International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-6, March 2020

Spam Detector: A Solution for Finding Bogus Opinions and Spammer Classification in E-Commerce

Nisha Kshirsagar, Amol Phatak

Abstract*: *In this paper we propose a system called Spam Detector to find out spam reviews of particular product. This framework uses spam features which helps to review datasets. In proposed system four different categories of features are included such as review behavioral (based on behaviour of review) , user behavioral (based on behaviour of user), review linguistic (based on linguistic pattern of review) and user linguistic (based on linguistic pattern of user). In today's world, most of people take decision based on information available through social media reviews on a topic or product. Due to this it is possible that anyone can post a review for a particular product which give a chance for spammers to post junk reviews related to particular product and facilities. To find out such spammers and the spam review is becoming important. Some methods exist to cope up with this problem, but these methods hardly detect spam reviews, and are not based on the extracted feature type. Weight of spam features are used to gain better results in the form of different aspects tested on real world review datasets. Here the used dataset is from Amazon websites. The experimental results show that Spam Detector beats the present method.

Keywords* : *spam, review, feature, product and users.

I. INTRODUCTION

We all know that in today's day to day life social Media or any online portals dramatically play an important role in information reproduction and expansion of same. For manufacturers, social media is important source in their advertising campaigns as well as for clients for making choice about products and services. In addition to this reviews of a particular product are helpful to service providers, manufacturers to increase the quality of their products and services. Hence for commercial success, these reviews and ratings are now become critical aspect . Positive reviews are beneficial for business and negative reviews leads to economic losses. The reviews which are deliberately written regarding product or service so that user's mind should get changed and users should think differently about that product or service are considered as spam. Such reviews are commonly written in exchange for money either to promote or demote business. Adding or removing features weight can scale time complexity and set it with some specific level of accuracy. This weighting results in and one can use less features with more weights to obtain improved accuracy having minimum time complexity. Classification of the features can be done in four different categories. Those are like which based on behaviour of review called review behavioral, user behavioral means based on behaviour of user , review linguistic i.e,based on linguistic pattern of review and user linguistic means based on linguistic pattern of user. This differentiation is helpful to interpret that how much is the contribution of each feature for spam detection.
We propose Spam Detector framework which implement new spam feature's weighting method. It determines the importance i.e weight of every feature and also it shows how features are effective in identifying spams out of normal reviews. Spam Detector improves time complexity. Time complexity depends on the number of features that are used to identify a spam review. Hence if features having more weights are used then fake reviews can be detected in less time complexity. Spam Detector find out the spam reviews based on feature weight

II. RELATED WORK

Following are some existing studies and approaches related for Spam Detector:-
In article [1] Author proposed that the reviews which are present on the Yelp website, out of that 20% reviews are actually spam reviews.
Article [2] and [3] justify the techniques which are used to determine spam reviews and spammers. It also state different type of analysis regarding same.
Article [4] many features which are heterogeneous are used pair wise to detect the colluders. Also they state that pair wise feature can directly model behaviour of colluders. Article [5] shows the classification of techniques into different family. Few of those uses linguistic patterns found in text and these are generally based on unigram and bigram and in [6] it stated that spammers writes spam reviews consistently and two view training algorithm gives better output than single view co-training algorithm .

Manuscript received on February 10, 2020.
Revised Manuscript received on February 20, 2020.
Manuscript published on March 30, 2020.
* Correspondence Author
Ms. Nisha Kshirsagar*, Dept. of Computer Science & Engineering, N. B. Navale Sinhgad College of Engineering, Solapur, India.. Email: nisha14395@gmail.com
Prof. Amol Phatak, Dept. of Computer Science & Engineering, N. B. Navale Sinhgad College of Engineering, Solapur, India.. Email: amol1911@gmail.com

Article [7], [8], [9] have explanation of classification of techniques based on user behaviour. Article [10] contains the categorization of methods depends on user behavioral patterns. And it is mostly metadata based.

Some classification techniques which uses graphs as well as graph-based algorithms and classifiers are discussed in article[11] and [12].

Also[13] have graph based techniques explained and it states that syntactic patterns is helpful to find dishonest writing. Article [14] model a behavioral movement to find out spam review. It possess scoring method of aggregated behaviour to rank reviews

FraudInformer- existing system consider only Linguistic features to find out spam reviews. It focuses on some linguistic pattern like content similarity in reviews, use of special characters and use of capitals letters. It shows that how users or clients are describing their feeling, notion or idea about what they have experienced as a customer of a certain product

III. SPAM DETECTOR SYSTEM

The Spam Detector framework consider feature's weight which is used to compute the final labels for reviews as spam or not spam. Spam Detector framework is proposed to state the comparative weight of each and every feature. Spam Detector is able to find feature's weight. And it can be happened depends on values which are calculated for every review. This will boost the accuracy in terms of time complexity as fake reviews can be detected easily within less time complexity by using some features which having more weights. Features involved in spam detection are:

1) Features based on Review-Behavioral fashion: This kind of feature is depends on meta data and not on the test present in review. It contains two features and those are Early time frame as well as Threshold rating deviation of review.

