International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 5 Issue: 5 935 – 941

A Survey on True-reputation Algorithm for Trustworthy Online Rating System

Chanakya G. M
Department of IT,
Sree Vidyanikethan Engineering College,
Tirupati, A.P, India
chanakya.gm@gmail.com

G.Uma Mahesh
Department of IT,
Sree Vidyanikethan Engineering College,
Tirupati, A.P, India
umamaheshg.it@gmail.com

Abstract: The average of customer ratings on a product, which we call a reputation, is one of the key factors in online shoping. The common way for customers to express their satisfaction level with their purchases is through online ratings. The overall buyer's satisfaction is quantified as the aggregated score of all ratings and is available to all buyers. This average score and reputation of a product acts as a guide for online buyers and highly influences consumer's final purchase decisions. The trustworthiness of a reputation can be achieved when a large number of buyers involved in ratings with honesty. If some users wantedly give unfair ratings to a item, especially when few users have participated, the reputation of the product could easily be modified. In order to improve the trustworthiness of the products in e-commerce sites a new model is proposed with a true - reputation algorithm that repeatedly adjusts the reputation based on the confidence of the user ratings.

Keywords: *False reputation, trust, unfair ratings.*

*****

I. INTRODUCTION

Social network analysis has recently gained a lot of interest because of the advent and the increasing popularity of social media, such social networking applications, customer review sites. While using online shopping sites, consumers share their purchasing experiences regarding both items and services to other buyers via evaluation. The most common way for consumers to express satisfaction level with their purchases is through online ratings. The overall buyers' satisfaction is quantified as the aggregated score of all ratings and is available to all active buyers.

In this online shopping, trust is becoming recommended quality among user interactions and trustful users is crucial for all the members of the network. One common type of analysis is finding of communities of users with similar interests. Another issue is the identification of content that could be of potential interest, whether this is a product review, a blog, or a tweet. Collaborative filtering is widely adopted technique used to predict future item ratings based on the user's past behavior as well as ratings of other similar users. The aggregated score for a product is called reputation. The reputation of a product plays an important role as a guide for potential buyers and influences consumer's final purchase decisions.

Reputation is the score of a product obtained through collective intelligence, i.e., The result of collaboration between many individuals. The trustworthiness of a reputation can be achieved when a large number of buyers participated in the ratings with honesty[1]. If some users wantedly give unfair ratings to a product, especially when few users have participated, the reputation of the product could easily be manipulated. Here it defines false reputation as the problem of a reputation being manipulated by unfair ratings. In the case of a newly-launched product, for example, a company may hire people in the early stages of promotion to provide high ratings for the product. By this a false reputation adversely affects the decision making of potential buyers of the product. This describes the scenarios in which a false reputation occurs and propose a general framework that resolves a false reputation[2].

The most common way to aggregate ratings is to use the average, which may result in a false reputation. For example, a group of users may inflate or deflate the overall rating of a particular product. The existing strategies avoid a false reputation by detecting and eliminating false users[3]. However, false users cannot always be detected, and it is possible that normal users may be regarded as false users. Consequently, existing strategies can exclude the ratings of normal users or allow the ratings of abusers to be included in the calculation of a reputation[4]. The proposed framework on the other hand, uses all ratings. It evaluates the level of trustworthiness (confidence) of each rating and adjusts the reputation based on the confidence of ratings. This has developed an algorithm that iteratively adjusts a reputation based on the confidence of customer ratings.

By adjusting a reputation based on the confidence scores of all ratings, the proposed algorithm calculates the reputation without the risk of omitting ratings by normal users while reducing the influence of unfair ratings by abusers. This algorithm, which solves the false reputation problem by computing the true reputation. The computation of a trustworthy reputation starts by measuring the confidence of a rating. Previous social science studies that analyzed the

characteristics of reliable online information and adopted three key characteristics that are suitable for determining the confidence of a rating. According to previous research, the reliability of online information increases when an information producer has no bias, maintains an objective perspective (objectivity) and has a consistent viewpoint (consistency). In addition, the reliability of information increases when an information producer actively interacts with users who have obtained information through him (activity). To determine the confidence of a rating.

