International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 01 | Jan 2021 www.irjet.net p-ISSN: 2395-0072

# Scrutiny of Fraudulent Product Reviews and Approach to Filtrate the Aforementioned

**Chinmay Gadkari[1], Saad Ahmed [2], Dhanashree Darekar[3], Devavrat Agnihotri[4], Reena Pagare[5]**

*[1-4]Students, Dept. of Computer Science & Engineering, School of Engineering, MIT-ADT University, Pune, India*
*[5]Professor, Dept. of Computer Science & Engineering, School of Engineering, MIT-ADT University, Pune, India*

---

**Abstract -** *The branding and promotion of product reviews is critical for online stores. They help build trust and loyalty, and typically establish the difference between your products and others. Since consumer interest could disrupt, fake reviews are a big challenge to websites and product search engines. While fake evaluations are good to everyone in the long run, the rise in this doubtful tactic is very fascinating. The fact that huge amounts of time, energy and resources are being poured into fake review spamming is an indicator of just how valuable it can be to have a decent number of reviews. In this manuscript, a conventional method is proposed for elimination of Fake Reviews on ecommerce sites. The solution is to use the reviewers' behavior features with review parameters such as the username, IP address and duplicate reviews to delete fake users.*

***Key Words*: *Fake Review, LCS, IP Address, Duplicate, Rating, Bias***

## 1. INTRODUCTION

Over the last decade, online reviews have been becoming an ever-more-common part of consumers' purchasing decisions. But, with reviews now being a huge part of online search results, a Fake Review can potentially disrupt the Customer interest.

Online Product reviews are a preeminent for people to make decision buying products online. Availability of many similar products makes it difficult for a person to find out which one is the best for the buck, so relying on reviews is a must. As anyone can write a review and get away with it, an increase in fake and spam reviews has been seen, fabricated to look original in order to manipulate the market.

Fake Reviews has caught a lot of attention lately. Specifically, the reviews that have been written either to popularize or benefit a brand or a product (therefore expressing a positive sentiment for a product) are called positive deceptive review spams. Whereas, the reviews that intend to malign or defame a competing product expressing a negative sentiment towards the product, are called negative deceptive review spams.

The main contributions of this paper are as follows:

1) Supervised method based on Longest Common Substring(LCS) algorithm in order to remove duplicate or near-duplicate reviews, i.e., fake reviews. The model calculates the likeness of a review that can be generated from another one.

2) Review relevancy is also checked if the review is related to the product/brand is not.

3) Finally, user data and review data like account used and IP address is used to detect Fake ones.

The remaining portion of the Paper is divided as follows. Section 2 for relevant previous works. Section 3 highlights on the Survey conducted by BrightLocal of Online Reviews Statistics. Section 4 classifies the use of Longest Common Subsubsequence Algorithm(LCS) for Similar Reviews, Later in Section it shows how use of Account data, Unique review ID, IP address can help detect fake Reviews. Section 5 concludes the work done and suggests direction for possible future work and improvements.

## 2. RELEVANT PRECEDENTS

There should be a set of meaningful, relevant previous work to allow any product to eventually be implemented and executed. The useful assessment of previous works that used comparable technology layer to bring similar benefits to the end consumer enables us to create more polished system.

There are some works available today on the internet which provide good functionalities to detect spam reviews. Below presented are some of the relevant precedents:

[1] This Publication suggests the use of Weka Tool for Text Classification and is Completely based on Sentiment Analysis for Detection of Fake Reviews. It also shows us the difference between popular text classifying techniques, so as per the findings Support Vector Machine(SVM) is most accurate at 81.75% but it takes double the time of Naïve Bayes(NB) to build the model and NB is at 81.45% accuracy. Also, detection processes for fake positive reviews and fake negative reviews depend on the best and more accurate method.

[2] An automated method is proposed to highlight review spam in product websites using review text based as well as reviewer-based methods. Supervised and unsupervised methods are applied

from two different data sets. Also compare the analysis using various feature sets.

[3] This paper classifies all the supervised, semi-supervised and unsupervised methods based on Hotel Reviews dataset and use of Naive Bayes, SVM, Random Forest, K-nn and many more.

[4] In this paper they calculate the rating of reviews using sentiment score and then compares it with the posted rating using self-developed dictionary. At first abusive reviews are filtered then the review sentence is divided into individual tokens, later sentiment score is calculated and compared.

