RESEARCH ARTICLE OPEN ACCESS

DETECTING SPAM REVIEWS USING USER BEHAVIOURS AND UNUSUAL REVIEW PATTERN

Saradha. R., Shanmathi. M. V., Vinodhini. P., V. Sathiya,
Department of Computer Science and Engineering,
Panimalar Engineering College, Chennai.

Abstract:

Online Social Media portals play an influential role in information propagation which is considered as an important source for producers in their advertising campaigns as well as for customers in selecting products and services. In online social media user can share their reviews about products and services. Nowadays most of the peoples make decision to purchase products based on user reviews, positive reviews are encouraging to select product or service and negative reviews are discouraging to select product or service. In online social media any user can leave their comments as a review, it is tempting spammers to post negative comments on the product or service, this fake reviews mislead user opinion. These negative reviews spread over internet and it will change the user perception of good/bad product or service. So here we use review based model to detect spam reviews and user based model to detect spammers.

Keywords — **Review, Fake Review, Spammer, Online.**

I.INTRODUCTION

This project aims to detect spam user reviews in online social media. Nowadays, time is of essence. Everything is done on the go. There is no time to stop and shop. So, online social forums play a major role in today's world. But products viewed online are intangible until they are delivered. Users cannot know the exact size, quality, quantity etc. since images can be deceptive. Thus they rely on the reviews posted for each product to know about the product. This triggers spammers to put up fake reviews. They greatly influence the view about a product, which is a negative view in most cases. This makes it necessary to detect and stop spam reviews and spammers. Previously, several methods such as linguistic analysis using unigram, bigram etc. have been used to detect spam reviews.

In this project, we do the same using two new methods, Spam Detection and Review Analysis. These methods provide increased accuracy over all the existing methods. It also enables us to detect a spam reviewer, not just the spam review. The spammer can be detected and blocked in this method.

II.RELATED WORKS

[4] Otto K.M. Cheng and Raymond Y.K. Lau, in the year 2014, discussed that with the rapid proliferation of the Social Web, there has been an exponential growth of the number of usercontributed online comments posted to the Internet these days. These online comments contain users' opinions about various entities such as consumer products, financial products, social events, political figures, and so on. Accordingly, firms or individuals can leverage these ever increasing online comments to extract valuable business intelligence to facilitate business strategy development or consumer comparison shopping. Meanwhile, firms have strong financial motivation to strategically manipulate online comments to boost sales, and political parties have the political motivation to strategically influence online comments to strengthen their political campaigns. As a result, there has been growing concerns about the quality and the truthfulness of user-contributed online comments. Although a lot of study about opinion digging has been carried out, relatively small work about the systematic assessment of the quality of online views is done. To improve the hygiene and the usefulness of online comments, there is a pressing need to develop a robust methodology for an objective and systematic assessment of the quality of online comments. The main contribution of this paper is the design, development, and evaluation of a novel information theory based methodology for the assessment of the quality of online comments. Our preliminary experiments show that the proposed quality assessment methodology is more effective than other baseline methods such as a peer-review based quality assessment approach.

[7] Guan Wang, Sihong Xie, Bing Liu, Philip S. Yu, in the year 2011, discussed that Online reviews provide valuable information about products and services to consumers. However, spammers are joining the community trying to mislead readers by writing fake reviews. Previous attempts for spammer detection used reviewers' behaviors, text similarity, linguistics features and rating patterns. Those studies are able to identify certain types of spammers, e.g., those who post many similar reviews about one target entity. However, in reality, there are other kinds of spammers who can manipulate their behaviors to act just like genuine reviewers, and thus cannot be detected by the available techniques. In this paper, we propose a novel concept of a heterogeneous review graph to capture the relationships among reviewers, reviews and stores that the reviewers have reviewed. We explore how interactions between nodes in this graph can reveal the cause of spam and propose an iterative model to identify suspicious reviewers. This is the first time such intricate relationships have been identified for review spam detection. We also develop an effective computation method to quantify the trustiness of reviewers, the honesty of reviews, and the reliability of stores. Different from existing approaches, we don't use review text information. Our model is thus complementary to existing approaches and able to find more difficult and subtle spamming activities, which are agreed upon by human judges after they evaluate our results.

