Fake Product Review Analysis

M. Kavitha[1], P. Dinesh[2], L. Meha Dhanushya[3], M. Thangamani[4]
[1, 2, 3, 4] Dept of Computer Science and Engineering
[1, 2, 3, 4] Kathir College of Engineering, Coimbatore, Tamilnadu, India.

Abstract- *In online shopping, the product sellers often take reviews from the customer for the product. As e-commerce is growing rapidly the number of reviews from the customer is also increasing day by day. Some spammers attempt to write fake(spam) reviews to affect customer opinions and increase their sales rating. It is a tediuos work for the customers to identify the fake(spam) reviews. We propose spam detection using Bi-gram algorithm and IP Address to filter the genuine reviews from the fake (spam) reviews.*

Keywords- product review, fake(spam) reviews, IP address detection, bi-gram.

I. INTRODUCTION

In the era of internet, everything has very are becoming very faster. Social media sites are used for interacting with people all over the world. Thoughts are shared on the internet. Internet provide the facility of online shopping like Amazon, Flipcart etc. Before purchasing anything people look for reviews. Based on the reviwes the people make their decision wheather to purchase the product or not. Based on the evaluatuons customers can compare the brands and finalize their interst. People are not aware about the crediblity of the reviews. It may be genuine or fake. This is not identified by the people. To address this issue, a few consumer sites have consolidated tips and clues to manually spot spam reviews. However, for online products with a huge number of reviews, it is practically impossible to manually check and distinguish the spam opinions from the real reviews. Several high-profile cases have been reported and spammers have transparently admitted to be paid to write fake reviews in media investigations. Many businesses have rewarded positive reviews with promotions and coupons.

Many of the, researchers have shown great interest in identifying truthfulness of reviews. Reviewer behavior analysis is conducted in to detect suspicious activities using the temporal footprints of the reviewers. and hypothesize that there are natural distributions of review star ratings and spam reviews can lead to skewed rating distribution. use content similarity analysis which treats duplicates and near-duplicate reviews as potential spam reviews based on the evidence that spammers often sign in with different identifies to reuse similar reviews on a same product. However, research in spam detection is far from adequate to address the challenges in this area. In this study, we propose an end-to-end system that works seamlessly on large data sets and generates user consumable reports. It integrates multiple methodologies in a practical fashion to overcome the ever-changing techniques employed by spammers.

EXISTING SYSTEM

Clearly consumers value the feedback given by other users as do the companies that sell such products. Blogs, websites, discussion boards etc. are a repository of customer suggestions which are valuable and important sources of textual data. Therefore, today's individuals and older ones extensively rely on reviews available online. It means that people make their decisions of whether to purchase the products or not by analyzing and reflecting the existing opinions on those products. The fact that is if the potential customer or users gets a genuine overall impression of a product by considering the present affect for that product, it is highly probable that he will actually purchase the product. Normally if the percentage of positive and effective opinions is considerable, it is likely that the overall impression will be highly positive. Likewise, if the overall impression is not proper, it is doubtful that they don't buy the product. The main disadvantage is if the social media optimization team uses different mail accounts to review the product it is not possible to detect the fake review. To overcome this a new frame work is proposed

II. PROPOSED SYSTEM

Many people require review about a product before spending their money on the product. People may come across various reviews in the website but these reviews are genuine or fake is not identified by the user. In some review websites some good reviews are added by the product company people itself in order to make product famous this people belong to Social Media Optimization team. Every one give good reviews for many different products manufactured by their own firm. User will don't know to find out whether the review is genuine or fake. To find out this" Fake Product Review Analysis" system is introduced. The proposed framework consists of two main methods namely IP address detection - to find out fake reviews made by the social media optimization team by

identifying the IP address. and bi-gram algorithm – to differentiate good and bad reviews.

