Fake review detection on Google Play Store apps

A DISSERTATION

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS

FOR THE AWARD OF DEGREE

OF

MASTER OF TECHNOLOGY

IN

COMPUTER SCIENCE AND ENGINEERING

Submitted By

ABHISHEK R AGRAWAL (2K19/CSE/02)

Under the supervision of

Mrs. Minni Jain

(Assistant Professor)

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

DELHI TECHNOLOGICAL UNIVERSITY

(Formerly Delhi College of Engineering)

Bawana Road, Delhi-110042

JUNE, 2021

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

DELHI TECHNOLOGICAL UNIVERSITY

(Formerly Delhi College of Engineering)

Bawana Road, Delhi-110042

DECLARATION

I, Abhishek R Agrawal, Roll No. 2K19/CSE/02 student of M.Tech (Computer Science & Engineering), hereby declare that the Project Dissertation titled "**Fake review detection on Google Play Store apps**" which is submitted by me to the Department of Computer Science & Engineering, Delhi Technological University, Delhi. Report of the Major II which is being submitted to Delhi Technological University, Delhi, in partial fulfillment for the requirement of the award of degree of Master of Technology, is original and not copied from any source without proper citation. This work has not previously formed the basis for the award of any Degree, Diploma Associate ship, Fellowship or other similar title or recognition.

Abhishek

Place: DTU, Delhi — Abhishek R Agrawal

Date: 28-06-2021 — (2K19/CSE/02)

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

DELHI TECHNOLOGICAL UNIVERSITY

(Formerly Delhi College Of engineering)

Bawana Road, Delhi-110042

CERTIFICATE

I, hereby certify that the Project Dissertation titled *"**Fake review detection on Google Play Store apps**"* which is submitted by Abhishek R Agrawal, Roll No. 2K19/CSE/02, Department of computer Science & Engineering, Delhi Technological University, Delhi in partial fulfillment for the requirement of the award of degree of Master of Technology (Computer Science and Engineering) is a record of a project work carried out by the student under my supervision. To the best of my knowledge this work has not been submitted in part or full for any Degree or Diploma to this University or elsewhere.

Minni Jain

Place: Delhi **Mrs. Minni Jain**

Date: 28/06/2021 **SUPERVISOR**

Assistant Professor

Dept. of Computer Science and Engineering

Delhi Technological University, Delhi

ACKNOWLEDGEMENT

I am most thankful to my family for constantly encouraging me and giving me unconditional support while pursuing this research.

I am extremely grateful to **Mrs. Minni Jain** Assistant Professor, Department of Computer Science Engineering, Delhi Technological University, Delhi for providing invaluable guidance and being a constant source of inspiration throughout my research. I will always be indebted to his for the extensive support and encouragement he provided.

I also convey my heartfelt gratitude to all the research scholars of the web Research Group at Delhi Technological University, for their valuable suggestions and helpful discussions throughout the course of this research work.

Abhishek R Agrawal

Roll.No. 2K19/CSE/02

ABSTRACT

There are millions of apps in google play store all of which allows the users to write reviews about the usage, quality, performance, issues on the particular app. These reviews help new users to get a brief insight into the app and help developers to improve constantly. Positive reviews help build the reputation of the app while negative reviews degrade the same. Now a days there are a lot of fake reviews posted on the google play store both of positive and negative nature which gets developers into trouble and the users not to see the reality about these apps. Fake review detection helps weed out these fake reviews and let the users and developers view an actual image of the app as it is. Previous methods of fake review detection for app store reviews lack on taking into consideration the important features necessary for high accuracy. In this paper we propose a supervised model for fake review detection of google play store apps which uses both review centric features and reviewer centric features and based on these features we build a naïve bayes classifier which successfully detects fake reviews on a given dataset of app reviews.

Keywords: Fake Review, Supervised model, Review Centric Features, Reviewer Centric Features, Naïve bayes Classifier.

CONTENTS

List of Figures

List of Tables

List of Symbols, Abbreviations

1. NB – Naïve Bayes
2. POS – Part Of Speech
3. RD - Rating Deviation
4. NR - Number of Reviews
5. CS – Content Similarity
6. RBu – Reviewer Burstness
7. EXR – Extreme Rating
8. BuA – Bursty Activity
9. CSBu – Content Similiraty in Burst

CHAPTER 1

INTRODUCTION

1.1 Overview

Due to development in technology, the quantity of individuals using cell applications in the course of the world, no matter the platforms, has been rising swiftly. This increase in mobile use has conjointly accelerated the mobile software package marketplace improvement. Figure 1.1 indicates the quantity of global phone customers from 2014 to 2020 [1]. It will be cited that phone users are increasing linearly each twelve months. This therefore, creates a imply further mobile applications to be developed for varied functions.