Three key factors of activity, objectivity, and consistency and defined these factors in the context of online ratings. First, the user who rates more items displays a higher level of activity. There exist, however, no interactions between users in an online rating system. Instead, there are actions by users of the products. Therefore, the user activity in an online rating system is measured based on the amount of actions by the user on products (i.e., The number of products he rates). The objectivity of a rating is defined as the deviation of the rating from the general reputation of the item.

The objectivity of a rating is calculated based on the deviation of the "rating" from the "reputation" of the product. The difficulty in computing a reputation lies in the fact that the reputation it is the sum of the ratings adjusted by the confidence, and the confidence of an individual rating is computed using the objectivity of the rating, which uses the reputation in its computation. In other words, the reputation and the confidence of a rating interact with each other in mutual reinforcement. A true reputation algorithm, an iterative method is proposed to compute these measures. The general process of truth-repudiation with a mini-example dataset containing nine users (u1–u9) and three items (m1–m3). An edge represents the rating given by a user to an item. Initially, the reputation of each item is the average of all user ratings. At each iteration, true-reputation computes the confidence of each rating based on the user activity, the user objectivity, and the rating consensus score. Then, true-reputation adjusts the reputation of each item based on the confidence of the ratings. True reputation performs these two steps (computing the confidence of ratings and adjusting the reputation of items) iteratively until all reputations converge to a stable state[5].

The proposed framework does not require clustering or classification, both of which necessitate considerable learning time. Though true-repudiation does not require any learning steps when solving a false reputation, extensive experiments show that true-reputation provides more trustworthy reputations than do algorithms based on clustering or classification[6]. First, the false reputation is defined and categorized various real-life scenarios in which a false reputation can occur.

The categorization of the false-reputation scenarios helps us design, experimental scenarios similar to real-life situations. Second, a general framework to address a false reputation by quantifying the level of confidence of a rating is proposed[7]. The framework includes true-reputation, an algorithm that iteratively adjusts the reputation based on the confidence of customer ratings. Third, the superiority of true reputation by comparing it with machine-learning based algorithms through extensive experiments are verified.

II. LITERATURE SURVEY

[1] Stacey Wrazien, Rachel Greenstadt, Michael Brennan proposed a collaborative filtering system that has been developed to manage information overload in online communities. In these systems, users rank content provided by other users on the validity or usefulness within their particular context. Slashdot is an example of such a community where peers rate each other's comments based on their relevance to the post. This work extracts a wide variety of features from the Slashdot metadata and posts linguistic contents to identify features that can predict the community rating.

This machine learning to augment collaborative filtering chose to mine data from Slashdot (slashdot.org), a technology news site and online community. In this method readers of the site submit articles which are reviewed by a team of editors, who select the best ones to post as the news items for that day. The community then discusses the articles and issues posted through a comment system. Each news post has its own comment series. Slashdot has implemented a collaborative filtering system for users to rank the comments on how relevant they are in the article and to other users on a scale from -1 to 5, with 5 signifying the comments most worth reading. Comments that receive a very low score are typically hidden, while comments with a higher score are highlighted, allowing the user to easily reach quality commentary. In addition to the numerical rating posts we can also be given a rating description such as "Insightful" if it is good and "Off topic" if it is bad, among others. The features used to classify Slashdot comments are divided into two groups: Linguistic features and contextual and author reputation feature.

The linguistic set represents features related to the words, their meanings, and the structure of the text. Most of the linguistic features were extracted from the comments using the Linguistic Inquiry and Word Count (LIWC) software, a text analysis database designed by psychologists to study various emotional, cognitive, and structural components of verbal and written speech.

The contextual and author reputation features are based upon information such as when it was posted or how much discussion, it generated, or information about the author such as what his or her recent comment ratings have been.
A full list of features can be found on the web.

All classification was performed using an SVM Classifier that used a Gaussian radial basis function kernel. The features were all discretized into four bins before being used for

classification (except LIWC sentiment which already had three discrete values).

