International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 20 Issue 3 – MARCH 2016.

MOBILE APP'S SECURITY MEASURE USING CFC

S.P.Neeraja[1], Mrs.P.Kanimozhi[2]

[1]*Under graduate,department of computer science and engineering, IFET college of engineering*

[2]*Head of department ,department of computer science and engineering, IFET college of engineering*

Abstract:-**The mobile devices have become popular day by day, which is the major target of malicious applications. The detection and removal of malicious apps from android is the major issue in now days. Due to the large number of mobile Apps, ranking fraud is the key challenge in front of the mobile App market. Ranking fraud refers to fraudulent or vulnerable activities which have a purpose of bumping up the Apps in the popularity list. Ranking fraud in the versatile App business alludes to false or tricky exercises which have a motivation behind knocking up the Apps in the popularity or leader board list. To be sure, it turns out to be more continuous for App designers to utilize doubtful or unethical means, for expanding their Apps' business. The primary aim of this project is to enhance the prevention of ranking frauds in mobile apps. This paper proposes techniques to accurately locate the ranking fraud by mining the active periods, namely leading sessions, of mobile Apps. Proposed approach 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. It proposes an optimization based aggregation method. The result of aggregation is the mobile app which decides the app is fraud able or not. At last, we assess the proposed framework with certifiable App information gathered from the IOS App Store for quite a while period.**

Keywords:- ***Mobile Apps, ranking fraud detection, evidence aggregation, historical ranking records, rating and review***

I. INTRODUCTION

The quantity of mobile Apps has developed at an amazing rate in the course of recent years. For instances, the growth of apps were increased by 1.6 million at Apple's App store and Google Play. To fortify the improvement of portable Apps, numerous App stores dispatched every day App leader boards, which exhibit the graph rankings of most prominent Apps. To be sure, the App leader board is a standout amongst the most essential courses for advancing mobile Apps. A higher rank on the leaderboard more often than not prompts countless and million dollars in income. In this way, App designers have a tendency to investigate different routes, for example, publicizing battles to advance their Apps keeping in mind the end goal to have their Apps positioned as high as could be expected under the circumstances in such App leader boards. Be that as it may, as a late pattern, rather than depending on customary showcasing arrangements, shady App engineers resort to some fake intends to intentionally help their Apps and in the end control the diagram rankings on an App store. This is typically actualized by utilizing purported "bot homesteads" or "human water armed forces" to blow up the App downloads, evaluations and surveys in a brief while. For instance, an article from Venture Beat [1] reported that, when an App was advanced with the assistance of positioning control, it could be impelled from number 1,800 to the main 25 in Apple's sans top leader board and more than 50,000-100,000 new clients could be gained inside of a few days. Truth be told, such positioning misrepresentation raises awesome worries to the portable App industry. For instance, Apple has cautioned of getting serious about App designers who confer positioning extortion in the Apple's App store [2].

In the writing, while there are some related work, for example, web ranking spam detection [3], [4], [5], online survey spam detection [6], [7], [8], and portable App proposal [9], [10], [11], the issue of distinguishing ranking fraud for versatile Apps is still under-explored. To fill this urgent void, in this paper, we propose to build up a ranking extortion recognition system for mobile Apps. Surely, our cautious perception uncovers that mobile Apps are not generally ranked high in the leader board, but rather just in some driving occasions, which form different leading sessions.

Careful observation shows that the mobile Apps are not always at top most position in leader board. But only in some time period called leading event which is form different leading sessions means ranking fraud particularly occur in this leading sessions.

Therefore detecting frauds in mobile apps is nothing but detecting ranking fraud in leading sessions. This leading session identify from each mobile app on the basis of historical record of mobile apps which is given to the mining algorithm. The evidences of fraud detection is then given to the three extracting functions ranking, review and rating then aggregation of these evidences is done by evidence aggregation method. The output gives mobile app with false or true result. In proposed system false apps are preventing from users recommendation and study some effective evidences of mobile apps.

The rest of the paper is arranged as follows: Section 2 presents the literature survey over the related work. In section

3, proposed system is presented. Finally, the section 4 concludes and section 5 reference of the review paper.

