JETIR.ORG

ISSN: 2349-5162 | ESTD Year: 2014 | Monthly Issue



JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Fake review monitoring using machine learning

 $Dr.R.N.DEVENDRA\ KUMAR*_{1}$

.VIJAYA VIKASHINI G*2,SHREEJITH S*2, NITHISH KUMAR V*2

*1 Assistant Professor(Senior Grade), Department of Computer Science and Engineering, Sri Ramakrishna Institute of Technology, Coimbatore-641 010, Tamil Nadu, India.

*2 Final year B.E(CSE), Sri Ramakrishna Institute of Technology, Coimbatore-641 010, Tamil Nadu, India.

ABSTRACT

The majority of individuals look for product reviews before spending their money on it. As a result, users come across many reviews on the website, but whether these reviews are legitimate or not is unknown to the customer. Some favorable reviews are added by product company people themselves to some review websites in order to create phony positive product reviews. They give positive feedback on a variety of products made by their own company. The user will be unable to determine whether the review is real or not. By recognizing the Detect fake review as well as review posting habits, this system will detect phone reviews created by submitting fake remarks about a product. The user will enter his user id and password to access the system and see numerous products before leaving a review. To determine if a review is false or genuine, the system will

look up the user's Detect fake review. If the system notices a pattern of fake reviews being detect review using machine learning, it will alert the administrator to delete the review from the system. This approach assists the consumer in locating accurate product reviews. The suggested system will employ supervised machine learning. Based on simulation results, the Support Vector Machine algorithm was chosen (SVM). Future study should focus on implementing the system and testing its performance against various benchmark data sets. Another study topic could be to compare the performance of several classification algorithms in order to discover the best one for our suggested opinion fake review categorization approach.

Keywords: Fake Review , Classifications , Prediction , Analysis , Online products review

1. INTRODUCTION

A review is an assessment of a publication, service, or company, such as a movie (a movie review), video game (a video game review), musical composition (a musical composition or recording review), book (a book review), or a piece of hardware, such as a car, home appliance, or computer; or an event or performance, such as a live music concert, play, musical theatre show, dance show, or art exhibition. In addition to a critical assessment, the reviewer may assign a rating to the work to indicate its relative merit. An author may review current events, trends, or news items in a broader sense. A user review is a product or service review published by a user or customer based on her own experience with the product or service. Consumer reviews can be found on e-commerce sites like Amazon and Zippos, as well as social media sites like TripAdvisor and Yelp. Consumer reviews for products and sellers are frequently seen on e-commerce platforms. Consumer reviews are typically composed of several lines of text followed by a numerical rating. This text is intended to assist a potential buyer in making a purchasing decision. A consumer review of a product usually comments on how well the product measures up to expectations based on the specifications provided by the manufacturer or seller.



Fig 1: Fake Review Monitoring

2. RELATED WORK

R. Fontugne, et.al,... [1] It makes remarks on things like delivery timeliness, packaging and correctness of delivered items, shipping prices, and return services for promises made, among other things. Because of the popularity of Trip Advisor, Yelp, and other online review services, consumer reviews have become a big element in corporate reputation and brand image. A poor review can harm a company's reputation, prompting a new industry called reputation management in which businesses strive to erase or hide unfavorable reviews so that more positive content is found when potential customers conduct research. An expert review is one written by someone who has tried a number of similar items or services to determine which provides the best value for money or the best set of features..

Wang, We, et.al, [1] Online reviews are a significant source of information that may be used to determine public opinion on certain items or services, and they are often the key element in a customer's choice to acquire a product or service. Customer comments and reviews are extremely important to manufacturers and retailers because of

their impact. Because of the reliance on internet reviews, there is a risk that wrongdoers will fabricate reviews to artificially promote or devalue items and services. Opinion (Review) Fake review is a process in which fake review mers manipulate and poison reviews (by creating phoney, untruthful, or deceptive evaluations) for financial advantage. Because not all internet reviews are reliable, it's critical to create tools for spotting review fake review.

