RESEARCH ARTICLE OPEN ACCESS

SEARCH POSITION SCAM AND MALWARE DISCOVERY IN GOOGLE PLAY

S Amaresan M.C.A., M.Phil, M.E.,*, C Akalya**
*(H.O.D., Assistant Professor, Department of Computer Science, PONNAIYAH RAMAJAYAM INSTITUTE OF SCIENCE AND TECHNOLOGY PRIST University, and THANJAVUR
Email: amaresan.cse.1974@gmail.com)
** (M.C.A., Scholar Department of Computer Science, PONNAIYAH RAMAJAYAM INSTITUTE OF SCIENCE AND TECHNOLOGY PRIST University, and THANJAVUR
Email: Akalyapandyan@gmail.com)

----------**********----------

Abstract:

The use of mobile devices including Tablets, Smart watch, and note books are increasing day by day. Android has the major share in the mobile application market. Android mobile applications become an easy target for the attackers because of its open source environment. Also user' ignorance the process of installing and usage of the apps. To identify fake and malware applications, all the previous methods focused on getting permission from the user and executing that particular mobile application. A malware detection framework that discovers and break traces left behind by fraudulent developers, to detect search rank fraud as well as malware in Google Play. The fraud app is detected by aggregating the three pieces of evidence such as ranking based, co-review based and rating based evidence. Additionally apply incremental learning approach to characterize a large number of data sets. It combined effectively for all the evidences for fraud detection. Detect fraud ranking in daily App leader board. Avoid ranking manipulation. Finds the better mobile app for the end user. Incremental learning approach effectively characterizes the large amount of app evidence details. In the proposed system the detecting of normal and harmful application is analysed by the **SVM Algorithm.** This system will analyse the uploaded application that are to be classifying the status which is dangerous application or normal application. The user can view the both the normal and harmful application. They can download the application after viewing the classified manner. After using the application the user can give the review on that downloaded application. By this the user can identify the application by the review given. By the given review for any application the admin will analyse the application for giving the ranking. The reviews are analysed by the **Collaborative Technique**. This proposed system will help to take the measures for the betterment of the end user.

Keywords **— Fraud, Malware detection, Framework, analysed, SVM Algorithm, Collaborative Technique, Application.**

----------**********----------

I. INTRODUCTION

In this paper the author proposed a new method to detect malware in mobile applications by examining the runtime behavior of that particular application in the mobile environment. The author proposes that unexpected behavior mobile app can vary from one application to other applications. Also, it varies from the

environment of that particular application running on different devices. The module integrates with our intrusion detection system which then analyzes and reports on the profiles. The proposed system first use reserves engineering technology to generate source code from suspicious APK files. Structure mapping component then builds structure tree of class and dependency of variables in APK file. Finally we use concept of data flow to build several threat patterns, and use them to detect mobile malware. A malware detection system is also developed which uses static analysis approach and concept of data flow. It proposes the Xposed framework to build a monitoring module that generates behavior profiles for applications. Using Xposed framework user can change the user and system application without modifying the application package (APK).Depend upon that user can set particular conditions to identify the malware in the mobile applications. The threat patterns are created manually. If new type of attack approaches are developed which have a different threat pattern, our system will not detect them. In the future, an auto threat pattern generation should be developed to detect zero day attacks. They are pretty heavy and complicated with a long time delay. The methods that are both lightweight and efficient thus can be installed in the mobile devices to realize real-time detection, are highly expected. This kind of methods can find newly generated malware initiated at app runtime during its execution. Although designing such a detection method is not easy, it is a very promising research direction. It uses this tool to detect malicious behaviour patterns using both a custom-written malware and a real one. This approach can also be generalized to detect unknown malware or expose exact application behaviour to the user.

II. OBTAINABLE SCHEME

It existing malware detection framework system that detects Google Play fraud and malware. To detect fraud and malware, it proposes the incremental learning approach to characterize the dataset. It formulates the notion of review modeling by applying Porter stemmer algorithm. This use temporal session of review post times to identify suspicious review spikes received by apps; the application evidence such as rating, ranking and review evidence will be integrated by an unsupervised evidence-aggregation method for evaluating the credibility of leading sessions from mobile Apps. The malware detection framework is scalable and can be extended with other domain generated evidence for ranking fraud detection. It identified that for the detection of the rank ranking, rating, and review based evidence are considered.

