

# Spam Review Detection of product reviews using machine learning techniques

<sup>1</sup>Ms.M.P.Geetha, <sup>2</sup>M.Narmadha, <sup>3</sup>S.Surya, <sup>4</sup>K.Tamilselvan

<sup>1</sup>Assistant Professor ,Sri Ramakrishna institute of technology,Coimbatore, Tamil Nadu

<sup>2</sup>Student, Sri Ramakrishna institute of technology,Coimbatore, Tamil Nadu

<sup>3</sup>Student,Sri Ramakrishna institute of technology,Coimbatore, Tamil Nadu

<sup>4</sup>Student, Sri Ramakrishna institute of technology,Coimbatore, Tamil Nadu

Submitted: 05-05-2022

Revised: 10-05-2022

Accepted: 13-05-2022

**ABSTRACT:**Machine Learning is one of the fastest growing research study area, which allows customer to make better-informed buy selections appropriate recognizing and analysis of reviews from the internet and social media. In lots of on-line sites, there are choices for publishing reviews, and therefore producing scopes for fake paid reviews or untruthful reviews. As purchasers can't ask about an item or assess previously purchasing from on-line, they check out reviews and after that choose to purchase some products. Although they looking for reviews throughout various sites, they might not have the ability to determine whether it is a spam review or not. Some business with their Social Media Optimization group include some great reviews by themselves in purchase to make the item popular. So the business will provide fake great review for various items produced by their very own business. So the individual will unable to discover whether the review is true or not . Recently, the spam review detection issue has acquired a lot interest from communities and scientists, however still they have to carry out experiments on real-world massive review datasets. This can help to reviews the effect of extensive opinion spam in on-line reviews. Bulk of present research study has focused on machine learning techniques, which need identified information - an insufficiency when it concerns online reviews. Amazon.com on-line reviews text information is utilized for categorizing the item reviews. Lots of traditional machine learning algorithms have been executed to categorize the reviews .However still there's range to enhance the precision. In order to achieve betterprecision Naïve Bayes formula is to be executed to categorize the reviews as spam and authentic reviews.

**KEYWORDS:**Fake reviews ,NLP(Natural Language Processing), Machine Learning, Machine Learning, Word Embedding , CountVectorizer

## I. INTRODUCTION

The Internet has become the part of our day to day life. By the true blessings of the internet, people don't need to go out from their the home of purchase anything. Nowadays buying items from on-line has become a normal thing as many people don't have time to wait in a line to pay. However everything has its advantages and disadvantages and on-line buying has its own disadvantages. As customers can't ask about a product or assess previously purchasing from on-line, they check out reviews and after that choose to purchase something. To improve the service and products - suppliers, sellers and provider gather client feedback through review.Positive. reviews can result in notable profit or prestige for businesses or individuals. This gives incentives for "Opinion Spamming". Spammers sponsor deceptive reviews to promote products or devalue services .. There are generally two types of spam reviews. The first type consists of those that intentionally mislead readers or computerized opinion mining systems which provide undeserving positive opinions to some target products in order to promote them The second type consists of non-reviews opinion about product. However, reviews that contain negative feedback as the true picture of a customer view cannot be classified as spam. . An individual review refers to a review written by an individual or customer for an item or a service based upon her experience as a customer of the reviewed item. Prominent resources for customer reviews are ecommerce websites like Amazon.com . Ecommerce websites frequently have customer reviews for products and vendors individually.. Popular sources for consumer reviews are e-commerce sites like Amazon .Therefore online reviews are valuable source of information about customer opinions Fake or spam review refers to

any unsolicited and irrelevant information about the product or service. Spammer writes fake reviews about the competitors' product and promotes own products. The reviews written by spammers are known as fake reviews or spam reviews. Thus fake reviews detection has become critical issue for customers to make better decision on products trustworthy as well as the vendors to make their purchase

## II. LITERATURE SURVEY

In paper [1] Spam crusades seen in widely known product investigate websites (e.g., amazon.com. com) drawn in expanding factor to consider beginning similarly profession likewise the academic community, gathering wired banners is utilized to cooperatively make challenging audits for some goal goad reduces. The goal is to manage seen notoriety of the goals for their ultimate advantages. they find disjoint collections linked directly and concrete ideal the social nearness betrayer e.g., appraising associated merchandises and stating related ideas in small duration.