[5] This paper makes use of semantic features to perform classification on Yelps' data, they propose two new features, readability and topic and prove that those are better than n-gram feature and use f-measure(mean of Precision and Recall values).

[6] The system is completely based in behavior features of the reviewer, like customer rank, deviation rate, bias rate, review similarity, review relevancy, content length and illustrations.

## 3. SURVEY

Methodologies have been established for conduction survey research aimed at ensuring that the research is rigorous and robust outputs are obtained.

In 2010, fewer than 70% trusted reviews as much as personal recommendations, fast forward to 2019, 90% of people say that positive reviews make them more likely to buy a product. The continued presence of faux reviews also tells us that reviews are an enormous a part of the buyer decision-making process.

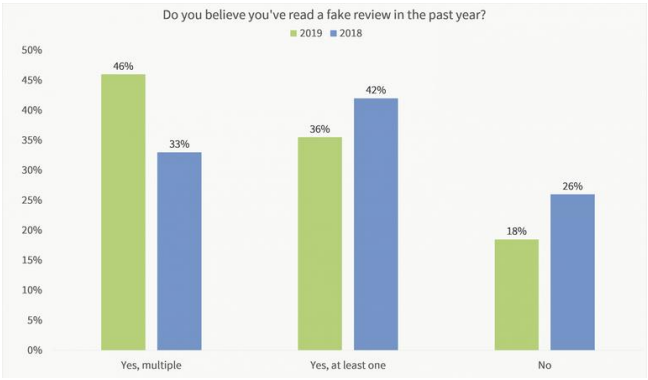


**Chart -1**: Survey on Fake Reviews

According to BrightLocal research, 82% of consumers have read a fake review in the last year. The share is even higher amongst 18-34-year-old users, with 92 percent claiming they've seen fake reviews.

It's obvious that 18-34-year-olds find it a lot easier to notice fake reviews. This may be because as digital millennials they have experienced life online and so are savvier when it comes to navigating the online world. It's also possible that this constant exposure has given them digital street smarts to the extent that they're naturally more suspicious or untrusting of user-generated content such as online reviews until given good reason to think otherwise.

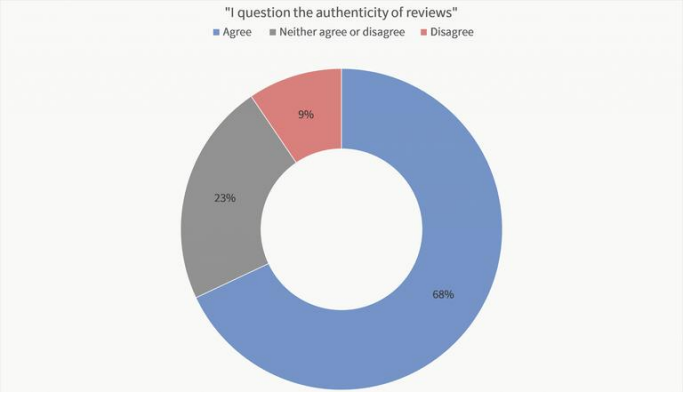


**Chart -1**: Customer Doubt

With 68 percent of consumers questioning the validity of reviews, it seems like not every customer is as skeptical. Only 9% said they did not doubt the validity of the reviews, and 23% said they were unsure of the authenticity of the reviews.

Deceptive reviews (those posted by customers who have not actually made a purchase from the company being reviewed) appear to use repeated exclamation points such as '!!!! As per research[7] conducted by MIT, 'And' and "!!! ' in the text of the review.

MIT researchers analyzing reviews without sales discovered that those leaving a review without having made a purchase contain considerably more terms and are much more likely to contain demands for the company such as 'please bring back', 'give more and go back to'. Research[8] carried out by The Washington Post found that 61 percent of Amazon electronics reviews are fraudulent. Categories such as wireless Bluetooth headphones and Bluetooth speakers are affected by the false reviews, though other categories such as testosterone pills and diet pills have also been found to be affected.

Consumer trust in reviews online is at an all-time peak. Reviews are now so critical that there is a growing prevalence of fake reviews. This poses many problems for companies and customers alike, with customers increasingly likely to face false reviews and companies increasingly being put at a disadvantage if they do not join unscrupulous rivals in purchasing or faking reviews to gain exposure on review websites and e-commerce sites.

### 3. ALGORITHM & FEATURES

In this section we have designed some spam indicators and the algorithms to predict those indicators.

