite of the fact that there are a few studies about trust calculation, they infrequently explored pairwise trust forecast that depicts a connection between two clients of Online Social Networks[OSN], particularly with machine learning based strategies, which have appeared to be viable in construing inert trust relations and outflank other traditional techniques [10], [11].

Commonly, trust models are framed based on combination of input features such as knowledge, experience, and reputation, and the weight of this linear combination determines the importance of each feature [35]. Machine learning techniques are developed to formulate the features which contribute to higher trust. Sometimes two low value features can contribute to a high trust when combined together. Since the research in this topic is lagging, this paper provides various means of researches in pairwise trust prediction using machine learning techniques from multiple perspectives. Finally, we discuss a number of potential future research directions in this research field. This work is addressed to researchers and practitioners interested in applying machine learning to predict pairwise trust in OSN.

## II. RELATED WORKS

Since OSN is rapidly developing advertisement platform, the colossal information produced straightforwardly by the clients are the data related to future costumers of the business associations. Let's see the researches done to improve the trust level in such associations in Social networks.

Trust related reviews are used in areas like Data Analytics, IoT, Computational Knowledge, MANET, etc. Zhu and Yan [29] examined trust assessment in Business-to-Client (B2C), Business-to-Business (B2B), Distributed (P2P), Client to-Client (C2C), and Government-to-Client (G2C).

Yan et al. [31] completed a far reaching writing audit on trust the executives in IoT with spotlight on subjects like trust assessment, trust system, information observation trust, personality trust and security conservation and so on.

Abdelghani et al. [33] talked about trust the executives in another worldview, social web of things which is a mix of IoT and informal organizations.

In the field of OSNs, references [2] and [3] are the two most related work. Sherchan et al. [2] introduced a review tending to three parts of social trust: trust data gathering, trust assessment and trust dispersal. While Ruan and Durresi [3] gave more consideration to confide in demonstrating, trust surmising and assaults. For the assault examination, they concentrated on local trust trust related assaults like naive attack, traitor attack, whitewashing attack, collusion attack instead of global trust related attack.

For the other related works, Cho et al. [5] gave a productive information on how to display trust in a given area. He concentrated on properties and definition of trust factors. Chomphoosang et al. [32] completed an exploration on watermark methods that can be utilized in Social networks to secure the substance of data. Pranata et al. [28] led an ease of use and adequacy examination on trust rating frameworks through mysterious online review. 5-star rating frameworks, Contrasted and parallel frameworks, and documentation based rating frameworks are favored regarding ease of use.

Despite the fact that there are a few overviews about trust computation, they seldom explored pairwise trust prediction, especially with machine learning based techniques. Numerous regular strategies simply considered a weighted capacity like whole of trust initiating factors [35].

## III. PAIRWISE TRUST PREDICTION CRITERIA IN SOCIAL NETWORKS

Trust can be referred as "Reliability, Confidence, Faith, Reputation, Competence, Belief and Honesty" [GH04]. Trust represents some quantitative value associated with it such that A trusts B, but to what extent is not clearly defined. Trust is multidirectional in which B may not trust A at all. For the purposes of our work trust can be seen as the aggregation of many of the synonyms used above in conjunction. Web services must be reliable and inspire confidence in their users. Their information must be realistic and honest to create a reputation of trust in web services. Some real case scenarios like e-life insurance, online shopping advertisements are some online services based on the trust level. Generally trust models can be split into socially based and observationally based models of trust. In Pairwise trust in social networks is represented as the edge of a directed graph G (V , E) where V represents a set of unique users and E denotes a set of edges (also known as relationships) between users. Some edges are labeled as EL, and all other edges are labeled as EU.

### A.Pairwise Trust Definition And Properties

Further, we can abridge the properties of pairwise trust as pursues

**Abstract:** Even though trust appraisal is unthinkable because of uncertainty of information, trust assessment is exceptionally affected by the individual interests. Therefore, subjectivity has been perceived as the inherent nature of trust.

**Logical:** Trust computing relies upon explicit con-writings. An online client whose audit is trustable in e-ticket portal may not be great in e-blogging. [6].

**Dynamic:** Trust level is dynamic since one's interest may change over some stretch of time.

**Uneven:** Trust dimension of client A need not be same as the trust dimension of client B over A. Trust is dependably multi directional and may varies in various proportions in various perspectives between clients.

**Propagative:** If A trusts B, and B confides in C with whom A has no association, the trust of A towards C can be concluded from the level of trust A to B and B to C making a trust chain.