[2] P. Chirita, W. Nejdl, and C. Zamfir [4] proposed a collaborative filtering techniques have been successfully employed in recommender systems in order to help users deal with information overload by making high quality personalized recommendations. However, such systems have been shown to be vulnerable to attacks in which malicious users with carefully chosen profiles are inserted into the system in order to push the predictions of some targeted items. In this paper the authors propose several metrics for analyzing rating patterns of malicious users and evaluate their potential for detecting such shilling attacks. Building upon these results, they propose and evaluate an algorithm for protecting recommender systems against shilling attacks.

The algorithm can be employed for monitoring user ratings and removing shilling attacker profiles from the process of computing recommendations, thus maintaining the high quality of the recommendations. Preventing shilling attacks in online recommender proposes several metrics for analyzing rating patterns of malicious users and evaluate their potential for detecting such shilling attacks. Building upon these results, we propose and evaluate an algorithm for protecting recommender systems against shilling attacks. The algorithm can be employed for monitoring user ratings and removing shilling attacker profiles from the prow of computing recommendations, thus maintaining the high quality of the recommendations. More specifically, the following metrics suitable to address the problem of detecting shilling attacks:

1. Number of Prediction-Differences (NPD)
2. Standard Deviation in User's Ratings
3. Degree of Agreement with Other Users
4. Degree of Similarity with Top Neighbors.

The algorithm computes for each user the values for all statistical metrics, and then decides, based on her assessed probability of being an attacker, whether her profile will be discarded from the computation of recommendations or not.

[3] MagdaliniEirinaki, Malamati D. Lute, Member and IraklisVarlamis, Member [5] proposed about the Trust-Aware which creates minimum awareness in people and by using recommendation it introduce a framework for handling trust in social networks, which is based on a reputation mechanism that captures the implicit and explicit connections between the network members, analyzes the semantics and dynamics of these connections, and provides personalized user recommendations to the network members. The proposed system provides users with personalized positive and/or negative recommendations that can be used to establish new trust/distrust connections in the social network. It assumes the notion of trust captures both the user's social context (e.g., Friends and enemies) expressed through explicit user-to-user connections, as well as users' common interests and desires inferred from explicit and implicit user-to-item connections.

The proposed recommender system is based on a reputation mechanism that rates participants using observations, past experiences, and other user's view/opinion. In order to compute the reputation of each member, it adopts several properties of trust such as:Transitivity, Personalization, Context, and Draw ideas from sociology axioms.

Additionally, in order to address the social network dynamics, it has incorporated in our system the element of time. To this direction, it suggests that reputation fades by time; thus, the positive (negative) reputation value of a user tends to zero unless new explicit or implicit trust and liking (disliking) statements are added frequently.

Finally, the context of trust is the same among community members. It exploits positive and negative, time-dependent trust-related information, expressed either explicitly or implicitly. The system can be applied to any type of social network, even in the absence of explicit trust connections, since in such cases only the implicit expressions of trust will be considered for the ranking and recommendation of users.

[4] Sanger, Johannes, Kunz, Michael [5] proposed a Reputation system which provides a valuable method to measure the trustworthiness of sellers or the quality of products in an e-commerce environment. Due to their economic importance, reputation systems are subject to many attacks. A common problem is unfair ratings which are used to unfairly increase or decrease the reputation of an entity. Although being of high practical relevance, unfair rating attacks have only rarely been considered in the literature.

The few approaches that have been proposed are furthermore quite non-transparent to the user. In this work, visual analytics are used to identify colluding digital identities. The ultimate benefit of our approach is the transparent revelation of the true reputation of an entity by interactively using both endogenous and exogenous discounting methods. They there to introduce a generic conceptual design of a visual analytic component that is independent of the underlying reputation system. It then describes how this concept was implemented in a software prototype. Subsequently, they demonstrate its proper functioning by means of an empirical study based on two real-world datasets from eBay and Epinions. Overall, they show that their approach, notably enhances transparency, bares an enormous potential and might thus lead to substantially more robust reputation systems and enhanced user experience.

A. Online Trust and Reputation Systems:

Trust is not only important for the computer science community, but also for various other research domains such as sociology, psychology, economics, philosophy, and media science. Consequently, there are just as many interpretations of it and a universally accepted definition is still missing. The

definition regards trust as the subjective probability with which the entity under observation assesses that another entity will perform a particular action. One way to come up with this probability is through reputation-based (as opposed to policy-based) trust establishment. Since the number of entities involved in an online environment may be of the order of millions, manually determining their reputation becomes unmanageable. Reputation systems encourage actors of a community to leave feedback about the behavior of an entity. They then collect all evidence available, aggregate the data and provide one or several reputation values as output.