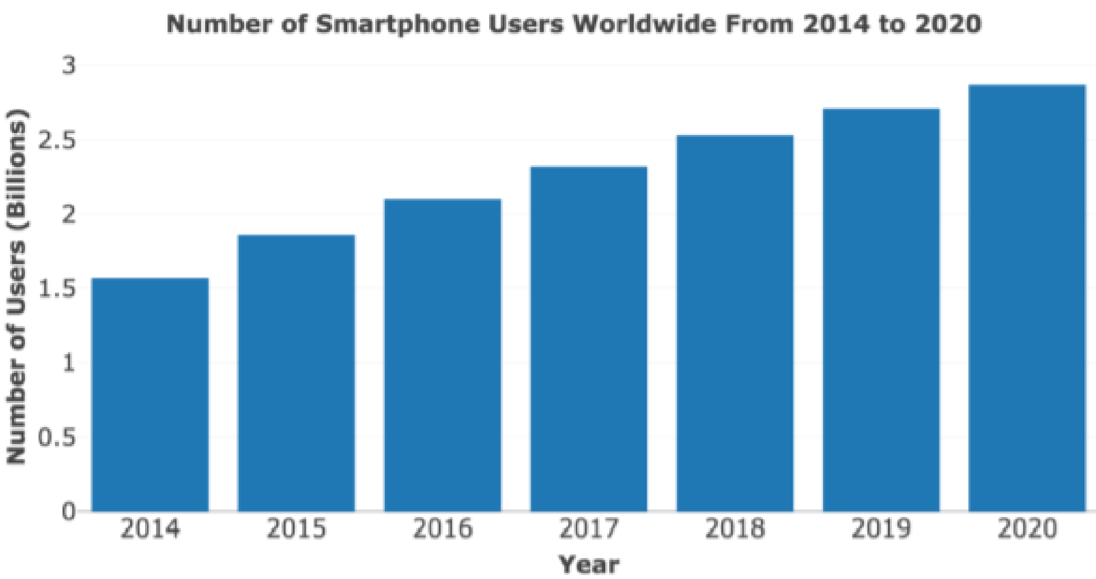

Fig 1.1- Year wise Number of smartphone users from 2014-2020

In Google play store, clients can rate downloaded applications and rate them on a scale from one to five stars and compose an audit message. Consequently, they can communicate fulfillment or disappointment, report messes with, or suggest new choices [2][3]. practically like diverse on-line stores, prior to downloading an application, clients regularly check through the audits. Examination found that appraisals and audits correspond with deals and download positions [4][5][6]. Stable fluctuated appraisals result in higher downloads and marketing projections.

As a viewpoint impact, an unlawful commercial center for imagine application audits has arisen, with the objective to supply benefits that work with application merchants work on their evaluations and positioning in application stores. in sync with application store administrators, in customary application surveys, genuine clients are theorized to be set off by their fulfillment or discontentedness of exploitation the application to supply criticism. imagine analysts, in any case, get compensated or similarly remunerated to submit surveys. they could or may not be genuine clients of the application. Their survey may or probably won't be right and intelligent their viewpoint. As of late, Google featured the adverse consequences of artificial surveys in a government official proclamation and explicitly requests that designers not buy and clients to not agree to installments to give counterfeit audits [7]. Indeed, even legislative rivalry specialists began making moves against companies exploitation imagine audits to embellish their applications. For example, the Canadian media transmission provider Bell was punished $1.25 million [8] for faking positive surveys to their applications. The other way around, the CNN application was tortured by a great many negative phony surveys to diminish its rating and positioning at spans the Apple App Store [9].

Reviews and ratings are manipulating teams in on line marketplaces worldwide and records show that ninety % of consumers create their call to buy for or not to shop for products/services based on on-line opinions.

1.2 Problem Statement

Despite efforts to contend with the matter throughout the last decade, Google Play Store continues to be troubled with pretend evaluations. Their persistence are going to be chalked the maximum amount because the West nature of enormously new mobile platforms, but what’s clear is that every firms have didn't offer you a solution.

Clients who give criticism through application keep investigates are doled out all over inside the worldwide, and it' miles astoundingly plausible that the custom during which clients are unmoving effects the strategy they supply remarks. Nonetheless, this advancement has not been concentrated up to now by abuse the code designing exploration local area.

In pretend review detection, each review wishes to be analyzed alright with the intention to differentiate them between everyday or junk reviews. Manual human judgement has been a fashion of police work opinion spams previous the introduction of sophisticated automatic strategies. In manual human judgement, the matter arises as a result of folks are less effective in distinctive between traditional opinions and spam opinion thanks to the presence of emotions and sentiments [10]. Moreover, spammers maintain evolving their spamming techniques if you wish to forestall detection so they hold to disrupt agencies aboard the way. The abundant opinions through the years makes it a job for the human eye for that reason there will be errors whereby spams can be wrong for everyday evaluations and vice versa. This will increase the considerations of the dependability and effectiveness of mistreatment human judgments in opinion spams detection.

Nonetheless, current studies advocate that there are many boundaries. For instance, those strategies used too several options that simultaneously, need intensive process time. to beat those barriers, a way was to lower the number of capabilities however doing therefore can scale back the spatiality of the datasets thereby allowing the trend of the knowledge to be envisioned effortlessly. Lowering the quantity of functions conjointly minimizes the model’s process coaching time for actual-global implementation that then will increase the detection performance. Nonetheless, doing away with too several functions will motivate an ineffective and unreliable prognostic version that's due to the shortage of ability of the version to properly distinguish between traditional and unsolicited mail critiques. Henceforth, this might assignment a decrease accuracy rate at intervals the predictive version for opinion spams detection. Given this example, it' way essential to stay in mind analyzing the functions so one can meet the expectations of the prognostic model. In precis, there's a necessity to conduct studies that appears for relevant however minimum functions and a dependable predictive version.

CHAPTER 2

LITERATURE REVIEW

2.1 Google Play store

Google Play store is a mobile application marketplace that hosts applications, games, books and films for android software package [11]. Developers and organizations broaden many android applications for cellular telephones, tablets and laptops. Figure 2.1 shows the logo of Google Play store.

Fig 2.1- Google Play Store Logo

Google Play become initially discharged in Gregorian calendar month 2008 to a lower place the decision golem Market. As Google's reliable app shop, it offers its customers a intensive vary of packages and digital media at the side of tune, magazines, books, movie, and TV. Currently, there are 2893806 android applications within the Google Play store [1]. Despite this, a number of the programs don't seem to be useful. Google Play store sporadically removes these sorts of programs from the market. Current data show that there are fourteen p.c of low-best apps that are eliminated from the store. Figure 2.2 demonstrates the range of android applications to be had in 2017 and they're supported the kinds of packages. Figure 2.2 initiatives three varieties of packages that embody all apps, low-nice apps and traditional apps. Current facts and traits to boot indicate that the quantity of applications has been increasing over the years. As a final result of this burgeoning of apps, it's necessary to conduct analysis at the Google Play reviews.

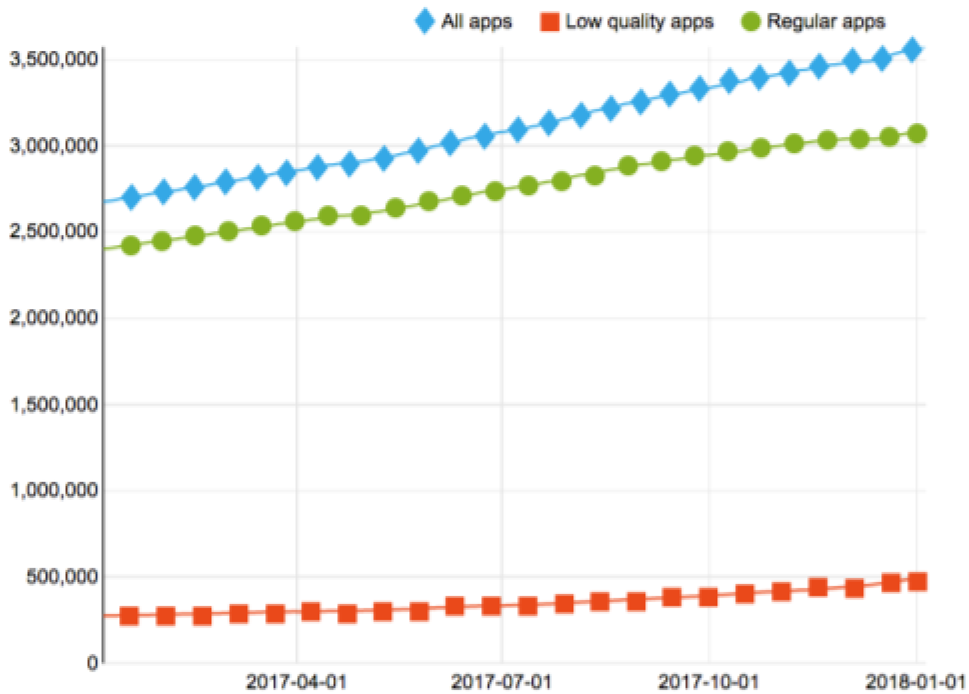

Fig 2.2- Year wise plot of number of apps on Google Play Store

2.2 Methods for fake reviewing

2.2.1 Sock Puppeting

"Sock puppets," are phoney debts created for the reason for inflating the amount of high-quality (or -- at intervals the case of a rival -- negative) reviews for a developer's product. Often, they're created by exploitation the developer themselves. typically those fake critiques are bought from third parties. "Sock puppet" interest isn't unnatural to app evaluations. identical behavior has been detected in remark threads and on social media platforms.

2.2.2 Astro Turfing

"Astroturfing" produce an influence of monumental grassroots support for a policy, person, or product, within which very little such guide exists. Like its football namesake, "AstroTurf," the fundamental measure refers to one thing artificial meant to seem natural.

Originally used as a political tactic, astroturfing is currently wide used on information superhighway as a fashion to bolster one's image via pretend comments, paid-for critiques, made-up claims, and testimonials. These "marketing" efforts typically incorporates the usage of blogs, message boards, and social media websites to construct artificial hype.

2.2.3 Crowd Turfing

Crowd turfing may be a combination of astroturfing associated crowdsourcing. Well, you may gift a fake message as real victimization an artificial target market by astroturfing, and you will get the assist of a actual target market by method of crowdsourcing. So, what will it counsel for those to come back back together? By crowd turfing, you could support an synthetic target market with a true target audience, making a fake message a great deal bigger smart than before. That’s why crowd turfing is a spanking new up to this point model of astroturfing. And like each new replace, it comes with a brand new feature, that's crowdsourcing.

2.2.4 Review Brushing

Review brushing refers to a pretend reviewing technique whereby the reviewer act as alternative true man or girl to down load and value the app. The individual whose identity is employed has no concept every one these items are dead on his/her behalf. This approach is specially used for generating fake reviews on product merchandising internet sites at the side of ‘Amazon’ wherever somebody orders a product on other individual’s traumatize and assessment the merchandise. The sufferer no longer having placed the order returns the product however the analysis stays.

2.3 Feature classification

There are two types of features we need to consider while designing a fake review detection system; Review centric and Reviewer centric features.

2.3.1 Review centric features

Review centrical capabilities are functions which could be created exploitation the statistics contained in a very single overview. Conversely, reviewer centric functions take a holistic take a glance in any respect of the opinions written by any specific writer, at the side of statistics regarding the distinctive author.

it's attainable to use multiple varieties of options from inside a given category, cherish bag-of-words with POS tags, proportion positive and negative reviews, lexical validity, lexical diversity and so forth

2.3.2 Reviewer centric features

Review centric capabilities are functions which could be created exploitation the statistics contained in a very single overview. Conversely, reviewer centric functions take a holistic take a glance in any respect of the opinions written by any specific writer, at the side of statistics regarding the distinctive author.

It's attainable to use multiple varieties of options from inside a given category, cherish bag-of-words with POS tags, proportion positive and negative reviews, lexical validity, lexical diversity and so forth

2.4 Naive Bayes Classifier

Naive bayes is one amongst the most common metric capacity unit algorithms that's frequently used for the aim of matter content category. It's a supervised mastering algorithm, that is based on Bayes theorem associate degreed used for determination class issues. Naïve Bayes classifier could be a probabilistic classifier supported Bayes' theorem, which assumes that every characteristic makes an unbiased and equal contribution to the target magnificence. NB classifier assumes that each feature is unbiased and will no longer interact with each different, specified each operate severally and equally contributes to the chance of a pattern to belong to a particular class. NB classifier is straightforward to place into impact and computationally speedy and performs nicely on giant datasets having excessive dimensionality. NB classifier is contributive for actual-time programs and isn't forever sensitive to noise. NB classifier strategies the education dataset to calculate the magnificence chances P(Yi) and also the conditional possibilities, that define the frequency of each feature value for a given magnificence fee divided with the help of the frequency of instances therewith elegance fee. NB classifier glorious performs once related to capabilities are eliminated thanks to the very fact correlated functions are often voted twice inside the version main to the emphasis of the importance of the related to features.

CHAPTER 3

RELATED WORK

Existing work, e.g., [12], [13], [14] has tended to the huge scope of surveys got by far reaching applications, their unstructured nature and going quality by proposing to precisely dissect the criticism with information preparing methods—lessening designers' and experts' work once examining the audits.

In 2017, SP.Rajamohana, Dr.K.Umamaheswari, M.Dharani, R.Vedackshya bestowed “Survey of review spam detection using machine learning techniques.” [15] focused lightweight on beguiling audits that are presented inside the web that an ever increasing number of effects organizations and clients. thereupon it's important to recognize and wipe out such false audits from on-line sites. This paper notable shows different systems utilized for valuate spam discovery and generally speaking execution measures had been analyzed.

In 2015, Daya L. Mevada, Prof.Viraj Daxini within their paper “An opinion spam analyzer for product Reviews using supervised machine Learning method.” [16] encouraged technique to look out fake assessment from Brobdingnagian amount of unstructured data has turned into a vital examination issue. This exploration proposes an assessment post office based mail analyzer that precisely arranges input matter substance records into each spontaneous mail or non-spam class. The projected doohickey can utilize framework learning directed technique.

In 2016, Miss. Rashmi Gomatesh Adike, Prof. Vivekanand Reddy [17] bestowed their views in the paper “Detection of Fake Review associate degreed complete Spam mistreatment data processing Technique”. This research proposes an action system to become checked out examination spammers of us that are trying to control the appraisals on certain items. Creator determine a mass lead strategies for rank analysts based at the endorsement that they need set up the spamming practices. They tried extended ways by participating in client assessment on an Amazon dataset that contains assessments of different association's product.

CHAPTER 4

METHODOLOGY

Our strategy partner endeavors to make a tough false evaluation recognition gadget through considering an assortment of we tend cost snared and acknowledged by mainstream researchers spam capacities associated with each action and commentator conduct. Concerning the application degree preparing, our form gets as enter an intense and fast of n surveys identifying with an application. Then, at that point, for each audit 'ri' we separate the essential records and data which fuses synopsis message, examination score, timestamp and commentator ID, that we first investigate all through a few fundamental spam markers. we will in general conjointly utilize burst test revelation as an integral investigation device to spot bursty time-frames and pinpoint "dubious" assessments, that we will in general then, at that point inspect all through 2 extra spam markers. In this way, our methodology thinks about all assessments of an item (no absence of insights), while looking extra into the chief high-peril ones. we will in general confirm the audit spam level by applying a direct weighted evaluating work [18] to the survey and framework a spam score limit to which we look at each audit's collected score. Subsequently, our procedure yields as imagine those studies whose rating surpasses the edge and genuine those surveys whose score doesn't surpass the edge. One investigation of the arranged approach might be seen in Fig.4.1.

