ISSN XXXX XXXX © 2018 IJESC

Research Article Volume 8 Issue No.4

App Store with Counterfeit Activity Detection and Restriction System

H.Madhuvanthi[1], R.Nirmala Devi[2], N.Nandhini[3], J.Geetha Priya[4]
UG Scholar[1, 2, 3], Assistant Professor[4]
Department of CSE
RMD Engineering College, India

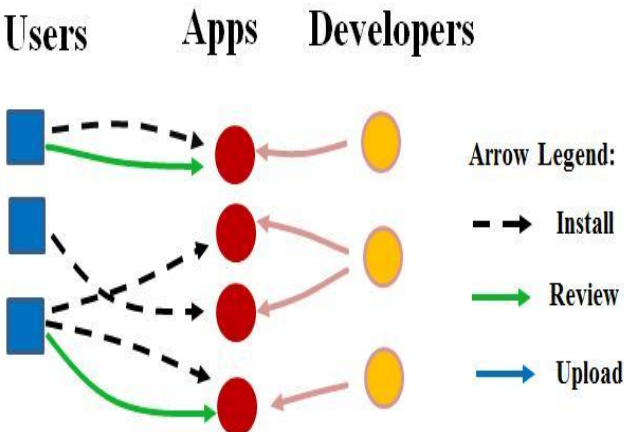
Abstract:
The counterfeit activities in the mobile App store refer to fraudulent or deceptive activities which have a bourn of raising up the apps in the popularity list. On the other hand, it becomes more frequent for people who develop apps to use devious means, toincrease their Apps' sales by posting forged App ratings to commit ranking barratry. Whereas the significance of hampering ranking fraud has been widely recognized, but there is only limited understanding and research in this area. In the end, this paper provides a comprehensive view of ranking guile. It also proposes a detection system for fraud ranking for mobile applications. Specifically, we first propose to accurately locate the ranking fraud by scooping the active periods, namely leading sessions of mobile Apps. And these leading sessions can be utilized for finding the anomaly which is local instead of the anomaly which is global in App rankings. And also we try to provide three types of evidences, such as evidences based on ranking, rating and reviews by casting Apps' ranking, rating and review behaviors through statistical hypotheses tests. And also we propose a method called optimization based aggregation to integrate all the evidences for graft detection.

INTRODUTION

At present there are more than 5.3million mobile applications on the biggest mobile app stores: And the most known examples are Apple's App Store and Google Play Store. These huge stores never stopped growing exponentially.The competition to achieve good reputation on these stores is still a challenge for all the developers and marketers [9]-[10]. The devices are kept safe and secured using Google Play Protect which runs a safety check on apps from the Google Play Store before you download them [1]. It also restricts your device from downloading potentially harmful apps from other resources. Malware is the common name for those harmful apps. It detects the likely harmful apps, warns you and also removes them from your device. Google Play Protect checks apps when you download them. It also periodically scans your device. If those apps are found running it force stops them. It also notifies you about the apps that are harmful to your device. One can remove them by tapping the uninstall option shown on the notification. And in some scenarios the harmful apps are removed automatically and shown as a notification to the user [3]-[5].Security status of your apps are checked regularly using Google Play Protect on your device. Your Android device'sGoogle Play store app is opened and turn on or off the Google Play Protect option. By default it is turned on and if needed it can be turned off. But it is always recommended to keep the Google Play Protect on for security reasons .Even it is kept on, the process of detecting malware is not always successful [2]. For example, the Bouncer system is used by the Google Play to remove malware [11]. Out of 7,756 apps in Google Play total 12% i.e.948 of apps were flanked by at least one anti-virus tool and 2% i.e.150 of them were identified as malware by at least 10 tools[12].Earlier these mobile malware detection work is done by dynamically analyzing the app executables and also doing static analysis of code and permissions. But recently it is found that these anti-virus tools are not secure enough to restrict those malware. Hereby, we try to track both search rankfraud activities and malware troubling in Google Play Store.