The application areas span multiple fields such as e-commerce (Resnick and Zeckhauser, 2002), P2P networks (Gupta et al., 2003), and virtual organizations (Winkler et al., 2007), just to name a few. In electronic marketplaces, for instance, buyers are able to rate sellers after each transaction. Based on these experiences, future customers can decide whether to trust a seller and as a consequence whether to buy. Hence, high reputation is not only an evidence of trustworthiness but also leads to an increased number of sales and higher prices.

B. Unfair Rating Attacks:

Because of their economic importance, reputation systems have been subject to various kinds of attacks. So far, most research activities have focused on seller attacks, meaning what an adversary is able to do with the role of the seller. Typical examples of seller attacks include playbooks, value imbalance exploitation, re-entry, discrimination, and reputation lag exploitation, to name the most important. Advisor attacks, in contrast, have received less attention. Advisor attacks can be summarized under the term "unfair rating attacks" because they are based on one or several digital identities providing unfair ratings to other digital identities.

Here there are different kinds of advisor attacks, according to two dimensions. Firstly, ratings can either be unfairly high or unfairly low. These two types of attacks are also referred to as "ballot stuffing" and "bad mouthing". Secondly, advisor attacks can be carried out either by one single digital identity. Since the multiple entities from multiple identities, the term is used in a different way in this work. Badmouthing is generally harder to perform than ballot stuffing as most reputation systems used in commerce only allow to provide feedback after a successful transaction. Since transactions are bound to costs, there usually is an investment barrier.

[5] Chung-Wei Hang, Zhe Zhang, and Munindar P. Singh explains the need for trust even when no suitable forward path exists, a generalized propagation technique that uses a probabilistic paradigm to estimate trust by comparing the assessments from acquaintances that the trustee and the trustee have in common. In developing Shin, they included two of CertProp's three trust propagation operators, but also extended CertProp to improve prediction accuracy for backward paths. Our evaluation of Shin's capabilities shows that it is superior to CertProp and other existing approaches when only a few trustworthy, forward paths exist from the trustee to the trustee.

Shin is based on the idea that it is possible to compute the trust relationship between a truster and trustee using the known direct trust relationships between agent pairs in the network that are proximal to the truster and trustee. Mathematically, a trust network T(V,E,d) captures agents as vertices V and direct trust relationships as directed, weighted edges E, with the weight d(a,b) of an edge from a to b expressing the amount of direct trust placed by truster a in trustee b. Shin measures direct trust as a value between zero and one, and assigns a trust network an edge if and only if the corresponding direct trust is nonzero.

In addition, Shin computes and uses the function t: $V \times V \rightarrow [0, 1]$ such that for $a,b \in V$, t(a, b) is the amount of (direct or indirect) trust that truster a places in trustee b. In simple terms, trust propagation is the problem of computing the amount of trust for a nonadjacent truster and trustee, or t (a, b). As part of that computation, Shin uses CertProp's concatenation operator ($\otimes$), which discounts trust values along a referral path, and its aggregation operator ($\oplus$), which combines trust from referral paths. The "Trust as Evidence and Belief Representations" sidebar describes the mathematical background of Shin's propagation approach in more detail.

[6] Siyuan Liu, Jie Zhang, Chunyan Miao, Yin-LengTheng, Alex C. Kot [7] proposed an integrated clustering-Based approach called iCLUB to filter unfair testimonies for reputation systems using multi-nominal testimonies, in multiagent based electronic commerce. It adopts clustering and considers buying agents' local and global knowledge about selling agents. Here the Local component first collects the local information regarding St. DBSCAN, a density based clustering routine, is then applied on the collected Testimonies LBSt to generate a set of clusters. After that, the Local component returns as honest witnesses the set of witnesses whose rating vectors are included in the same cluster as the buying agent's rating vector.