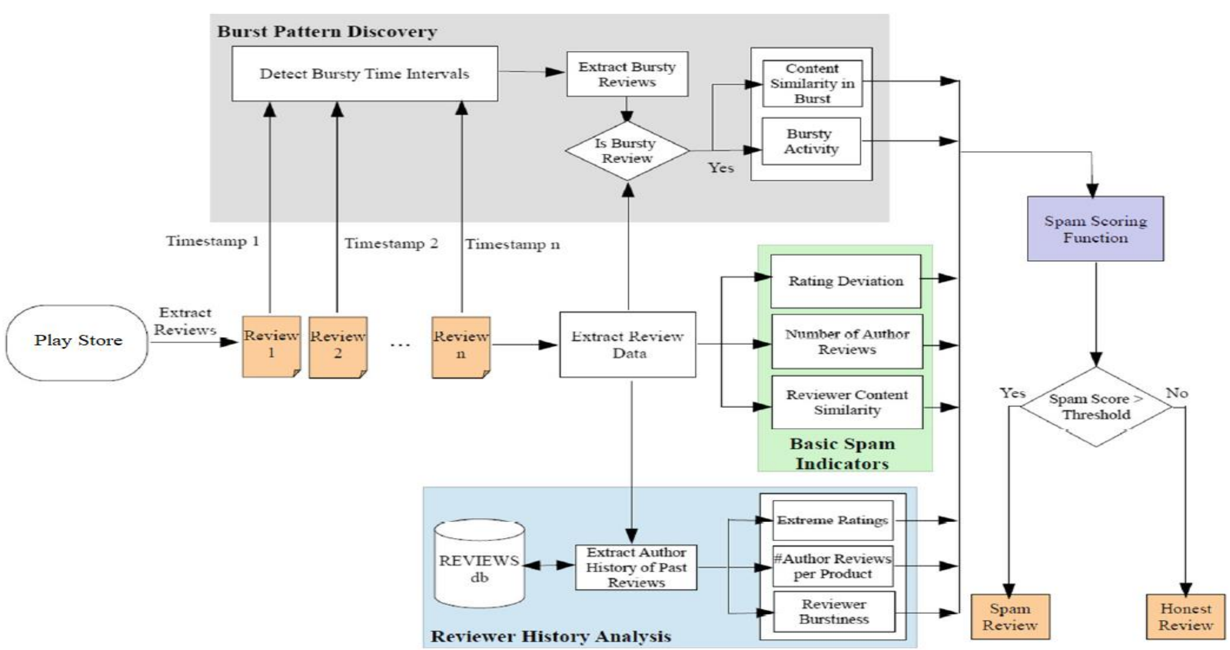

Figure 4.1- Method Workflow

4.1 Basic Spam Indicators

This segment presents and depicts the 3 fundamental fake pointers utilized in our model to identify validity in application audits.

4.1.1 Rating Deviation (RD)

An unsought audit can by and large objective at developing or bringing down partner application's customary position with the assistance of controlling its direction score toward a specific course and, along these lines, veers off from the infer. Thinking about $S_{mean}(p)$ because of the mean rating of an item p and normalizing in accordance with a five rating scale, the rating deviation score [0, 1] of an audit 'ri' is set to be

:
$$RD(r_i) = \frac{|r_{i,rt} - S_{mean}(p)|}{4} \quad (4.1)$$

4.1.2 Number of Reviews (NR)

It is a typical spammer practice to make some of feelings for the equivalent application for you to apply extra have a control on open audits and control the suggest rating. Normally, the unsought rating of an audit 'r_i' made by implies that of analyst $a(r_i)$ ought to also be blasted by the huge selection of evaluates the creator has contributed for a comparable application:

$$NR(a(r_i)) = |R_{a,j}| \quad (4.2)$$

4.1.3 Content Similarity (CS)

Counterfeit analysts typically reproduce a comparative measure text as writing unmistakable substance would conceivably show tedious. In this manner, we tend to can go over spammers through thinking about the overall substance material similitude in their assessments. As per this writing [19][20], we utilize the round work similitude for this reason. The substance material comparability rating [0, 1] of an analyst $a(r_i)$, ascribed to audit ri, is that the normal of the likenesses of each rundown r_j has a place with R_{aj}:

$$CS(a(r_i)) = Avg\left(\frac{\sum_{z=1}^{|R_{a,j}|} cosine(r_j, r_z)}{|R_{a,j}|}\right), \ j \neq z \quad (4.3)$$

4.2 Burst Pattern Detection

Spammers at times produce a huge amount of audits partner degree really respectably present moment for you to quick invalidate the consequences of and rule fair studies. Such over the top posting might result inside the appearance of unexpected can increment in an application's evaluating interest, making "explodes" or tops in certain time-frames. Our model consolidates a burst test recognition strategy, that has effectively been utilized with progress at stretches the past [21], as a procedure of narrowing down the most extreme dubious time terms and, eventually, the greatest without a doubt perilous surveys. while the creators of [21] exclusively contemplated these assessments, missing the alleviation of an item's viewpoints, we tend to make due with as evident immediately they need to not be the main genuine awareness of an identification model as spam furtherly may additionally exist outside of blasts likewise. Along these lines, we only test those assessments, just as their singular commentators, to also examination with two extra spam markers. Consequently, our methodology examines all scrutinizes of an item for the lifetime of excluded mail, perusing bigger totally those made in bursty time spans. The arrangement of rules for burst design revelation is given under.

Algorithm 1 Calculation to distinguish bursty time spans for an application related with

n surveys $R = \{r_1, \ldots, r_n\}$. Information sources are the comparing survey creation dates $T =$

$\{d_1, \ldots, d_n\}$ nd the time window dt, what separates the survey's course of events into

spans $\{I_1, \ldots, I_k\}$ of duration *dt*, where k is the quantity of audits posted during

the j-th span. d_t is set to 7 days [21]. Output is whether I_j is bursty.

