International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 4 Issue 6, September-October 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Fraud and Malware Detection in Google Play by using Search Rank

A. Brahma Reddy[1], K. V. Ranga Rao[2], V. Vinay Kumar[3]

[1]Associate Professor, Department of CSE, Malla Reddy College of Engineering for Women, Telangana, India
[2]Professor & HOD, Department of CSE, Neil Gogte Institute of Technology, Telangana, India
[3]Associate Professor, Department of ECE, Anurag University, Venkatapur, Telangana, India

ABSTRACT

Fraudulent behaviors in Google Play, the most popular Android app market, fuel search rank abuse and malware proliferation. To identify malware, previous work has focused on app executable and permission analysis. In this paper, we introduce FairPlay, a novel system that discovers and leverages traces left behind by fraudsters, to detect both malware and apps subjected to search rank fraud. . Fair Play discovers hundreds of fraudulent apps that currently evade Google Bouncer's detection technology.

KEYWORDS: *FairPlay, Google Bouncer's detection technology, fuel search rank, fraudsters*

How to cite this paper*:* A. Brahma Reddy | K. V. Ranga Rao | V. Vinay Kumar "Fraud and Malware Detection in Google Play by using Search Rank" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-4 | Issue-6, October 2020, pp.1579-1586, URL: www.ijtsrd.com/papers/ijtsrd35728.pdf

IJTSRD35728

1. Introduction to Data Mining:

Generally, data mining is the process of analyzing data from different perspectives and summarizing it into useful information information that can be used to increase revenue, cuts costs, or both. Data mining software is one of a number of analytical tools for analyzing data. It allows users to analyze data from many different dimensions or angles, categorize it, and summarize the relationships identified. Technically, data mining is the process of finding correlations or patterns among dozens of fields in large relational databases. Data mining is an interdisciplinary subfield of computer science and statistics with an overall goal to extract information from a data set and transform the information into a comprehensible structure for further use. Data mining is the analysis step of the "knowledge discovery in databases" process or KDD. Aside from the raw analysis step, it also involves database and the data management aspects, data pre- processing, model and inference considerations, interestingness metric.

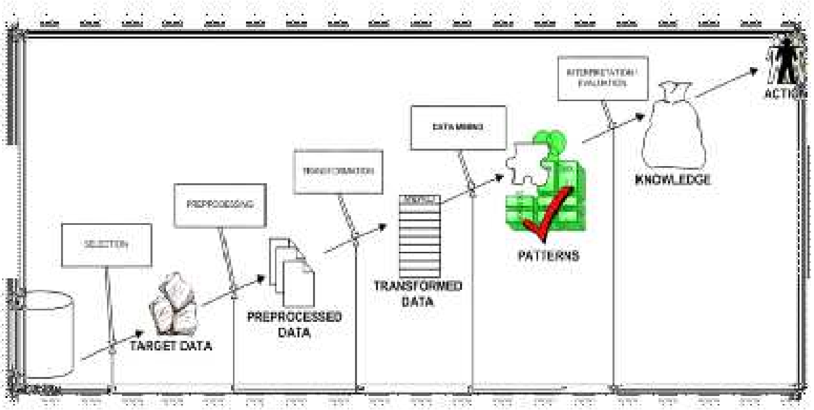


Fig 1: Structure of Data Mining

2. Existing System:

1. Google Play uses the Bouncer system to remove malware. However, out of the 7, 756 Google Play apps we analyzed using Virus Total, 12% (948)were flagged by at least one anti-virus tool and 2% (150) were identified

as malware by at least 10 tools.

2. Sarma et al. use risk signals extracted from app permissions, e.g., rare critical permissions (RCP) and rare pairs of critical permissions (RPCP), to train SVM and inform users of the risks vs. benefits tradeoffs of apps.
3. Peng et al. propose a score to measure the risk of apps, based on probabilistic generative models such as Naive Bayes.
4. Yerima et al. also use features extracted from app permissions, API calls and commands extracted from the app executables.

2.1. Disadvantages Of Existing System:

1. Previous work has focused on app executable and permission analysis only.
2. Not Efficient
3. Lower percentage of detection rate
4. Takes more time.

3. Proposed System:

1. We propose Fair Play, a system that leverages to efficiently detect Google Play fraud and malware. Our major contributions are:
2. To detect fraud and malware, we propose and generate relational, behavioral and linguistic features, that we use to train supervised learning algorithms
3. We formulate the notion of *co-review graphs* to model reviewing relations between users.
4. We develop PCF, an efficient algorithm to identify temporallyconstrained, co-review pseudo-cliques — formed by reviewers with substantially overlapping co-reviewing activities across short time windows.
5. We use temporal dimensions of review post times to identify suspicious review spikes received by apps; we show that to compensate for a negative review, for an app that has rating R, a fraudster needs to post at least positive reviews. We also identify apps with "unbalanced" review, rating and install counts, as well as apps with permission request ramps.
6. We use linguistic and behavioral information to (i) detect genuine reviews from which we then (ii) extract user-identified fraud and malware indicators.

3.1. Advantages Of Proposed System:

1. We build this work on the observation that fraudulent and malicious behaviors leave behind telltale signs on app markets.
2. Fair Play achieves over 97% accuracy in classifying fraudulent and benign apps, and over 95% accuracy in classifying malware and benign apps.
3. Fair Play significantly outperforms the malware indicators of Sharma et al. Furthermore, we show that malware often engages in search rank fraud as well. When trained on fraudulent and benign apps, Fair Play flagged as fraudulent more than 75% of the gold standard malware apps
4. Fair Play discovers hundreds of fraudulent apps.
5. Fair Play also enabled us to discover a novel, *coercive review campaign* attack type, where app users are harassed into writing a positive review for the app, and install and review other apps