In paper[2] trade views regarding different approaches adjusted for spotting fakereviews and viewpoint spammers. The remainder of the paper talks about regarding the kinds of review spam and precision degree accomplished utilizing innovation. Type-I Un-honest reviews - the review composed are not based upon authentic experiences of customers of utilizing the services or products. The reviews published are categorized into 2 -hyper spam (include undeserving favorable viewpoints regarding some target entities in purchase to advertise the entities) and defaming spam (contains incorrect unfavorable viewpoints regarding other entities in purchase to damages their online reputations). Type-II Reviews on brand name only-remarks just on the brand names or the producers of the items. Some might be authentic, however are thought about as spam as they are not targeted at particular items. Type-III Non- Review - it's not an evaluation, however has ads and various other unimportant review including no viewpoints (e.g., concerns, responses, and arbitrary text). A spammer might work separately, or intentionally or unconsciously work as a participant of a team.

In paper[3] Reviews spam discovery has obtained considerable interest in both company and academic community because of the prospective effect fakereview can carry customer habits and buying choices. This study covers artificial intelligence methods and methods that have been suggested for the discovery of on-line spam review. Monitored discovering is one of the most regular

artificial intelligence method for carrying out reviews spam detection; nevertheless, acquiring identified review for educating is challenging and hands-on recognition of fakereview has bad precision. This has resulted in lots of experiments utilizing artificial or little datasets. Functions drawn out from reviews text (e.g., bag of words, POS tags) are frequently utilized to educate spam discovery classifiers. An option method is to essence functions relates to the metadata of the reviews, or functions connected with the habits of individuals that compose the review. Disparities in efficiency of classifiers on various datasets might suggest that reviews spam discovery might take advantage of extra go across domain name experiments to assist establish more durable classifiers. Several experiments have revealed that integrating several kinds of functions can lead to greater classifier efficiency compared to utilizing any type of solitary kind of function.

In paper[4], They have talked about various functions thoroughly like linguistic functions, behavior and relational functions. They have likewise contrasted various methods to determine fakereview and talked about significant difficulties of fakereviews discovery. Utilizing various category formulas like logistic regression, k-nearest next-door neighbor, arbitrary woodland, naive bayes and assistance vector device, the review are categorized as fake and authentic review. They either utilize publically offered dataset or produce very own dataset.

In paper [5] The paper demonstrates that support vector machine (SVM) outflank compared to the different provided techniques for study spam recognition. Determined relapse classifier furthermore provides fantastic exactness in study spam recognition. All the same, when the plan of preparing info is bit, a Naive Bayes classifier might be more appropriate since SVMs should use big plan of info to produce an incredible classifier. More future work is needed on additional improving the implementation of the Reviews spam exploration. There's an enormous require in business for such applications because of that each company have to understand how buyers really feel regarding their products and managements and those of their competitors. Unique kind of systems should be consolidated with a particular finish objective to dominate their private drawbacks and benefit from every others benefits, and update the Reviews spam exploration implementation. Right below They use the compound of study simply to differentiate spam reviews. The future program to enhance accuracy of every technique is to usage of various aspects, for instance, using evaluations of

studies, variety of fitting objections, time of inspected on, and so forth.

In paper[6], They determined the spams and spammers provide in a twitter dataset with the assistance of artificial intelligence formulas and NLP ideas. By evaluating the spam, the whole information regarding the spammer are accessed and showed, which consequently assists in identifying various other spams, spammers and their method of composing messages. We thought about 2 characteristic collections that includes web content and individual habits, the web content is identified with the assistance of typical web content similitude, optimal web content similitude, proportion of exclamation sentences and the proportion of initially individual pronouns. The individual habits is identified with the assistance of residential or commercial homes such as review composed and approximately unfavorable proportion provided. Therefore, production it an extremely efficient and precise spam discovery structure. The system that's suggested on this paper integrates arbitrary woodland formula, which is a monitored category formula with NLP ideas to classify and spot spam review amongst all current review on the TWITTER dataset. Automation of spam discovery utilizing a well-defined artificial intelligence structure can significantly help in reducing spam review that are deceptive or fake. Our system utilizes Artificial intelligence formulas consisting of Arbitrary woodland, Bayes Network, Naïve Bayes, K-nearest next-door neighbor and assistance vector device integrated with NLP methods to spot and eliminate spam and to determine the spammer.