2) Features based on Review-Linguistic fashion : This sort of features are based on the review itself. These are extracted directly from the text and content of the review. In this work we use two main features those are the Ratio of 1st Personal Pronouns and the Ratio of exclamation sentences which contain '!' in review.

3) Features based on User-Behavioral fashion: This type of features are particularized to individual client and they can be calculated per client. This sort of feature is useful to check out all of the reviews written and posted by that particular user. This category has two main features and those are review burstiness, and the average of a user's negative ratio given to the product.

4) Features based on User-Linguistic fashion: These features are pull out from the user's language and it shows how they are sharing their feeling regarding what the have experienced as a consumer of a product. This type of of features can be used to understand how a spammer communicates in terms of wording .It contain feature like - Average Content . It show how much two reviews given by two different clients are similar with other because spammers generally use existing template to write similar reviews for a product.

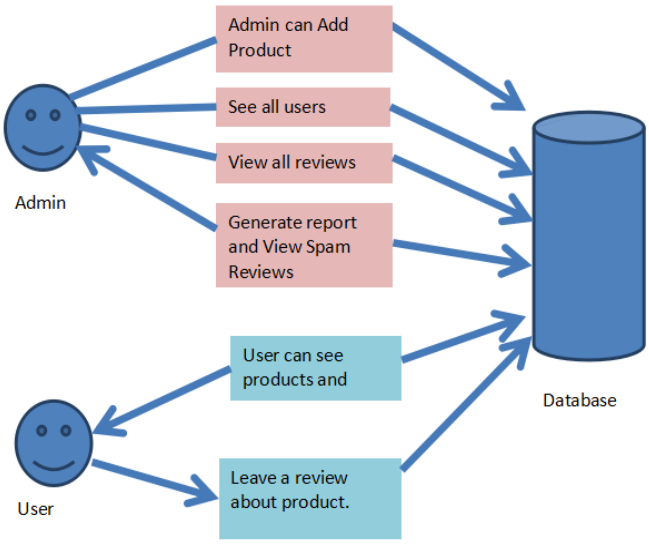

Fig. 1. **System layout**

TECHNIQUES

Burstiness : Generally spammers write and post their spam reviews in little time period. This is because of two reasons: first- because they want to influence readers. Second is - because they are very temporal users. And in short period, they are willing to write as many as reviews they can.

$$x_{BST}(i) = \begin{cases} 0 & (L_i - F_i) \notin (0, \tau) \\ 1 - \frac{L_i - F_i}{\tau} & (L_i - F_i) \in (0, \tau) \end{cases}$$

Here Li - Fi mention days between last review and first review for τ = 28.If measured value is more than 0.5 then users take value 1 and otherswise they take 0.

Negative Ratio : The spammers have contract with the business and are advised to write and post reviews to discredit businesses which are considered as challenger with the ones they have contract with. This can make happen by giving spam reviews or low rating. Users having average rate equal to 2 or 1 then it take 1 and others take 0.

Early Time Frame: Spammers usually try to write their reviews as soon as possible so that review can be at top position and other users should visit them sooner.

$$x_{ETF}(i) = \begin{cases} 0 & (T_i - F_i) \notin (0, \delta) \\ 1 - \frac{T_i - F_i}{\delta} & (T_i - F_i) \in (0, \delta) \end{cases}$$

where Li - Fi mention days between last review and first review for τ = 7 .If calculated value is greater than 0.5 then users take value 1 and others they take 0.

Rate Deviation: Spammers give high rate to promote businesses with which they have contract. This leads high diversity in their given scores to different businesses.

$$x_{DEV}(i) = \begin{cases} 0 & otherwise \\ 1 - \frac{r_{ij} - avg_{e \in E_{*j}} r(e)}{4} > \beta_1 \end{cases}$$

Average Content Similarity: Spammers generally don't want to write an original review and waste their time to so they write their reviews using same template .

And hence at the end they have similar reviews.

Number of first Person Pronouns in review, Ratio of Exclamation Sentences containing '!' in review: Previous studies show that spammers generally use first personal pronouns in less fashion and they mostly use second personal pronouns more. And over again spammers place '!' in their review to increase visual aspect on users and foreground their reviews among all.