4. System Architecture:

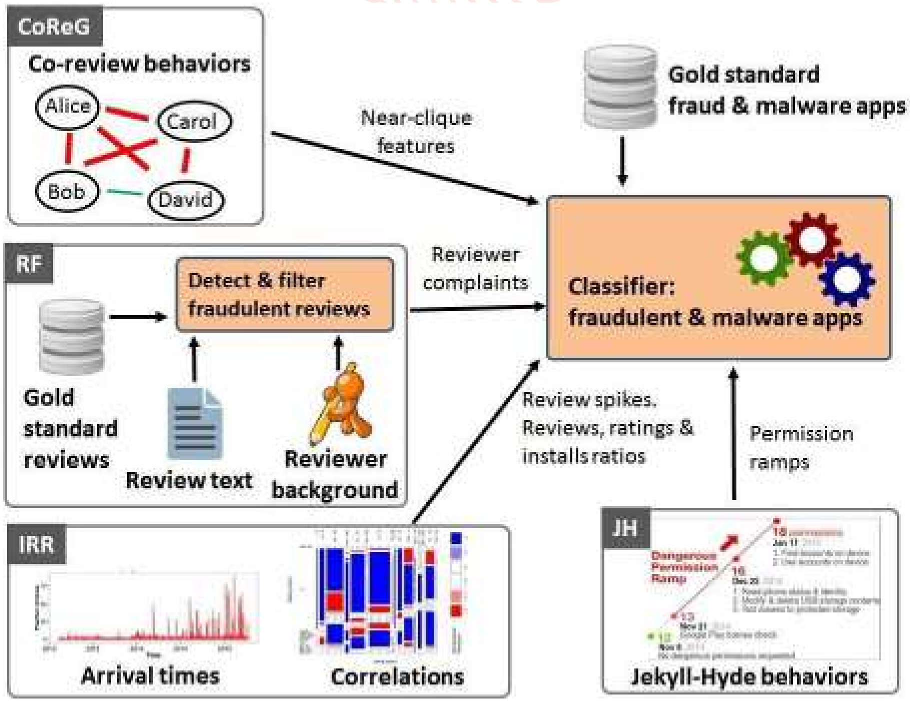


Figure 1 :System Architecture

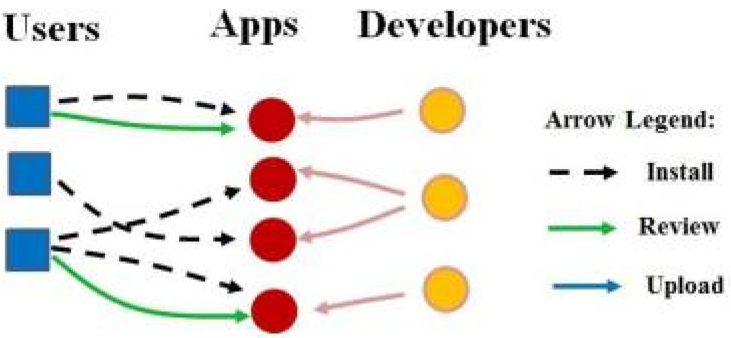
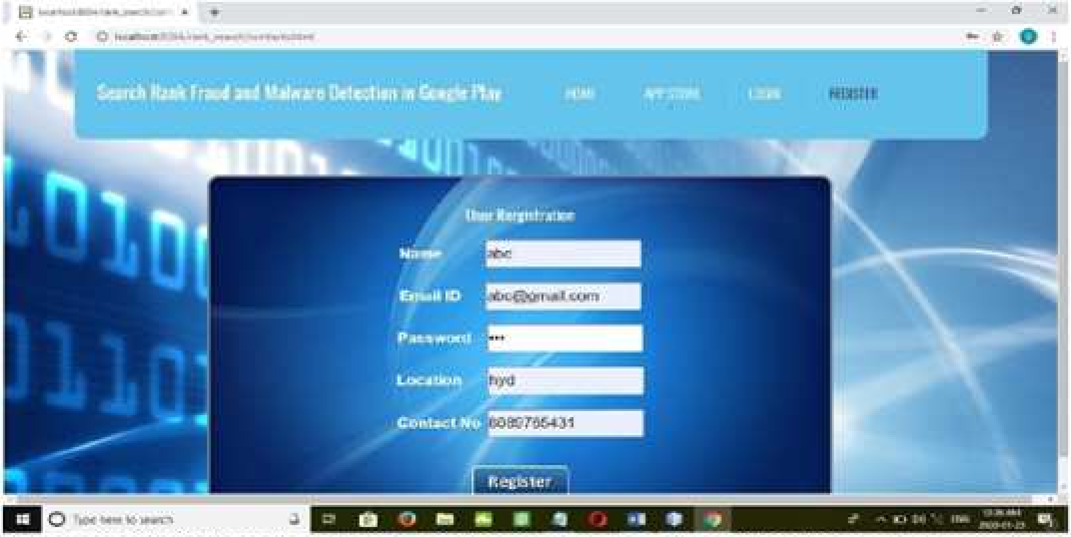


Figure 2: System Architecture

5. Results:



User Registration

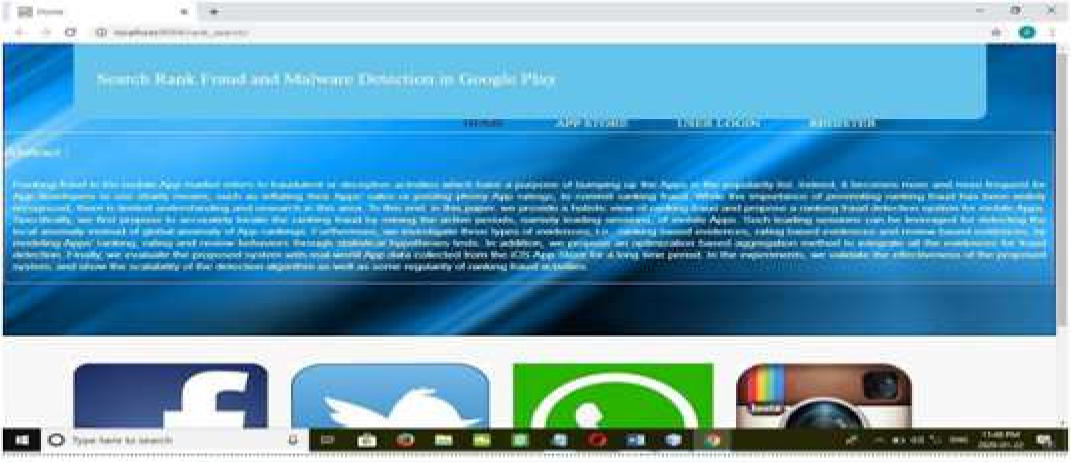
Name abc

Email ID abc@gmail.com

Password ***

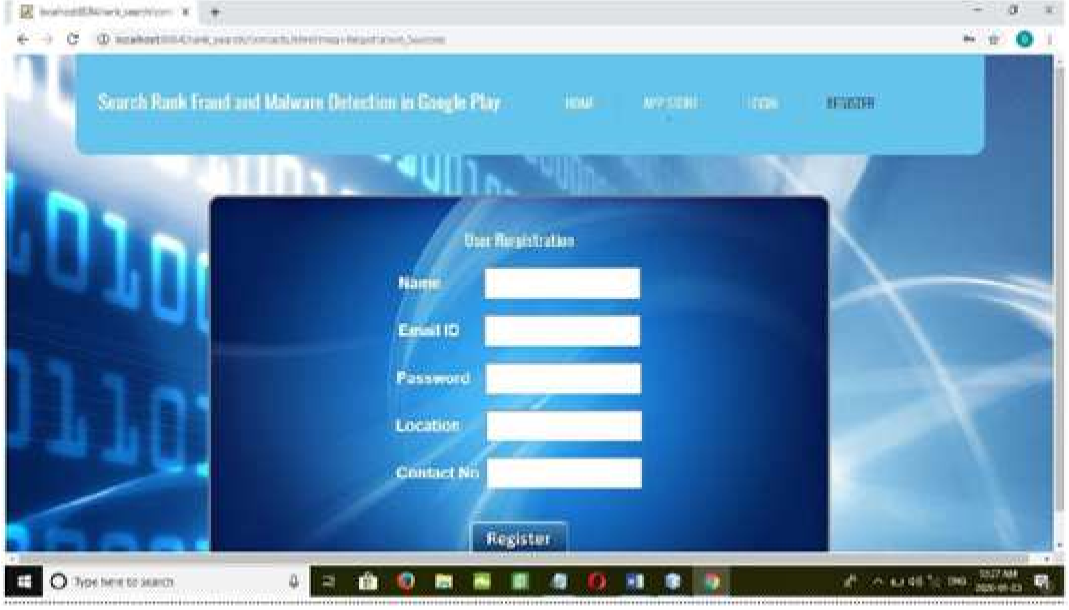
Location hyd

Contact No 8080765431



Abstract

Ranking fraud in the mobile App market refers to fraudulent or deceptive activities which have a purpose of bumping up the Apps in the popularity list. Indeed, it becomes more and more frequent for App developers to use shady means, such as inflating their Apps' sales or posting phony App ratings, to commit ranking fraud. While the importance of preventing ranking fraud has been widely recognized, there is limited understanding and research in this area. To this end, in this paper, we provide a holistic view of ranking fraud and propose a ranking fraud detection system for mobile Apps. Specifically, we first propose to accurately locate the ranking fraud by mining the active periods, namely leading sessions, of mobile Apps. Such leading sessions can be leveraged for detecting the local anomaly instead of global anomaly of App rankings. Furthermore, we investigate three types of evidences, i.e., ranking based evidences, rating based evidences and review based evidences, by modeling Apps' ranking, rating and review behaviors through statistical hypotheses tests. In addition, we propose an optimization based aggregation method to integrate all the evidences for fraud detection. Finally, we evaluate the proposed system with real-world App data collected from the iOS App Store for a long time period. In the experiments, we validate the effectiveness of the proposed system, and show the scalability of the detection algorithm as well as some regularity of ranking fraud activities.