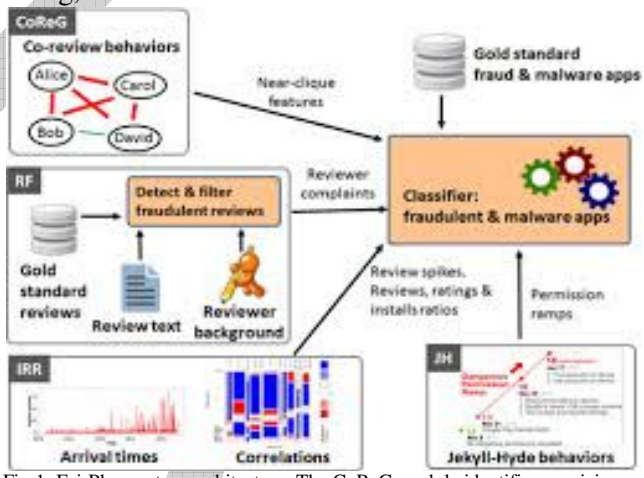

Fig 1. FairPlay system architecture. The CoReG module identifies suspicious, time related co-review behaviours. The RF module uses linguistic tools to detect suspicious behaviours reported by genuine reviews. The IRR module uses behavioural information to detect suspicious apps.The JH module identifies permission ramps to pinpoint possible Jekyll Hyde app transitions

A. DISADVANTAGES

- Google Play uses the Bouncer system to note remove malware.
- Use risk signals extracted from app permissions
- A score to measure the risk of apps, based on probabilistic generative models
- The classification of application based on the keywords is not identified.

III. PLANNED SCHEME

In the proposed system the detecting of normal and harmful application is analyzed by the **SVM Algorithm.** This system will analyze the uploaded application that are to be classifying the status which is dangerous application or normal

application. The user can view the both the normal and harmful application. They can download the application after viewing the classified manner. After using the application the user can give the review on that downloaded application. By this the user can identify the application by the review given. By the given review for any application the admin will analyze the application for giving the ranking. The reviews are analyzed by the **Collaborative Technique**. This proposed system will help to take the measures for the betterment of the end user.

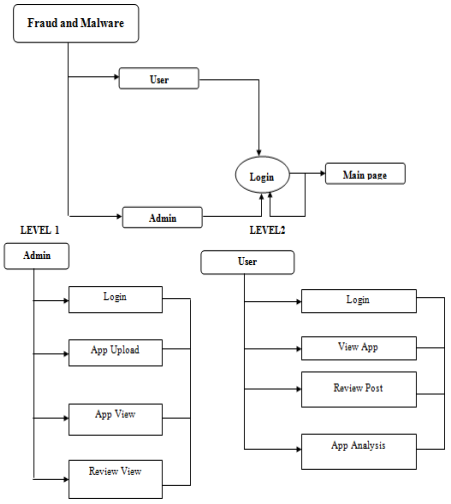

Fig 1.1 flow chart of the proposed system

B.ADVANTAGES

- Fraudulent and malicious behaviours leave behind telltale signs on app markets.
- FairPlay achieves over 97% accuracy in classifying fraudulent and benign apps, and over 95% accuracy in classifying malware and benign apps.
- FairPlay 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

IV. COMPONENTS EXPLANATION

C. ADMIN

- ➢ Login
- ➢ App Upload
- ➢ App View
- ➢ Reviews View

D. USER

- ✓ Register
- ✓ Login
- ✓ View App
- ✓ Review Post
- ✓ App Analysis

C. ADMIN

1). Login

In the login module the authenticated admin will enter the valid username and the password to enter in the home page. This module will be accessed by the authorized user who knows the password which is developed. This module will be the gateway module for the project that will help to enter the data.

2). App Upload

In this module the admin will upload the created app to analyze the categories that are in that application. By this the application is categorized on the basis of the description in the content. The app is categorized by **fetching the keywords** that are stored in the database which is harmful or not.