**Delicate:** Trust can be effectively crushed as opposed to building. Significantly higher trust esteems may lost its trust by few negative audits about the client.

### B.Pairwise Trust Evaluation Scale

Based on the range of value used to measure the trust, three different trust scaling methods are in practice namely binary, discrete and continuous. Binary uses only two cases either to be trusted are not.

The discrete scale uses different words to represent different levels of trust viz., distrust, moderate distrust, moderate trust and complete trust. Continuous value is more expressive and can describe the extent to which one trusts another. Marsh scales trust in [1, 1] where 0 indicates the state of being completely ignorant or uncertain [8]. This section covers some of the models to predict trust using machine learning methods

## IV.VARIOUS MODELS TO PREDICT TRUST

This section covers some of the models to predict trust using machine learning methods.

According to Mitchell "A computer program is said to learn from experience E with respect to some class of tasks T and performance measure P, if its performance at tasks in T, as measured by P, improves with experience" [9]. According to this definition, a dataset with some common interest and relationship of user pairs are trained with an experience, E for a Task T, to measure the trust level to evaluate the performance P.

### A.Feature Engineering

Feature engineering makes use of domain knowledge to create useful features from a raw dataset. It is needed since raw dataset is usually not amenable to learning. Feature engineering is the key element in deciding whether a machine learning project can succeed or not. This is because a good feature set with many independent features that correlate well with the result makes the learning process much easier [12]. Moreover, well engineered features can help to avoid overfitting theory. These theories are often examined on trust-related datasets first before training a model. The features can be created either from the contextual interaction data between two users or from the structural trust network underlying raw datasets. Features derived from the interaction history represent direct knowledge of a user towards his candidate trustee. However, they might be unavailable for two users who has not involved any kind of interactions.

In the context of OSNs, trust is more closely related to the social trust derived from the discipline of sociology and psychology. ``Social trust between two individuals is often studied by examining interaction history, similarity in preferences, background, demographics, reputation or recommendation from third parties, different life experiences and so forth" [5]. Here, we classify the trust features according to the view of both trustor and trustee with considering different context as the following five aspects, namely, trustor's objective factors, trustor's subjective factors, trustee's objective factors, trustee's subjective factors and context [27].

**Trustor's objective factors:** It refers to the criteria or policies specified by the trustor for a trust decision such as the trustor's standards, regulations, laws and etc.,

**Trustor's subjective factors:** Different from objective factors, trustor's subjective factors rely more on trustor's.

**Trustee's objective factors:** It includes reputation, ability, integrity, dependability and so on. It is the most used one.

**Trustee's subjective factors:** Honesty, benevolence, goodness and propensity are the main subjective factors of trustee.

**Context:** It describes when, where and why the trust relationship is applied. Notably, the inducing factors could be different and paid different attention by a trustor in different situations and contexts. In this paper, we focus on the context of OSNs where trust predictions are implied mainly for social activities. It is worth to note that these features might be independent, dependent, or conflicting with each other. Thus, it is desirable to examine the correlation among the constructed features before training a model.

### B.Machine Learning Models

In this subsection, we analyze the machine learning models most widely applied in predicting trust. At the same time, it is remarkable that machine learning models cannot achieve the best performance by just combining trust features and standard classifiers without considering optimization techniques. Hence, we also present optimization techniques in terms of imbalance problems, new data integration and over fitting.

#### 1. Machine Learning Algorithms

Three major classifications of machine learning algorithms are supervised learning, unsupervised learning and reinforcement learning. In supervised learning the labeled dataset is trained to predict the future judgments via mapping the relationship. In unsupervised learning, patterns are identified from the unlabelled dataset. In Reinforcement method the system is allowed to behave in an interactive environment to learn through its trial and error.

As we mentioned before, trust prediction has often been modeled as a classification problem. In machine learning classification can be done through supervised learning methods like Decision tree, K-NN, SVM, Neural networks, Naïve Bayesian Classification, ensemble Logistic and Linear regression techniques. Its performances are mentioned in table 1. The performance of all the variants may vary depends on the parameters. In our analysis, we considered the implicit conversion factor as a factor for determining the performance.

#### 2. Optimization Techniques

To achieve the high level accuracy in pairwise trust prediction in social networks, the following cases need to be practiced while training the models.

In most of the trust related datasets the ratio of positive trust is higher than distrust ratio. Usually the datasets hold 70% trust data. Supervised learning classification techniques are sensitive towards imbalance distribution. Resampling method uses under sampling strategy to build a better classifier than over-sampling strategy.