Here the Global component first finds the honest witnesses for each seller with which the buyer has transactions, using the Local () procedure. Then, a set of common honest witnesses WF are formed as the intersection of the set of the honest witnesses for each seller except. The Global component obtains the clustering result for St. It then calculates the intersection of WF with the witnesses whose rating vectors are in each cluster achieved if WF is not an empty set. Finally, it returns as honest witnesses the ones whose rating vectors are in the cluster which has the largest intersection result with WF.

This iCLUB approach further integrates the Local and Global components using a threshold ε. If the number of transactions between B and S t is greater than ε, Global ()

procedure will be triggered, otherwise Local () procedure will be called.

III. SYSTEM ANALYSIS

The main purpose of trustworthy online rating system is evaluating the level of trustworthiness i.e., confidence of each rating and adjusts the reputation based on the confidence of ratings.

3.1 Existing system:

Various strategies have been proposed to handle abusers who attack the vulnerability of the system. Multi agent systems compute and publish the reputation scores of sellers based on a collection of buyer opinions which can be viewed as ratings[8]. Considering the collection of majority the second group of strategies computes the reputation score of the opinions more than half the opinions as fair, this group of strategies excludes the collection of minority opinions, viewed as biased, when calculating the reputation seller based on the ratings of a target buyer and the ratings of a selected group of users whose rating patterns are very similar to that of the target buyer. This group of strategies considers the ratings of the buyers whose rating patterns are different from that of the target buyer as biased and excludes these ratings when calculating the reputation.

Recommendation systems predict the preference of a user for an item that they have not yet purchased using a model based on either the characteristics of an item content-based approaches, the user's rating history collaborative filtering approaches, or both hybrid approaches that combine both content-based and collaborative-filtering approaches. These systems are known to be vulnerable to a profile injection attack which is also called a shilling attack where malicious users try to insert fake profiles into the recommendation systems in order to increase the popularity of target items.

In order to enhance the robustness of recommendation systems, it is imperative to develop detection methods against shilling attacks. Major research in shilling attack detection falls into three categories. First it classifies shilling attacks according to different types of attacks. Second it extracts attributes that represent the characteristics of the shilling attacks and quantifying the attributes and then it develops robust classification algorithms based on the quantified attributes used to detect shilling attacks.

Drawbacks of the existing system:

Here there is a risk of considering normal users as abusers and abusers may be considered as normal users, therefore there is a scope of false rating as the collection of majority opinions as fair, this group of strategies excludes the collection of minority opinions.

3.2 Proposed system:

The proposed framework, on the other hand, uses all ratings. It evaluates the level of trustworthiness confidence of each rating and adjusts the reputation based on the confidence of ratings. An algorithm that iteratively adjusts a reputation based on the confidence of customer ratings. By adjusting a reputation based on the confidence scores of all ratings, the proposed algorithm calculates the reputation without the risk of omitting ratings by normal users while reducing the influence of unfair ratings by abusers[9]. This algorithm, which solves the false reputation problem by computing the true reputation, TRUE-REPUTATION.

The computation of a trustworthy reputation starts by measuring the confidence of a rating. The reliability of online information increases when an information producer has no bias, maintains an objective perspective i.e., objectivity and has a consistent viewpoint i.e., consistency[10]. In addition, the reliability of information increases when an information producer actively interacts with users who have obtained information through him i.e., activity.

To determine the confidence of a rating, therefore, this have adopted three key factors of activity, objectivity, and consistency and defined these factors in the context of online ratings.

3.2.1 User Activity:

The user who rates more items displays a higher level of activity. The above description of activity implies that the activity is defined by the amount of interactions between an information producer and the users obtaining his information. There exist, however, no interactions between users in an online rating system; instead, there are actions by users on products. Therefore, it measure user activity in an online rating system based on the amount of actions by the user on products (i.e., the number of products he rates).

In Fig3.1 the user on the left shows a higher level of activity than the user on the right because the number of ratings by the user on the left is greater than that by the user on the right.