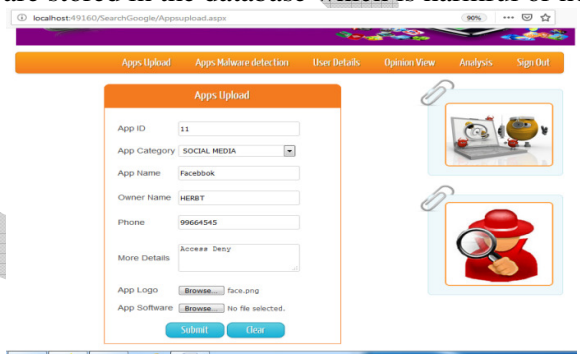

Fig 2 Upload page processing screen

3).App View

The App View module the uploaded app will be categorized by the description in the app content using the **SVM algorithm.** This application will have the normal and the harmful application that are seen by the client before downloading.

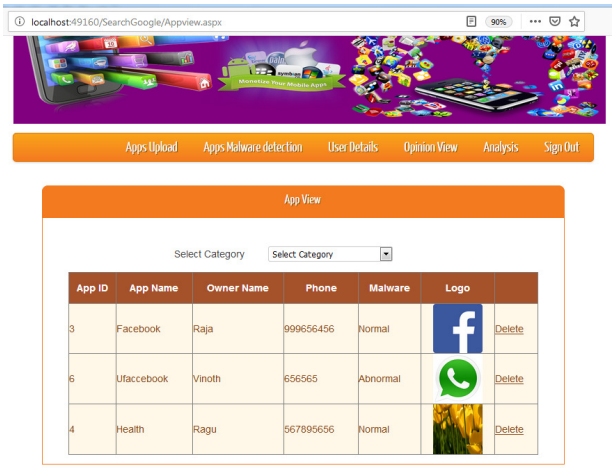

Fig 3 Application View screen

D. USER

1).Register

In the registration module the new user will register for the authentication purpose. By this registration the admin will view the user details and retrieve for the further verification. This module is the first module for the user which is the gateway for the other module

2). Login

In the login module the authenticated user will enter the valid username and the password to enter in the home page. This module will be accessed by the authorized user who knows the password which is given. This module will be the gateway module for the project that will help to enter the data.

3). View App

In this module the user can view the applications that are normal of harmful. They can know the feedback of the application by the review in the bottom of the application. This module will be the classification module in which the admin will classify the application.

4). Review Post

In the review post module the user will post the review on the applications that are downloaded while using this application. This module will help the user to give their opinion on that application.

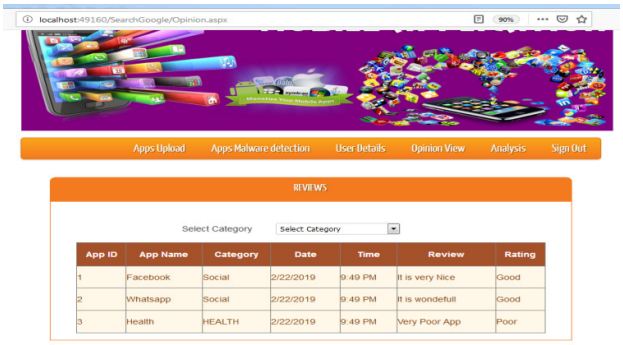

Fig 4 Applications review processing screen

5). App Analysis

In the app analysis module the user can view the app analysis on the basis of ranking with the collaborative technique by the collection of various reviews given by the end user.

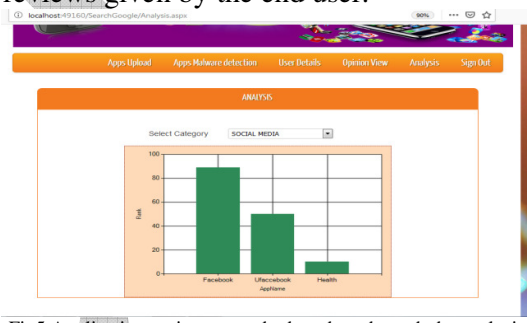

Fig5 Application review report by bar chart through the analysis

V. CONCLUSIONS

In this project developed a fraud detection system for mobile Apps. Specifically first showed that fraud happened in leading sessions and provided a method for mining leading sessions for each App from its historical ranking records. An identified that for the detection of the rank ranking, rating, and review based evidence are considered. Moreover proposed an optimization based aggregation method to integrate all the evidence for evaluating the credibility of leading sessions from mobile Apps. A unique perspective of this approach is that all the evidence can be modeled by statistical hypothesis tests, thus it is easy to be extended with other evidence from domain knowledge to detect ranking fraud. Finally validate the proposed system with extensive experiments on real-world App data collected from the Apple's App Store. Experimental results showed the

effectiveness of the proposed approach. In the future, we plan to study more effective fraud evidence and analyze the latent relationship among rating, review, and rankings. Moreover, we will extend our ranking fraud detection approach with other mobile App related services, such as mobile Apps recommendation, for enhancing user experience.