SMOTE as a variation uses under-sampling strategy along with over-sampling strategy to avoid minority class replication. Cost sensitive method assigns cost to minority classes. Higher cost represents error in minority class. Some researchers discussed about cost-sensitive C4.5 [13], cost-sensitive NB [14],cost- sensitive SVN[15], cost-sensitive MLP [16], cost-sensitive logistic regression [17] and cost-sensitive ensemble of decision trees [18].

| Classifier | Pros | Cons |
|---|---|---|
| DT | Handles both discrete and categorical features. | Not suitable for imbalanced datasets. |
| K-NN | No parameters to tune | Require large space for feature selection |
| NB | Accurate with small dataset too. | Deals only with discrete features. |
| SVM | Complex irrespective of applied features | Large dataset is needed |
| NN | Suitable for non-linear classification | Feature sensitive; time consuming |
| LR | Flexible with new data; robust | Cannot deal with continuous result |
| Ensemble | Can reduce the generalization error; reliable and accurate | Requires additional computation |

TABLE 1: Comparisons of typical Classifiers

Similarly SVM and NN are also used to predict the pairwise trust level efficiently [19][20]. In machine learning, "it is generation that counts" [12]. Therefore, a trained model must be tested on unseen data. Cross validation techniques can be used to make dynamic subset of data and utilize it randomly for training and testing .An iterative based 5 fold or 10 fold cross validations are practiced for better result.

## 3. Performance Evaluation

Most regularly utilized execution measurements in paired arrangement are perplexity network. Table 10 speaks to the disarray grid in trust expectation with the equations. The classifier assemble the datasets in 4 classes with an ostensible qualities spoke to as evident positives (TP), false positives (FP), genuine negatives (TN) and false negatives (FN).TP-The quantity of models effectively delegated trust. FP-The quantity of questioned occasions mistakenly marked as trust. TN-The quantity of precedents with doubt relationship effectively anticipated as doubt. TN-The quantity of confided in things that are misclassified as doubt.

Based on the above discussion, we argue that FP and TN are more important than TP and FN in trust prediction for real life applications. However, working out a set of formulas to describe their relative gains of correct prediction and cost of incorrect prediction involves multiple disciplines.

### Confusion Matrix and ROC Curve

TN - True Negative
FP - False Positive
FN – False ?Negative
TP - -True Positive

| | | Predicted Class | |
|---|---|---|---|
| | | No | Yes |
| Observed Class | No | TN | FP |
| | Yes | FN | TP |

TABLE 2: The Confusion Matrix and ROC Curve

### Accuracy

Accuracy represents the percentage of correctly classified trust pairs. In table 11 both the classifiers hold 80% accuracy. However, classifier 2 clearly predicts distrust much better than classier 1 Thus accuracy alone is not suitable for trust prediction.

### Precision/ Recall

This metric differentiates the strength of each classifier to predict trust level but it fails to predict the distrust proportion correctly. If recall is used, it reflects the capacity of distrust ratio but fails to evaluate trust value.

### Model performance

Accuracy = (TN+TP)/(TN+FP+FN+TP)

Precision =TP/(FP+TP)

Sensitivity =TP(TP+FN)

Specificity =TN/(TN+FP)

### F-Measure

In F-measure precision and recall are treated as single metric. F-measure can be used to obtain a trade-off between precision and recall. However, like precision and recall, F-measure cannot reflect how well a classifier handles negative cases [21].

### Receiver Operator Character (Roc)

When using a scalar quantity values, the prediction will be more accurate. In the figure, the diagonal line is used as a base line. It is clear that classifer2 is closer to true positive which depicts the most trusted pair value with higher TP. Tom Fawcett recommends averaging the ROC curves of multiple testset when comparing classifiers in order to take into account variance [22].

Even though ROC curve is mostly preferred to evaluate a binary classifier, it has following pitfalls:

Firstly, direct comparisons of classifiers of different families with different thresholds are impossible. Secondly, discrete classifiers must be converted to scoring versions to generate a full ROC curve. Thirdly, it is suitable for applications like trust prediction only after performing certain transformations[22].

### Precision-Recall (Pr) Curve

PR curve plots recall on x-axis and precision on y-axis. Even though it shares many common characteristics with ROC curve, PR curve is different in terms of optimal classifiers sit on upper right hand corner in the PR space. Unlike ROC with fixed base line, the base line of PR curve changes with the ratio of positive instance to negative instance.



Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

ROC curve for tasks with imbalanced datasets since PR plots precision that can capture the poor performance of a classifier for imbalanced datasets. As a result, PR curve has been proposed to be an alternative to ROC curve for tasks with strongly imbalanced datasets [23].