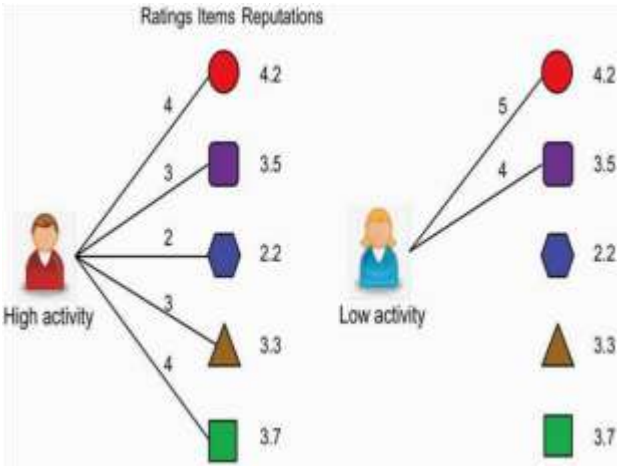

Fig: 3.1 Two different states of user activity

3.2.2 Objectivity:

Rating is considered more objective if it is closer to the public's evaluation i.e., a reputation. The objectivity of a rating is defined as the deviation of the rating from the general reputation of the item[11]. The more similar are the rating and the reputation, the higher is the objectivity of a rating; the more dissimilar they are, the lower the objectivity of a rating. Additionally, a user whose ratings exhibit higher objectivities should also have a higher level of user objectivity.

The user objectivity is measured by the normalized average of the objectivities of the ratings submitted by that user. In Fig3.2 the user on the left whose ratings are similar to the reputations of the items exhibits higher objectivity than the user on the right whose ratings are quite different from the reputations of the items.

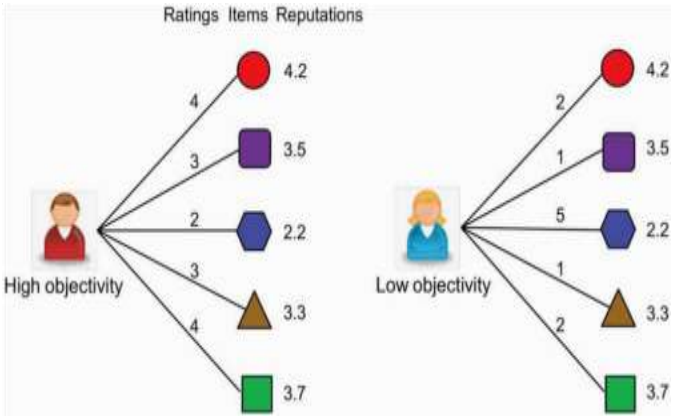

Fig: 3.2 Two different states of user objectivity

3.2.3 Consistency:

Third, it define the user consistency as how consistent the user is in rating products; in other words, how consistently he keeps his objectivities of ratings. In Fig. 3, the user on the left has rated with consistency[12]. The user on the right, on the other hand, was consist until she rated the last item. That is, the user on the left has higher consistency in his ratings compared to the user on the right. An abnormal rating that deviates from the user's consistency is penalized by assigning a low consensus score when computing the confidence of the rating.

In each iteration, TRUE-REPUTATION computes the confidence of each rating based on the user activity denoted by the diamond, the user objectivity denoted by the circle, and the rating consensus score denoted by the square. Then, TRUEREPUTATION adjusts the reputation of each item based on the confidence of the ratings.

TRUE-REPUTATION performs these two steps computing the confidence of ratings and adjusting the reputation of items iteratively until all reputations converge to a stable state.

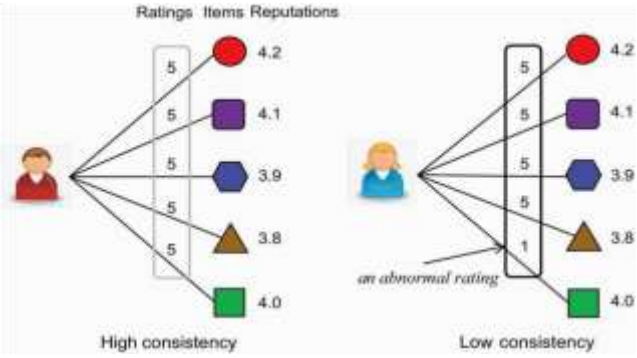

Fig: 3.3 Two different states of consistency

In fig: 3.3 it shows two different states of user as high consistency and low consistency. Where user of high consistency gives equal rating to every product.