II. RELATED WORKS

In this section, we have studied previous research papers related to the detection of ranking fraud for mobile Apps. 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. Spam city 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 method does not need training and also cost effective. A real data set is used to evaluate the effectiveness and the efficiency [11].

For example, Ntoulas et al. [12] have studied various aspects of content-based spam on the Web and presented a number of heuristic methods for detecting content based spam.

D. M. Blei, A. Y. Ng, and M. I. Jordan, introduces a unique model called as Dirichlet allocation (LDA) [13] a generative probabilistic model for collections of discrete data such as text amount. Basically it is a three level hierarchical Bayesian model in which each element of a group is demonstrated as a finite mixture over a fundamental set of topics. Each topic is demonstrated as an infinite mixture over fundamental set of topic probabilities. With the reference of text modelling, the topic probabilities provide an open representation of a document. An efficient approximation inference technique is presented based on various methods and an EM algorithm for empirical Bayes parameter estimation is also presented. The results are reported in document modelling, text classification and collaborative filtering, which compares to a collection of unigrams and probabilistic LSI model.

Recently, B. Spirin et al. [14] 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.

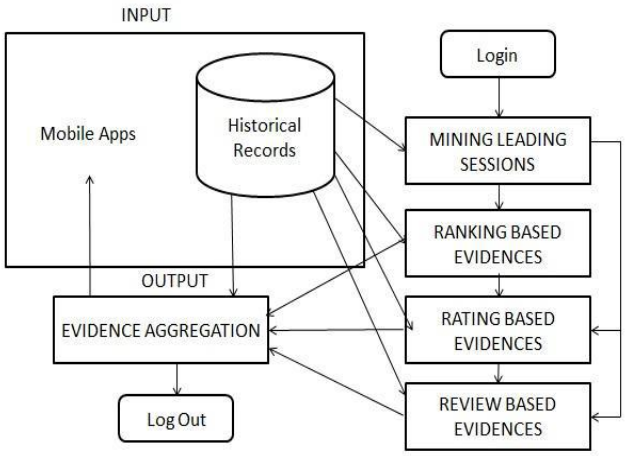
III. PROPOSED SYSTEM

The scope of this paper is 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. 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 analyzing the ranking behaviors 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.

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. Experimental results show the effectiveness of the proposed system, the scalability of the detection algorithm as well as some regularity of ranking fraud activities. An unique perspective of this approach is that all the evidences can be modeled by statistical hypothesis tests, thus it is easy to be extended with other evidences from domain knowledge to detect ranking fraud. Identified ranking based evidences, rating based evidences and review based evidences for detecting ranking fraud.

3.1 System Architecture



The system model in this paper incorporates substances are: Mobile Apps, historical record, mining session, three evidences that are ranking, rating and review and aggregation of all evidences at last as illustrated in above Figure. Mining leading session: This method calculates the mining leading session from historical records of mobile apps of apps industry. Because the fraud is not occurring in overall mobile apps it occurs at particular leading event. This leading event is form different leading sessions. Then apply mining method on these leading sessions. After that three different evidences apply on this sessions that are ranking, rating and review.

Evidence aggregation: Aggregation method is applied on these three evidences. If false mobile app is the output of this aggregation system then this app is prevent from recommendation of user's this is a future scope of this paper.

3.2 Modules

3.2.1 Mining

We further propose two types of fraud evidences based on Apps' rating and review history, which reflect some anomaly patterns from Apps' historical rating and review records. All the products in the play stores are reviewed by the application users ,which neither or nor user only reviewed that which may or may not some fraud developer can be reviewed.in such reviewed to has been under taken in to mining module.

In a mining module all review will be collected and sent into ranking application process.

3.2.2 Ranking application

In Ranking application by analysing the Apps' historical ranking records, we observe that Apps' ranking behaviours 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.

After mined all the review it will be automatically process to finding the correct order of application which is proceed the full review format .is this module ranking will be given to application. Each application will get correct rank order which is perfect match to review by user's .with correct evidence which provide by users.

3.2.3 Rating rightly

In Rating 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.

While all the application revived correct ranking order, in this module starts given correct rating for each application such a way that application will getting proper rating and reviews for further users of that application. Further user can read correct review for that application by this module.

3.2.4 Review evidence

In 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.

In rating based evidences rating pattern is used for ranking fraud detection in app. This rating is done after downloading the app by user and then user gives rating to that app. If the rating is high in the leader board of app industry then that app is attracted by more mobile app users. In this the fraud occurred during rating is performed in leading session

In review based evidences reviews are the textual comments that is given by mobile app users after using or downloading that app. Before downloading the app user always preferred to view these comments given by most users. Based on previous work on review spam detection there are still some issues for locating local anomaly in leading events e for ranking fraud detection system.

IV. CONCLUSION

In this paper, we developed a ranking fraud detection system for mobile Apps. Specifically, we first showed that ranking

fraud happened in leading sessions and provided a method for mining leading sessions for each App from its historical ranking records. Then, we identified ranking bas evidences, rating based evidences and review based evidences for detecting ranking fraud .Moreover, we proposed an optimization based aggregation method to integrate all the evidences for evaluating the credibility of leading sessions from mobile Apps. A novel point of view of this methodology is that every one of the proofs can be displayed by measurable theory tests; in this way it is anything but difficult to be reached out with different confirmations from space information to distinguish positioning misrepresentation. At last, we accept the proposed framework with broad examinations on certifiable App information gathered from the Apple's App store.

In the future, we plan to study more effective fraud evidences 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.

REFERENCES

[1] (2012). [Online]. Available: https://developer.apple.com/news/index.php?id=02062012a
[2] (2012). [Online]. Available: http://venturebeat.com/2012/07/03/ apples-crackdown-on-app-ranking-manipulation/
[3]. D. F. Gleich and L.-h. Lim, "Rank aggregation via nuclear norm minimization," in Proc. 17th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining, 2011, pp. 60–68.

[4]. T. L. Griffiths and M. Steyvers, "Finding scientific topics," Proc. Nat. Acad. Sci. USA, vol. 101, pp. 5228–5235, 2004.

[5]. G. Heinrich, Parameter estimation for text analysis, "Univ. Leipzig, Leipzig, Germany, Tech. Rep., http://faculty.cs.byu.edu/~ringger/CS601R/papers/Heinrich-GibbsLDA.pdf, 2008.

[6]. N. Jindal and B. Liu, "Opinion spam and analysis," in Proc. Int.Conf. Web Search Data Mining, 2008, pp. 219–230.

[7]. A. Klementiev, D. Roth, and K. Small, "An unsupervised learning algorithm for rank aggregation," in Proc. 18th Eur. Conf. Mach. Learn., 2007, pp. 616–623.

[8]. A. Klementiev, D. Roth, and K. Small, "Unsupervised rank aggregation with distance-based models," in Proc. 25th Int. Conf. Mach. Learn., 2008, pp. 472–479.

[9]. A. Klementiev, D. Roth, K. Small, and I. Titov, "Unsupervised rank aggregation with domain-specific expertise," in Proc. 21st Int. Joint Conf. Artif. Intell., 2009, pp. 1101–1106.

[10] 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.
[11] B. Zhou, J. Pei, and Z. Tang. A spamicity approach to web spam detection. In Proceedings of the 2008 SIAM International Conference on Data Mining, SDM'08, pages 277–288, 2008.

[12] A. Ntoulas, M. Najork, M. Manasse, and D. Fetterly. Detecting spam web pages through content analysis. In Proceedings of the 15th international conference on World Wide Web, WWW '06, pages 83–92, 2006

[13] D. M. Blei, A. Y. Ng, and M. I. Jordan, "Latent Dirichlet allocation," J. Mach. Learn. Res., pp. 993–1022, 2003.
[14] 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.
[15] Tejaswini B. Gade, Nilesh G. Pardeshi, " A Survey on Ranking Fraud Detection Using Opinion Mining for Mobile Apps," nternational Journal of Advanced Research in Computer and Communication Engineering ,Vol. 4, Issue 12, December 2015.
[16] Prajakta Gayke , Sanjay Thakre, "Detection of Ranking Fraud for Mobile App," IOSR Journal of Computer Engineering (IOSR-JCE), PP 68-71,2015.
[17] M. N. Volkovs and R. S. Zemel, "A flexible generative model for preference aggregation," in Proc. 21st Int. Conf. World Wide Web, 2012, pp. 479–488.