Input: $T = \{ , \ldots, \}, d_t$

Output: whether Ij interval is bursty

$len = d_n - d_1$

$k = \#Intervals = len/dt$

$I = \{I_1, \ldots, I_k\}$

$Avg( ) = n/k, 1 \leq j \leq k$

for $j = 1 : k$ **do**

  if $I_j > Avg(I_j)$ **then**

    if $j = 1$ & $I_j > I_{j+1}$ **then** $I_j \leftarrow$ Bursty

    else if $1 < j < k$ & $I_{j-1} < I_j > I_{j+1}$ **then** $\leftarrow$ Bursty

    else if $j = k$ & $I_j > I_{j-1}$ **then** $\leftarrow$ Bursty

end for

We then, at that point extricate the surveys fallen in bursty stretches and apply the below two after spam markers to them.

4.2.1 Content Similarity in Burst (CSBu)

A high enough similarity rating among a assessment and completely different analysiss of identical "burst" ought to recommend that a evaluation is suspiciously like different evaluations. we tend to as a result calculate the trigonometric function similarity among Ocean State and every one different I_{j-1} critiques of the identical burst:

$$CSBu(r_i) = \begin{cases} \frac{\sum_{z=1}^{I_j} cosine(r_i, r_z)}{I_j - 1} - 0.5, & \frac{\sum_{z=1}^{I_j} cosine(r_i, r_z)}{I_j - 1} > 0.5 \\ 0, & otherwise \end{cases} \tag{4.4}$$

Assuming that a similarity rating of 0.5 is taken into thought traditional, we've changed the CSBu metric a decent thanks to solely have an impact on those critiques that show higher similarity than normal to not punish evaluations really for being printed in a very bursty time interval.

4.2.2 Bursty Activity (BuA)

A spammer is expected to make tremendous quantities of assessments in little eruptions of movement to quick administration the assessment. we will in general conjecture that an earnest commentator would make all things considered two bursty assessments, along these lines the bursty leisure activity score for an analyst and ultimately for his/her surveys, is estimated as:

$$BuA(a(r_i)) = \begin{cases} 1, & bursty\ reviews > 2 \\ 0, & otherwise \end{cases} \tag{4.5}$$

4.3 Reviewer Reputation

There is sufficient open records regarding creator on the far side investigating interest, that would engage our model to higher analyze a commentator's ordinary name and, inside the end, the quality of his/her evaluation(s), through an analyst degree examination. This leads us to the ensuing definition: Definition three (Author Reputation). Creator quality alludes to a commentator's standard reliability put together for the most part entire with respect to their conduct and leisure activity all through their past conclusions. An analyst is said to an extreme and speedy of studies, his/her past looking into records, all through assortment of yelling items, that our rendition takes advantage of with the assistance of considering two expansion commentator history-based entire spam signs.

4.3.1 Extreme Rating (EXR)

Most spammers give an outrageous evaluations (for example one or five in a five star scale) on the gratitude to apace increment or lower the mean score of an application.

To the present end, the number of excessive scores on a 5-megastar scale among all past rankings RS_{aj} of an creator $a(r_i)$is gathered, and divided by the whole style of given scores RS_{aj} main to the reviewer's quantitative relation [0, 1] of maximum rankings, that within the long-term adds to his/her normal recognition rating:

$$EXR(a(r_i)) = \frac{|RS_{a,j} \in \{1,5\}|}{|RS_{a,j}|} \tag{4.6}$$

4.3.2 Reviewer Burstiness (RBu)

Spammers will in general frame every one of their surveys in enormous volume and in an exceptionally brief time frame window (burst) in order to rapidly rule fair audits. Looking at a time window of d = thirty days [22], the burstiness score of an analyst $a(r_i)$ is estimated like so:

$$RBu(a(r_i)) = \begin{cases} 0, LR(a(r_i)) - FR(a(r_i)) > \delta \\ \quad 1 - \frac{LR(a(r_i)) - FR(a(r_i))}{\delta}, \ otherwise \end{cases} \tag{4.7}$$

where $LR(a(r_i))$ addresses the creation date of the analyst's last and most recent audit, while $FR(a(r_i))$ demonstrates the creation date of the main composed survey by this commentator account.

Taking into thought the over three history-based spam markers, we will in general promoter measure an analyst's name through adding the gathered pointer scores. Along these lines, we present the resulting blended strategy that models trustiness or quality for an analyst a(ri). each produced rating is improved by a few weight for every the popular effect of the pointer on the latest rating:irst composed survey by this analyst account:

$$Rep(a(r_i)) = \frac{1}{2}\ EXR(a(r_i)) + RBu(a(r_i)) \tag{4.8}$$

A low score is a marker of good standing, while a high score infers dubious conduct.

