International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 03 | Mar 2019 www.irjet.net p-ISSN: 2395-0072

Search Rank Fraud Detection for Android Application Based On Reviews And Rating

Komal Bodade.

Department of Information Technology

Bharati Vidyapeeth College of Engineering,

CBD Belapur, Navi Mumbai
bodadekomal@gmail.com

Urmila Gaikwad

Department of Information Technology

Bharati Vidyapeeth College of Engineering,

CBD Belapur, Navi Mumbai
gaikwadurmila995@gmail.com

Abstract - *Search Rank Fraud means that something which is searched and abnormal while ranking, and detection is nothing but identifying that abnormal. In this paper, we have created a web application where the user submits their reviews, ratings on our application with comments, and on the server side it has been verified with a PCF (Pseudo Clique Finder) algorithm and the results are carried out on two parameters' i.e. positive and negative.*

***Key Words*: Search, Google Play, Ranking, Review, Rank Fraud analysis**

1. INTRODUCTION

Now-a-days with increase craze towards android mobiles the craze of mobile applications has also increased. According to the recent study, the number of application in Google play store, which is also known as Android. The app developers try false mechanism so that the app developed by them should have high rank in the app leaderboard. So, the developers of the app try various methods to promote their apps, like advertising which helps them to have higher rank in the app leader board. However, instead of using ethical mechanism to promote their apps, the app developers try unethical means to promote their apps which manipulates the chart ranking of the app in the leaderboard and hence the app is ranked high in the leaderboard. This kind of unethical mechanism is generally carried out using internet water army.

Internet water army is a group of internet ghost writers who are paid to post online comments with particular content. Thus, this helps the app developers to promote their apps using fake reviews and ratings. Mostly fraud detecting systems classifies reviews and ratings of the apps into two groups i.e., positive and negative. Since Android is open source environment all the detail about the application users can be easily accessed by the application developers through Google play

2. LITERATURE REVIEW

- **Mahmudur Rahman, Mizanur -Rahman,Bogdan and Duen Horng Chau, June 2017** proposed Fairplay, a novel system that discovers and leverages traces left behind by fraudsters, to detect both malware and apps subjected to search rank fraud. FairPlay correlates review activities and uniquely combines detected review relations with linguistic and behavioral signals gleaned from Google Play app data, in order to identify suspicious apps [1].

- **Olga Ivanova, 2017** proposed a consumer shopping experience, most online marketplaces introduced online rating systems, which provide consumers with the opportunity of exchanging their opinions on sellers and purchased products. [2]

- **Michael Wessel, Ferdinand Thies, Benlian, 2016** proposed has led to proliferation of social information in electronic markets for consumers to use for decision support, as online transactions restrict the consumer's ability to assess a product's quality due to the lack of direct interaction [3]

- **Hengshu Zhu, Hui Xiong, 2014**proposed a recent trend shady App to deliberately boost their Apps and eventually manipulate the chart rankings on an App store. [4]

- **Arjun Mukherjee, Bing Liu, Natalie Glance, April 2012** hence proposed a opinion spamming for their decision making. However, due to the reason of profit or fame, people try to game the system by opinion spamming (e.g., writing fake reviews) to promote or demote some target products [5].

3. METHODOLOGY

Searching the rank fraud of the applications or their apks can be done with the help of Pseudo Clique Finder (PCF) Algorithm. The algorithm consists of four modules and they are:

Inter-Review Relation (IRR) Module:

1. One user gives review or rating without download the app --> this user may be malicious user
2. One user gives more +ve reviews for one app --> this app may be malware app

- **Reviewer Feedback (RF) Module:**

1. Check malware indicator words are available in reviews --> this app may be malware app
2. Check Fraud indicator words are available in reviews --> this app may be malware app
3. Check Benign indicator words are available in reviews --> this app may be malware app

- **Jekyll-Hyde App Detection (JH) Module:**

1. Which apps want above 3 dangerous Permissions while download --> These apps are called malware app

➢ **Most dangerous Permissions:**

1. Read Phone Status and Identity
2. Modify & Delete USB Storage Contents
3. Test access to Protected Storage
4. Find Accounts on Device
5. Use Accounts on Device

➢ **Co-Review Graph (CoReG) Module:**

1.2 users give the same reviews for many app at a particular time (this review is called co-reviews) --> these users may be malicious users (i set Threshold value theta = 3 (you can change this value))

This algorithm considers the ratings and reviews as the input for determining the reviews on daily basis given by the users who have given rating along with review to the application. After these ratings and reviews are taken into consideration, they are analyzed on the basis of their download status i.e. whether the application is downloaded or not along with the permissions given by the developer for the particular application. If the app is given its rating and review without downloading then the application may have been given a fake rating and review and may have caused a rank fraud. If the user downloads an application and there are more than three permissions asked by the app before downloading then the application can be considered as the malware. This proposed method helps the users from getting persuaded into using fake apps that absolutely goes against the description given by the developer to make it appear as a legit application. Our method also comprises of sentimental analysis which helps the developer to find the exact positive and negative review which enhances our proposed method. Using this sentimental analysis and the algorithm the developer can analyze and can warn the user from using this application.