1) Review Similarity rate

Some reviewers also copy the reviews of other customers to save time, and use them as their own reviews without or with a few minor adjustments. The same product or related goods come from these plagiarized reviews. We refer to [9] to use the modelled bag-of-words to stand for each content of the review and to use the cosine function to measure the similarity between two reviews. The review similarity rate between two reviews $r_a$ and $r_b$ is defined as follows:

$$RCS(r_a, r_b) = {}^{r_a}/_{r_b}$$

Note that the phenomenon of copying reviews of other customers is very popular. So, the efficient identification algorithm is the key to recognizing similar reviews from massive volume of reviews.

Hence, we present a non-recursive **longest common subsequence** (LCS) algorithm.

**Algorithm 1** LCS

```
Input: two strings s1 and s2 as two reviews;
Output: A large common sub-string of both s1 and
s2. if s1==s2 then return s1;
else if s1=="" or s2=="" then return "";
end if
index ← 0;
length ← 0;
for i = 0 → s1.length do
    for j = 0 → s2.length do
        if i - 1 >= 0 and j - 1 >= 0 then n ← d[i - 1, j - 1];
        else n ← 0;
        end if
        if s1[i] == s2[j] then d[i, j] ← 1 + n;
        else d[i, j] ← 0;
        end if
        if d[i, j] > length then
            length = d[i, j];
            index = i;
        end if
    end for
end for
return s1.Substring(index - length + 1, length);
```

We are developing Algorithm 2 to measure the similarity of all reviews based on the LCS algorithm. In Algorithm 3, several pruning statements are introduced to reduce the call times of the LCS algorithm. 1) We use the "if(s1==s2)" expression to cut the call times of the LCS algorithm when both s1 and s2 are equal. 2) We do not measure their similarity when we compare the similarity of both s1 and s2, if s2 is a copied analysis. We therefore use the "if (similarity[j]>ε)" argument. 3) Since the plagiarist does not change too much content of the copied review, Algorithm 2 does not need to get all common substrings between two reviews and calls the LCS algorithm up to a maximum of four times. Thus, in the function *CalculateTwoSimilarity*(s1, s2) we add two statements "**while** k<4 and s1.length>5 and s2.length>5 **do**" and "**if** sub.length<=4".

**Algorithm 2** *CalculateSimilarly*

```
Input: a set of reviews s1, s2, ..., si;
Output: the array similarity[i] denoting between si
and sj, where 0≤j<i.
for each si,
    for each sj and 0≤j<i,
        If s1==s2 then //is similar
            similarity[i]=1.0; //is similar.
            continue;
        else if (similarity[j]>ε) then
        continue; else
          similarity[i] ← CalculateTwoSimilarity(s1, s2);
        end if
    end for
end for
return similarity;

float CalculateTwoSimilarity(s1, s2)
k ← 0, f ← 0, len=s1.length;
while k<4 and s1.length>5 and s2.length>5
        do sub ← LCS(s1,s2);
        if sub.length<=4 then break; s1
            ← s1.Replace(sub2, ""); s2 ←
            s2.Replace(sub2, "")
             f1 ← (float)sub.Length /len;
             f ← f+f1;
             k ← k + 1;
         end if
end while
return f;
```

2) Review Relevancy Rate

Often the review has nothing to do with the product itself, such as an advertisement, or a connection, or irrelevant material pre-prepared. We need to analyze the relationship between the review and the subject of the product in order to detect this form of review. The review relevancy rate refers to the relevance between the content of the review and the subject of the product. To promote the purchase of the customer, each product has a particular topic to define its characteristics, such as the product model, feature, and range of the application. The review relevant rate is defined as follows:

$$RSS = e^{\langle |w(s) \cap w(r)| / w(s) \rangle} - 1$$

where W(s) is the set of all segmented words of the product's topic, and W(r) is the set of all segmented words of a review. The higher review relevancy rates a review has, the more plausible the review.

We use the word segmentation method to obtain the relevance between the subject and the analysis of the product. The method of obtaining relevance is shown in Fig.1. From Fig.1, we first look for the subject of the item and get some word segmentations for this topic. To explain the kind of feedback, a few word segmentations are then planned. For example, the word "phone" segmentation is for reviews of mobile phones, and "beer" for those reviews of beer. Finally, with each analysis, we create a set of word segmentations for the product and a set of word segmentations. We can find the relevance between the subject and the product review by comparing two sets of word segmentations.

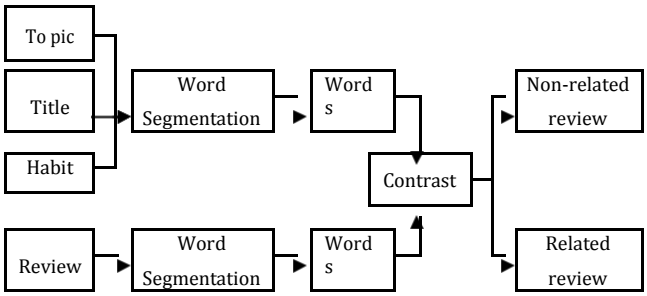


**Fig -1**: The process of dealing with the relevancy between the review and the topic of the product.

3) Burst Reviews with IP address

Burst reviews apply to when a user/customer has written a large number of reviews for various items within a short period of time. This can also be used if a large number of reviews are written for the same product from the same IP address within a short period of time. We define burst reviews as follows:

$$Burst(u,t) = \begin{cases} 0 & t < \beta \\ 1 - \dfrac{N(u,t)}{N(u)} & t \geq \beta \end{cases}$$

Where β is the time coefficient, N($u$,$t$) denotes the numbers of reviews written by a user/IP $u$ within $t$, and N($u$)denotes the total number of reviews from customer $u$ .

4) Bias rate

Multiple reviews on a product/brand from the same client cannot be reliable. The first review of a product/brand by the client does not represent the actual experience of the product, and the second review often represents the true experience of the product/brand by the customer. However, if 3 or more reviews have been written by a customer for the same product/brand, such reviews are likely to contain product bias. Thus, we define the bias rate of the customer u for as follows:

$$BR(u,r) = \begin{cases} 0.6 & c_p = 1 \\ 0.9 & c_p = 2 \\ 0.1 & c_p \geq 3 \end{cases}$$

Where $c_p$ denotes the number of reviews on same brand/product.

5) Deviation Rate:

Fair reviews are consistent with the quality of the item and do not deviate from the average of all reviews. We can determine if a review is fake according to this feature. Of course, we do not rule out a scenario in which the customer has purchased a low-quality product. The e-commerce website would allow the customer to refund his money or replace a new product with the issue product in that situation. So a reasonably fair review will still be offered by the customers. We define the deviation rate of a review r as follows:

$$RD(r) = \frac{|r_p - \overline{r_p}|}{5}$$

Where $r_p$ denotes the review rating of product $p$ given by $r$, and $\overline{r_p}$ is the average review rating of the product $p$

## 5. CONCLUSION

Fake reviews have some typical behavioral characteristics. This paper therefore constructs five methods of indicating Fake reviews and also algorithms to help achieve these functions. We hope to explore future work in various areas such as how length of the content affects reviews and also work on how the review is illustrated.

## REFERENCES

[1] Elmurngi, Elshrif, and Abdelouahed Gherbi. "An empirical study on detecting fake reviews using machine learning techniques." 2017 seventh international conference on innovative computing technology (INTECH). IEEE, 2017.

[2] Rout, Jitendra Kumar, et al. "Deceptive review detection using labeled and unlabeled data." Multimedia Tools and Applications 76.3 (2017): 3187-3211.

[3] Patel, Nidhi A., and Rakesh Patel. "A survey on fake review detection using machine learning techniques." 2018 4th International Conference on Computing Communication and Automation (ICCCA). IEEE, 2018.

[4] Chauhan, Shashank Kumar, et al. "Research on product review analysis and spam review detection." 2017 4th International Conference on Signal Processing and Integrated Networks (SPIN). IEEE, 2017.

[5] Wang, Xinyue, et al. "Identification of fake reviews using semantic and behavioral features." 2018 4th International Conference on Information Management (ICIM). IEEE, 2018.

[6] Liu, Pan, et al. "Identifying Indicators of Fake Reviews Based on Spammer's Behavior Features." 2017 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C). IEEE, 2017.

[7] Anderson, Eric T., and Duncan I. Simester. "Reviews without a purchase: Low ratings, loyal customers, and deception." Journal of Marketing Research 51.3 (2014): 249-269.

[8] Dwoskin, Elizabeth, and Craig Timberg. "How merchants use Facebook to flood Amazon with fake reviews." Washington Post (2018).

[9] Fei, Geli, et al. "Exploiting burstiness in reviews for review spammer detection." Icwsm 13 (2013): 175-184.