iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** IV **Month of publication:** April 2019

DOI: https://doi.org/10.22214/ijraset.2019.4472

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue IV, Apr 2019- Available at www.ijraset.com

Efficient and Secure Model for Detect Malware and Fake Ranking Apps

V. RakeshDatta[1], Dr. K. Rajeshkhanna2
[1] *M.Tech Student,* [2]*Assist.prof, CSE, Vaagdevi college of Engineering, Warangal, TS*

Abstract: ***Nowadays most of the people using smart phones for daily activities so android apps in smart phones plays major role in the market to perform various activities. Previous works describes the information about on app executable and permission analysis. Users mostly will download apps from Google play based on ranking and review. Malware is any piece of code that is meant to cause damage to your system or network. Malware is completely different from common programs during a approach that they most of them have the flexibility to unfold itself within the network, it will damage entire system performance and network. Another issue is search fraud due to these users will change their opinions on app .In this paper we implement novel system called Fairplay to uncover malware and search rank fraud by fraudsters, it will analyze longitudinal app data. FairPlay's PCF algorithmic rule analyzes review process and relations between various users posted reviews from dataset. We implement FairPlay in this article to detect Google Play fraud and malware. In this supervised learning techniques used to provide relational and behavioral and linguistic features, Novel system provides 95% accuracy in datasets of malware, fraudulent and accurate apps. We analyze and show experimental results that 75% of the found malware apps employ with fake rank fraud.***
Keywords: Fairplay, search rank fraud, malware detection

I. INTRODUCTION

Android app market most commercial success in worldwide. So most of the people using apps for daily activities like pay bills, shopping so on .Google play provides number of apps to users [1].To increase profits in market few fraudulent developers providing fake ranking to popular their company apps in the market. With fake reviews and false installation counts fraudulent release fake apps into market [2]. Previous solution of malware detection has some disadvantages. For example, while Google Play utilizes the Bouncer system [7] to detect malware, 7, 756 Google Play apps as per we analyzed utilizing VirusTotal [8], 12%(948) were flagged by at least one anti-virus tool , 2% (150) were found as malware by at least 10 tools. Previous works describes the information about the app executable and permission analysis [9,10].In our research article we implement secure system to identify malware and search rank frauds in Google play store. With this implemented work we will observe fraudulent and malicious behaviors and characteristics on market. Mainly in Google play fraudsters will use existing accounts again again to write reviews for apps to popularity, creating them mostly likely to re-view more apps in ordinary than normal users. In my paper as per my analysis we show better results with Fairplay than existing solution to detect malware apps and fake ranking apps in Google play store.

II. RELATED WORKS

In previous various literatures found to detect malware and search rank fraud . Google Play utilizes the Bouncer system [7] to detect malware, 7, 756 Google Play apps as per we analyzed utilizing VirusTotal [8], 12%(948) were flagged by at least one anti-virus tool , 2% (150) were found as malware by at least 10 tools. Previous works describes the information about the app executable and permission analysis.Sarma et al. describes the information regarding the risk signals removed from app permissions, e.g., rare critical permissions (RCP) and rare pairs of complexl permissions (RPCP), to train SVM and notify users of the risks vs. benefits tradeoffs of apps.

III. PROPOSED SYSTEM

We implement secure system to detect search rank fraud and malware .For this we proposes In this supervised learning techniques used to provide relational and behavioral and linguistic features . Co-Review Graph is one of the part of Fairplay its (CoReG) module finds apps reviewed and relations by various users. FairPlay's PCF algorithmic rule analyzes review process and relations between various users posted reviews from dataset. We implement FairPlay to detect Google Play rank fraud and malware. . We utilize sequential dimensions of review post times to find apprehensive review points received by android apps; as per we analyze Find negative reviews and positive reviews posted by fraudsters based on posting time between reviews and rating of the app and also finds unbalanced review ,install counts and rating. We utilize linguistic and behavioral data to detect genuine reviews from app dataset