IV. CONCLUSIONS AND FUTURE WORK

Trust and reputation systems represent a significant trend in decision support for Internet mediated service provision. A natural side effect is that it also provides an incentive for good behavior, and therefore tends to have a positive effect on market quality. Reputation systems are already being used in successful commercial online applications. The false reputation problem in online rating systems and categorizes various real-life situations in which a false reputation may occur. Through extensive experiments, it showed that the true-reputation can reduce the influence of various RAs. It also showed that true-reputation is superior to the existing approaches that use machine-learning algorithms such as clustering and classification to solve the false reputation problem[13]. There are more factors known to be elemental in assessing the trust of users in the field of social and behavioral sciences.

In order to solve the false reputation problem, a general framework that quantifies the confidence of a rating based on activity, objectivity, and consistency is proposed. The framework includes true-reputation, an algorithm that iteratively adjusts the reputation based on the confidence of user ratings.

The rating given by a buyer indicates the degree of his satisfaction not only with the item (e.g., the quality) but also with its seller (e.g., the promptness of delivery). In a further study, we plan to develop an approach to accurately separate an item score and a seller score from a user rating. Separating the true reputation of items and that of sellers would enable customers to judge items and sellers independently.

REFERENCES

[1] Hyun-Kyo Oh, Sang-Wook Kim, Member, IEEE ,Sunju Park, and Ming Zhou" Can You Trust Online Ratings? A Mutual Reinforcement Model for Trustworthy Online Rating Systems", IEEE transactions on systems, man, and cybernetics: systems ,year 2015

[2] M. Brennan, S. Wrazien, and R. Greenstadt, "Using machine learning to augment collaborative filtering of community discussions," in *Proc.9th Int. Joint Conf. Auton. Agents Multiagent Syst. (AAMAS)*, Toronto, ON, Canada, 2010, pp. 1569–1570.

[3] V. Barnett and T. Lewis, *Outliers in Statistical Data*, 3rd ed. Chichester, U.K.: Wiley, 1994.

[4] P. Chirita, W. Nejdl, and C. Zamfir, "Preventing shilling attacks in online recommender systems," in *Proc. 7th Annu. ACM Int. Workshop Web Inf.Data Manage. (WIDM)*, Bremen, Germany, 2005, pp. 67–74.

[5] M. Eirinaki, M. D. Louta, and I. Varlamis, "A trust-aware system for personalized user recommendations in social networks," *IEEE Trans.Syst., Man, Cybern., Syst.*, vol. 44, no. 4, pp. 409–421, Apr. 2014.

[6] Sanger, Johannes, Kunz, Michael "Visualizing unfair ratings in online reputation systems", Twenty-Third European Conference on Information Systems, Münster, Germany, 2015.

[7] Chung-Wei Hang, Zhe Zhang, and Munindar P. Singh "*Generalized Trust Propagation with Limited Evidence"* Published by the IEEE Computer Society, 0018-9162, 2013.

[8] S. Liu, J. Zhang, C. Miao, Y. Theng, and A. Kot, "iCLUB: An integrated clustering-based approach to improve the robustness of reputation systems," in *Proc. 10th Int. Joint Conf. Auton. Agents Multiagent Syst. (AAMAS)*, Taipei, Taiwan, 2011, pp. 1151–1152.

[9] G. Häuubl and V. Trifts, "Consumer decision making in online shopping environments: The effects of interactive decision aids," *Market. Sci.*, vol. 10, no. 1, pp. 4–21, 2000.

[10] G. Häuubl and V. Trifts, "Consumer decision making in online shopping environments: The effects of interactive decision aids," *Market. Sci.*, vol. 10, no. 1, pp. 4–21, 2000.

[11] N. Hurley, Z. Cheng, and M. Zhang, "Statistical attack detection," in *Proc. ACM Conference Recommender System* ,Vienna, Austria, 2009, pp. 149–156.

[12] J. A. Konstan and J. Riedl, "Recommender systems: From algorithms to user experience," *User Model. User-Adapt. Interact.*, vol. 22, nos. 1–2, pp. 101–123, 2012.

[13] C. Leadbeater, *WE-THINK: Mass Innovation, Not Mass Production*. London, U.K.: Profile Books, 2008.