ISSN(Online) : 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

A Communal Fortification Model for Reliable Online Rating System

Dravya Dechamma ML[*1], Myna AN[*2], Neelamma AP[*3], Preetham Thangamma K[*4], Yathiraj GR[*5]

UG Scholar, Dept. of CSE, Coorg Institute of Technology, Ponnampet, India[*1,*2,*3,*4]

Asst. Professor, Dept. of CSE, Coorg Institute of Technology, Ponnampet, India [*5]

ABSTRACT: The standard of customer ratings on merchandise, which we call a reputation, is one of the key factors in online purchasing decisions. There is, however, no guarantee of the trust- worthiness of a reputation since it can be manipulated rather easily. In this paper, we define false reputation as the problem of a reputation being manipulated by unfair ratings and design a general framework that provides trustworthy reputations. For this purpose, we propose TRUE-REPUTATION, an algorithm that iteratively adjusts a reputation based on the confidence of customer ratings. We also show the effectiveness of TRUE-REPUTATION through extensive experiments in comparisons to state-of-the-art approaches.

KEYWORDS: False reputation, robustness, trust, unfair ratings**.**

I. INTRODUCTION

The trustworthiness of a standing can be achieved when a large number of buyers take part in ratings with truthfulness [10], [13], [15], [25]. If some users intentionally give unfair ratings to a product, especially when few users have participated, the standing of the product could easily be manipulated. In this paper, we define 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. In this case, a false reputation adversely affects the decision making of potential buyers of the product.

In this paper, we describe the scenario in which a false reputation occurs and propose a general framework that resolves a false reputation. The most common way to aggregate ratings is to use the average which may result in false reputation

While using online shopping channels, consumers share their purchasing experiences regarding both goods and services with other potential buyers via evaluation. The most common way for consumers to express their level of satisfaction 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 potential buyers. In this paper, we call this aggregated score for a product its reputation. The reputation of a item for consumption plays a significant role as a guide for potential buyers and significantly influence consumers final purchasing decisions [7], [9], [17], [21].

"Is the Product's Reputation Trustworthy?" Reputation is the score of a product obtained through collective intelligence, i.e., the result of collaboration between many individuals. For example, a group of abusers may inflate or deflate the overall rating of a targeted product. The existing strategies [2], [4], [11], [20], [29], [33] avoid a false reputation by detecting and eliminating abusers. However, abusers can- not always be detected, and it is promising that normal users may be regarded as abusers. Consequently, existing approach can exclude the ratings of normal users or allow the ratings of abusers to be included in the calculation of a reputation.

The proposed support, 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. We have developed an algorithm that iteratively adjusts a character 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 with- out the risk of omitting ratings by normal users while reducing the influence of unfair ratings by abusers. We call this algorithm, which solves the false reputation problem by computing the true reputation, TRUE-REPUTATION.

The computation of a trustworthy standing starts by measuring the confidence of a rating. We have surveyed previous

ISSN(Online) : 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

social science studies to facilitate analyze the characteristics of reliable online information and adopted three key characteristics that are suitable for determining the confidence of a rating [6], [23]. According to previous research, the reliability of online information increases when an information producer has no bias, maintains an objective point of view (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).

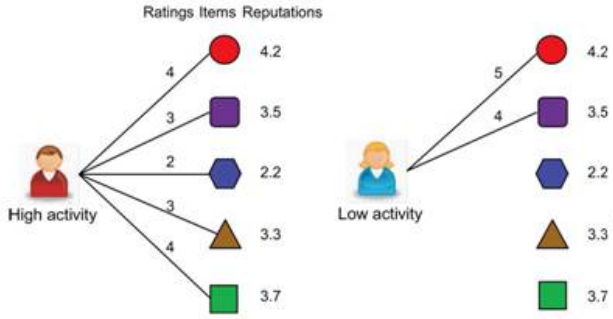

Fig 1. Two different states of user activity.

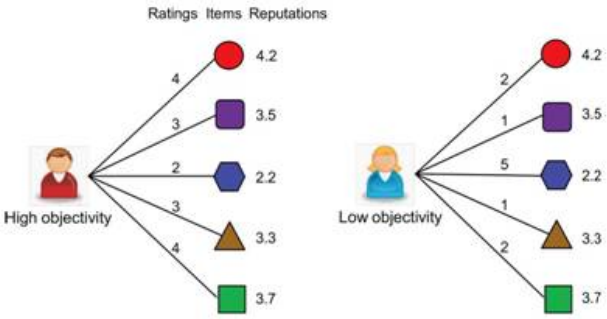

Fig 2. Two different states of user objectivity.