SYSTEM DESIGN AND IMPLEMENTATION

The algorithm designed will give credits to the applications based on their download counts and also rank them according to it. And if the app is downloaded once and uninstalled after some time it will have a negative impact on its rankings. And hence the count of downloads is the one which boosts the app's rankings .Reviews and ratings also play a vital roles in the algorithm. It decides the global rating of your app in average. Similarly the Play Store always tries to provide the best quality content to their users.An app with 5 star will rank better than an app with 2 star The ratings will provide confidence to the users to download your app and hence boosting your rank. Sometimes the ranking is also done based on how frequently your app is opened and used. Some users may download your app and never use it which will never raise your ranks on the leader board. Apple always wants its app store to provide updated content to its users. Thus, the algorithm usually favors the apps that are regularly updated. Your app should also rank high on the relevant keywords. Hence it is important to find the most prevailing keywords for your app. It should be potent in terms of relevance, competition and volume. And these keywords must be included into your app's metadata field.



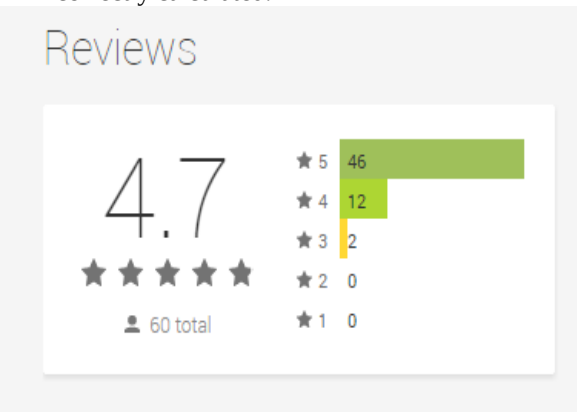
It also introduces a graph based approach to tackle the spam based on opinion of the users. Ye and Akoglu quantify the chance of a product to be a spam campaign target, then cluster spammers on a 2-hop subgraph induced by the products with the highest chance values. Akoglu et al framed a fraud detection system as a signed network classification problem and tried to classify users and products, whichformed a network which is bipartite using analgorithm that is propagation-based.FairPlay's relational approach differs from other approaches as it finds apps reviewed in a regular time interval, by bunch of users with a record of reviewing apps in common. And then it integrates the results of this approach with behavioral and linguistic clues, extracted from longitudinal app data [13]-[14].And thereby it detects both search rank fraud and malware apps. We accentuate that search rank fraud detection system goes far beyond opinion spam, as it ranks apps not only based on reviews but also based on download counts, install events and ratings.

EXISTING SYSTEM

The mobile Apps numbers had been increasing in past few years due to the development in the technology field. For example, as of the end of April 2013, there are more than 1.3 million Apps at Apple's App store and Google Play. To restorative the development of mobile Apps, many App stores launched daily App leader boards, which signify the chart rankings of most popular Apps. Indeed, the App leader board is one of the most important ways for promoting mobile Apps. A higher rank on the leader board usually leads to a huge number of downloads and million dollars in revenue. Therefore App developers promotes many advertising campaigns in order to have their Apps ranked as high as possible in such App leader boards.

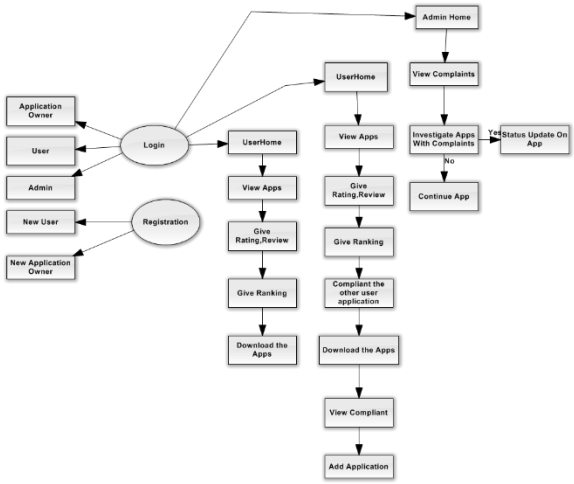
Disadvantages:

- They allow fake applications in the app store.
- If the user couldn't understand the fake apps then the user also give the reviews in the fake application.
- Exact review or ratings or ranking percentage are not correctly calculated.