X Song, et,al,... [2] It is feasible to do review fake review detection using various machine learning algorithms by extracting meaningful aspects from the text using Natural Language Processing (NLP). Aside from the content itself, reviewer information can be used to help in this process. In this research, we examine the most popular machine learning strategies for detecting review fake review, as well as the performance of several approaches for categorization and detection of review fake review. The majority of recent research has concentrated on supervised learning approaches, which necessitate labelled data, which is scarce in the case of online review fake review. Because there are millions of online evaluations and thousands more being created every day, research into Big Data approaches is of interest.

Kuphkug [3] Fake review emails cost both individuals and businesses a significant amount of time, storage space, and money each year. Finding and prosecuting fake review mars, as well as eventual fake review email stakeholders, should enable a direct attack on the problem's source. To make such a challenging study easier, we present in this research a methodology for quickly and effectively dividing vast amounts of fake

review emails into homogeneous campaigns using structural similarity.

[4] Lazarevic. Aleksandar. et.al.... Nowadays, e-mail communication is essential, yet the e-mail fake review problem is rapidly expanding. The idea of collaborative fake review filtering with a near-duplicate similarity matching algorithm has been frequently discussed in recent years. The basic goal of the fake review detection similarity matching system is to keep a known fake review database, which is built by user feedback, in order to prevent further near-duplicate fake review s. Prior works primarily represented each e-mail by a brief abstraction built from e-mail content text in order to achieve effective similarity matching and reduce storage use. However, these e-mail abstractions cannot properly capture the dynamic nature of fake review s, and so are ineffective in detecting nearduplicates. In this research, we offer a unique e-mail abstraction method that uses the structure of e-mails to represent them. The purpose of Mahout is to create scalable machine learning libraries. We mean scalable to moderately large data sets when we say scalable. The map/reduce paradigm is used to develop our key algorithms for clustering, classification, and batch-based collaborative filtering on top of Apache review. We do not, however, limit contributions to review implementations; contributions that run on a single node or in a non-review cluster are also welcome. The main libraries have been fine-tuned to provide excellent performance even for non-distributed algorithms. Scalable enough to back up your business case. Mahout is released under the Apache Software licence, which allows for commercial use.

3. EXISTING METHODOLOGIES

The majority of individuals look for product reviews before investing their money in it. As a result, users come across many reviews on the website, but whether these reviews are legitimate or not is unknown to the customer. Some favorable reviews are added by product company people themselves to some review websites in order to create review positive product reviews. They give positive feedback on a variety of products made by their own company. The user will be unable to determine whether the review is real or not. The user has no way of knowing whether or not the product is a duplicate.

3.1 Fake Review model:

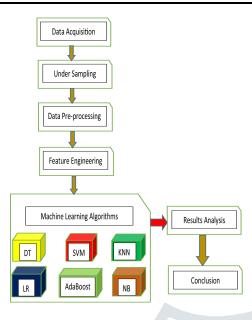
Nowadays, all customers purchase products online, but they have no way of knowing whether the product review is legitimate or not. The proposed "Fake Product Review Monitoring and Filtering for Genuine Online Product Reviews" system is presented. By recognizing the IP address as well as review posting trends, this system will detect false reviews created by posting bogus remarks about a product. The user will enter his user id and password to access the system and see numerous products before leaving a review. To determine if a review is false or genuine, the system will look up the user's IP address. If the system notices a pattern of fake reviews being sent from the same IP address, it will notify the administrator and request that the review be removed from the system. If the IP address is fraudulent, the user product order id can be used to locate the phoney review. This approach assists the consumer in locating accurate product reviews.

3.2 Principle Fake review analysis:

- User gets genuine reviews about the product.
- User can post to own review about the product.
- User can spend money on valuable products.

4. PROPOSED METHODOLOGY

Proposed a methodology of combining text clustering using Naïve Bayes (NB), algorithm with various classification mechanisms to improve accuracy of classification of emails into spam or non-The conjunction of clustering spam. classification mechanisms was carried out by adding extra features classification and also the classifier's performance was improved by clustering, results of this work show that combining K-means clustering with supervised classification in this methodology does not improve the classification performance for all mails. Further, the situations where the classifiers performance is improved by clustering, is found to be only slight increase in the the performance of classifiers in terms of accuracy with a very small amount which is not enough to meet requirements.