ALGORITHM : Spam Detector
Input: Review dataset
Output: Feature weight and spamicity label
1: Start: Load dataset in database
2: for each user(u)
3: for each written reviwe (r) about each product (p)
4: if r> 1 i.e multiple review for same product by same user in minimun time then
5: calculate Burstiness
6: end if
7: for each rating (ri)
8: Calculate rate deviation
9: End for
10: for each review
11: Calculate negative ratio
12: End for
13: for each review
14: Calculate early time frame
15: End for
16: If this review matches with some other
17: Calculate average content similarity
18: End if
19: for each review
20: Calculate first person pronoun
21: End for
22: End for
23: End

IV. RESULT AND DISCUSSION

Four datasets are used For result analysis. Size of each datasets is different like 11, 12, 13 and 500. Same input dataset is provided to both systems and result is recorded. Below are observation tables:

Table- I: Observation Table for first dataset

System	Input dataset size	Expected result		Obtained Result	
		Spam	*Not Spam*	*Spam*	*Not Spam*
Spam Detector	11	4	7	4	7
FraudInformer				5	6

Table- II: Observation Table for second dataset

System	Input dataset size	Expected result		Obtained Result	
		Spam	*Not Spam*	*Spam*	*Not Spam*
Spam Detector	12	6	6	6	6
FraudInformer				4	8

Table- III: Observation Table for third dataset

System	Input dataset size	Expected result		Obtained Result	
		Spam	*Not Spam*	*Spam*	*Not Spam*
Spam Detector	13	8	5	8	5
FraudInformer				2	11

Table- IV: Observation Table for fourth dataset

System	Input dataset size	Expected result		Obtained Result	
		Spam	*Not Spam*	*Spam*	*Not Spam*
Spam Detector	500	185	315	185	315
FraudInformer				224	276