4.4 Spam Scoring Function

We as of now present our direct Spam Scoring Function, which blends the individual rankings created through each aforesaid refered to marker and yields a middle spam rating for each outline. In this way, the standard mail rating of an assessment ri, composed by approach of an analyst $a(r_i)$, is estimated by abuse the resulting approach:

$$S(r_i) = RD(r_i) + \frac{1}{3}NR(a(r_i)) + 1.5\,CS(a(r_i)) + 2\,CSBu(r_i) + BuA(a(r_i)) + Rep(a(r_i)) \tag{4.9}$$

The loads of our form's marker scores are partner degreed error} first class upheld include significance likewise as worth reach. Content Similarity in Burst (CSBu) includes an expense of [0, 0.5] so we offer it a load of two to development its impact, while Extreme Rating (EXR) is taken into thought the most fragile pointer, in light of the fact that a legit analyst may building to serious appraisals, and is given a more modest weight. the 2 spam abilities (NR, NRP) associated with steep exploring are given awesomely low loads to offset their likely unreasonable qualities. At long last, we settle for as obvious therewith analyst Content Similarity (CS) offers strong evidence of spam so we tend to development its weight consequently. At long last, an addressed edge isolates the fake assessments from the genuine conclusions. while reviewing the expected rating esteems for fair assessments, also with respect to spam scrutinizes, we set the verge to a couple. Accordingly, suppositions with garbage rankings uncommon the limit are set apart as artificial, while evaluates with spam appraisals decline than the verge are taken into thought real.

CHAPTER 5

EXPERIMENT AND RESULT

5.1 Dataset

A dataset of reviews is made by scraping the google play store ap reviews with the help of google_play_scraper library available in python. The dataset consists of 33287 reviews from different apps in the google play store.

The dataset created then is sampled into two datasets. One dataset is labeled manually to train the model and other data set is unlabeled for testing the model.

The testing data set consists of about 15000 reviews and the training data consists of 18287 reviews.

userName	userImage	content	score	thumbsUpCount	reviewCreatedVersion	at
Ismail Skoreb ahana	https://play-lh.googleusercontent.com/a-/AOh14...	Amazing application	4	0	21.5.0.361	2021-05-27 15:38:32
Anisha	https://play-lh.googleusercontent.com/a-/AOh14...	Nice app	2	0	None	2021-04-21 05:44:49
Inga Zakharova	https://play-lh.googleusercontent.com/a-/AOh14...	😍😍😍	5	0	21.1.2.343	2021-04-04 08:12:56
Sarilho TV	https://play-lh.googleusercontent.com/a-/AOh14...	Awesome!!! <3	5	0	21.1.2.343	2021-03-24 07:47:15
Rebeca Fernandes	https://play-lh.googleusercontent.com/a-/AOh14...	I like	3	0	19.4.0.325	2021-03-22 20:53:46

Table 5.1: Dataset overview

5.2 Evaluation by Supervised Text Classification

We rehash over all reviews in our dataset and rating their perspectives. Then, all assumptions are characterized in down demand, with the pinnacle 2000 tending to the extraordinary quality (unconstrained mail) class and thusly the last 2000 tending to the negative (certifiable) prominence. we will overall pick the apex 2000 examines, as they're basic spam cases and have a lot of unsought mail-like matter substance. A Naïve Thomas Bayes classifier is then moved toward these assessment set up generally whole concerning UNIGRAM capacities and the Bag-of-Words model. we will overall perform 10-overlay move endorsement and archive the results. Given the disadvantage that it' way overall astonishing to see appraisal validness by content without any other person, sort accuracy procured be totally illustrative of our certified precision nor will it consider a protected assessment to elective strategies. it'll in any case recommend whether our variation is convincing and has considering the way that it ought to be requested the assessment reviews. Precision is assessed with the put in estimations of exactness, recollect and F-rating to ensure consistency with different works inside the field.

5.3 Experimentation Results

To show the impact of all pre-owned techniques of our interpretation, we will overall beginning dissect the suitability of the three simple assessment trash markers. Then, we stock out envision assessment disclosure with the extension of burst test distinguishing proof. Finally, we exemplify investigator quality inside the acknowledgment technique and appearance at its impact. For the investigator affirmation rating region, we use the whole non-assessed dataset, which contains adequate records regarding pundit records all through arrangement awing things, as our model dataset won't reserve abundant records. Table two reports the consequences of our model's sufficiency once playing 10-overlay cross-endorsement of the class of our dataset studies. Incredibly, the thought of burst plan disclosure has every one of the reserves of being reducing accuracy through 1% when appeared differently in relation to the implications of the unmistakable spam signs. The qualification, regardless, is negligible adequate to be credited to the constraints of assessment matter substance sort henceforth no certifiable finish is in like manner made. The extension of investigator quality in spite of the way that showed an outsized improvement in revelation accuracy, reporting practically 75%. Contemplating again the objectives of our appraisal approach, this is consistently an incredibly wonderful result, that confirms the meaning of expert affirmation in discovering spam ends. This makes us ensured that enhancing clear spam markers and burst test disclosure with assessment of reporter on the far side activity permits our model to effectively discover hazardous envision reviews.

Method	Precision	Recall	F-score
Basic	67.6	66.2	65.4
Basic + burst pattern	66.9	65.2	64.3
Basic + burst pattern + reviewer reputation	75.2	75	**74.9**

Table 5.2 : Results of 10-fold cross validation for different combinations of indicators.

CHAPTER 6

CONCLUSION AND FUTURE WORK

We with progress made a model for machine-driven fake survey identification with a precision of 75.2, Recall of 75 and a F-sore of 74.9. we will in general endeavor an assortment of arranged spam signs on an item degree comparative with each action and commentator conduct so as gather and use each bit of possible records. Besides, our model abilities further investigation capacities fundamentally dependent on burst test revelation, which permits the recognizable proof of dubious time spans and evaluates. At long last, we degree commentator fame, by investigating their set of experiences of on the far side scrutinizes and hobby, to higher choose the validity of their extra most recent audits. The investigation of our projected method become accomplished on a dataset of Google play search assessments and furthermore the experimentation results affirmed that our homogenized strategy is incredible in identification hurtful artificial assessments.