In paper [7] They methods to fake reviews discovery are based upon information owned techniques that think about a number of functions connected with review, customers, and the network framework of the social media network that can be utilized to categorize review in regards to their reliability. Monitored classifiers remain in basic more efficient, and typically utilize reviews and reviewer-centric functions. Without supervision services remain in basic much less efficient, however have the benefit that they don't require identified datasets for educating. Monitored services, on the other hand, have shown their efficiency relative to as well little or review-site-dependent identified datasets, and relative to little subsets of functions. Most of monitored classifiers to deal with the provide of viewpoint spam discovery are based upon Naive Bayes or support Vector machine (SVM). To execute the classifier, the Python programs language was utilized, as it's utilized by a big neighborhood of designers,

therefore providing a large establish of devices and collections for various objectives. Unbalanced information stands for among the significant problems that need to be tackled when carrying out monitored category. In the educating stage, if the unbalancing of educating information is ruled out, there's the danger that the classifier learns primarily from the biggest course of identified information for that reason overlooking the minority course. The oversampling technique is thought about, it is composed in augmenting the minority course to stabilize it with the biggest one.

In [8] paper examine checks out the literary works study based upon reviews spam discovery methods, which includes review's function design techniques. The functions are drawn out and dispersed in behalf of reviews, customer, and item info within its file as discussed over in tables. The approach area explains the preprocessing, tokenization, change and function choice thoroughly. There are different soft computer methods which are discussed correctly, and can be utilized in the reviews spam discovery for offering much far better services. Additionally, a comprehensive examine can be done on discovering the soft computer formulas and executing them on actual atmosphere. The enhanced outcomes are assessed for reality issues where datasets can likewise be discussed and dealt with, simply to offer precise outcomes. The stage includes building of complication matrix where precision, remember worth, accuracy and F ratings are determined to discover the efficiency of the system, and are given up 4 worths TP (Real positive), TN (Real negative), FP (Incorrect favorable) and FN (Incorrect unfavorable). The precision prices can be compared to the various other methods for much far better evaluations of outcomes.

In paper [9] Before purchasing an item, people typically notify themselves by reviewing on-line review. To create more revenue vendors frequently attempt to fake individual experience. As clients are being tricked by doing this, acknowledging and eliminating fakereview is of fantastic significance. Their paper review spam discovery techniques, based upon artificial intelligence, and provides their summary and outcomes. The paper a short summary of spam discovery techniques released throughout the last years existed. It was revealed that utilizing various datasets yields incredibly various outcomes. Furthermore, the absence of an appropriate gold basic dataset was acknowledged as a significant issue in spam discovery. Although linguistic methods control in variety of research study

documents, spammer discovery methods have revealed guaranteeing outcomes. For that reason, future research study ought to be concentrated on integrating content-based and reviewer-based techniques for accomplishing the very best outcomes.

In [10] paper, On-line studies on products and managements can be useful for clients, nevertheless they ought to be protected from manage. Up previously, many evaluations have no know dissecting online studies from a solitary facilitating website. How may one affect information from various investigate facilitating locations? This is the important query in our work. Appropriately, develop an accurate viewpoint to union, take a look at, and reviews audits from different facilitating locations. No know accommodations studies and use greater than 15million audits from more than 3.5million customers spreading out over 3 visible take a trip locations.

### III. PROPOSED METHODS

This section explains about the datasets ,preprocessing ,Feature selection methods and classifiers used in our experimental setup.

**Dataset** We used a dataset containing reviews could be for product or service like hotel reviews. Dataset (2600 reviews) were collected to detect whether the reviews are spam or ham

**Data pre-processing:** In next step, data is processed as per the requirements .The raw data collected from amazon dataset .Data pre-processing is applied like punctuation marks removal, stemming, stop word removal etc. In punctuation marks removal, the whole text is divided into sentences, phrases or paragraphs. In the stemming process, stem will be created from every word in dataset. In stop word removal phase, frequently used group of words like determiners, articles and preposition will be detected and removed. After removing these words, only important words will be retained for the next step

#### Using Count Vectorizer to Extracting Features from Text:

**Count Vectorizer** is a great tool provided by the scikit-learn library in Python. It is used to transform a given text into a vector on the basis of the frequency (count) of each word that occurs in the entire text. This is helpful when we have multiple such texts, and wish to convert each word in each text into vectors (for using in further text analysis).