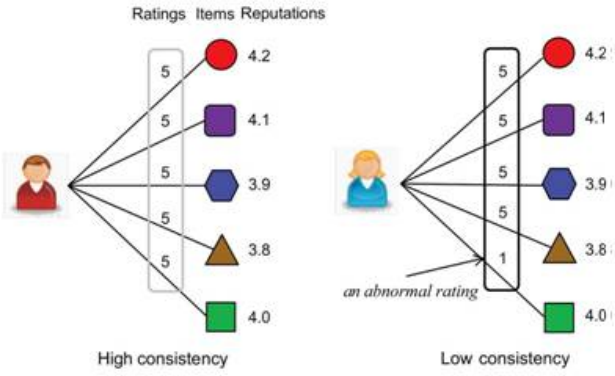

Fig 3. Two different states of user consistency.

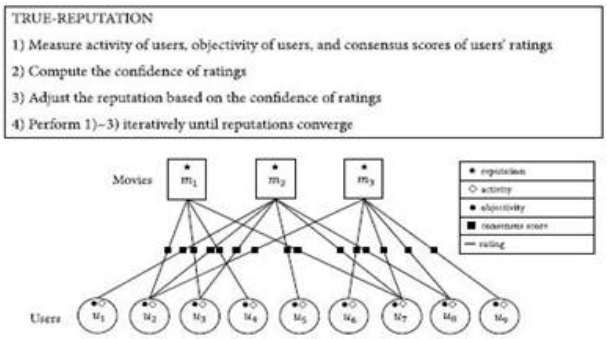

Fig 4. General process of TRUE-REPUTATION.

To determine the confidence of a rating, therefore, we have adopted 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. The above description of activity implies that the activity is defined by the amount of communications between an information producer and the users obtain his information. There exist, however, no relations between users in an online rating system; instead, there are actions by users on products. Therefore, we 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 Fig. 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.

Second, a rating is considered more objective if it is closer to the public's valuation (i.e., a reputation). The objectivity of a rating is defined as the deviation of the rating from the general reputation of the item. 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 Fig. 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 standing of the items.

Third, we define the user consistency as how consistent the user is in rating products; in other words, how

ISSN(Online) : 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

consistently he keeps his objectivities of ratings. In Fig. 3, the user on the left has rated with consistency. The user on the right, on the other hand, was consisting 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 penalizing by assigning a low compromise score when computing the confidence of the rating.

The objectivity of a rating is calculated based on the variation of the "rating" from the "reputation" of the product. The difficulty in computing a standing lies in the fact that the reputation itself 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 standing in its computation. In other words, the standing and the confidence of a rating interact with each other in mutual support. We propose TRUE-REPUTATION, an iterative method, to compute these measures.

Fig. 4 shows the general process of TRUE-REPUTATION 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 (denoted by the black star) is the average of all user ratings. At each iteration, TRUE-REPUTATION computes the confidence of each rating based on the user activity (denoted by the white diamond), the user objectivity (denoted by the black circle), and the rating consensus score (denoted by the black square). 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 standing come together to a stable state.

The proposed frame work does not require clustering or classification, both of which necessitate considerable learning time. Though TRUE-REPUTATION 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.

The contributions of this paper are as follows. First, we have defined false reputation and categorized various real-life scenarios in which a false reputation can occur. The categorization of the false-reputation scenarios helps us design untried scenarios similar to real-life situations. Second, we have proposed a general framework to address a false reputation by quantify the level of confidence of a rating. The framework includes TRUE-REPUTATION, an algorithm that iteratively adjusts the reputation based on the confidence of customer ratings. Third, we have verified the superiority of TRUE-REPUTATION by comparing it with machine-learning- based algorithms through extensive experiments.

II. RELATED WORK

Numerous studies have been conduct to improve the trust worthiness of online shopping malls by detecting abusers who have participated in the rating system for the sole purpose of manipulating the information provided to potential buyers (e.g., reputations of sellers and recommended items). Especially in the fields of multi agent and recommendation systems, 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). Strategy for improving the robustness of multi agent systems can be classified into two categories. The first group of strategies is based on the principle of majority rule. Considering the collection of majority 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 [2], [24], [29]. The second group of strategies computes the reputation score of the 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 [18], [22], [28], [31], [32]. 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.