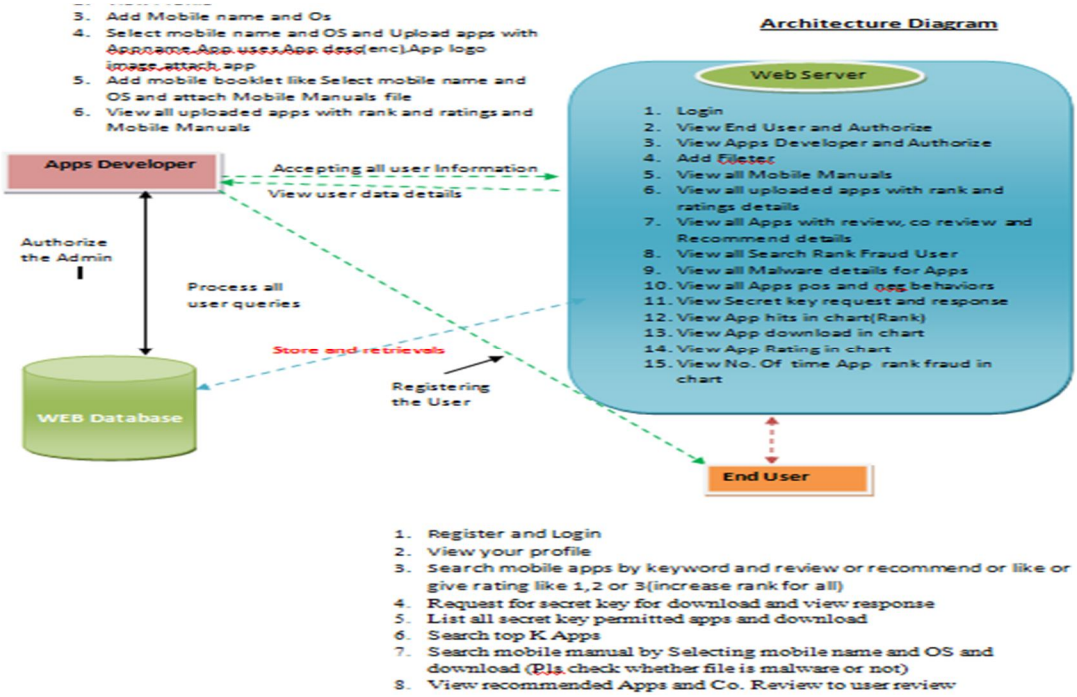


Fig 1: System Architecture:

IV. METHODOLOGY

FairPlay classifies the analysis of longitudinal android app data into the following steps. Step1 the Co-Review the CoReG module finds suspicious, time connected co-review behaviors. Step 2: The RF module utilizes linguistic tools to discover suspicious behaviors reported by real reviews. Step 3 The IRR module finds relation between reviews and ratings also app install counts. Last step is JH module observes app permit ions with a focus on unsafe ones, to finds apps that exchange from benign to malware. This proposed system uses common general app futures apps ratings and total reviews, ratings and installation counts.

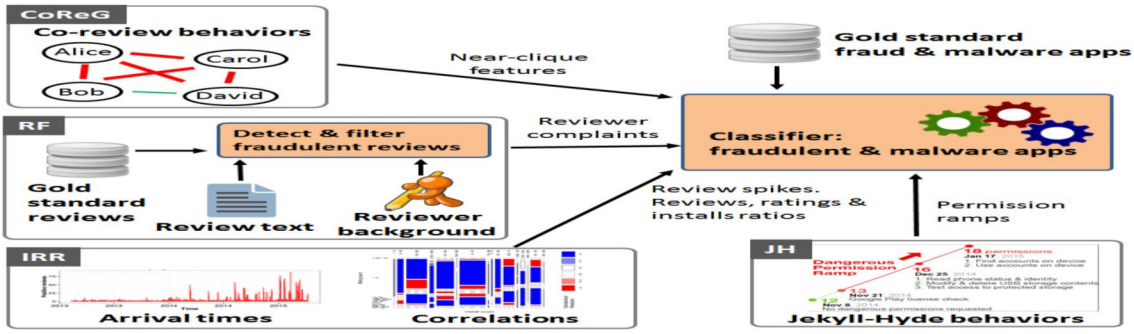


Fig 2: Fairplay architecture

V. IMPLEMENTATION

This implemented system divides into following modules

A. Web Server

Web server need to login with valid username and password. After login we can access system and perform few operations like view end user and authorize, below operations we can perform in this module.