#### Classification-Naive Bayes algorithm:

**Bernoulli Model** A document is generated through a succession of VI Bernoulli experiments, one for each word  $w_t$  in the vocabulary  $V$ , according to the multi-variate Bernoulli event model. The result of each trial determines whether the matching word will appear in the document at least once. Thus a document  $d_i$  can be represented as a binary feature vector of length  $I \times V$ , indicates whether word  $w_t$  occurs at least once in  $d_i$ . The Naive Bayes assumption holds that the  $V$  trials are unrelated to one another. We can determine the chance of a document given a class from the probabilities of the words given the class using the Naive Bayes assumption.

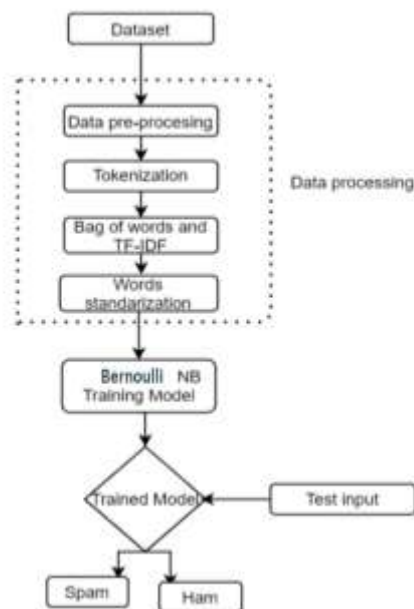


Fig1 Bernoulli Model

**Multinomial Model** The program guesses the tag of a text, such as an email or a newspaper story, using the Bayes theorem. It evaluates each tag's likelihood for a given sample and returns the tag with the highest chance. The multinomial event model proposes that a document  $d_i$  of length  $d_i$  is formed by a series of word events, each of which produces a word from the vocabulary  $V$  as the result. According to McCallum and Nigam (1998), the document length distribution  $P(I)$  is unaffected by the class. Thus a document  $d_i$  can be represented as a vector of length  $I \times V$ , number of times word  $w_t$  occurs in  $d_i$ . Thus a document  $d_i$  can be represented as a vector of length  $I \times V$ , number of times word  $w_t$  occurs in  $d_i$ . The Naive Bayes assumption states that the  $d_i$  trials are unrelated to one another.. The probability of the reviews, that contains words  $(w_1, w_2, w_3, \dots)$  to be spam is proportional to the probability to get the spam



multiplied by a product of probabilities for every word in the reviews text to belong to a spam reviews.

For every word in the reviews, we calculate a probability of it to be found in spam. In our context:

- $P_{spam}$  — the part of spam reviews in our dataset
- $P_{wi\_spam}$  — the probability of a word to be found in the spam reviews. By the same logic we define:
- $P_{not\_spam}$  — the part of non-spam reviews in the dataset
- $P_{wi\_non\_spam}$  — the probability of a word to be found in the non-spam reviews

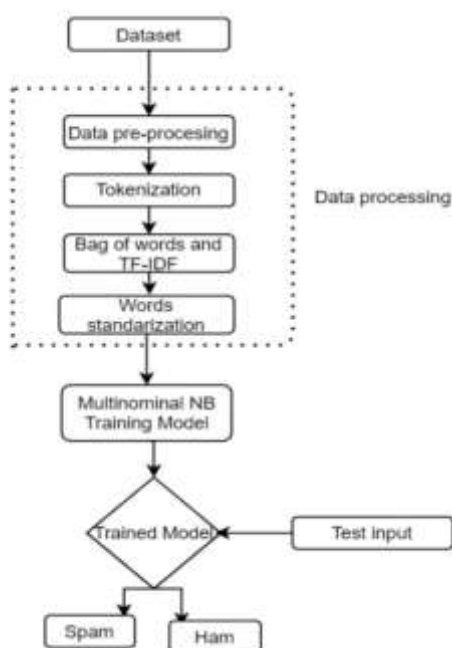


Fig 2 Multinomial model

#### IV. RESULTS AND DISCUSSION

This work proposes a system to detect spam reviews that is used to detecting the spam reviews that are written in online websites. researchers have been working to find out the best classifiers. So there is a need to develop more robust classifiers to filter spam reviews. Naïve bayes a more appropriate classifier is to be applied over the Amazon online text review data to classify the reviews.