Our framework for online rating systems and the existing strategies in multi agent systems serve the same purpose in that they are trying to address unfair ratings by abusers. It should be noted that the "seller" is the object evaluated in multi agent systems, while the "item" is the object evaluated in online rating systems. In multi agent systems, a buyer can evaluate a seller multiple times since he rates a seller when- ever he purchases an item. In online rating systems, on the other hand, a buyer can give only a single rating per item. Thus, the relationship between buyers and items is significantly different from the relationship between buyers and sellers; as such, the graph structure of an online rating system is very different from that of a multi agent system. This paper uses an approach that considers the relation between buyers and items.

ISSN(Online) : 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

Recommendation systems predict the preference of a user for an item (such as books or movies) 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) [5], [12], [26], [27]. 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 pro- files into the recommendation systems in order to increase the popularity of target item(s) [1], [4], [8], [20], [30].

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: 1) classifying shilling attacks according to different types of attacks [4]; 2) extracting attributes that represent the characteristics of the shilling attacks and quantifying the attributes [1], [33]; and 3) developing robust classification algorithms based on the quantified attributes used to detect shilling attacks [11], [14], [20], [30], [33].

The purpose of our framework is the same as that of existing strategies against shilling attacks; all are trying to prevent the manipulation of ratings by abusers. The classification algorithms for detecting shilling attacks, however, may face situations where malicious users cannot be detected and/or where normal users are considered as malicious. As a result, there may be instances when a reputation is calculated without the ratings of normal users or including the ratings of malicious users. Additionally, a significant amount of time is required to collect training data and extract attributes related to the abusers. The performance of the classifier is sensitive to the choice of the training data and the attributes used.

III. PROPOSED SYSTEM

The proposed framework does not require clustering or classification, both of which necessitate considerable learning time. Though TRUE-REPUTATION 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. The contributions of this paper are as follows. First, we have defined false reputation 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, we have proposed a general framework to address a false reputation by quantifying the level of confidence of a rating. The framework includes TRUE-REPUTATION, an algorithm that iteratively adjusts the reputation based on the confidence of customer ratings. Third, we have verified the superiority of TRUE-REPUTATION by comparing it with machine-learning based algorithms through extensive experiments.

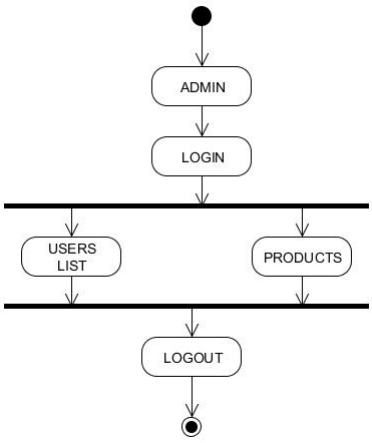

Fig 5. Admin Module

ISSN(Online) : 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

Modules

1. Admin

Login: admin will login by entering his credentials.
Add products: admin will add products along with details such as price of the product, product image, product name, specification etc. based on the category
View products: admin can view the products he has added.
View users list: admin can view users and he can send confirmation mail and secret key to the user's email id.

2. User

Register: user will get registered to the application by entering the details.
Login: user can login with his user name
Password verification: admin will send users confirmation mail and secret key to the user's email id
View product: user can view products along with details such as price of the product, product image, product name, specification etc. based on the category rate product: user can rate the product by entering secret key product will be rated based on 3 layer security i.e. activity check, object activity, unfair rating, if the rating is valid, it will be accepted. If the rating is invalid then it is rejected.

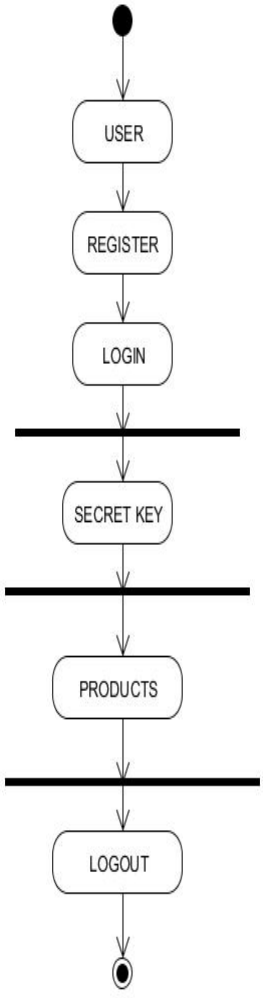

Fig 6. User Module.