User Registration

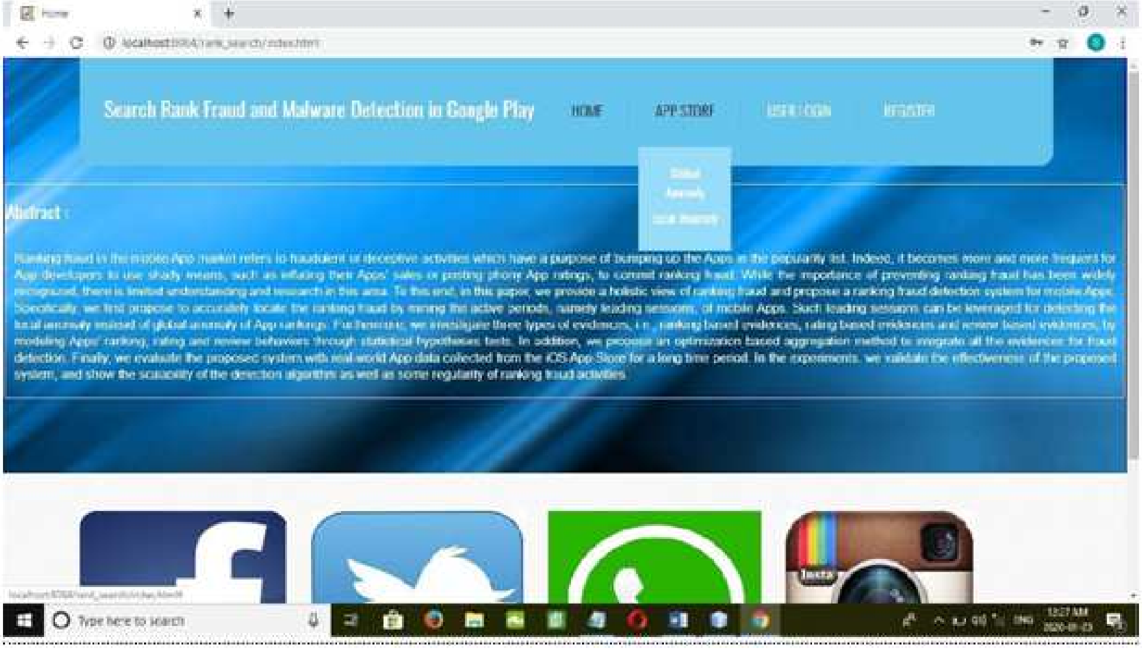
Name

Email ID

Password

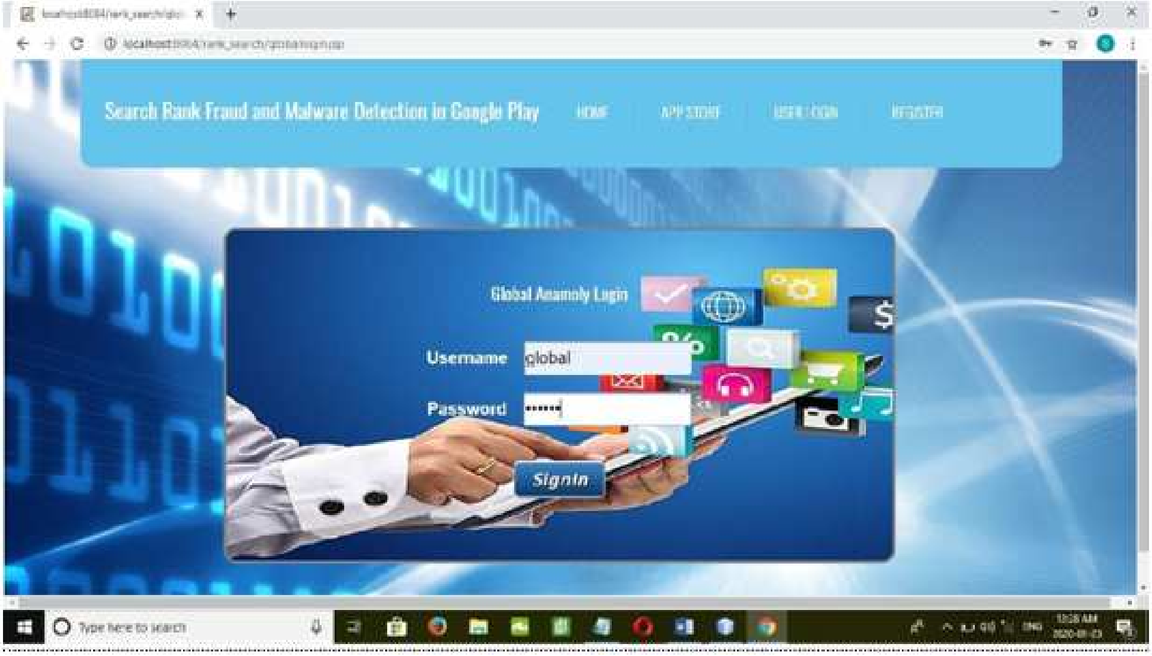
Location

Contact No


Home
localhost:8084/rank_search/index.html
Search Rank Fraud and Malware Detection in Google Play
HOME
APP STORE
USER LOGIN
REGISTER
Global Anomaly
Local Anomaly
Type here to search

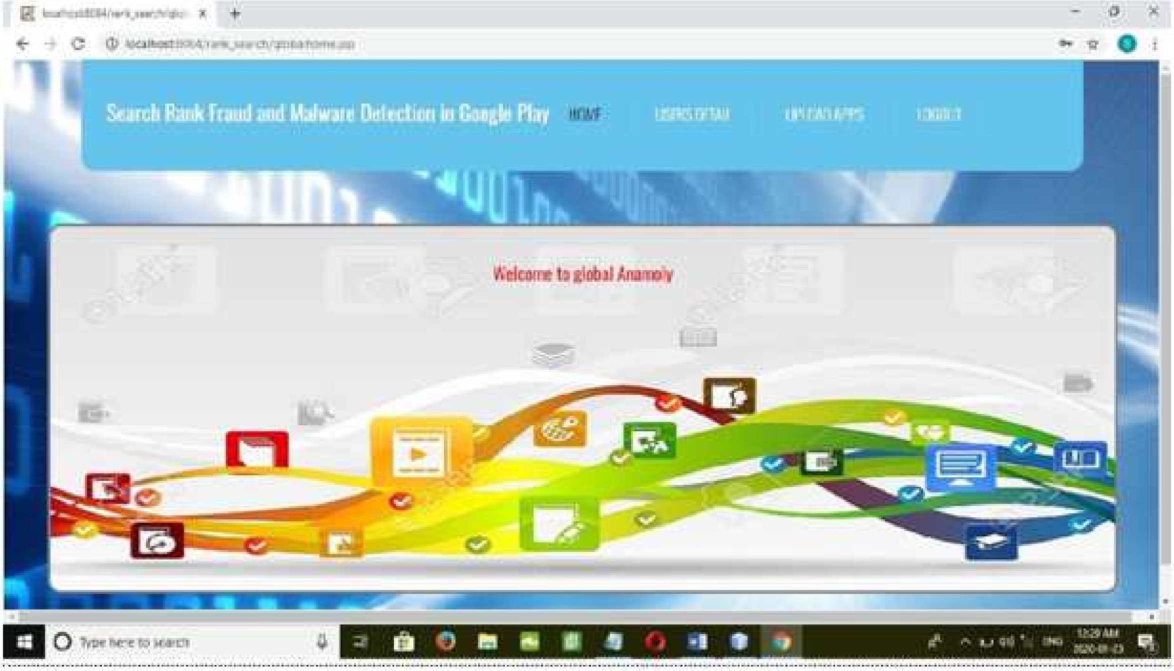
Abstract :

