International Journal
of Computer Sciences
ISSN Number: 4142 3453

Elimination of Fraud by Optimization to Integrate Evidences in Mobile Play Store Applications

Syed Hussain Basha[1], C. Praveen Kumar[2], R.M. Noorullah[3]

[1]M.Tech. Akshaya Bharathi Institute Of Technology, R.S. Nagar,, Siddavatam,, Kadapa

[2]Assistant Professor, Akshaya Bharathi Institute Of Technology, R.S. Nagar,, Siddavatam,, Kadapa

[3]Associate Professor, Akshaya Bharathi Institute Of Technology, R.S. Nagar,, Siddavatam,, Kadapa

Abstract- Ranking extortion in the portable App business sector alludes to fake or misleading exercises which have a motivation behind knocking up the Apps in the fame list. For sure, it turns out to be more successive for App designers to utilize shady means, for example, swelling their Apps' business or posting fake App appraisals, to submit positioning extortion. While the significance of averting positioning extortion has been broadly perceived, there is restricted comprehension and examination here. To this end, in this paper, we give an all-encompassing perspective of positioning misrepresentation and propose a positioning extortion recognition framework for portable Apps. In particular, we first propose to precisely find the mining so as to position misrepresentation the dynamic periods, to be specific driving sessions, of versatile Apps. This paper gives a whole perspective of positioning misrepresentation and describes a Ranking fraud identification framework for mobile Apps. This work is grouped into three category. First is web ranking spam detection, second is online review spam detection and last one is mobile app recommendation. The Web ranking spam refers to any deliberate actions which bring to selected Web pages an unjustifiable favorable relevance or importance. Review spam is designed to give unfair view of some products so as to influence the consumers' perception of the products by directly or indirectly influating or damaging the product's reputation.

Keywords: Mobile Apps, Ranking Fraud Detection, Evidence Aggregation, Historical Ranking Records, Rating and Review,Recommendation app, KNN..

1. INTRODUCTION

Most of us use android Mobile these days and also uses the play store capability normally. Play store provide great number of application but unluckily few of those applications are fraud. Such applications dose damage to phone and also may be data thefts. Hence such applications must be marked, so that they will be identifiable for play store users. So we are proposing a web application which will process the information , comments and thee reviews of the application with natural language processing to give results in the form of graph. So it will be easier to decide which application is fraud or not. Multiple application can be processed at a time with the web application. Also User can not always get correct or true reviews about the product on internet. So we can check for more than 2 sites, for reviews of same product. Hence we can get higher probability of getting real reviews.

The recent trend in market used by the dishonest App developers for App boosting is to use fraudulent means to consciously boost their apps. At last, they also distort the chart rankings on a App store. This is usually implemented by using so-called "internet bots" or "human water armies" to raise the App downloads, ratings and reviews in a very little time. For example, VentureBeat [1] reported that, when an App was promoted using ranking manipulation, it could be precipitated from number 1,800 to the upmost 25 in Apple's top free leaderboard and more than 50,000-100,000 new users could be acquired within a couple of days. In actuality, such ranking fraud promotes great concerns to the mobile App industry. For example, Apple has notified of cracking down on App developers who commit ranking fraud [2] in the App store. Leading events of mobile Apps forms different leading sessions. The mobile Apps not always ranked high in the leaderboards, but it usually happens in the leading sessions. So, detecting ranking fraud of mob Apps is actually the process to detect it within the leading session of the mobile Apps. Especially, this paper proposes a simple and effective algorithm to recognize the leading sessions of each mobile App based on its historical ranking records. This is one of the fraud evidence. Also, two types of fraud evidences are proposed based on Apps' rating and review history, which gives some anomaly patterns from Apps' historical rating and review records. In addition, we propose an unsupervised evidenceaggregation method to consolidate these three types of evidences for assessing the credibility of leading sessions from mobile Apps

II LITERATURE SURVEY

In this section, we have studied previous research papers related to the detection of ranking fraud for mobile Apps. The research work of this study is divided into three categories. They are i) web ranking spam detection [3], [4], [5], ii) online review spam detection [6], [7], [8] and iii) mobile App recommendation [9], [10], [11]. The first category is Web ranking spam detection. The web ranking spam refers to any intentional actions which bring to selected webpages an inexcusable auspicious relevant importance [5]. Following is the work done on web ranking spam detection A.Ntoulas et al. [3] presented a number of heuristic methods for detecting content based spam. He studied different aspects of content based spam on the web to find the heuristic methods.