2.1. IP ADDRESS DETECTION

2.1.1 EMAIL ID

Every E-commerce website we could the patron avail its offerings and permit transactions most effective after verifying his identification i.E. The user has to make an account on that platform. Majorly, one such piece of information that each line service company demands is the customer's Gmail ID. This work has exploited this statistics. In our prototype, a customer can put up best 1 assessment on a specific product with a given Gmail ID. One vital feature that distinguishes Gmail IDs is the usage of prevent phrases (full prevent, commas, etc.). In a situation wherein if a consumer login to a website with Gmail ID say-'abc@gmail.Com', and the subsequent time the spammer tries to login the usage of 'ab.C@gmail.Com', then in that case majority of the present E-commerce websites deal with these of them as separate debts or two exclusive customers. But in fact these are the same IDs with admire to Gmail. Thus, it turns into smooth for the spammers to login through distinctive bills and submit multiple evaluations with a extraordinary identification every time. To avoid this, we have proposed a new framework the elimination of prevent phrases and then compare if the email IDs given are identical or exceptional. A better idea would be permit Gmail handle the process of authentication and in preference to having separate signup, virtually permit the client surf thru the internetsite the usage of his Gmail ID. We have adopted both these processes in our prototype. But what if the spammer makes another Gmail ID? Though it will be tedious to make a new ID every time before posting a overview however yes there is a possibility. To counter assault this issue, we can hint the IP address of the device.

2.1.2 IP ADDRESS

The spammers can use any of the devices (smartphones, laptops)to publish fake critiques.However, the system getting preserve the IP cope with of the tool can help in uniquely identifying the device. we have proposed the prototype puts a prevent on the number of attempts or times a consumer allowed to submit online evaluations from his tool on one specific producet. A proper user will now not try to put up multiple reviews for the one unique product greater than.once. Thi technique prevents review unsolicited mail that would in any other case lie to the users, which is extremely obnoxious.

Algorithm: To detect spam review

Input: A review

1. Authenticate the Gmail ID of the user
2. If the user has already posted a review for the same product, discard the review.
3. If he is posting for the first time, check the IP address of the device being used
4. If number of reviews for a specific product from that device >= Threshold, review is manipulated.
5. If number of reviews for a specific product from that device < Threshold, review is considered to be genuine. If multiple reviews from the same IP Address have been made in the same day then restrict the user from posting the review.

2.1.3 SPAM WORD DICTIONARY

Another problem posing hazard is the non-evaluations. A unsolicited mail word dictionary is used to stumble on irrelevant reviews. We have taken the inspiration of that the elimination of the unsolicited mail words from the beyond studies which many of the researchers have attempted to locate junk mail emails. Phrases like 'buy direct', 'different offer', 'money back' and lots of extra are used steer the people or promote it their very own services. Thus, such opinions can not be taken into consideration genuine. We have, therefore, modelled our framework approach that does not keep in mind a evaluate containing such spam words as genuine. database is being maintained that consists of all such spam words and terms. The content analysis of the online evaluations is made in opposition to these saved spam phrases the usage of the n-gram model and Jaccard's coefficient preserving the brink as 80%. The opinions containing any of these junk mail words or phrases are considered to be misleading. The textual analysis of the online opinions further restricts the spammers to a first rate extent.

Algorithm: To detect non-review

Input: A review

If the review contains any word present in the spam dictionary, it is considered as a non-review.

2.2. DETECTION OF DUPLICATE REVIEWS USING BI-GRAM ALGORITHM

we introduce bi-gram algorithm to improve the computational efficiency and to optimize the process.