Fake Review analysis

4.1 Fake Review:

Misinformation, or opinion spam, becoming increasingly prevalent on review sites, with the goal of supporting or harming some target businesses by deceiving either human readers or automated opinion mining and sentiment analysis algorithms. As a result, numerous data-driven ways to assessing the legitimacy of user-generated material disseminated through social media in the form of online reviews have been presented in recent years. Different methodologies frequently consider different subsets of characteristics, i.e. traits, linked to both reviews and reviewers, as well as the network structure joining different entities on the review-site in exam.

4.2 Classifications:

It is totaled up the probability of each phrase into a priority value of mail to be spam using email classification algorithms. However, in the actual world, each word's spam likelihood is independent of the other, and the spam probability of two words combined is independent of the spam probability of the identical terms individually. Consider the following example: "Bumper" is a ham word, and "Prize" is a ham word, however the combination of these "Fake Review monitoring" will result in spam that will not be examined using present methodologies.

- Data Set
- Classifications
- Review Predictions
- Analysis monitoring
- Performances Evaluations

This paper seeks to provide an overview of the main review- and reviewer-centric features that have been proposed in the literature to detect fake reviews, with a focus on algorithms that use supervised machine learning techniques. These solutions outperform completely unsupervised alternatives, which are frequently based on graph-based methods that take into account relational links in review sites. Additionally, this study suggests and examines certain novel criteria that could be useful in classifying real and false reviews. A supervised

classifier based on Random Forests has been constructed for this goal, taking into account both well-known and new features, as well as a large-scale labelled dataset from which all of these features were retrieved.

5. CONCLUSION

The system allows the website fake review monitoring to see the product purchase details. The administrator can see how many people have visited

the website and bought something. The information is stored in the database automatically. The product report can be generated by the system and shown on the website. The proposed system has previously been built utilizing sym, Sentimental analysis, NB, Natural language processing approaches, and a few other technologies. All of them have resulted in the intended system being successfully implemented. Using the experiment, an efficient solution was obtained from a bank dataset. The SVM classifier is also performing well. The study's experiment outcomes are regarding categorization accuracy and cost analysis. Fake product review detection system will be useful to business organization as well as to customers. When used on e-commerce dataset the accuracy will be around 90%-96% if the data is going to be a labeled and supervised data, but, if the data is a unsupervised unlabeled data then the accuracy might vary in comparison to supervised data.

References:

- [1] Nitin Jindal and Bing Liu. Review spam detection. In Proceedings of the 16th international conference on World Wide Web,pages 1189-1190. ACM, 2020.
- [2] Song Feng, Longfei Xing, Anupam Gogar, and Yejin Choi. Distributional footprints of deceptive product reviews. ICWSM,12:98-105, 2019.
- [3] Eileen Fitzpatrick, Joan Bachenko, and Tommaso Fornaciari. Automatic detection of verbal deception. **Synthesis** Lectures on Human Language Technologies, 8(3):1–119, 2020.
- [4] Myle Ott, Yejin Choi, Claire Cardie, and Jeffrey T Hancock. Finding deceptive opinion spam by any

- stretch of the imagination. In Proceedings of the 49th Annual Meeting of the Association Computational Linguistics: Human Language Technologies-Volume 1, pages 309-319. Association for Computational Linguistics, 2019.
- [5] Yla R Tausczik and James W Pennebaker. The psychological meaning of words: Liwc and computerized text analysis methods. Journal of language and social psychology, 29(1):24–54, 2019.
- [6] Arjun Mukherjee, Vivek Venkataraman, Bing Liu, and Natalie S Glance. What Yelp fake review filter might be doing? In ICWSM, pages 409-418, 2019.
- [7] M.N. Istiaq Ahsan, Tamzid Nahian, Abdullah All Kafi, Md. Ismail Hossain, and Faisal Muhammad Shah. An ensemble approach to detect review spam using hybrid machine learning technique. 19th Conference International on Computer and Information Technology, Dhaka, December 18-20, 2019.
- [8] Yoon Kim. Convolutional neural networks for sentence classification. Proceedings of the 2014 Conference on Empirical Methods in Natural Language Processing, pages: 1746-1751, EMNLP, 2018.
- [13] S. Zhao, Z. Xu, L. Liu, and M. Guo. Towards accurate deceptive opinion spam detection based on word order-preserving CNN. Available Online http://arxiv.org/abs/1711.09181, CoRR, vol. abs/1711.09181, 2017.