To sum up, an evaluation process must be executed after training a model in order to evaluate the performance of the trained model. In addition, evaluation is needed when comparing several different models to select an optimal one.

## V.FUTURE SCOPE

First, the robustness of trust prediction to overcome potential attacks is discussed in [10]. We recommend Whitewashing attacks by setting a forgetting factor. But it is still vulnerable to other attacks. Second, trust building and fading time are not exactly available due to dynamic user signup and leaving the OSNs which is discussed in [24] and [25]. Third, users behavior data like ratings, reviews, search history, friends list, hobby, community status are maintained with less security. Forth, trust can be treated as a continuous value as discussed in [7] and [26] and can be examined using regression algorithms.

## VI. CONCLUSION

In this paper, we performed trust prediction with machine learning techniques in OSNs from many perspectives. Specifically, we implemented and analyzed the pipeline of trust predicting models. We also analyzed the feature extracting process and recognized its crucial role in predicting trust. In addition, we examined different families of machine learners and presented their cost-sensitive and incremental variants that can help fighting against class imbalance and continuous system growth problems. The important performance metrics were also discussed before we walked through existing trust prediction models and enumerated their pros and cons.

## REFERENCES

1. A. Mohaisen, N. Hopper, and Y. Kim, ``Keep your friends close: Incorpo-rating trust into social network-based sybil defenses," in Proc. INFOCOM, vol. 11, Apr. 2011, pp. 336 340.
2. W. Sherchan, S. Nepal, and C. Paris, ``A survey of trust in social networks," ACM Comput. Surv., vol. 45, no. 4, Aug. 2013, Art. no. 47.
3. Y. Ruan and A. Durresi, ``A survey of trust management systems for online social communities Trust modeling, trust inference and attacks," Knowl.-Based Syst., vol. 106, pp. 150 163, Aug. 2016.
4. A. Jøsang, R. Ismail, and C. Boyd, ``A survey of trust and reputation systems for online service provision," Decis. Support Syst., vol. 43, no. 2, pp 618 644, Mar. 2007.
5. J.-H. Cho, K. Chan, and S. Adali, ``A survey on trust modeling," ACM Comput. Surv., vol. 48, no. 2, Nov. 2015, Art. no. 28.
6. J. Tang, H. Gao, and H. Liu, ``mTrust: Discerning multi-faceted trust in a connected world," in Proc. 5th ACM Int. Conf. Web Search Data Mining, Feb. 2012, pp. 93 102.
7. H. Fang, G. Guo, and J. Zhang, ``Multi-faceted trust and distrust prediction for recommender systems," Decis. Support Syst., vol. 71, pp. 37 47, Mar. 2015.
8. S. P. Marsh, ``Formalising trust as a computational concept," Ph.D. dissertation, Dept. Math. Comput. Sci., Stirling Univ., Stirling, Scotland, 1994.
9. T. M. Mitchell, Machine Learning. New York, NY, USA: McGraw-Hill, 1997.
10. J. López, and S. Maag, ``Towards a generic trust management frame-work using a machine-learning-based trust model," in Proc. Trust-com/BigDataSE/ISPA, vol. 1, Aug. 2015, pp. 1343 1348.
11. E. Khadangi and A. Bagheri, ``Comparing MLP, SVM and KNN for predicting trust between users in Facebook," in Proc. Comput. Knowl. Eng. (ICCKE), Oct./Nov. 2013, pp. 466 470.
12. P. Domingos, ``A few useful things to know about machine learning," Commun. ACM, vol. 55, no. 10, pp. 78 87, 2012.
13. K. M. Ting, ``An instance-weighting method to induce cost-sensitive trees," IEEE Trans. Knowl. Data Eng., vol. 14, no. 3, pp. 659 665, May 2002.
14. A. Ibáñez, C. Bielza, and P. Larrañaga, ``Cost-sensitive selective Naïve Bayes classi ers for predicting the increase of the h-index for scienti c journals," Neurocomputing, vol. 135, pp. 42 52, Jul. 2014.