Ranking fraud in the mobile App market refers to fraudulent or deceptive activities which have a purpose of bumping up the Apps in the popularity list. Indeed, it becomes more and more frequent for App developers to use shady means, such as inflating their Apps' sales or posting phony App ratings, to commit ranking fraud. While the importance of preventing ranking fraud has been widely recognized, there is limited understanding and research in this area. To this end, in this paper, we provide a holistic view of ranking fraud and propose a ranking fraud detection system for mobile Apps. Specifically, we first propose to accurately locate the ranking fraud by mining the active periods, namely leading sessions, of mobile Apps. Such leading sessions can be leveraged for detecting the local anomaly instead of global anomaly of App rankings. Furthermore, we investigate three types of evidences, i.e., ranking based evidences, rating based evidences and review based evidences, by modeling Apps' ranking, rating and review behaviors through statistical hypotheses tests. In addition, we propose an optimization based aggregation method to integrate all the evidences for fraud detection. Finally, we evaluate the proposed system with real-world App data collected from the iOS App Store for a long time period. In the experiments, we validate the effectiveness of the proposed system, and show the scalability of the detection algorithms as well as some regularity of ranking fraud activities.

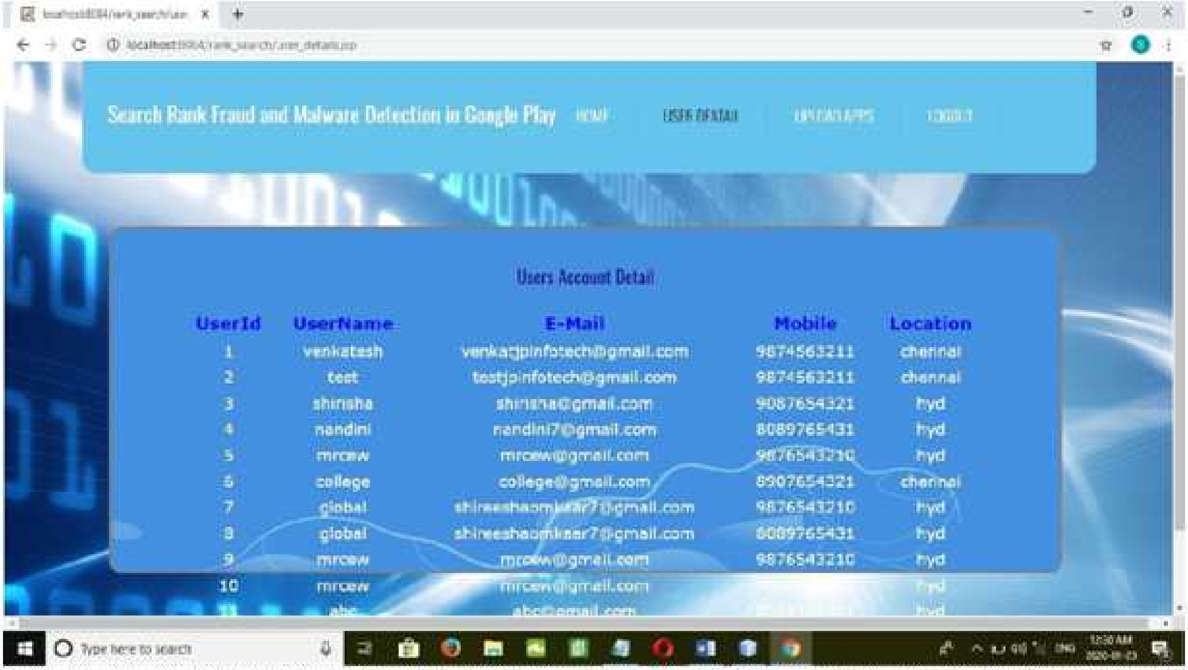

localhost:8084/rank_search/globalsignin.jsp
Search Rank Fraud and Malware Detection in Google Play
HOME
APP STORE
USER LOGIN
REGISTER
Global Anamoly Login
SignIn
Type here to search

Username global

Password ••••••

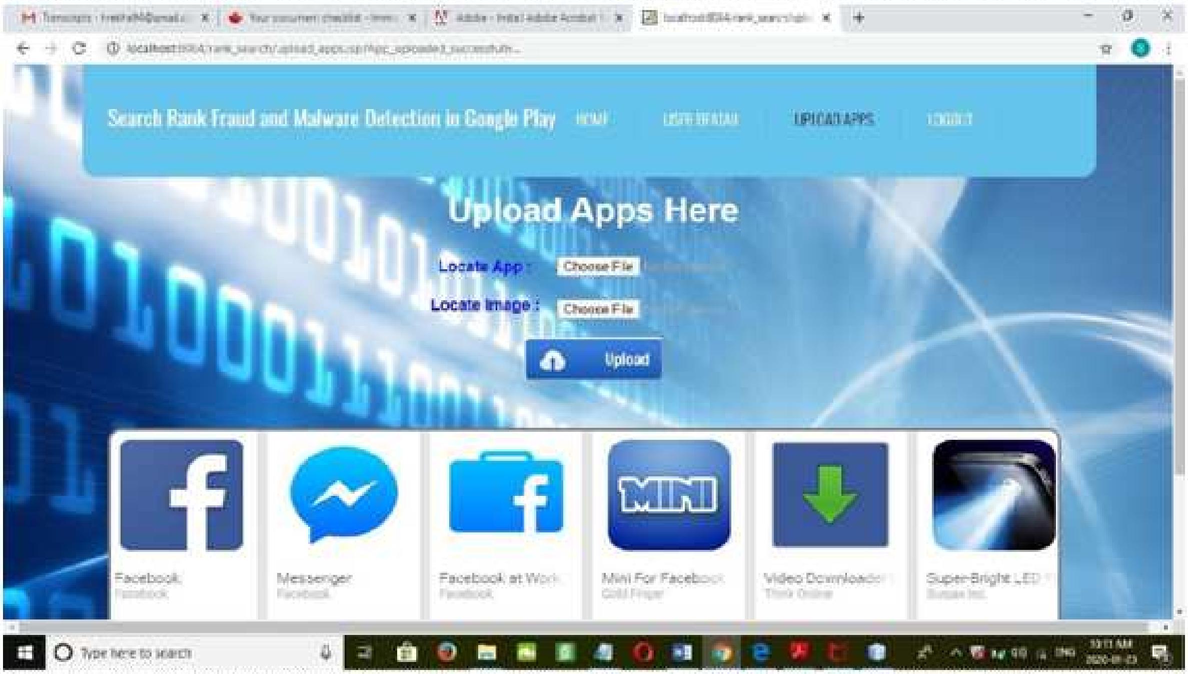

localhost:8084/rank_search/globalhome.jsp
Search Rank Fraud and Malware Detection in Google Play
HOME
USERS DETAIL
UPLOAD APPS
LOGOUT
Type here to search

