Global Journal of Computer Science and Technology: D
Neural & Artificial Intelligence
Volume 19 Issue 4 Version 1.0 Year 2019
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Cloud based Framework for Fake Review Detection

By Md. Towhidul Islam Robin
Stamford University

Abstract- Online reviews are one of the significant factors in a customer's purchase decision or to avail of any service. Online reviews give rise to the potential threats that fake reviewers may write a false review to artificially promote a product or defaming value of a service. Using Natural Language Processing, many methods have already been developed to detect fake reviews, especially reviews written in the English language. In this paper, I propose a novel framework where authenticity of a feedback will check through two perspectives. Firstly, the system checks whether the review is fake or not. Secondly, it also checks the authenticity of the reviewer. The outcome result accumulates in cloud storage for providing further business analytics.

Keywords: *NLP, SLM, language modeling, LIWC, anagram, lexical feature.*

GJCST-D Classification: *F.1.m*

Strictly as per the compliance and regulations of:

Cloud based Framework for Fake Review Detection

Md. Towhidul Islam Robin

Abstract- Online reviews are one of the significant factors in a customer's purchase decision or to avail of any service. Online reviews give rise to the potential threats that fake reviewers may write a false review to artificially promote a product or defaming value of a service. Using Natural Language Processing, many methods have already been developed to detect fake reviews, especially reviews written in the English language. In this paper, I propose a novel framework where authenticity of a feedback will check through two perspectives. Firstly, the system checks whether the review is fake or not. Secondly, it also checks the authenticity of the reviewer. The outcome result accumulates in cloud storage for providing further business analytics.

General Terms: natural language processing, machine learning, private cloud, cloud security, naïve byes, support vector machine.

Keywords: NLP, SLM, language modeling, LIWC, anagram, lexical feature.

I. Introduction

Online reviews generally generated for a variety of purposes. These reviews categorized into three groups, Untruthful Reviews, Reviews on Brands (comments only concerned with brand promotion), and Non-review (unrelated text or advertisements) [1]. There is a challenge to detect fake reviews because of the large verity of data and the quality level of data. Standard Machine Learning algorithms tend to inefficient because of a large number of unlabeled data. However, Fake review detection is inclined to opinion mining (find whether any opinion is positive or negative) but differs in terms of features selection. Lack of distinguishing features may outperform a robust classifier algorithm. It can also be associated with the reviewer behavior, for example, a fake review can be classified as genuine but, reviewer behavior can detect as suspicious. Therefore, features can be review centric, or features can be reviewer centric. Most common review centric features are a bag of words, LIWC (Linguistic Inquiry and Word Count), bag of words with POS (Part of Speech) tags, character and word-based lexical features, semantic features. As mentioned earlier, identifying forged reviewers can advance the accuracy of false review detection where for detecting fake reviewers most common features are the maximum number of reviews written by the reviewers.

Author: Department of Computer Science and Engineering Stamford University Bangladesh. e-mail: towhid.austcse@gmail.com

II. Literature Review

For identifying fake reviews Supervised, Unsupervised, and Semi-supervised methods have been used so far where most of the models based on supervised learning. Ott M [2] proposed and compared three different methods for identifying spam detection. For their study, they created a new dataset using Amazon Mechanical Turk. A group of people deliberately write 400 fake reviews with positive sentiment. Besides, 400 positive reviews collected from TripAdvisor. In a later work, they created same size dataset but balanced with negative comments. Their proposed model achieved 89.8% accuracy using SVM as a classifier. Another study performed by Jindal N [3] who summarized opinions from text. The result showed that characteristics of the aberrant behavior, which classified as spam. They collected 5.8 million reviews from Amazon and successfully identified fake reviews with a score of over 90%. One study by Hammad [4], first proposed review detection in Arabic language. Hammad also illustrated that their model could extend to multiple languages. A novel unsupervised learning Semantic Language Model first developed by Raymond [5]. Li [6] collected 6000 reviews from Epinions to construct a semi-supervised fake review classifier. Their model predicts the degree of untruthfulness through clustering. On the other hand, Mukharjee [7] showed that fake reviewers have different characteristics than genuine reviewers. They classified fake reviews by analyzing behavioral attributes using Yelp's real-life data.

III. Methodology

The above study observes the different researchers used different learner algorithms and performance metrics to evaluate their model.

a) Classifier

Support Vector Machine (SVM): SVM is a Linear model to map higher dimension features. For review centric features, it is needed to classify the review with different categories such as fake, genuine, biased, etc.