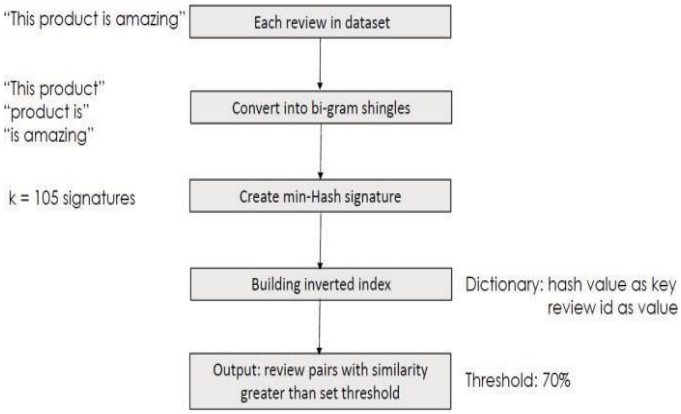

Figure 1. Overall process of bi-gram algorithm

The overall process is illustrated in Figure. 1 First, each review is converted into a set of bi-gram shingles that are formed by combining two consecutive words together. For example, “This product is amazing,” a set of bigram shingles is generated containing “This product,” “product is,” and “is amazing.” Usage of such bigrams is more meaningful than tokenizing each word as it helps increase the relevance between the contexts. The similarity between two opinions are regularly computed by using checking the ratio of interactions of their sets of bi-gram shingles. There are various similarity measures in the literature like Euclidean distance,Cosine similarity,Minkowski distance and Jaccard similarity.For this research, Jaccard similarity is applied due to the fact as compared to other measures that compute similarity measures for facts objects represented assets a chunk like units of bi-gram shingles.

2.2.1 Cyclic Redundancy Check (CRC)

Hash and min-hash for simpler computation to get the Jaccard similarity cost, the shingles are first mapped to shingles ID’s the use of the CRC32 hash characteristic that converts any variable duration string right into a hexadecimal value of 32-bit binary sequence. Now, the set for every review is represented as a set of integers instead of substring shingles. Still the scale of the set is large to compute the similarity.

Our primary goal is to have a smaller illustration of these large sets known as “signatures”. The key belonging to such signatures is that they should be an excellent representation of the large set with mile smaller size. Signatures for each set are derived the use of min hash scheme with k hash functions, where k is a fast and hard integer. The valve of k is ready to one zero five for this research. According to chernoffBound the predicted mistakes charge by using min-hash is $0(1/\sqrt{k})$ and in general having a okay around 100 ends in a small error probability. Using min hash values prevents from having to explicitly compute random diversifications of all of the shingles IDs

2.2.2 Inverted index

After reap min-hash values to represent each review, the Jaccard similarity is converted into the range of equal signatures in opinion A and B divided by the full wide variety of specific signatures in them. However, to examine min-hash values among critiques still requires the complexity of O(n2) where n is the wide variety of evaluations indexes are constructed the usage of the min-hash values. Inverted index is the broadly adopted technique in the statistics retrieval. In our study, a dictionary is constructed by the use of all min-hash value of a product as index keys, where every index keys factors to opinions containing the corresponding min-hash cost. This inverted index returned all the goods with a given min-hash fee in a O(log n) time.

III. EXPERIMENTAL RESULTS

3.1 IP ADDRESS DETECTION

The maximum widevariety of instances a reviewer can post evaluations from a given e-mail ID was set to 1, with aselected IP dealwith to2, and from aspecific location to 3. The proposed prototype changed into testedand opinions from special users.It confirmed that the accuracy percentage of 65%.The proposed model couldn't determine out the spammers in a few cases. For example, in a rooted mobile device, the person can alternate the ways of configurations of his tool inclusiveof its IP address anytime. Secondly, there are few area converting applications available thatpermit the users togovern the place of the device easily. Another element that are at the times interfered with the right working of these prototype turnedinto the precision and accuracy of the geo-coordinates retrieved. In certain cases, the range and longitude of an area have been retrieved of then up to number that is four decimal places, whereas in some other cases up to2or three places of the decimals. In thissortof scenario, the server facet database shops exclusive values of geo-coordinates for the identical place. Hence, this inconsistency of these recent facts needs to be resolved when similarly paintings is performed inthis domain.