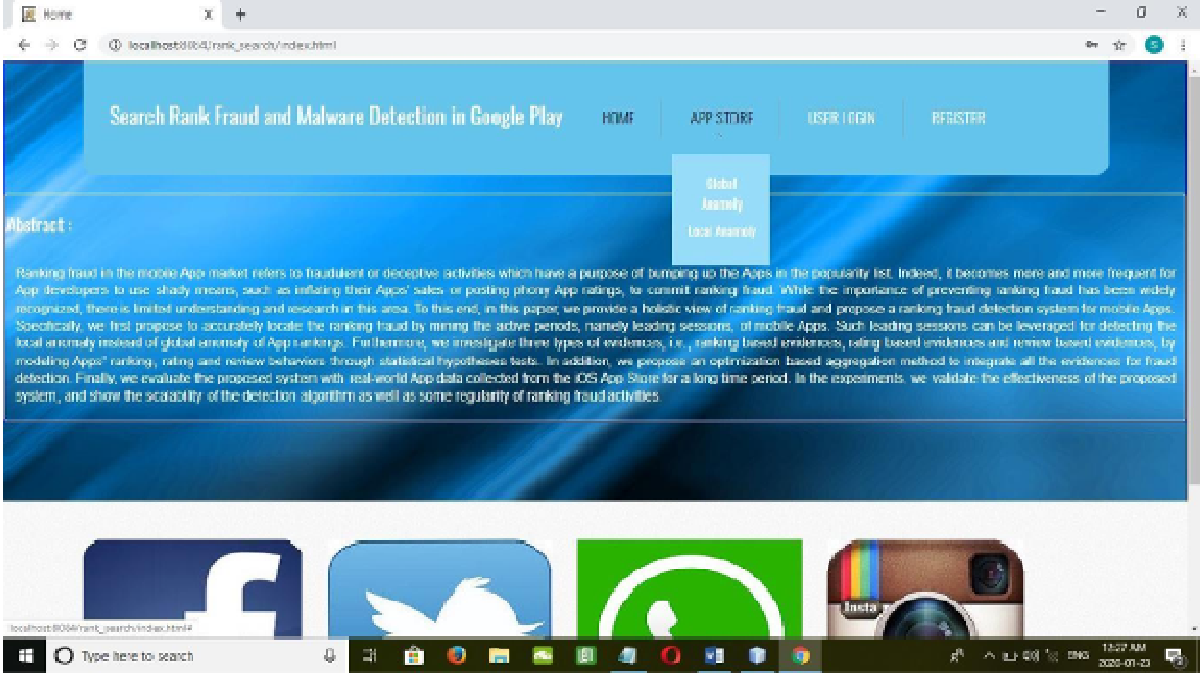
Welcome to global Anamoly


localhost:8084/rank_search/user_details.jsp
Search Rank Fraud and Malware Detection in Google Play
HOME
USER DETAIL
UPLOAD APPS
LOGOUT
Type here to search

Users Account Detail

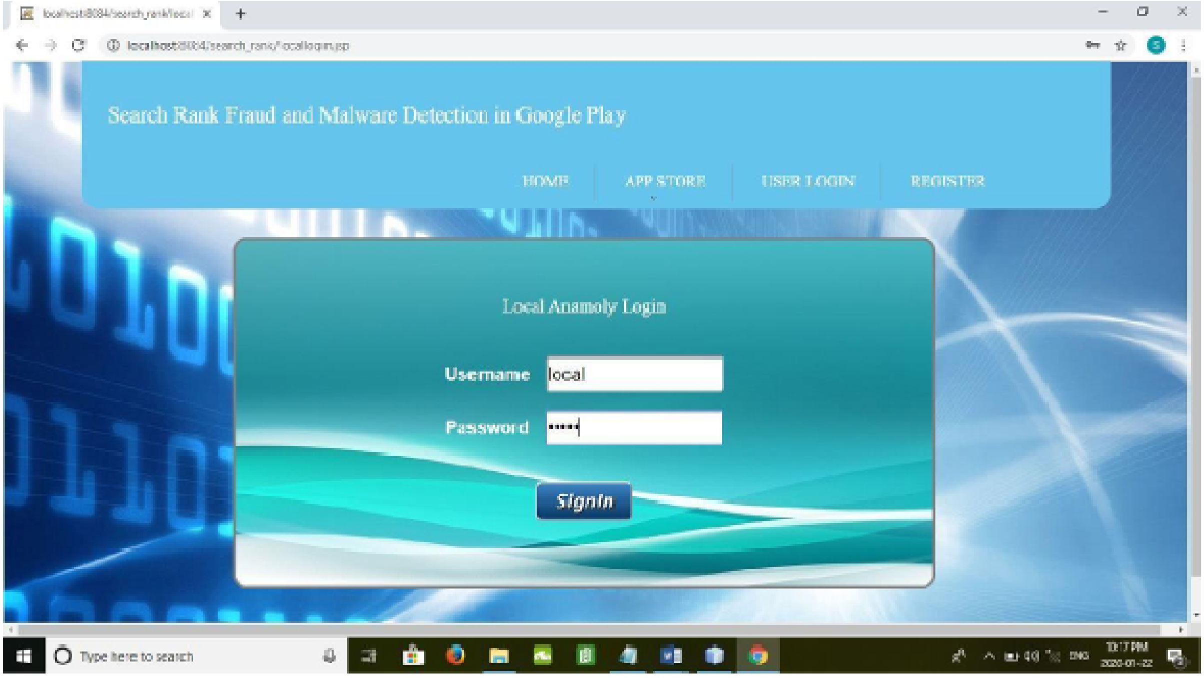
UserId	UserName	E-Mail	Mobile	Location
1	venkatesh	venkatjpinfotech@gmail.com	9874563211	chennai
2	test	testjpinfotech@gmail.com	9874563211	chennai
3	shirisha	shirisha@gmail.com	9087654321	hyd
4	nandini	nandini7@gmail.com	8089765431	hyd
5	mrcew	mrcew@gmail.com	9876543210	hyd
6	college	college@gmail.com	8907654321	chennai
7	global	shireeshaomkaar7@gmail.com	9876543210	hyd
8	global	shireeshaomkaar7@gmail.com	8089765431	hyd
9	mrcew	mrcew@gmail.com	9876543210	hyd
10	mrcew	mrcew@gmail.com	[illegible]	hyd
11	abc	abc@gmail.com	[illegible]	hyd




Home
localhost:8084/rank_search/index.html
Search Rank Fraud and Malware Detection in Google Play
HOME
APP STORE
USER LOGIN
REGISTER
Global Anomaly
Local Anomaly
Insta
Type here to search

Abstract :