[10] Manasa. S. M. in the year 2017, discussed that Social networks are the platform for the users to get connected with other social network users based on their interest and life styles. Existing social networks have millions of users and the data generated by them are huge and it is difficult to differentiate the real users and the fake users. Hence a trust worthy system is recommended for differentiating the real and fake users. Social networking enables users to send friend requests, upload photos and tag their friends and even suggest them the web links based on the interest of the users. The friends recommended, the photos tagged and web links suggested may be a malware or an untrusted activity. Users on social networks are authorised by providing the personal data. This personal raw data is available to all other users online and there is no protection or methods to secure this data from unknown users. Hence to provide a trustworthy system and to enable real users activities a review on different methods to achieve trustworthy social networking systems are examined in this paper.

[12] Rajesh Sharma, in the year 2015, discussed that, Several systems can be modeled as sets of interconnected networks or networks with multiple types of connections, here generally called multilayer networks. Spreading processes such as information propagation among users of an online social networks, or the diffusion of pathogens among individuals through their contact network, are fundamental phenomena occurring in these networks. However, while information diffusion in single networks has received considerable attention from various disciplines for over a decade, spreading processes in multilayer networks is still a young research area presenting many challenging research issues. In this paper we review the main models, results and applications of multilayer spreading processes and discuss some promising research directions.

[15] Arjun Mukherjee, in the year 2012, discussed that, Opinionated social media such as product reviews are now widely used by individuals and organizations for their decision making.

However, due to the reason of profit or fame, people try to game the system by opinion spamming (e.g., writing fake reviews) to promote or demote some target products. For reviews to reflect genuine user experiences and opinions, such spam reviews should be detected. Prior works on opinion spam focused on detecting fake reviews and individual fake reviewers. However, a fake reviewer group (a group of reviewers who work collaboratively to write fake reviews) is even more damaging as they can take total control of the sentiment on the target product due to its size. This paper studies spam detection in the collaborative setting, i.e., to discover fake reviewer groups. The proposed method first uses a frequent itemset mining method to find a set of candidate groups. It then uses several behavioral models derived from the collusion phenomenon among fake reviewers and relation models based on the relationships among groups, individual reviewers, and products they reviewed to detect fake reviewer groups. Additionally, we also built a labeled dataset of fake reviewer groups. Although labeling individual fake reviews and reviewers is very hard, to our surprise labeling fake reviewer groups is much easier. We also note that the proposed technique departs from the traditional supervised learning approach for spam detection because of the inherent nature of our problem which makes the classic supervised learning approach less effective. Experimental results show that the proposed method outperforms multiple strong baselines including the state-of-the-art supervised classification, regression, and learning to rank algorithms.

III.EXISTING SYSTEM

In an existing system, linguistic based detection mechanism is used to detect spam reviews by using unigram, bigram and their composition. The system also used other features like pair wise features (features between two reviews) ,in a reviews and use a probabilistic language modeling to spot spam. But a major drawback with the existing system is that the accuracy of detecting spam is low. Also, it is not able to detect spammers using the linguistic based, that is, language modeled spam detection method.

IV.PROPOSED SYSTEM

In our proposed system we propose to determine the relative importance of each feature and show how effective each of features are in identifying spam from normal reviews and also improves the accuracy.

Early Time Frame: Spammers, usually write their spam reviews in short period of time for two reasons first, because they want to impact readers and other users, and second because they are temporal users, they have to write as much as reviews they can in short time. Spammers try to write their reviews, in order to keep their review in the top reviews which other users visit them sooner. To avoid this type of spam reviews we can calculate the days between last and first review of the particular user to detect spam reviews.

Content Similarity: Spammers, often write their reviews with same template and they prefer not to waste their time to write an original review. In result, they have similar reviews. To avoid this each and every user review will be compared with spam review templates to detect spam reviews.

V. ARCHITECTURAL DIAGRAM

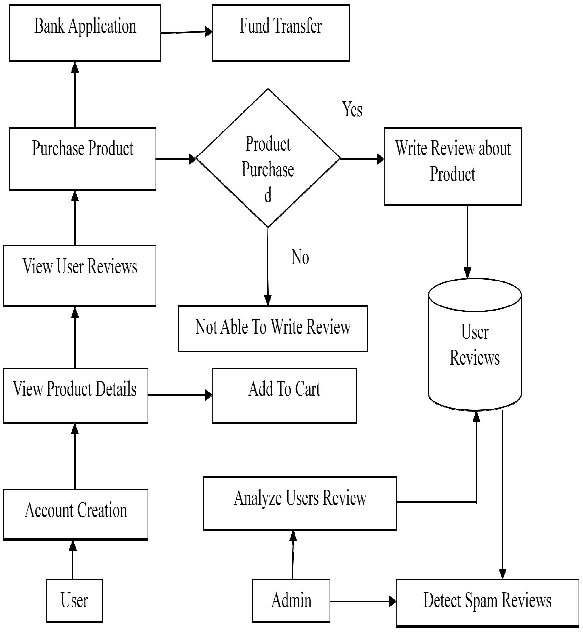

Fig. Block diagram

VI.CATALOGING OF USERS AND VIEW PRODUCTS

In this module user has to register to become a member to purchase product. Once he/she created account they can login to their account, now user can view the list of products available and view the particular product complete specification and cost of the product. User can view other user reviews before purchase the particular product.