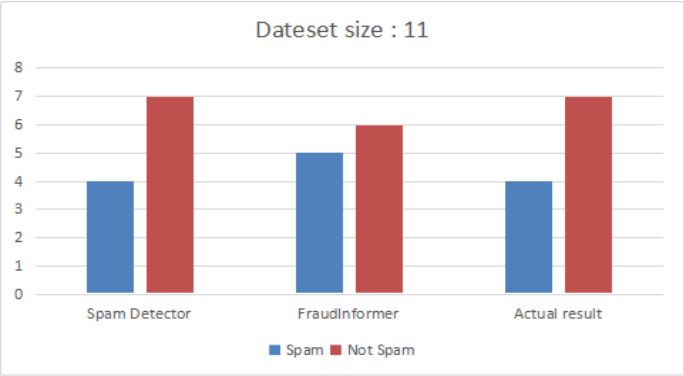

Fig. 2. **Analysis of Table I**

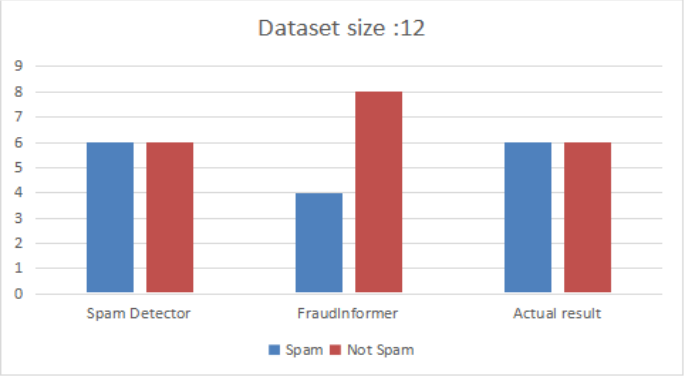

Fig. 3. **Analysis of Table II**

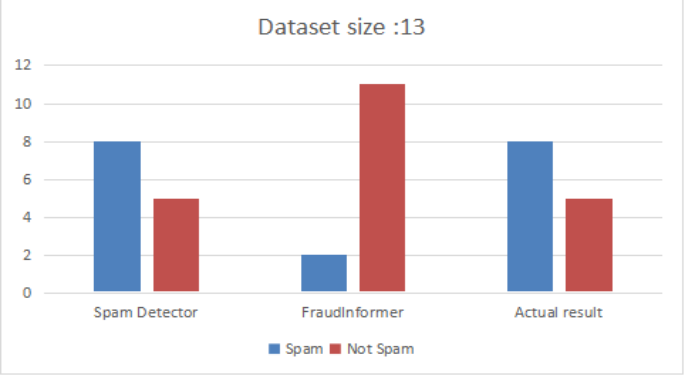

Fig. 4. **Analysis of Table III**

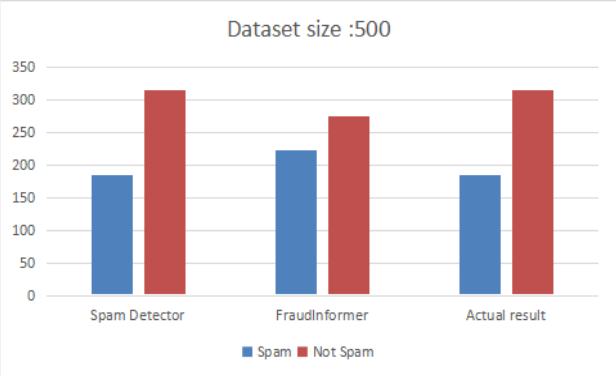

Fig. 5. **Analysis of Table IV**

From above obtained result it is observed that Spam detector performs better than FraudInformer in terms of accuracy.

V. CONCLUSION

Spam detector introduces and enclose a novel spam detection framework. This is based on features weight calculation to label reviews in rank-based labeling approach. In addition, to increase the accuracy, Spam Detector also calculates the importance and weight of each feature which output better performance and hence we can conclude that Spam Detector can beat existing method in terms of accuracy. This same work can be extended to identify spammer community instead of identifying only fake and spam reviews.

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. A. Heydari, M. A. Tavakoli, N. Salim, and Z. Heydari. Detection of review spam: A survey. Expert Systems with Applicants, Elsevier, 2014.
3. M. Crawford, T. D. Khoshgoftar, J. N. Prusa, A. Al. Ritcher, and H. Najada.Survey of Review Spam Detection Using Machine Learning Techniques.Journal of Big Data. 2015
4. M. Ott, C. Cardie, and J. T. Hancock.Estimating the prevalence of deception in online review communities.In ACM WWW, 2012.
5. M. Ott, Y. Choi, C. Cardie, and J. T. Hancock.Finding deceptive opinion spam by any stretch of the imagination.In ACL, 2011.
6. Ch. Xu and J. Zhang. Combating product review spam campaigns via multiple heterogeneous pairwise features. In SIAM International Conference on Data Mining, 2014.
7. F. Li, M. Huang, Y. Yang, and X. Zhu. Learning to identify review spam.Proceedingsofthe22ndInternationalJointConferenceonArtificial Intelligence; IJCAI, 2011.
8. G. Fei, A. Mukherjee, B. Liu, M. Hsu, M. Castellanos, and R. Ghosh.Exploitingburstiness in reviews for review spammer detection.In ICWSM, 2013.
9. A. j. Minnich, N. Chavoshi, A. Mueen, S. Luan, and M. Faloutsos. Trueview: Harnessing the power of multiple review sites. In ACM WWW, 2015.
10. 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.
11. H. Li, Z. Chen, B. Liu, X. Wei, and J. Shao. Spotting fake reviews via collective PU learning.In ICDM, 2014.
12. L. Akoglu, R. Chandy, and C. Faloutsos.Opinion fraud detection in online reviews bynetworkeffects.In ICWSM, 2013.
13. R. Shebuti and L. Akoglu. Collective opinion spam detection: bridging review networksand metadata. In ACM KDD, 2015.Reviews.In ACM WWW, 2012.
14. NetSpam: a Network-based Spam Detection Framework for Reviews in Online Social Media by SaeedrezaShehnepoor, Mostafa Salehi*, Reza Farahbakshah, Noel Crespi.

AUTHORS PROFILE

Ms. Nisha Kshirsagar has completed her Bachelor's Degree in Computer Science and Engineering in 2016 from Solapur university, Solapur. Maharashtra, India. She is currently pursuing Masters Degree in Computer Science and Engineering from N B Navale Sinhgad College of Engineering, Kegaon-Solapur, Maharashtra, India. She has 3 years of teaching experience. Her areas of interest are Computer Network, Data mining and analysis etc. She is working as senior software developer in IT industry. She has hands on practice of Java and Mulesoft,

Prof. Amol Phatak obtained his Bachelor's Degree in CSE from Shivaji University, Kolhapur in the year 2001, Masters Degree in CSE from Walchand College of Engineering, Sangli Maharashtra in year 2008 and pursuing Ph. D in CSE at Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, Tamilnadu, India. He is also working as Head of CSE department, N B Navale Sinhgad College of Engineering, Kegaon-Solapur, Maharashtra, India. He has 18 years of Teaching Experience, 15+ students had completed Post Graduation under his guidance and his areas of interest are Distributed Systems, Computer Network Security, Artificial Neural Network, IoT Security etc