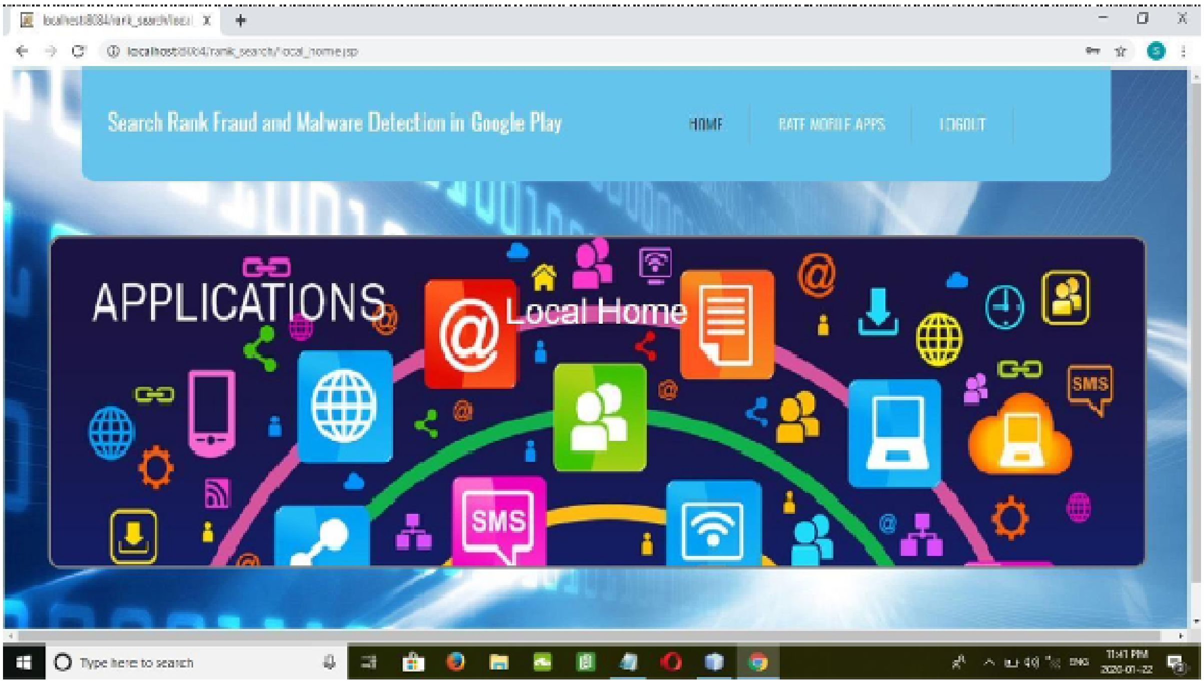
Ranking fraud in the mobile App market refers to fraudulent or deceptive activities which have a purpose of bumping up the Apps in the popularity list. Indeed, it becomes more and more frequent for App developers to use shady means, such as inflating their Apps' sales or posting phony App ratings, to commit ranking fraud. While the importance of preventing ranking fraud has been widely recognized, there is limited understanding and research in this area. To this end, in this paper, we provide a holistic view of ranking fraud and propose a ranking fraud detection system for mobile Apps. Specifically, we first propose to accurately locate the ranking fraud by mining the active periods, namely leading sessions, of mobile Apps. Such leading sessions can be leveraged for detecting the local anomaly instead of global anomaly of App rankings. Furthermore, we investigate three types of evidences, i.e., ranking based evidences, rating based evidences and review based evidences, by modeling Apps" ranking, rating and review behaviors through statistical hypotheses tests. In addition, we propose an optimization based aggregation method to integrate all the evidences for fraud detection. Finally, we evaluate the proposed system with real-world App data collected from the iOS App Store for a long time period. In the experiments, we validate the effectiveness of the proposed system, and show the scalability of the detection algorithm as well as some regularity of ranking fraud activities



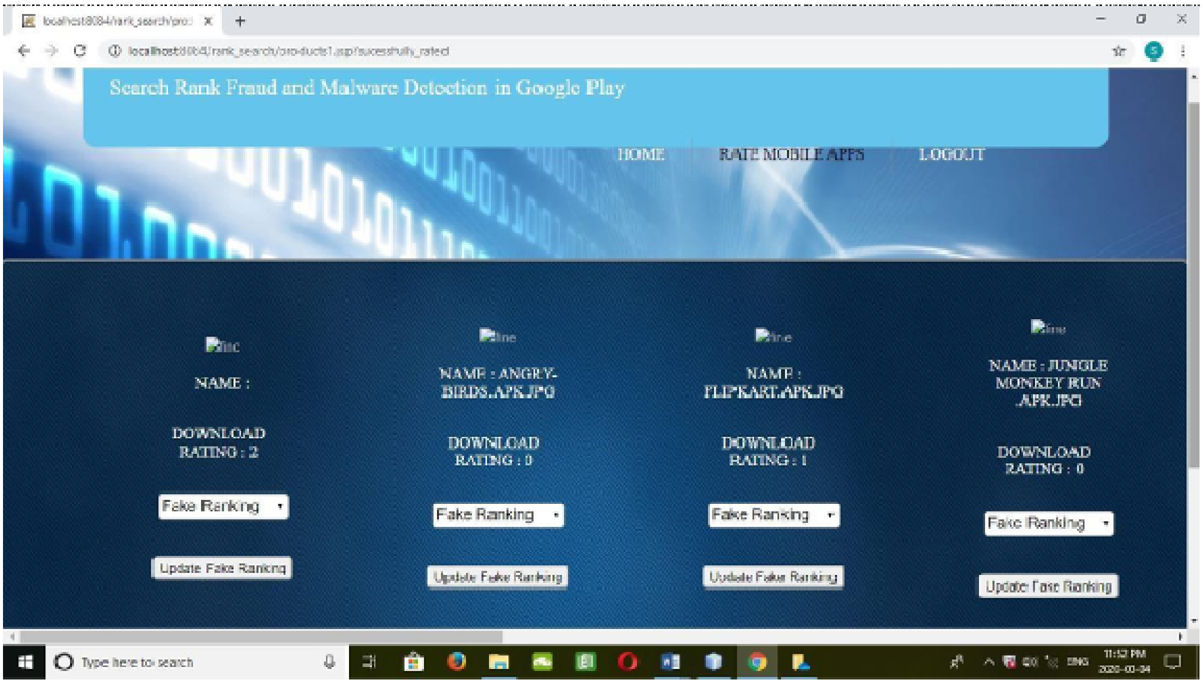
localhost:8084/search_rank/localogin.jsp
Search Rank Fraud and Malware Detection in Google Play
HOME
APP STORE
USER LOGIN
REGISTER
Local Anamoly Login
SignIn
Type here to search