FUTURE ENHANCEMENT

To detect fraud and malware, the input parameters considered were mobile apps, permissions, and ratings. This paper proposed a technique to compare weight of the apps permission for detecting fraud apps and making their rank zero and further blocking the developer from uploading malware apps. Further, the significant improvement in the detection of malware apps and rank genuine apps with different access permissions. We demonstrated the effectiveness of the proposed technique using App Permissions dataset which is verified using weightage parameter. A significant improvement in security by blocking the malware apps in the initial stage of uploading and ranking is done effectively by using download count.

REFERENCES

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

[2] E. Siegel, "Fake reviews in Google Play and Apple App Store,"Appentive, Seattle, WA, USA, 2014.

[3] Z. Miners. (2014, Feb. 19). "Report: Malware-infected Android apps spike in the Google Play store," PC World. Available: http://www.pcworld.com/article/2099421/report-malwareinfectedandroid-apps-spike-in-the-google-play-store.html

[4] S. Mlot. (2014, Apr. 8). "Top Android App a Scam, Pulled From Google Play," PCMag. Available: http://www.pcmag.com/ article2/0,2817,2456165,00.asp

[5] D. Roberts. (2015, Jul. 8). "How to spot fake apps on the Google Play store," Fortune. Available: http://fortune.com/2015/07/08/google-play-fake-app/

[6] A. Greenberg (2012, May 23). "Researchers say they snuckmalware app past Google's 'Bouncer' Android market scanner,"Forbes Security, [Online]. Available: http://www.forbes.com/sites/andygreenberg/2012/05/23/researchers-say-they-snuckmalware-app-past-googles-bouncer-android-market-scanner/#52c8818d1041

[7] Freelancer. [Online]. Available: http://www.freelancer.com

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

[9] BestAppPromotion. [Online]. Available: www.bestreviewapp.com/

[10] G. Wang, et al., "Serf and turf: Crowdturfing for fun and profit,"in Proc. ACM WWW, 2012. [Online]. Available: http://doi.acm.org/10.1145/2187836.2187928

[11] J. Oberheide and C. Miller, "Dissecting the Android Bouncer,"presented at the SummerCon2012, New York, NY, USA, 2012.

[12] VirusTotal - free online virus, Malware and URL scanner.[Online]. Available: https://www.virustotal.com/, Last accessedon: May 2015.

[13] I. Burguera, U. Zurutuza, and S. Nadjm-Tehrani , "Crowdroid: Behavior-based Malware detection system for Android," in Proc. ACM SPSM, 2011, pp. 15–26.

[14] A. Shabtai, U. Kanonov, Y. Elovici, C. Glezer, and Y. Weiss, "Andromaly: A behavioral malware detection framework for Android devices," Intell. Inform. Syst., vol. 38, no. 1, pp. 161–190, 2012.

[15] M. Grace, Y. Zhou, Q. Zhang, S. Zou, and X. Jiang, "RiskRanker: Scalable and accurate zero-day Android malware detection," in Proc. ACM MobiSys, 2012, pp. 281–294.

[16] B. P. Sarma, N. Li, C. Gates, R. Potharaju, C. Nita-Rotaru, and I. Molloy, "Android Permissions: A Perspective Combining Risks and Benefits," in Proc. 17th ACM Symp. Access Control Models Technol., 2012, pp. 13–22.

[17] H. Peng, et al., "Using probabilistic generative models for ranking risks of Android Apps," in Proc. ACM Conf. Comput. Commun. Secur., 2012, pp. 241–252.

[18] S. Yerima, S. Sezer, and I. Muttik, "Android Malware detection using parallel machine learning classifiers," in Proc. NGMAST, Sep. 2014, pp. 37–42.

[19] Y. Zhou and X. Jiang, "Dissecting Android malware: Characterization and evolution," in Proc. IEEE Symp. Secur. Privacy, 2012, pp. 95–109. Fraud detection in social networks, [Online]. Available: https:// users.cs.fiu.edu/ carbunar/caspr.lab/socialfraud.html