VII.BANK APPLICATION AND PURCHASE PRODUCT

In this module bank user can create account in our bank application, here account will be created by bank admin. Now user can purchase the product from the list of available products. Once the user initiate the purchasing process bank application portal will be open. User can enter the account details and OTP to pay amount. Now amount will be debited from user account.

VIII.POSTING REVIEWS

In this module user can post their reviews about the products. Every users not able to post the reviews about products, those who all are purchased the particular product they all are post the review about the product others not able to write review they can only read the other reviews this is one type of detecting spammers in this module. Because by using the above technique we can reduce the spammers count initially.

IX. DETECTING SPAM REVIEWS

In this module admin will analyze the each and every reviews posted by users about their purchased product. Admin can apply user based and review based methods to detect spam reviews, admin will compare user reviews with spam review templates, and calculate the date difference between particular user reviews and mark the review if it is spam. Once the review is marked as spam then the users not able to view the spam review, and also threshold will be calculated for every user. If the user repeatedly misbehaves then the user account will be blocked by admin.

IV.SPAM DETECTION

Spam detection algorithm is used to detect the spam reviews by using Templates. A template of spam reviews is created by analyzing previously input reviews. A spam reviewer will not waste his time on typing each review. He will copy-paste most of it to save time and make his review come on top of the list. Thus all reviews will be the same. This allows us to compare the template with the reviews to detect spam reviews.

V.REVIEW ANALYSIS

Review analysis algorithm formulates the time frame between successive reviews to detect spammers. Spammers tend to write reviews at small time frames in order to make their reviews appear at the top. Hence if too many reviews are logged in from the same user, they can be identified as spam.

X.CONCLUSION

Hence we proposed and developed spam detection mechanism to detect spam reviews and block spammers from online social media using user based and review based detection scheme.

XI.REFERENCES

1. J.Donfro, A whopping 20 % of yelp reviews are fake. http://www.businessinsider.com/20-percent-of-yelp-reviews-fake-2013-9. Accessed: 2015-07-30.

2. M. Ott, C. Cardie, and J. T. Hancock. Estimating the prevalence of deception in online review communities. In ACM WWW, 2012.

3. M. Ott, Y. Choi, C. Cardie, and J. T. Hancock. Finding deceptive opinion spam

by any stretch of the imagination.In ACL, 2011.

4. M. Ott, and K. Ray. Towards an Information Theory Based Methodology for the Quality Assessment of Online Comments,2014.

5. Ch. Xu and J. Zhang. Combating product review spam campaigns via multiple heterogeneous pair wise features. In SIAM International Conference on Data Mining, 2014.

6. N. Jindal and B. Liu. Opinion spam and analysis. In WSDM, 2008.

7. G. Wang, S. Xie, B. Liu, Philip S. Yu. Review Graph based Online Store Review Spammer Detection, 2011

8.F. Li, M. Huang, Y. Yang, and X. Zhu. Learning to identify review spam. Proceedings of the 22nd International Joint Conference on Artificial Intelligence; IJCAI, 2011.

9. G. Fei, A. Mukherjee, B. Liu, M. Hsu, M. Castellanos, and R. Ghosh. Exploiting burstiness in reviews for review spammer detection. In ICWSM, 2013.

10. Manasa S. M. Trust Aware System for Social Networks: A Comprehensive Survey, 2017.11.A. j. Minnich, N. Chavoshi, A. Mueen, S. Luan, and M. Faloutsos. Trueview: Harnessing the power of multiple review sites 2015.

12. R. Sharma, Spreading processes in Multilayer Networks, 2015.

13. B. Viswanath, M. Ahmad Bashir, M. Crovella, S. Guah, K. P. Gummadi, B. Krishnamurthy, and A. Mislove. Towards detecting anomalous user behavior in online social networks. In USENIX, 2014.

14. H. Li, Z. Chen, B. Liu, X. Wei, and J. Shao. Spotting fake reviews via collective PU learning. In ICDM, 2014.

15. A. Mukherjee, Spotting Fake Reviewer Groups in Consumer Reviews, 2012.