Username local

Password •••••

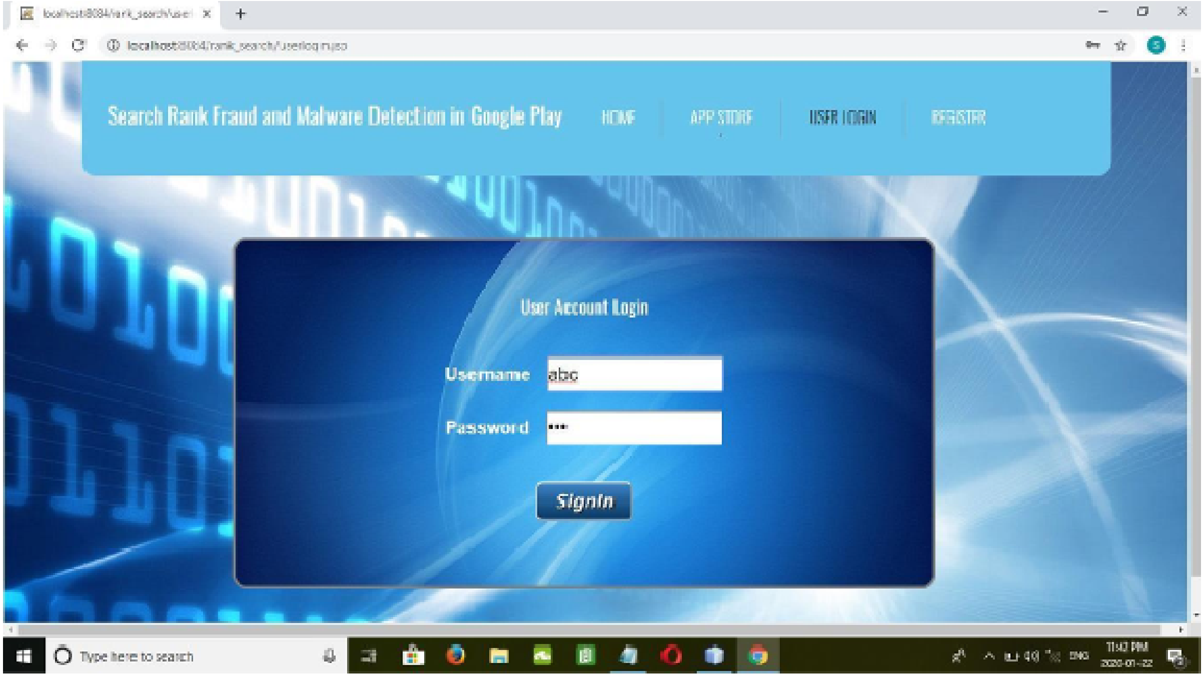


localhost:8084/rank_search/local_home.jsp
Search Rank Fraud and Malware Detection in Google Play
HOME
RATE MOBILE APPS
LOGOUT
APPLICATIONS
Local Home
SMS
Type here to search



localhost:8084/rank_search/products1.jsp?sucesshully_rated
Search Rank Fraud and Malware Detection in Google Play
HOME
RATE MOBILE APPS
LOGOUT
Update Fake Ranking
Type here to search

NAME :	NAME : ANGRY-BIRDS.APK.JPG	NAME : FLIPKART.APK.JPG	NAME : JUNGLE MONKEY RUN APK.JPG
DOWNLOAD RATING : 2	DOWNLOAD RATING : 0	DOWNLOAD RATING : 1	DOWNLOAD RATING : 0
Fake Ranking	Fake Ranking	Fake Ranking	Fake Ranking

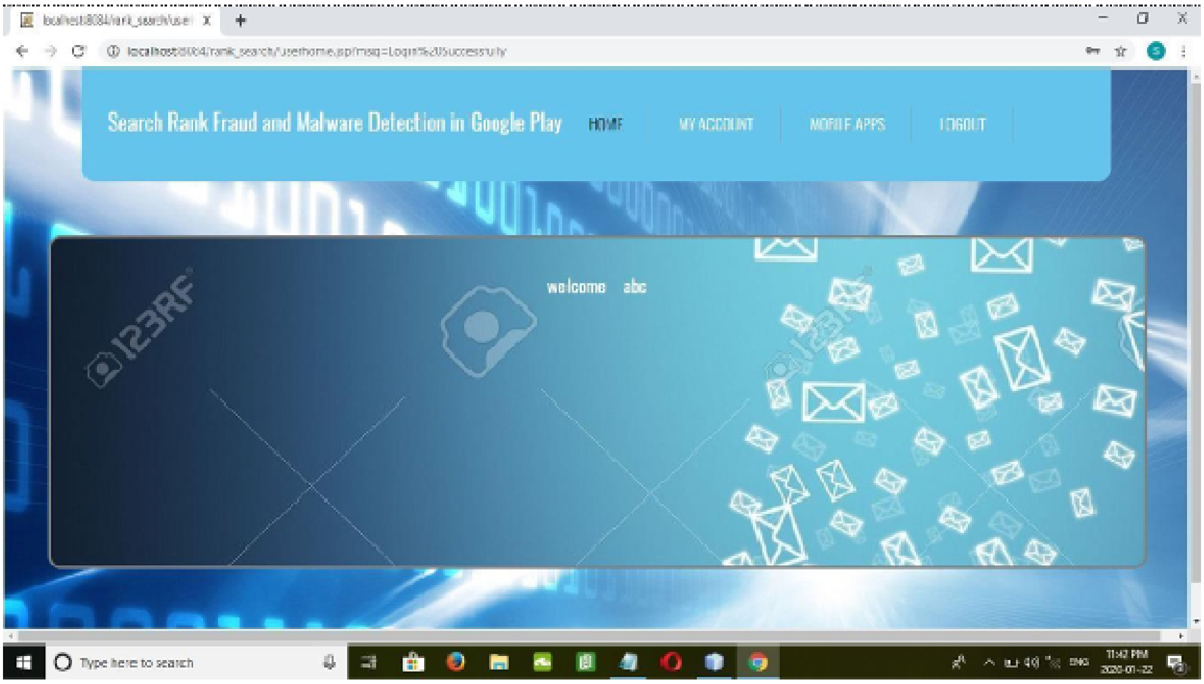

localhost:8084/rank_search/userlogin.jsp
Search Rank Fraud and Malware Detection in Google Play
HOME
APP STORE
USER LOGIN
REGISTER
Type here to search