Naïve Byes: Probabilistic model to classify data and based on likelihood value driven from probabilistic scheming. Samples belong to a distinct class only after satisfying the threshold value.

Semantic Language Model (SLM): Unsupervised learning model to cluster data

b) Performance Metric

Area under the Curve (AUC): The region under ROC bend irregularly utilizes as a proportion of the nature of the arrangement models. An arbitrary classifier has under the turn of 0.5, while AUC for an ideal classifier is equivalent to 1. By and by, a large portion of the grouping models have an AUC somewhere in the range of 0.5 and 1.F-measure use for statistical analysis of binary classification.

Accuracy: Determines the number of correct predictions. It is the most natural presentation measure, and it is essentially a proportion of anticipated perceptions. If we have high precision, at that point, our model is ideal. Indeed, it is an extraordinary measure, yet just when you have symmetric datasets where estimations of false positive and false negatives are practically the same.

F1 Score: F1 Score is the weighted normal of Precision and Recall. Along these lines, this score considers both false positives and false negatives. Naturally, it isn't as straightforward as exactness.

IV. Proposed Cloud Model

For storing reviews for further analysis and better learning, I propose private cloud infrastructure because it requires data isolation and encrypted database. The private cloud also allows you to schedule updates and allows for direct access to your SQL database. This choice may require some contribution for inner IT. This choice can be accessible soon after buying into the administration. Integrity additionally offers the adaptability to go past our standard Cloud multi-occupant offering to have your private cloud arrangement that improves the security and confinement of your information. It is overseen by integrity, which means no licenses will require.

a) Cloud Security of Proposed Model

Private cloud security requires every one of the segments of a conventional resistance inside and out a methodology for ensuring strategic frameworks. Notwithstanding these accepted procedures, there are suggestions and provokes one of a kind to a private cloud that ought to consider. If it resolves that the information being put away in the private cloud is strategic, then further developed security systems might be required. It is an arrangement of activities, advancement, and security that should be carefully taken care of with the goal that one of these viewpoints are not ignored and effectively misused. The objective is for an association to build up a propelled security engineering structure that tends to every one of these suggestions.

A center's ability of virtualization is to extract the equipment from the product enabling various occasions of the product to imitate solitary equipment. Permeability into this virtualized registering framework is significant.

Lifecycle, the board of equipment parts, temperature controls, data security, stockpiling clusters, and system gadgets are altogether factors when building a versatile foundation. At every one of these layers, there is a need to settle on choices that will decide the accessibility and unwavering quality of the proposed cloud. In cloud executions, the edge of the system is re-imagined. An association's IT group should think outside about the container and accept that the whole Internet and each article interfacing with it is currently its border. Open system availability and interoperability with different mists generally come connected at the hip with the organization of another private cloud.

Data arrangement, security, and partition together help structure an information assurance methodology. When information is arranged, it very well may be isolated into zones and ensured at the degree of security merits.

In our model cloud executions, the edge of the system has redefined. Open system availability and interoperability with different mists generally come connected at the hip with the organization of another private cloud. Data arrangement, security, and partition together help structure an information assurance methodology. When information is arranged, it very well may be isolated into zones and appropriately ensured at the degree of security it merits.

Table 1: Comparison of performance, methods, and results of fake review detection

Method	Dataset	Features Used	Features	Metric	Score
SVM [2]	Amazon Mechanical Turk	Bigrams	Review Centric	Accuracy	89.6%
LR[3]	5.8 million review from Amazon website	Product characteristics	Review Centric	AUC	78%

NB [4]	Arabic reviews from tripvisr.com	LIWC	Review Centric	F-measure	.995
SLM[5]	Review from amazon.com	Lexical Feature	Review Centric	AUC	.998
NB [6]	6000 reviews from epinions.	LIWC	Review Centric	F-measure	0.63
SVM [7]	Behavioral Features	Behavioral Features	Reviewer Centric	Accuracy	86.1%

V. Result Analysis

Most of the datasets used for the previous studies created synthetically for which their model not efficient enough for the practical scenarios. Besides, no classifier is designed for Bangla fake review detection. Again, most of the study based on either review centric or either reviewer centric, not both. Therefore, a well written fake feedback may deceive such classifies. If review authenticity can check through a reviewer perspective, it may give better result. By analyzing the ratio of reviews from a particular vendor may help the user to become careful when availing services from them. It also helps the commercial organization to identify potential frauds who try to defame their reputation.