N. Zhou et al. [5] studied the unsupervised web ranking spam detection. Using a spamicity, he proposed an efficient online link spam and spam detection methods. Recently, B. Spirin et al. [4] has done a survey on Web spam detection. This survey thoroughly introduces the principles and algorithm in the literature. Certainly, the work of Web ranking spam is mainly based on the study of ranking principles of search engines, like page rank and query term frequency. This different from ranking

fraud detection for mobile Apps.

Detection of ranking fraud for mobile Apps is still under a subject to research. To fill this crucial lack, we propose to develop a ranking fraud detection system for mobile Apps. We also determine several important challenges. First challenge, in the whole life cycle of an App, the ranking fraud does not always happen, so we need to detect the time when fraud happens. This challenge can be considered as detecting the local anomaly in place of global anomaly of mobile Apps. Second challenge, it is
important to have a scalable way to positively detect ranking fraud without using any basis information, as there are huge number of mobile Apps, it is very difficult to manually label ranking fraud for each App. Finally, due to the dynamic nature of chart rankings, it is difficult to find and verify the evidences associated with ranking fraud, which motivates us to discover some implicit fraud patterns of mobile Apps as evidences.

III. RELATED WORK

The related works of this study is grouped into three categories. The first category is about Web ranking spam detection. Specifically, the Web ranking spam refers to any deliberate actions which bring to selected Web pages an unjustifiable favorable relevance or importance. In this, the problem of unsupervised web spam detection is studied. They introduce the concept of spamicity to measure how likely a page is spam. Spamicity is more flexible and user-controllable measure than the traditional supervised classification methods. They propose efficient online link spam and term spam detection methods using spamicity. This methods do not need training and also cost effective. A real data set is used to evaluate the effectiveness and the efficiency [1].

With the increase in the number of web Apps, to detect the fraudulent Apps, we have propose a simple and effective algorithm which identifies the leading sessions of each App based on its historical ranking of records. By analysing the ranking behaviours of Apps, we discover that the fraudulent Apps often have different ranking patterns in each leading session compared with normal Apps. Thus, we identify some fraud evidences from Apps' historical ranking records and develop three functions to obtain such ranking based fraud evidences

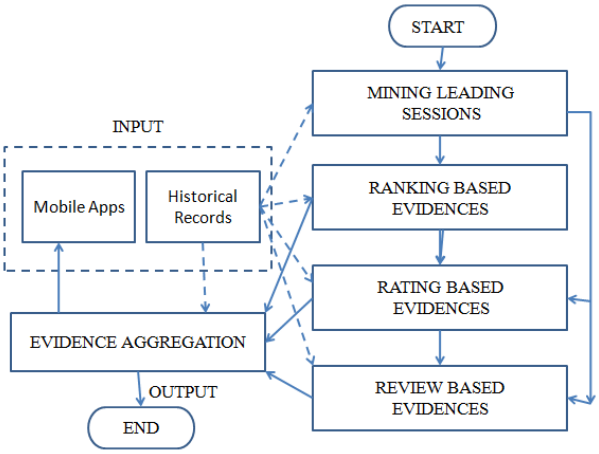


Fig. 1. Ranking fraud detection system framework

IV. PROPOSED WORK

Proposed a scheme that provides a secure way for key distribution without secure communication channels. In which the user can securely obtain their private keys from the group manager without any certificate authority due to the verification for the public key of user. This scheme can achieve fine grained access control. This scheme uses the polynomial function for user revocation so it protect form collusion attack. This scheme support dynamic group efficiency in which private key will not be recomputed and update at the new user joining or user revocation.