15. P. Cao, D. Zhao, and O. Zaiane, ``An optimized cost-sensitive SVM for imbalanced data learning," in Proc. Paci c Asia Conf. Knowl. Discovery Data Mining. Berlin, Germany: Springer, Apr. 2013, pp. 280 292.
16. C. L. Castro and A. P. Braga, ``Novel cost-sensitive approach to improve the multilayer perceptron performance on imbalanced data," IEEE Trans. Neural Netw. Learn. Syst., vol. 24, no. 6, pp. 888 899, Jun. 2013.
17. A. C. Bahnsen, D. Aouada, and B. Ottersten, ``Example-dependent cost-sensitive logistic regression for credit scoring," in Proc. Mach. Learn. Appl. (ICMLA), Dec. 2014, pp. 263 269.
18. B. Krawczyk, M. Wo¹niak, and G. Schaefer, ``Cost-sensitive decision tree ensembles for effective imbalanced classi cation," Appl. Soft Comput., vol. 14, pp. 554 562, Jan. 2014.
19. G. Cauwenberghs and T. Poggio, ``Incremental and decremental sup-port vector machine learning," in Proc. Adv. Neural Inf. Syst., 2001, pp. 409 415.
20. R. Polikar, L. Upda, S. S. Upda, and V. Honavar, ``LearnCC: An incre-mental learning algorithm for supervised neural networks," IEEE Trans. Syst., Man, Cybern. C, Appl. Rev., vol. 31, no. 4, pp. 497 508, Nov. 2001.
21. D. M. Powers, ``Evaluation: From precision, recall and F-measure to ROC, informedness, markedness and correlation," J. Mach. Learn. Technol., vol. 2, no. 1, pp. 37 63, 2011.
22. T. Fawcett, ``ROC graphs: Notes and practical considerations for researchers," Mach. Learn., vol. 31, no. 1, pp. 1 38, 2004.
23. T. Saito and M. Rehmsmeier, ``The precision-recall plot is more informa-tive than the ROC plot when evaluating binary classi ers on imbalanced datasets," PLoS ONE, vol. 10, no. 3, p. e0118432, Mar. 2015.
24. H. Liu et al., ``Predicting trusts among users of online communities: An Epinions case study," in Proc. 9th ACM Conf. Electron. Commerce, Jul. 2008, pp. 310 319.
25. N. Ma, E.-P. Lim, V.-A. Nguyen, A. Sun, and H. Liu, ``Trust relationship prediction using online product review data," in Proc. 1st ACM Int. Work-shop Complex Netw. Meet Inf. Knowl. Manage., Nov. 2009, pp. 47 54.
26. K. Zhao and L. Pan, ``A machine learning based trust evaluation framework for online social networks," in Proc. IEEE 13th Int. Conf. Trust, Secur. Privacy Comput. Commun. (TrustCom), Sep. 2014, pp. 69 74.
27. I. Pranata, G. Skinner, and R. Athauda, ``A survey on the usability and effectiveness of Web-based trust rating systems," in Proc. IEEE/ACIS 12th Int. Conf. Comput. Inf. Sci. (ICIS), Jun. 2013, pp. 455 460.
28. Y. Zhu and Z. Yan, ``A survey on trust evaluation in e-commerce," in Proc. 9th EAI Int. Conf. Mobile Multimedia Commun., 2016, pp. 130 139.
29. G. Xu and Z. Yan, ``A survey on trust evaluation in mobile ad hoc net-works," in Proc. 9th EAI Int. Conf. Mobile Multimedia Commun., 2016,pp.140 148.
30. Z. Yan, P. Zhang, and A. V. Vasilakos, ``A survey on trust management for Internet of Things," J. Netw. Comput. Appl., vol. 42, pp. 120 134, Jun. 2014.
31. P. Chomphoosang, P. Zhang, A. Durresi, and L. Barolli, ``Survey of trust based communications in social networks," in Proc. 14th Int. Conf. Netw.-Based Inf. Syst. (NBiS), Sep. 2011, pp. 663 666.
32. W. Abdelghani, C. A. Zayani, I. Amous, and F. Sèdes, ``Trust management in social Internet of Things: A survey," in Proc. Conf. e-Bus., e-Services e-Soc. Cham, Switzerland: Springer, 2016, pp. 430 441.
33. K. Hoffman, D. Zage, and C. Nita-Rotaru, ``A survey of attack and defense techniques for reputation systems," ACM Comput. Surv., vol. 42, no. 1, 2009, Art. no. 1.

34. J. Golbeck, ``Introduction to computing with social trust," in Computing With Social Trust. London, U.K.: Springer, 2009, pp. 1 5.
35. [GH04] Golbeck, J. and Hendler, J.: Accuracy of metrics for inferring trust and reputation in semantic web-based social networks. In Proceedings of 14th International Conference on Knowledge Engineering and Knowledge Management (EKAW'04), 5-8th October, Northamptonshire, UK (2004).