As future work, we will in general endeavor to manage the extra strategy to higher record for singleton spam surveys. though those studies as individual things of content material do not have the effect on an item's fundamental rating and notoriety, nonetheless, as one they'll make a real danger to clueless assessment perusers and customers.

Bibliography

[1] Number of available applications in the Google Play Store from December 2009 to July 2021 https://www.statista.com/statistics/266210/number-of-available-applications-in-the-google-play-store/

[2] Carreno LVG, Winbladh K (2013) Analysis of user comments: an approach for software requirements evolution. In: 2013 35th international conference on software engineering (ICSE), pp 582–591. https://doi.org/10.1109/ICSE.2013.6606604

[3] Pagano D, Maalej W (2013) User feedback in the appstore—an empirical study, pp 125–134.https://doi.org/10.1109/RE.2013.6636712 http://ieeexplore.ieee.org/document/6636712/

[4] Harman M, Jia Y, Zhang Y (2012) App store mining and analysis: MSR for app stores. In: 2012 9th IEEE working conference on mining software repositories (MSR 2012). IEEE, pp

[5] Martin W, Sarro F, Jia Y, Zhang Y, Harman M (2016) A survey of app store analysis for software engineering. IEEE Trans Softw Eng PP(99):1–1. https://doi.org/10.1109/TSE.2016.2630689. http://ieeexplore. ieee.org/document/7765038/

[6] Finkelstein A, Harman M, Jia Y, Martin W, Sarro F, Zhang Y (2017) Investigating the relationship between price, rating, and popularity in the blackberry world app store. Inf Softw Technol 87:119–139. https://doi.org/10.1016/j.infsof.2017.03.002. http://www.sciencedirect.com/science/article/ pii/S095058491730215X

[7] Google (2019) In reviews we trust - making Google Play ratings and reviews more trustworthy. https:// android-developers.googleblog.com/2018/12/in-reviews-we-trust-making-google-play.html

[8] 9to5Mac (2017) Bell faces $1.25M fine for posting fake reviews of its app in the App Store. https://9to5mac. com/2015/10/14/bell-fake-app-store-reviews/

[9] DigitalTrends (2018) Can you really trust app store ratings? We asked the experts. https://www.digitaltrends. com/android/can-you-really-trust-app-store-ratings/

[10] 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, HLT ’11. Association for

Computational Linguistics, Stroudsburg, pp 309–319. http://dl.acm.org/citation.cfm?id=2002472.2002512

[11] Google (2017) Google play user ratings, reviews, and installs. https://play.google.com/about/storelistingpromotional/ratings-reviews-installs/

[12] Ning Chen, Jialiu Lin, Steven CH Hoi, Xiaokui Xiao, and Boshen Zhang. 2014. ARMiner: Mining informative reviews for developers from mobile app marketplace. In 36th International Conference on Software Engineering (ICSE 2014). 767–778.

[13] Andrea Di Sorbo, Sebastiano Panichella, Carol V Alexandru, Junji Shimagaki, Corrado A Visaggio, Gerardo Canfora, and Harald C Gall. 2016. What would users change in my app? Summarizing app reviews for recommending software changes. In 24th ACM SIGSOFT International Symposium on Foundations of Software Engineering (FSE 2016). 499–510.

[14] Emitza Guzman and Walid Maalej. 2014. How do users like this feature? A fine grained sentiment analysis of app reviews. In 22nd IEEE International Requirements Engineering Conference (RE'14). 153–162.

[15] Rajamohana S. P, Umamaheswari K., Dharani M., Vedackshya R., "Survey of review spam detection using machine learning techniques." ,978-1-5090- 5778-8, pp.17 (2017). 4) Mevada D. L., Daxini V., "An opinion spam analyzer for product Reviews using supervised machine Learning method." pp.03, (2015).

[16] Adike R. G., Reddy V,. "Detection of Fake Review and Brand Spam Using Data Mining Technique.", pp.02,(2016).

[17] Adike R. G., Reddy V,. "Detection of Fake Review and Brand Spam Using Data Mining Technique.", pp.02,(2016).

[18] Lim, E.-P., Nguyen, V.-A., Jindal, N., Liu, B., Lauw, H.W.: Detecting product review spammers using rating behaviors. In: Proceedings of the 19th ACM International Conference on Information and Knowledge Management, pp. 939–948. ACM (2010)

[19] Lin, Y., Zhu, T., Wang, X., Zhang, J., Zhou, A.: Towards online anti-opinion spam: spotting fake reviews from the review sequence. In: 2014 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), pp. 261–264. IEEE (2014)

[20] Lau, R.Y., Liao, S., Kwok, R.C.W., Xu, K., Xia, Y., Li, Y.: Text mining and probabilistic language modeling for online review spam detecting. ACM Trans. Manag. Inf. Syst. 2(4), 1–30 (2011)

[21] Heydari, A., Tavakoli, M., Salim, N.: Detection of fake opinions using time series. Expert Syst. Appl. 58, 83–92 (2016)

[22] Mukherjee, A., Kumar, A., Liu, B., Wang, J., Hsu, M., Castellanos, M., Ghosh, R.: Spotting opinion spammers using behavioral footprints. In: Proceedings of the 19th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, pp. 632–640. ACM (2013)