Review	ID	IP	Spam Words	Impact
Great product	abc@gmail.com	192.168.65.1	-	No spam
Nice features	abc@gmail.com	192.168.65.1	-	Spam
Amazing quality	id@gmail.com	223.190.33.131	-	No spam
Not up to the mark	myd@gmail.com	223.180.23.1	-	No spam
Money gaurantee	sim@gmail.com	190.120.10.1	money back	Spam

Figure 2. Results of sample test cases

3.2 DETECTION OF DUPLICATEREVIEWS USING BI-GRAM ALGORITHM

The output from duplicate detection approach is kept in a CSV file one by one for every product category. Product X's asin, review rating, unixtime, product Y's asin, review rating, unixtime, and similarity score between X and Y are the column headings for this CSV file.

365	B00147820Q	4	1368403200	B004QQLR4M	4	1368403200	0.85571429
366	B00155237W	5	1365984000	B00063X7KG	5	1365984000	0.85714286
367	B00155237W	5	1365984000	B002XOXSI2	5	1365984000	0.83809524
368	B0015KROXU	2	1309046400	B00008BKX5	5	1313020800	1

Figure 3. Screenshot of the example duplicate detection output

In order to examine the results of the output, example duplicate detection results are presented. The highlighted rows 366 and 367 show high similarity scores that indicate potential duplicate reviews between products B00155237W and B00063X7KG; and between B00155237Wand B002XOXSI2. To validate the results, the product asins are used to find the product description fromAmazon.com:

- B00155237W: Cruiser Accessories 76200 Tuf Flat Shield Novelty / License Plate Shield
- B00063X7KG: Meguiar's G1016 Smooth Surface ClayKit
- B002XOXSI2: Meguiar's G110V2 Professional Dual ActionPolisher

Based on the unixtime, the reviewer "Mack Wu" haswritten similar reviews to all the three different types of products and at the same time which indicates spams.

IV. EFFICIENCY

The system can perform fake review analysis efficiently. By running the test on a MacBook Pro, the system is in a position to generate the credibility report for the product categories within an hour. This makes the system usable for online website deployment. It's well adapted to large datasets and also might be used for other datasets with little changes to the feature names.

V. CONCLUSION

In this paper, we present a multi-dimensional analysis to detect the fake reviews. It generates credibility reports for given products detection based on two methods: IP Address detection to and Bi-gram algorithm. All the methods provide useful information, serving as an overlay to enable the discovery of fake reviews. To our best knowledge, no other work in the literature has investigated the integration of algorithms into a practical and deployable framework to determine the credibility. Theresults show the effectiveness and efficiency of our proposed approach.

REFERENCES

[1] [1 Adhav K, Gawali SZ, Murumkar R. Survey on Online Spam Review Detection Methods. In: International Journal of Computer Science and Information Technologies, vol. 5(6).

[2] [2 Crawford M, Khoshgoftaar TM, Prusa JD, Richter AN, Najada HA. Survey of review spam detectionusing machine learning techniques. In: Journal of Big Data.

[3] Feng, S., Xing, L., Gogar, A., and Choi, Y. Distributional footprints of deceptive product reviews. ICWSM12

[4] Fusilier, D. H., Montes-y Gómez, M., Rosso, P., and Cabrera, R. G. Detection of opinion spam with character n-grams. In International Conference on Intelligent Text Processing and Computational Linguistics,Springer.

[5] He, R., and McAuley, J. Ups and downs: Modeling the visual evolution of fashion trends with one-class collaborative filtering. In proceedings of the 25th international conference on world wide web, International World Wide Web Conferences Steering Committee,pp.507

[6] Hellman, M., and Raviv, J. Probability of error, equivocation, and the chernoff bound. IEEE Transactions on Information Theory.

[7] Hochenbaum, J., Vallis, O. S., and Kejariwal, A. Automatic anomaly detection in the cloud via statistical learning. arXiv preprint arXiv:1704.07706 .

[8] Hu, N., Koh, N. S., and Reddy, S. K. Ratings lead you to the product, reviews help you clinch it? the mediating role of online review sentiments on product sales. Decision support systems 57.

[9] Jindal, N., and Liu, B. Review spam detection. In Proceedings of the 16th international conference on World Wide Web.

[10] Jindal, N., and Liu, B. Opinion spam and analysis. In Proceedings of the 2008 International Conference on Web Search and Data Mining, ACM.