In this paper we proposed a scheme that provides the anti-collusion data sharing in multiuser cloud. Firstly the user registration user can register in the system in which user provides the information about him and complete the registration process system provides the user id and Further, we propose two types of fraud evidences based on Apps' rating and review history. It reflects some anomaly patterns from Apps' historical rating and review records. Fig. 1 shows the framework of our ranking fraud detection system for mobile Apps.
The leading sessions of mobile App signify the period of popularity, and so these leading sessions will comprise of ranking manipulation only. Hence, the issue of identifying ranking fraud is to identify vulnerable leading sessions. Along with this, the main task is to extract the leading sessions of a mobile App from its historical ranking records. There are two main phases for detecting the ranking fraud:

i) Identifying the leading sessions for mobile apps
ii) Identifying evidences for ranking fraud detection

Let us see them in brief

A. Identifying the leading sessions for mobile apps Primarily, mining leading sessions has two types of steps concerning with mobile fraud apps. First, from the Apps historical ranking records, discovery of leading events is done and then second merging of adjacent leading events is done which appeared for constructing leading sessions. Certainly, some specific algorithm is demonstrated from the pseudo code of

mining sessions of given mobile App and that algorithm is able to identify the certain leading events and sessions by scanning historical records one by one.

B. Identifying evidences for ranking fraud detection

Let us see these in brief:

1) Ranking based evidences:

It concludes that leading session comprises of various leading events. Hence by analysis of basic behaviour of leading events for finding fraud evidences and also for the app historical ranking records, it is been observed that a specific ranking pattern is always satisfied by app ranking behaviour in a leading event

2) Rating based evidences:

Previous ranking based evidences are useful for detection purpose but it is not sufficient. Resolving the "restrict time depletion" problem, fraud evidences recognition is planned due to app historical rating records. As we know that rating is been done after downloading it by the user, and if the rating is high in leaderboard considerably that is attracted by most of the mobile app users. Spontaneously, the ratings during the leading session gives rise to the anomaly pattern which happens during rating fraud. These historical records can be used for developing rating based evidences.

3) Review based evidences:

We are familiar with the review which contains some textual comments as reviews by app user and before downloading or using the app user mostly prefer to refer the reviews given by most of the users. Therefore, although due to some previous works on review spam detection [13] there still issue on locating the local anomaly of reviews in leading sessions. So based on apps review behaviors, fraud evidences are used to detect the ranking fraud in Mobile App.

V METHODOLOGY

Identifying Leading Sessions : Ranking fraud usually happens in leading sessions. Therefore, detecting ranking fraud of mobile Apps is actually to detect ranking fraud within leading sessions of mobile Apps. Specifically, we first propose a simple yet effective algorithm to identify the leading sessions of each App based on its historical ranking records. Then, with the analysis of Apps' ranking 'behaviors, we find that the fraudulent Apps often have different ranking patterns in each leading session compared with normal Apps.

Mining Leading Sessions: There are two main steps for mining leading sessions. First, we need to discover leading events from the App's historical, ranking records. Second, we need to merge adjacent leading events for constructing leading sessions.

Ranking Based Evidences: A leading session is composed of several leading events. Therefore, we should first analyze the basic characteristics of leading events for extracting fraud evidences. By analyzing the Apps' historical ranking records, we observe that Apps' ranking
behaviors in a leading event always satisfy a specific ranking pattern, which consists of three different ranking phases, namely, rising phase, maintaining phase and recession phase. Specifically, in each leading event, an App's ranking first increases to a peak position in the leader board (i.e., rising phase), then keeps such peak position for a period (i.e., maintaining phase), and finally decreases till the end of the event (i. e., recession phase).

Rating Based Evidences

The ranking based evidences are useful for ranking fraud detection. However, sometimes, it is not sufficient to only use ranking based evidences. Specifically, after an App has been published, it can be rated by any user who downloaded it. Indeed, user rating is one of the most important features of App advertisement. An App which has higher rating may attract more users to download and can also be ranked higher in the leader board. Thus, rating manipulation is also an important perspective of ranking fraud. Intuitively, if an App has ranking fraud in a leading session s, the ratings during the time period of s may have
anomaly patterns compared with its historical ratings, which can be used for constructing rating based evidences.

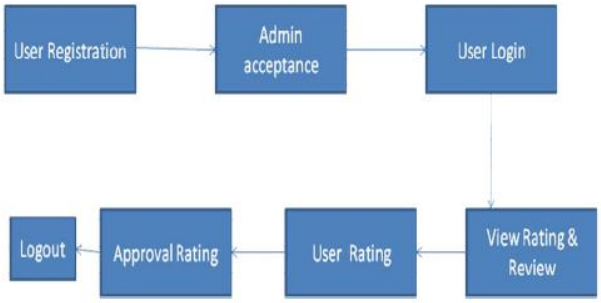


Figure 2.Rating based evidence

Review Based Evidences

Besides ratings, most of the App stores also allow users to write some textual comments as App reviews. Such reviews can reflect the personal perceptions and usage experiences of existing users for particular mobile Apps. Indeed, review manipulation is one of the most important perspectives of App ranking fraud.