View End User and Authorize, View Apps Developer and Authorize, Add Fileter, View all Mobile Manuals, View all uploaded apps with rank and ratings details, View all Apps with review, co review and Recommend details, View all Search Rank Fraud User, View all Malware details for Apps, View all Apps pos and neg behaviors, View Secret key request and response, View App hits in chart (Rank),View App download in chart, View App Rating in chart, View No. Of time App rank fraud in chart.

B. Apps Developer

C. Add App

In implemented system this is one of the phases for adding apps.Here admin can add app with below information

Application name, app description, mobile type, users, file name, application images and click on register. The details will be stored in the database.

D. View Application

In this module, when the admin clicks on view application, application name, app description, mobile type, users, file name, application images will be displayed.

E. Ranking Fraud Details

This modules describes the information about fraud ranking app details the following details will be provided.

Ranking fraud count, user name, mobile type, application name, application ID, date and time will be displayed.

F. Proof for Frauds

This module describes the information about fraud details like following details it will be provided. Once admin clicks on proof for fraud details,

user name, mobile type, application name, application ID, fraud IP address, fraud system name, date and time will be displayed.

G. User

This module in implemented system so present number of users is there. So in this user should register first then they will get username and password .With credentials he will enter into system. Then following operation user can perform

,View Profile, Add Mobile name and Os,Select mobile name and OS and Upload apps with Appname,App uses,App desc(enc),App logo image, attach app,Add mobile booklet like Select mobile name and OS and attach Mobile Manuals file, View all uploaded apps with rank and ratings and Mobile Manuals

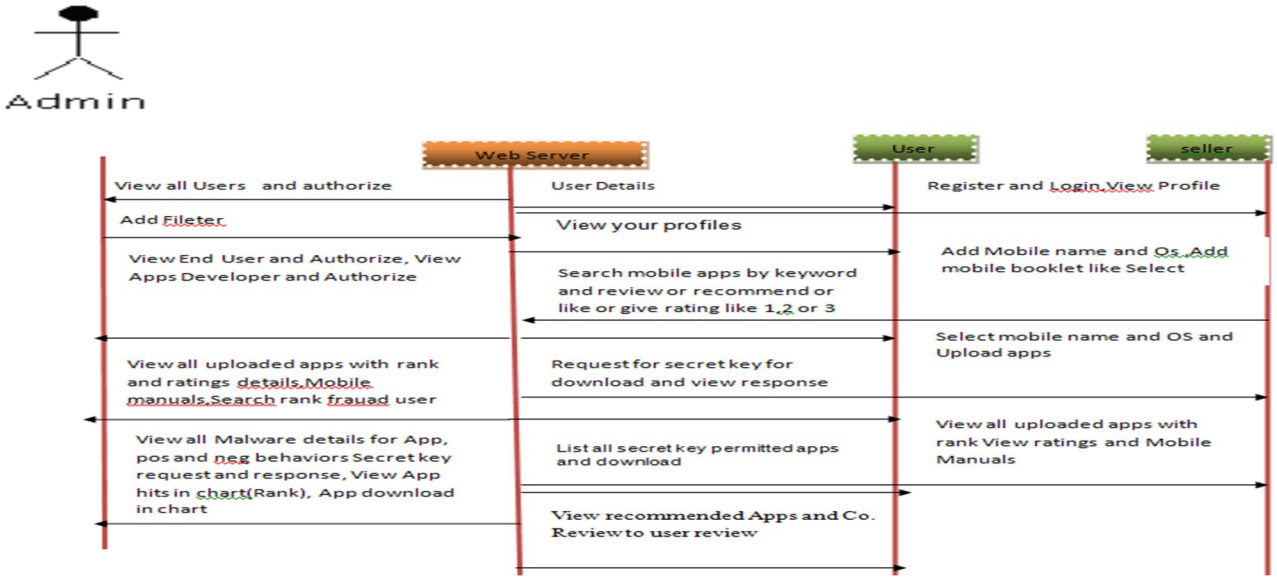
H. Search and Download Mobile Apps

In this phase in implemented system android mobile user can search required app. Based on secret key he will download the app from server.