VI. Proposed Framework

In my proposed system, users have to give input to the system, including reviewer information. Features will extract for both review and reviewers and classify as fake whether the content is fake or the reviewer profile is not genuine. Store the result, including primary input into the cloud. After analyzing cloud data, the system can provide various business analytics.

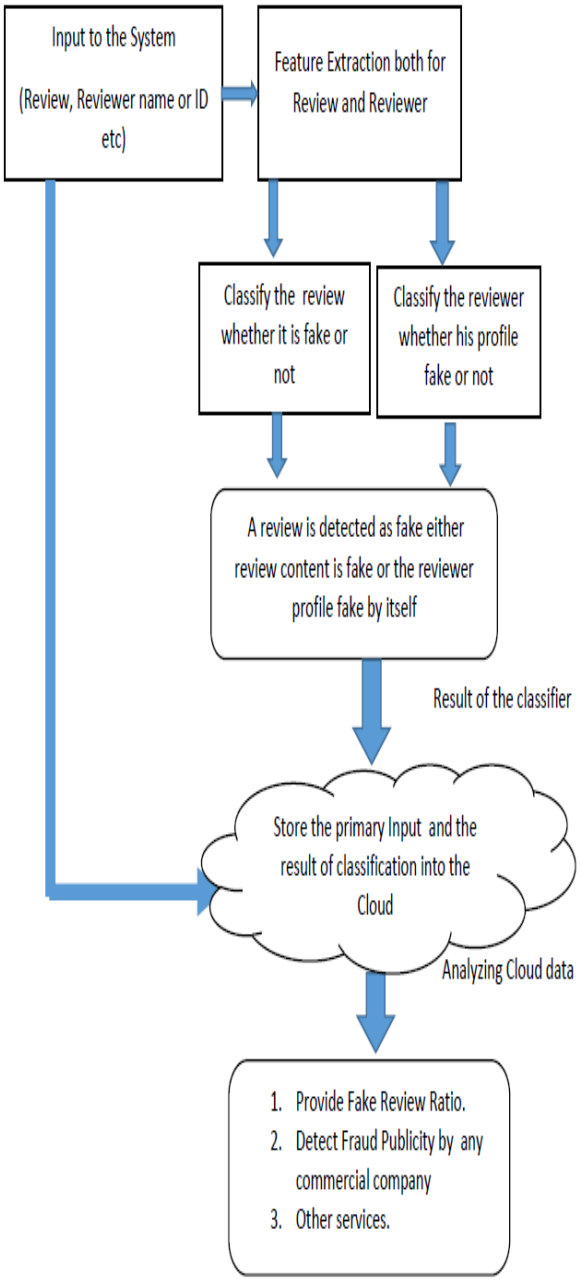

Figure 1: Conceptual block diagram of proposed fake review detection System

VII. Conclusion

Fake review detection has a significant impact on consumer behavior and purchasing decisions. To date, there is no cloud-based review detector exists, which can affect the decision of a potential consumer. Although the proposed system is just a prototype, many practical issues may arise when it will implement in real-world scenario.

References Références Referencias

1. Dixit S, Agrawal AJ (2013) Survey on review spam detection. Int J Comput Commun Technol ISSN (PRINT) 4:0975–7449.
2. Ott M, Choi Y, Cardie C, Hancock JT (2011) Finding deceptive opinion spam by any stretch of the imagination. In Proceedings of the 49th Annual Meeting of the Association for Computational Linguistics: Human Language Technologies-Volume 1 (pp. 309–319). Association for Computational Linguistics..
3. Jindal N, Liu B (2008) Opinion spam and analysis. In: Proceedings of the 2008 International Conference on Web Search and Data Mining (pp. 219–230). ACM, Stanford, CA Tavel, P. 2007 Modeling and Simulation Design. AK Peters Ltd.
4. Hammad ASA (2013) An Approach for Detecting Spam in Arabic Opinion Reviews. Doctoral dissertation, Islamic University of Gaza Forman, G. 2003. An extensive empirical study of feature selection metrics for text classification. J. Mach. Learn. Res. 3 (Mar. 2003), 1289-1305.
5. Lau RY, Liao SY, Kwok RCW, Xu K, Xia Y, Li Y (2011) Text mining and probabilistic language modeling for online review spam detecting. ACM Trans Manage Inf Syst 2(4):1–30.
6. Lau RY, Liao SY, Kwok RCW, Xu K, Xia Y, Li Y (2011) Text mining and probabilistic language modeling for online review spam detecting. ACM Trans Manage Inf Syst 2(4):1–30.