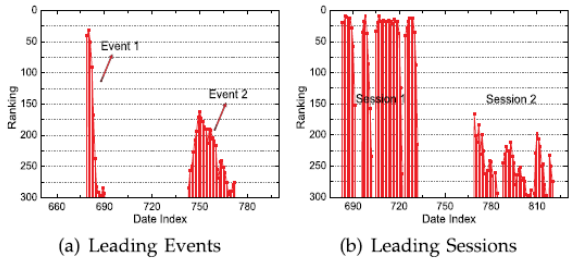
Specifically, before downloading or purchasing a new mobile App, users often firstly 5, read its historical reviews to ease their decision making, and a mobile App contains more positive reviews may attract more users to download.

International Journal
of Computer Sciences
ISSN Number: 4142 3453

Therefore, imposters often post fake reviews in the leading sessions of a specific App in order to inflate the App downloads, and thus propel the App's ranking position in the leader board. Although some previous works on review spam detection have been reported in recent years, the problem of detecting the local anomaly of reviews in the leading sessions and capturing them as evidences for ranking fraud detection are still under-explored.

VI. RESULT

By analyzing the historical ranking records of mobile Apps, we observe that Apps are not always ranked high in the leader board, but only in some leading events. For example, Fig. 1 shows an example of leading events of a mobile App. Formally, we define a leading event as follows



(a) Leading Events (b) Leading Sessions

Fig 3: Example of Leading Events and Leading Sessions of Mobile Apps

IV. CONCLUSION

This paper reviews various existing methods used for web spam detection, which is related to the ranking fraud for mobile Apps. Also, we have seen references for online review spam detection and mobile App recommendation. This paper introduces more effective fraud evidences and analyze the latent relationship among rating, review and rankings.We extended our ranking fraud detection approach with other mobile app related services,such as m

REFERENCE

[1](2012).[Online].Available: venturebeat.com/2012/07/03/apples-crackdown-on-app-ranking-manipulation/

[2](2012).[Online].Available: developer.apple.com/news/index.php?id=02062012a

[3] A. Ntoulas, M. Najork, M. Manasse, and D. Fetterly, "Detecting spam web pages through content analysis," in Proc. 15th Int. Conf. World Wide Web, 2006, pp. 83–92.

[4] N. Spirin and J. Han, "Survey on web spam detection: Principles and algorithms," SIGKDD Explor. Newslett., vol. 13, no. 2, pp. 50– 64, May 2012.

[5] B. Zhou, J. Pei, and Z. Tang, "A spamicity approach to web spam detection," in Proc. SIAM Int. Conf. Data Mining, 2008, pp. 277– 288.

[6] E.-P. Lim, V.-A. Nguyen, N. Jindal, B. Liu, and H. W. Lauw, "Detecting product review spammers using rating behaviors," in Proc. 19thACMInt. Conf. Inform. Knowl. Manage., 2010, pp. 939–948.

[7] Z. Wu, J. Wu, J. Cao, and D. Tao, "HySAD: A semi-supervised hybrid shilling attack detector for trustworthy product recommendation," in Proc. 18th ACM SIGKDD Int. Conf. Knowl.Discovery Data Mining, 2012, pp. 985–993.

[8] S. Xie, G. Wang, S. Lin, and P. S. Yu, "Review spam detection via temporal pattern discovery," in Proc. 18th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining, 2012, pp. 823–831.

[9] K. Shi and K. Ali, "Getjar mobile application recommendations with very sparse datasets," in Proc. 18th ACM SIGKDD Int. Conf.Knowl. Discovery Data Mining, 2012, pp. 204–212.

[10] B. Yan and G. Chen, "AppJoy: Personalized mobile application discovery," in Proc. 9th Int. Conf. Mobile Syst., Appl., Serv., 2011,pp. 113–126.

[11]Hengshu Zhu, Hui XiongDiscovery of Ranking Fraud for Mobile Apps. IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING,2013.