ISSN(Online) : 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

IV. EXPERIMENTAL RESULTS

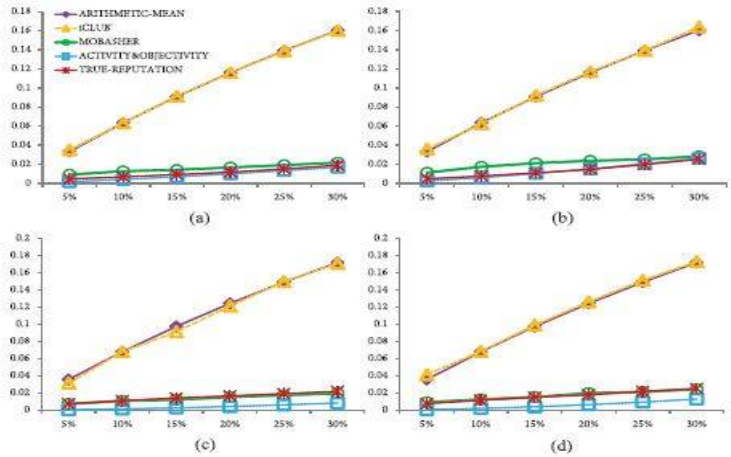

Fig 7. Reputation-change rates by target-only RA. Push RA (a) rating frequency = 2 and (b) rating frequency = 32. Nuke RA (c) rating frequency=2 and (d) rating frequency = 32.

Fig.7 shows the results comparing the baseline with the four standing adjustment algorithms. iCLUB shows the worst routine amongst the four algorithms. Its performance is similar or even inferior to that of baseline regardless of the number of target-only RAs. Since DBSCAN in iCLUB groups the users by their similarity, RAs are grouped separately from ordinary users. Since a user is supposed to consult the users in his group when adjusting reputations, iCLUB behaves almost the same as the baseline in which the user uses his own information only. The performance of iCLUB confirms that it cannot reduce the impact of target-only RAs and cannot adjust reputations properly. The performance of MOBASHER, on the other hand, is similar to that of the proposed algo- rithms, because the classifier of MOBASHER is able to detect target-only RAs with a high probability.

As shown in Fig. 7, the performance of iCLUB worsens with an increase in the number of RAs, while that of MOBASHER remains strong although not as good as those of A&O and TRUE-REPUTATION. When push target-only RAs are present and the rating frequency of the RAs is 32, the *t*-test results show that all the *p* values between TRUE-REPUTATION and A&O, or MOBASHER are greater than 0.05, which indicates that the algorithms are statistically indifferent.

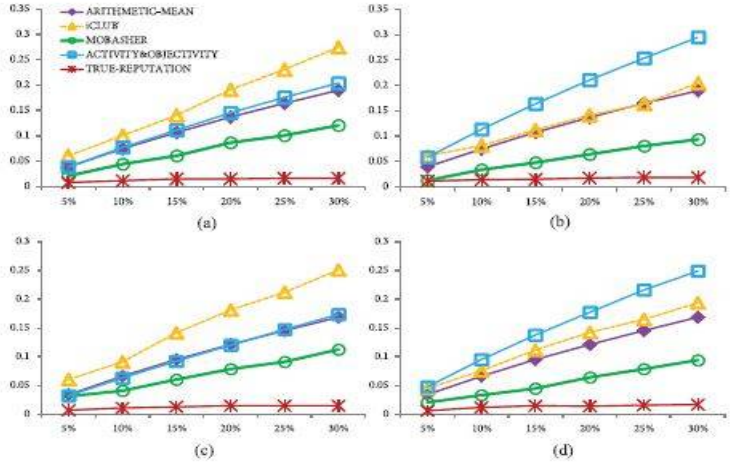

Fig. 8. Reputation change rates by average RA. Push RA (a) rating frequency = 50 and (b) rating frequency = 100. Nuke RA (c) rating frequency = 50 and (d) rating frequency = 100.

ISSN(Online) : 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

Fig. 8 shows that A&O, the most robust algorithm in target- only RA, is more vulnerable to average RA. The reputation change rate of A&O is greater than 0.3, when the number of average RAs is 30% of the targeted movie's total number of ratings and the occurrence of the ratings by average RAs is 100. A&O is not able to reduce the influence of the average RAs because most ratings by average RAs are regarded as fair.

IV. CONCLUSION AND FUTURE WORK

This paper defines the false reputation problem in online rating systems and categorizes various real-life situations in which a false standing may occur. The understanding of why and when a false standing occurs helps us establish experimental situations. In order to solve the false reputation problem, we proposed a general framework that quantifies the confidence of a rating based on activity, objectivity, and consistency. The framework includes TRUE-REPUTATION, an algorithm that iteratively adjusts the reputation based on the confidence of user ratings. Through extensive experiments, we showed with the intention of TRUE-REPUTATION can reduce the influence of various RAs. We 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.