I. Search for Top K Applications

In this phase app user will enter the app name and choose the top K app information then after it will be providing information regarding leading app information like app name,description,type of mobile, file name, images also ratings will be displayed.

Sequence Diagram for Implemented System:



VI. RESULTS

Fig 3: various applications

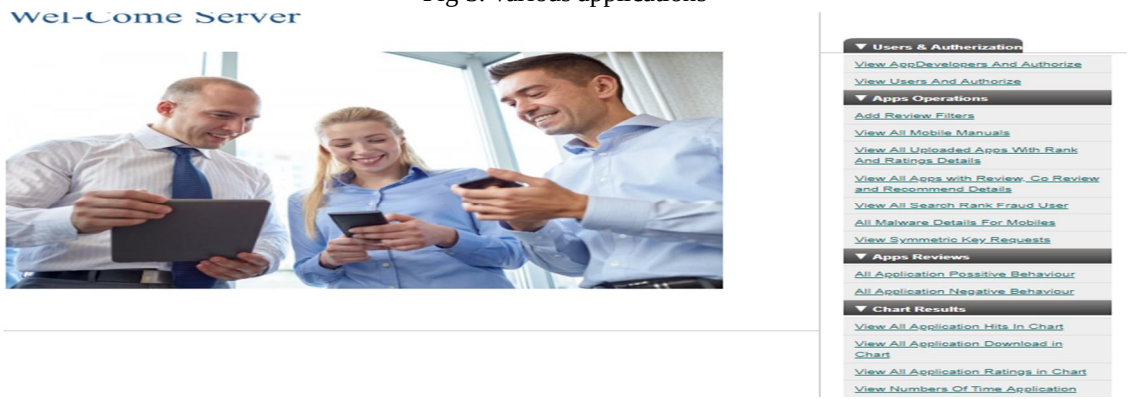


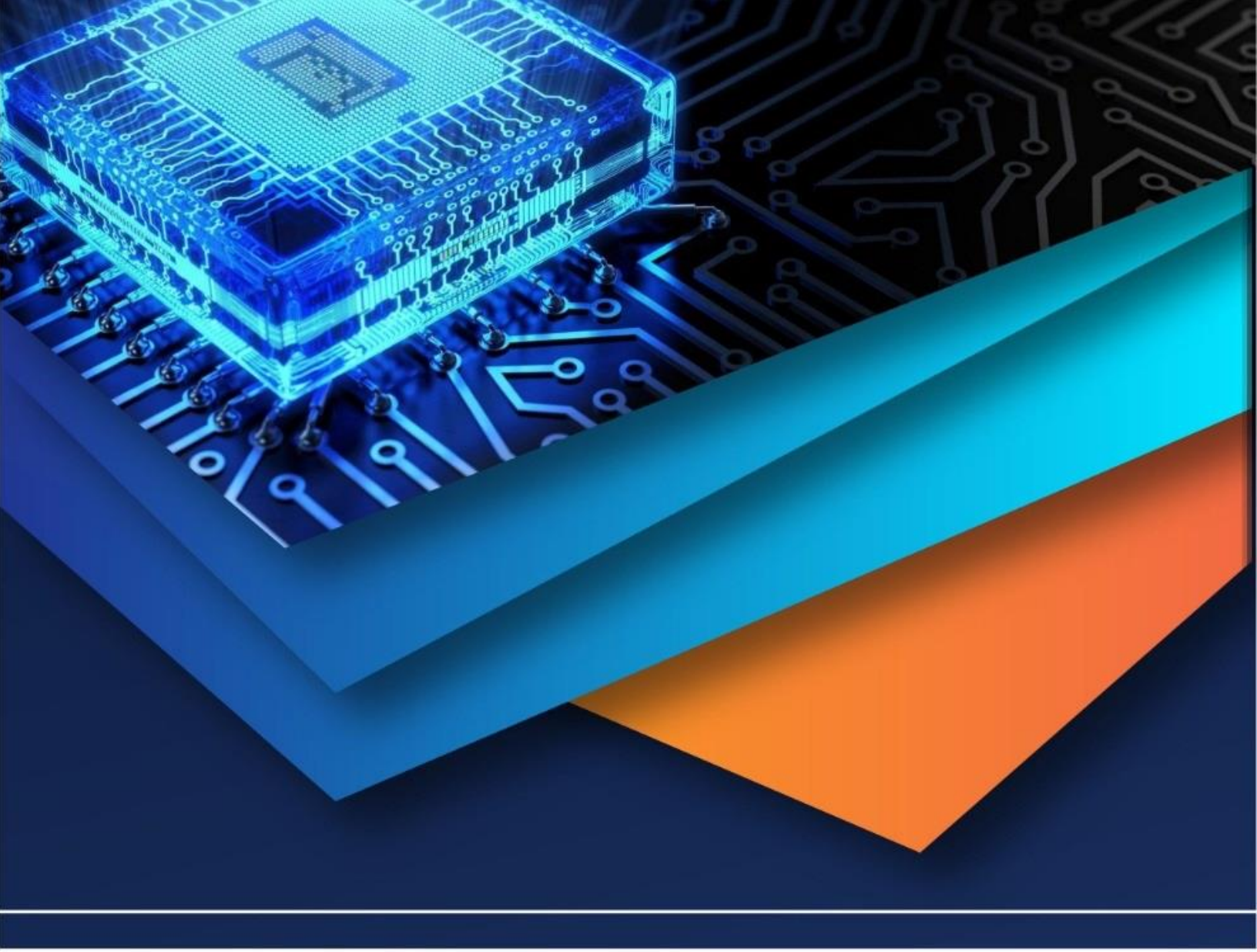
Fig 3: welcome server page

VII. CONCLUSION

As per Analysis we implemented system used to detect malware and rank fraud apps.This system produce better results than previous system. In this we are using differ models to analyze reviews and ratings, installetion counts to find fraudsters. Novel system provides 95% accuracy in datasets of malware, fraudulent and accurate apps. We analyze and show experimental results that 75% of the found malware apps employ with fake rank fraud.

REFERENCES

[1] Google Play. https://play.google.com/.
[2] Ezra Siegel. Fake Reviews in Google Play and Apple App Store. Appentive, 2014.
[3] Zach Miners. Report: Malware-infected Android apps spike in the Google Play store. PCWorld, 2014.
[4] Stephanie Mlot. Top Android App a Scam, Pulled From Google Play. PCMag, 2014.
[5] Daniel Roberts. How to spot fake apps on the Google Play store. Fortune, 2015.
[6] Andy Greenberg. Malware Apps Spoof Android Market To Infect Phones. Forbes Security, 2014.
[7] Jon Oberheide and Charlie Miller. Dissecting the Android Bouncer. SummerCon2012, New York, 2012.
[8] VirusTotal - Free Online Virus, Malware and URL Scanner. https://www.virustotal.com/, Last accessed on May 2015.
[9] Iker Burguera, Urko Zurutuza, and Simin NadjmTehrani. Crowdroid: Behavior-Based Malware Detection System for Android. In Proceedings of ACM SPSM, pages 15–26. ACM, 2011
[10] Asaf Shabtai, Uri Kanonov, Yuval Elovici, Chanan Glezer, and Yael Weiss. Andromaly: a Behavioral Malware Detection Framework for Android Devices. Intelligent Information Systems, 38(1):161–190, 2012.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY