A Review on Fraud and Malware Detection in Google Play

Ashwini Kidile[1] Shweta Jadhav[2] Amruta Mane[3] Sushant Borate[4] Kalpana Kadam[5]
[1,2,3,4]Student [5]Assistant Professor
[1,2,3,4,5]Department of Computer Engineering
[1,2,3,4,5]SKN Sinhgad Institute of Technology & Science, Lonavala, India

Abstract— Detection is one of the oldest areas of research. The requirement of an effective system that detects frauds effectively with zero loss exists until now. This is due to the increase in the technology, that influences both the ends; the user and the fraudster. Hence it becomes mandatory that the users need to stay a step ahead in this scenario. This paper discusses the changes that had taken place in the area of fraud detection. We have analyzed papers regarding the fraud rating detection and malware detection of application. In this proposed system time stamp of rating and reviews is considered for detecting the review and rank fraud. Malware is also detected before the time of downloading.

Key words: Android Applications, Fairplay, Fraud Rating

I. INTRODUCTION

The industrial success of android app markets like Google Play and therefore the incentive model they provide to well-liked apps, create them appealing targets for dishonest and malicious behaviors. We use behavioral data to notice real reviews from that we tend to then extract user-identified fraud and malware indicators. Review consists of a star rating move between 1-5 stars, and a few text and app developers who need to extend rating of application install that application multiple times. We introduce a system that discovers and leverages traces left behind by fraudsters, to detect each malware and apps subjected to look rank fraud. We tend to contemplate not solely malicious developers, World Health Organization transfer malware, however additionally dishonest developers. Fraudulent developers arrange to tamper with the search rank of their apps.We area unit detective work fraud rating and reviews concerning application and additionally trace the malware on the premise of installations and downloading application victimization single registration ID.Fairplay is used for organizing the analysis knowledge of application.

II. RELATED WORK

Author Ian Molloy in this paper has a tendency to exploit earlier approaches for dynamic analysis of application behavior as a method for detection malware within the mechanical man platform. The detector is embedded associate degree exceedingly overall framework for assortment of traces from an unlimited variety of real users supported crowd sourcing. Our framework has been incontestable by analyzing the information collected within the central server victimization two varieties of knowledge sets: those from artificial malware created for take a look at functions, and those from real malware found within the wild. [1]

In this paper, author developed four malicious applications, and evaluated Andromalyability to notice new malware supported samples of renowned malware. We evaluated many mixtures of anomaly detection algorithms, feature selection technique and also the variety of high options so as to seek out the mixture that yields the most effective performance in detection new malware on mechanical man. Empirical results counsel that the projected framework is effective in detection malware on mobile devices normally and on mechanical man specifically.

In this paper, author proposes a proactive theme to identify zero-day mechanical man malware. Without wishing on malware samples and their signatures, our scheme. [3] Is actuated to assess potential security risks expose by these untrusted apps. Specifically, we've developed an automatic system referred to as RiskRanker to scalably analyze whether or not a specific app exhibits dangerous behavior (e.g,launchinga root exploit or causing background SMS messages. [4]

In this paper author have a tendency to study a way to conduct effective risk communication for mobile devices. We have a tendency to target the mechanical man platform. The mechanical man platform has emerged jointly of the quickest growing operative systems. In Gregorian calendar month 2012, Google announced that four hundred million mechanical man devices are activated, with one million devices being activated daily. Associate in nursing increasing variety of apps are on the market for mechanical man. The Google Play (formerly referred to as mechanical man Market) crossed more than fifteen billion downloads in could of 2012, and was adding regarding one billion downloads per month from Dec 2011 to could 2012. Such a large user base let alone simple developing and sharing applications makes mechanical manan attractive target for malicious application developers that ask for personal gain while cost accounting user's knowledge and causing SMS messages to premium rate numbers.[5]

III. MOTIVATION

Fraudulent developers ofttimes exploit crowdsourcing sites (e.g., Freelancer, Fiver, BestAppPromotion) to rent groups of willing employees to commit fraud put together, emulating realistic, spontaneous activities from unrelated folks. We tend to decision this behavior search rank fraud. Additionally, the efforts of automaton markets to spot and take away malware don't seem to be perpetually roaring. For instance, Google Play uses the guard system to get rid of malware. However, out of the seven, 756 apps we tend to analyzed victimization Virus Total , 12-tone system were aged by a minimum of one anti-virus tool and a couple of there have been identified as malware by a minimum of ten tools. Previous mobile malware detection work has targeted on dynamic analysis of app executables as well as static analysis of code and permissions. However, recent automaton malware analysis discovered that malware evolves quickly to bypass anti-virus tools.

IV. EXISTING SYSTEM

Previous mobile malware detection work has targeted on dynamic analysis of app executables furthermore as static analysis of code and permissions but, recent Android malware analysis discovered that malware evolves quickly to bypass anti-virus tools

V. DISADVANTAGES OF EXISTING SYSTEM

Existing system was not able detect malware before the installation of application.

VI. PROPOSED SYSTEM

We propose PCF (Pseudo set Finder), associate degree algorithmic program that exploits the observation that fraudsters employed to review associate degree app area unit probably to post those reviews within comparatively short time intervals (e.g., days). PCF takes as input the set of the reviews of associate degree app, organized by days, and a threshold worth. PCF outputs a set of known pseudo-cliques thereupon were shaped throughout contiguous time frames. for every day once the app has received a review , PCF finds the times most promising pseudo-clique begin with every review, then avariciously add alternative reviews to a candidate pseudo-clique; keep th1e pseudo set (of the day) with the highest density. Thereupon work-in- progress pseudo-clique, move on to the next day

VII. ARCHITECTURE

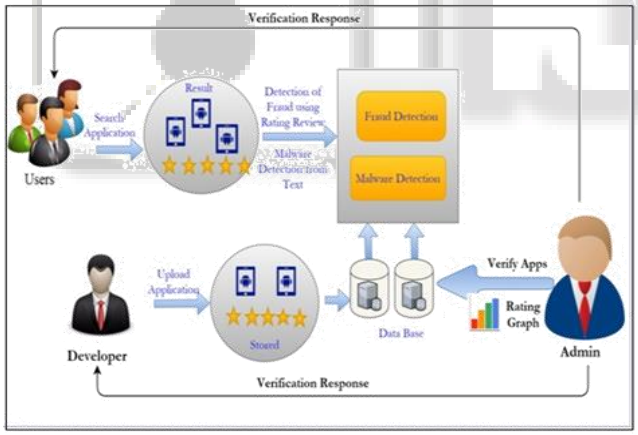

Fig. 1: Architecture

Avariciously add alternative reviews whereas the weighted density of the new pseudo-clique equals or exceeds. Once no new nodes are side to the Work-in-progress pseudo-clique, we have a tendency to add the pseudo set to the output, then move to successive day. In proposed system User and developer will do the registration. Developer will login to the system and upload the application. After that user will login and search for the application. User can see the application uploaded by the developer. After finding application which user wants to download user will go for search rank fraud detection and after that he will check the malware in the application. After users satisfaction user will download the application.

VIII. ADVANTAGES OF PROPOSED SYSTEM

1) The proposed system is able to detect malware before the installation
2) This system is more efficient than existing system

IX. CONCLUSION

We have search and analyze the review on search rank fraud and malware detection of applications. Today Rank and review fraud is happens frequently. To detect that fraud and malware in the application we have analyzed research papers regarding that. This paper explains the Fairplay solution on the problem. Time stamp of review and rating is considered to detect the fraud regarding review and rating. Data mining techniques are used to detect the malware in the application.

REFERENCES

[1] Mahmudur Rahman, Mizanur Rahman, Bogdan Carbunar, Duen Horng Chau "Search Rank Fraud and Malware Detection inGoogle Play"
[2] Bhaskar Pratim Sarma, Ninghui Li, Chris Gates, Rahul Potharaju, CristinaNita-Rotaru, and Ian Molloy. "Android Permissions: a Perspective CombiningRisks and Benets." In Proceedings of ACM SACMAT, 2012
[3] D. H. Chau, C. Nachenberg, J. Wilhelm, A. Wright, and C. Faloutsos. "Polonium: Tera-scale graph mining and inference for malware detection."In Proceedings of the SIAM SDM, 2011.
[4] Junting Ye and Leman Akoglu. "Discovering opinion spammer groupsby network footprints In Machine Learning and Knowledge Discoveryin Databases", 2015.
[5] "Android Malware Detection Using Parallel Machine Learning Classifiers"(2014)
[6] "Android Permissions: A Perspective Combining Risks and Benefits" (2012)
[7] "Dissecting Android Malware: Characterization and Evolution" (2012)
[8] "A Machine Learning Approach to Android Malware Detection."(2012)