There are more factors (other than those addressed in this paper) known to be elemental in assessing the trust of users in the field of social and behavioral sciences. We plan to learn how to incorporate them into our model to compute the reputation of items more accurately. In the e-market place such as Amazon.com and eBay.com, buyers give ratings on items they have purchased. We note, however, that 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. Straightening out the true standing of items and that of sellers would enable customers to umpire items and sellers in parallel.

REFERENCES

1. R. Burke, B. Mobasher, C. Williams, and R. Bhaumik, "Classification features for attack detection in collaborative recommender systems," in *Proc. 12th Int. Conf. Knowl. Disc. Data Min. (KDD)*, Philadelphia, PA, USA, 2006, pp. 542-547.
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. M. Eisend, "Source credibility dimensions in marketing communication—A generalized solution," *J. Empir. Gener. Market. Sci.*, vol. 10, no. 2, pp. 1-33, 2006.
7. S. Grazioli and S. L. Jarvenpaa, "Perils of Internet fraud: An empirical investigation of deception and trust with experienced Internet consumers," *IEEE Trans. Syst., Man, Cybern. A, Syst., Humans*, vol. 30, no. 4, pp. 395-410, Jul. 2000.
8. I. Gunes, C. Kaleli, A. Bilge, and H. Polat, "Shilling attacks against recommender systems: A comprehensive survey," *Artif. Intell. Rev.*, vol. 42, no. 4, pp. 767-799, 2014.
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. J. Howe, "The rise of crowdsourcing," *Wired Mag.*, vol. 14, no. 6, pp. 1-4, 2006.
11. N. Hurley, Z. Cheng, and M. Zhang, "Statistical attack detection," in *Proc. ACM Conf. Recommender Syst. (RecSys)*, 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.
14. J.-S. Lee and D. Zhu, "Shilling attack detection—A new approach for a trustworthy recommender system," *INFORMS J. Comput.*, vol. 24, no. 1, pp. 117-131, 2012.
15. P. Levy, *L'Intelligence Collective: Pour Une Anthropologie du Cyberspace*. Paris, France: La Découverte, 1997.
16. E. P. Lim, V. A. Nguyen, N. Jindal, B. Liu, and H. W. Lauw, "Detecting product review spammers using rating behaviors," in *Proc. 19th ACM Int. Conf. Inf. Knowl. Manage. (CIKM)*, Toronto, ON, Canada, 2010, pp. 939-948.
17. M. Limayem, M. Khalifa, and A. Frini, "What makes consumers buy from Internet? A longitudinal study of online shopping," *IEEE Trans. Syst., Man, Cybern. A, Syst., Humans*, vol. 30, no. 4, pp. 421-432, Jul. 2000.
18. 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.
19. A. Mukherjee, B. Liu, J. Wang, N. Glance, and N. Jindal, "Detecting group review spam," in *Proc. 20th Int. Conf. World Wide Web (WWW)*, Hyderabad, India, 2011, pp. 93-94.

ISSN(Online) : 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

20. B. Mobasher, R. Burke, R. Bhaumik, and C. Williams, "Towards trustworthy recommender systems: An analysis of attack models and algorithm robustness," *ACM Trans. Internet Technol.*, vol. 7, no. 2, pp. 1-40, 2007.
21. The Nielsen Company, *Trends in Online Shopping*, Global Nielsen Consum. Rep., Feb. 2008. [Online]. Available: http://www.freshgraphics.net/BlogLinks/GlobalOnlineShoppingReportFeb08.pdf
22. Z. Noorian, S. Marsh, and M. Fleming, "Multi-layer cognitive filtering by behavioral modeling," in *Proc. 10th Int. Joint Conf. Auton. Agents Multiagent Syst. (AAMAS)*, Taipei, Taiwan, 2011, pp. 871-878.
23. S. Y. Rieh and D. Danielson, "Credibility: A multidisciplinary framework," *Annu. Rev. Inf. Sci. Technol.*, vol. 41, no. 1, pp. 307-364, 2007.
24. E. Santos and D. Li, "On deception detection in multiagent systems," *IEEE Trans. Syst., Man, Cybern. A, Syst., Humans*, vol. 40, no. 2, pp. 224-235, Mar. 2010.
25. J. Surowiecki, *The Wisdom of Crowds: Why the Many are Smarter Than the Few and How Collective Wisdom Shapes Business, Economies, Societies, and Nations*. New York, NY, USA: Doubleday, 2004.