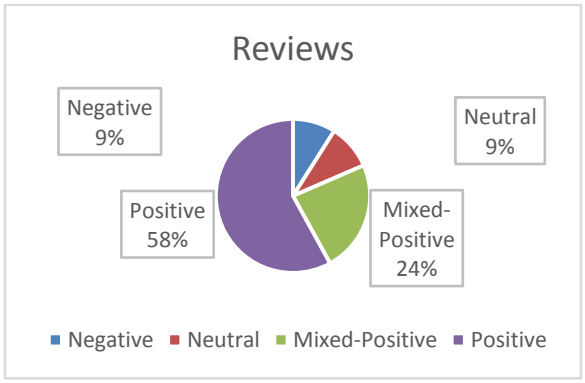
PROPOSED SYSTEM

To detect the fraudulent app in the app store we have contrived a method calledranking fraud detection system for mobile AppsWe identify several important challenges in this existing system. First, ranking fraud does not always happen in the whole life cycle of an App, so we need to detect the time when fraud happens. Such provocation can be regarded as detecting the local anomaly instead of detecting it has global anomaly of mobile Apps. Second, due to hike in mobile Apps, it is difficult to manuallytag ranking fraud for each App, so it is important to have a extensible way to automatically detect ranking fraud without using any benchmark information.Finally, due to the lively nature of chart rankings, it is tough to identify and confirm the evidences linked to ranking fraud, which motivates us to find some insinuated fraud patterns of mobile Apps as evidences. We first propose a simple yet effective algorithm to identify the leading sessions of each App based on all its previous ranking records.



Advantages:

- They allow fake application but user see the status of the application and they know the application is fake.
- The user give the review or rating or ranking are correctly calculated so, the application is worth or not.



SYSTEM CONFIGURATION:

H/W SYSTEM CONFIGURATION:

- Processor - Pentium –III
- Speed - 1.1 GHz
- RAM - 256 MB (min)
- Hard Disk - 20 GB
- Floppy Drive - 1.44 MB
- Key Board - Standard Windows Keyboard
- Mouse - Two or Three Button Mouse
- Monitor - SVGA

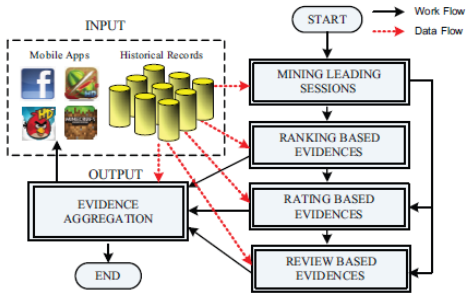
S/W SYSTEM CONFIGURATION:

- Operating System - Windows95/98/2000/XP
- Application Server -Tomcat5.0/6.X
- Front End - HTML, Java, Jsp
- Scripts - JavaScript.
- Server side Script - Java Server Pages.
- Database - MySQL
- Database Connectivity - JDBC.

METHODOLOGY

RESTRICT FRAUDULENT REVIEWS

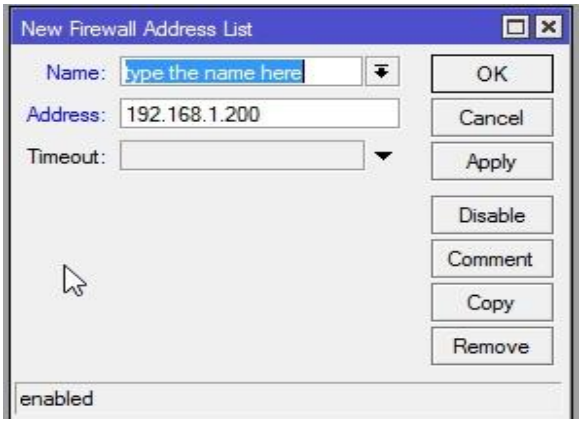
If you are a Google Apps user, you can always restrict the review to accept entries only from users who are authenticate by this domain and the response spreadsheet will then record the username of the review submitter. However if you have a regular Gmail / Google Account, you have another option now to prevent multiple review submissions from the same user. When the unique option is enabled for a review, respondents will have to sign-in with their Google account to access the form. Their email address won't be recorded in the response sheet but detecting IP address the same user will not allow another entry from the same Google Account. Even the same user who sign in with multiple accounts can be detected with the systems IP address and the download option can be disabled when multiple downloads happens from the same system. If someone tries to download the same application again from the same IP address, a warning message will be displayed saying "You are not allowed to download. You can only download it only up to certain given condition. Try contacting the owner of the application if you think this is a mistake". This is the easiest method where it does not put your reviews out of reach to the people who do not have Google Account or those who are sceptical of associating the email address with their review entry (though this association is complete).