Name	Reviews	Training accuracy	Testing accuracy
Bernoulli (Naïve Bayes)	2400	95%	89%
Multinomial (Naïve Bayes)	2400	97%	92%

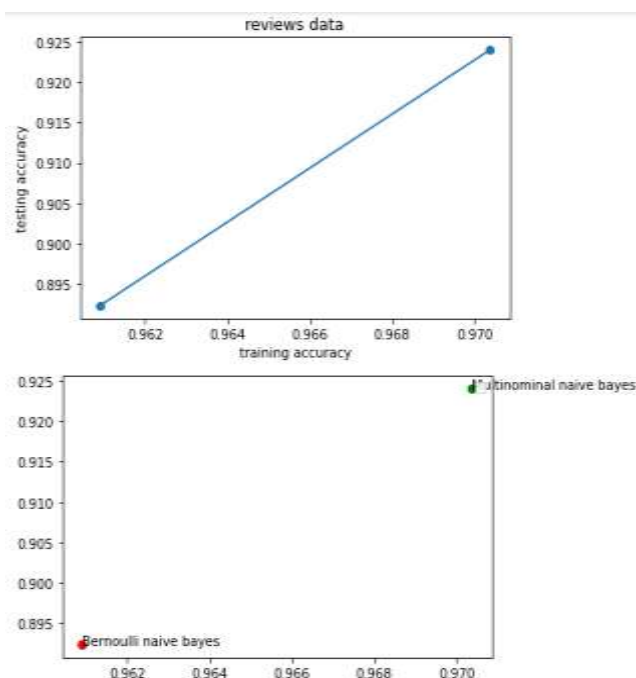


Fig3 Accuracy Result of Bernoulli and Multinomial Algorithm

#### V. CONCLUSION

In this project performed experiments with two different statistical event models (a multivariate Bernoulli model and a multinomial model) for a Naive Bayes text classifier. The main conclusion we can draw from these studies is that the multinomial model is less biased towards one class and can achieve higher accuracy than the multivariate Bernoulli model, especially when frequency information is taken into the feature selection process.

#### REFERENCES

- [1]. Crawford, Michael, et al. "Survey of review spam detection using machine learning techniques." *Journal Of Big Data* 2.1 (2015): 1-24.
- [2]. Hussain, Naveed & Mirza, Hamid & Rasool, Ghulam & Hussain, Ibrar & Kaleem,

- Mohammad. Spam Review Detection Techniques: A Systematic Literature Review. Applied Sciences. 9. 987. 10.3390/app9050987, 2019
- [3]. Hussain, Naveed & Mirza, Hamid & Hussain, Ibrar & Iqbal, Faiza & Memon, Imran. Spam Review Detection Using the Linguistic and Spammer Behavioral Methods. IEEE Access. PP. 1-1. 10.1109/ACCESS.2020.2979226, 2020
- [4]. Yuejun Li, Xiao Feng, ShuwuZhang, "Detecting Fake Reviews Utilizing Semantic and Emotion Model" IEEE, 2021
- [5]. KolliShivagangadhar, Sagar H, SohanSathyan, Vanipriya C.H, "Fraud Detection in Online Reviews using Machine Learning Techniques." IJCIER-2020.
- [6]. SushantKokate, Bharat Tidke, "Fake Review and Brand Spam Detection using J48 Classifier." IJCSIT, 2015.
- [7]. Amir Karam, Bin Zhou, "Online Review Spam Detection by New Linguistic Features." UNIVERSITY OF MARYLAND BALTIMORE COUNTY, 2019
- [8]. Kolhe N.M., Joshi M.M.Jadhav A.B., Abhang P.D., "Fake Reviewer Groups" Detection System." IOSR-JCE, 2019.
- [9]. Arjun Mukherjee, Vivek Venkataraman, Bing Liu, NatalieGlance, "Fake Review Detection: Classification and Analysis of Real and Pseudo-Reviews." CS'13
- [10]. DayaMevada, Viraj Daxini, "An opinion spam analyzer for product Reviews using supervised machine Learning method", Journal of Information, Knowledge And Research In Computer Engineering, 2015.