User Account Login

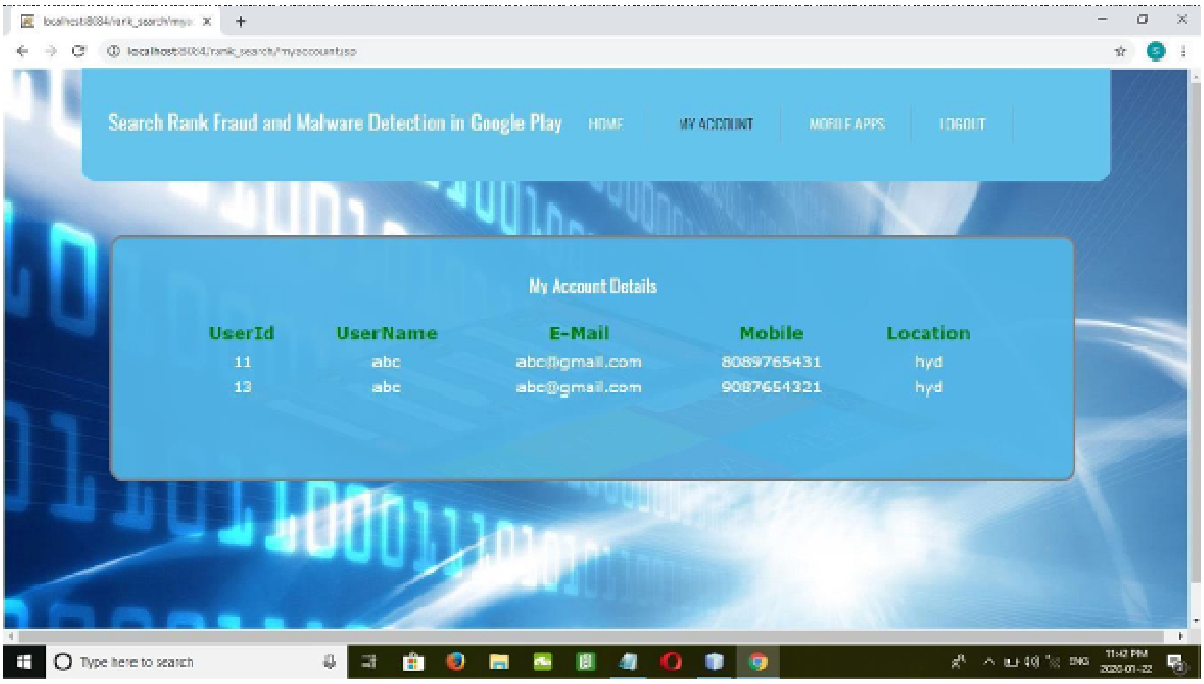
Username: abc

Password: •••

SignIn

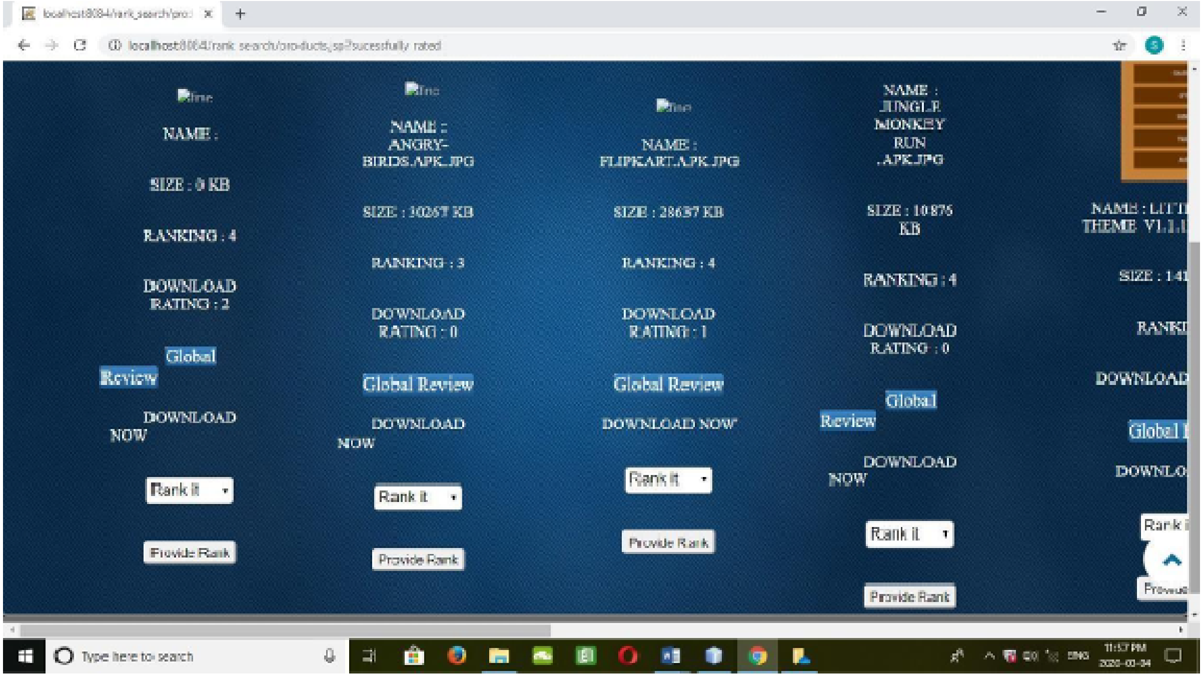

localhost:8084/rank_search/userhome.jsp?msg=Login%20Successfully
Search Rank Fraud and Malware Detection in Google Play
HOME
MY ACCOUNT
MOBILE APPS
LOGOUT
Type here to search

welcome abc


localhost:8084/rank_search/myaccount.jsp
Search Rank Fraud and Malware Detection in Google Play
HOME
MY ACCOUNT
MOBILE APPS
LOGOUT
Type here to search

My Account Details

UserId	UserName	E-Mail	Mobile	Location
11	abc	abc@gmail.com	8089765431	hyd
13	abc	abc@gmail.com	9087654321	hyd



localhost:8084/rank_search/products.jsp?sucessfully rated

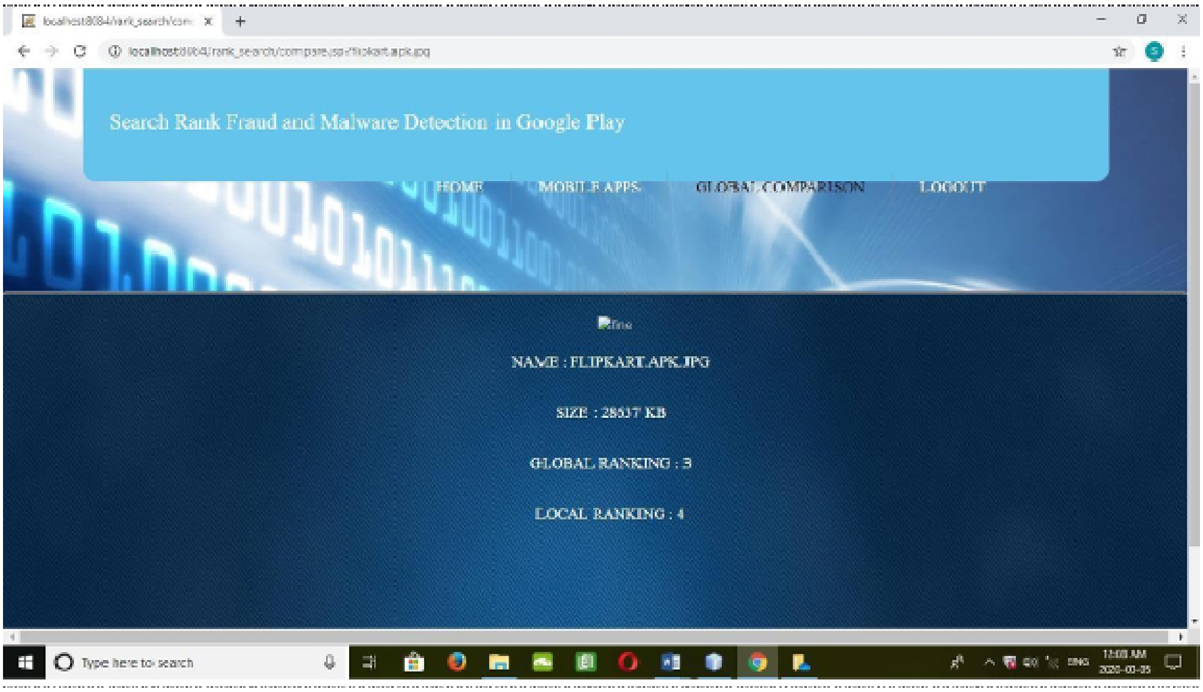
NAME :
SIZE : 0 KB
RANKING : 4
DOWNLOAD RATING : 2

NAME : ANGRY-BIRDS.APK.JPG
SIZE : 30267 KB
RANKING : 3
DOWNLOAD RATING : 0

NAME : FLIPKART.APK.JPG
SIZE : 28637 KB
RANKING : 4
DOWNLOAD RATING : 1

NAME : JUNGLE MONKEY RUN .APK.JPG
SIZE : 10875 KB
RANKING : 4
DOWNLOAD RATING : 0

NAME : LITT THEME V1.1.
SIZE : 141



localhost:8084/rank_search/compare.jsp?flipkart.apk.jpg

Search Rank Fraud and Malware Detection in Google Play

NAME : FLIPKART.APK.JPG
SIZE : 28637 KB
GLOBAL RANKING : 3
LOCAL RANKING : 4

6. Conclusion:

We have introduced FairPlay, a system to detect both fraudulent and malware Google Play apps. Our experiments on a newly contributed longitudinal app dataset, have shown that a high percentage of malware is involved in search rank fraud; both are accurately identified by FairPlay. In addition, we showed FairPlay's ability to discover hundreds of apps that evade Google Play's detection technology, including a new type of coercive fraud attack.

7. 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] Gang Wang, Christo Wilson, Xiaohan Zhao, Yibo Zhu, Manish Mohanlal, Haitao Zheng, and Ben Y. Zhao. Serf and Turf: Crowdturfing for Fun and Profit. In Proceedings of ACM WWW. ACM, 2012.