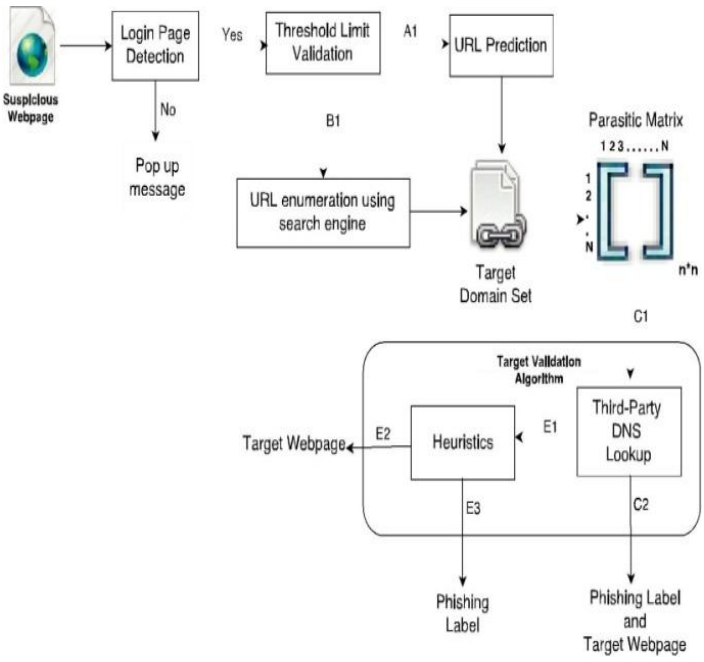
ARCHITECTURE DIAGRAM

PHISING SYSTEM

The method proposed in this paper detects phishing web pages and its target domain by working on all the anticipated lacunas. Moreover, this method identifies legitimacy of the suspicious web pages without depending completely on the external information repositories such as search engines, and other third party data sources. Here, we take the suspicious webpage under scrutiny; visit its links up to level two to check for the possible number of domains that can be reached. This domain count value determines the method to be followed in generating the Target Do-main Set. We then formulate a cost matrix based on the relation-ships that exist between the domains in the Target Domain Set. This cost matrix in turn exposes the strength of feigning relation-ships which exist between the domains in the Target Domain Set and webpage the user visits. The domain with higher in degree feign relationship will be considered as a target domain. The tar-get domain is further validated using Target Validation (TVD) algorithm to ensure its correctness. Finally, the legitimacy of the web-page will be determined by comparing it with the confirmed tar-get domain. Thus, as the content of the suspicious webpage is the only subject on which our proposed methodology is built on, neither prior knowledge about the site is required nor does it require the training data.



ENABLING FIREWALL FOR PHISING



PHISING PROCESS

CONCLUSION

Hereby we have proposed a system to detect both fraudulent and malware apps in the app store. Our experiments on a

newly contributed longitudinal app, have shown that a high percentage of malware is involved in these kind of counterfeit activities; both are accurately identified by our detection system. In addition, we showed Fair Play's ability to discover hundreds of apps that escape from Google Play's detection technology using Bouncers system.

REFERENCES

[1] Google Play. https://play.google.com/.

[2] 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] Freelancer. http://www.freelancer.com.

[8] Fiverr. https://www.fiverr.com/.

[9] BestAppPromotion. www.bestreviewapp.com/.

[10] Gang Wang, Christo Wilson, Xiaohan Zhao, Yibo Zhu, Manish Mohanlal, Haitao Zheng, and Ben Y. Zhao. Serf and Turf: Crowd-turfing for Fun and Profit. In *Proceedings of ACM WWW*. ACM, 2012.

[11] Jon Oberheide and Charlie Miller. Dissecting the Android Bouncer. *SummerCon2012, New York*, 2012.

[12] VirusTotal - Free Online Virus, Malware and URL Scanner. https: //www.virustotal.com/, Last accessed on May 2015.

[13] Iker Burguera, Urko Zurutuza, and Simin Nadjm-Tehrani. Crow-droid: Behavior-Based Malware Detection System for Android. In *Proceedings of ACM SPSM*, pages 15–26. ACM, 2011.

[14] 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