4. ARCHITECTURE

The architecture of this proposed contains three major entities user, developer and the admin. The user searches the application using the categories and accordingly either gives rating and reviews or downloads the app or does both. As the user gives ratings and reviews and downloads the app this response is stored at the database. The role of admin is to analyze these apps which depend upon the ratings and reviews and find out whether these apps are causing rank fraud or contains malware or not. If these apps contain malware or cause rank fraud then the admin requests the google play admin to advise the users not to use those apps.

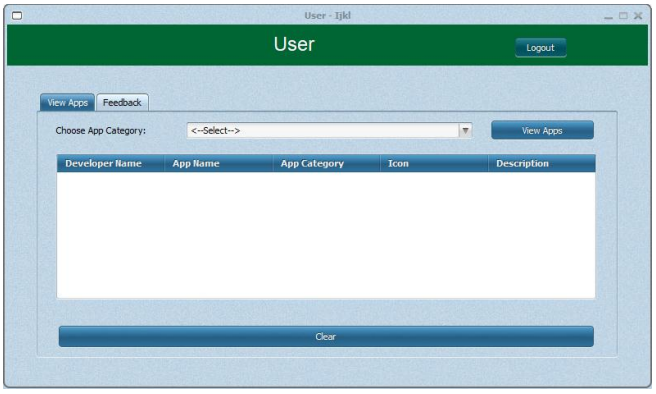

Fig. a User Frame

The fig.a. consist of App Category and Feedback through which if there is a need for the query about an app then the Admin may reply the query through it.

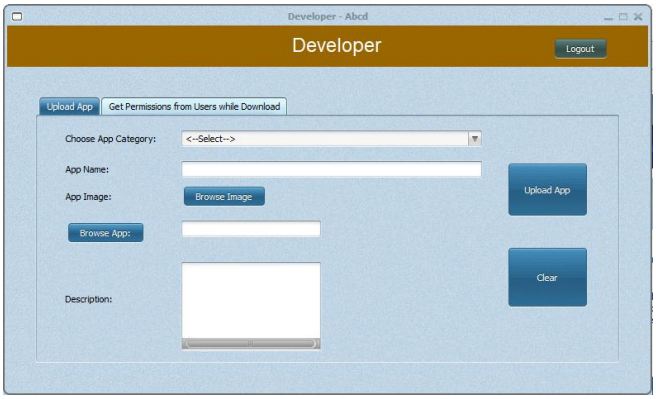

Fig.b.1. Developer Frame

The Fig b.1. consist of App details about the category of App, App name, image of App and description related to it.

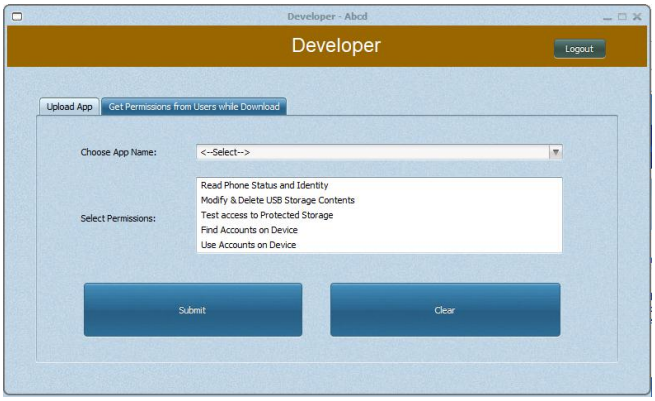

Fig.b.2. Developer Frame

The fig.b.2. focuses on the permissions that the developer sets for an app.

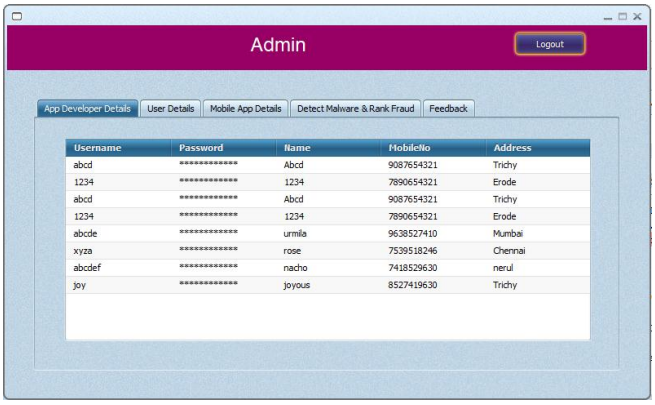

Fig.c.1. Admin Frame

The fig.c.1. focuses on App Developer Details,User Details,Mobile App Details, Detect Malware & Ran, k Fraud and Feedback .

5.CONCLUSION

This system proposes the avoidance of rank fraud using this web application. This search rank fraud is based on the PCF algorithm

which will help in segregating the data that will lead the admin towards the results. In the proposed system the use of comments and ratings etc. are majorly considered as the analyzing process is based on these comments due to which the user would not be cheated with such applications

REFERENCES

[1] Mahmudur Rahman, Mizanur -Rahman, Bogdan and Duen Horng Chau, search rank fraud and malware detection in Google Play.

[2] Olga Ivanova, how can market places reduce rating manipulation? A new approach on dynamic aggregation of online ratings.

[3] Michael Wessel, Ferdinand Thies, Benlian, The emergence and effects of fake social information: Evidence from crowd funding

[4] Hengshu Zhu, Hui Xiong, Discovery of ranking fraud for mobile apps.

[5] Arjun Mukherjee, Bing Liu, Natalie Glance, Spotting fake reviewer groups in consumer reviews.