Case Study on- Ranking Fraud for Mobile Application

Vanmathi C[1], Krithika L. B[2], Asha N[3], Mangayarkarasi R[4]
[1, 2, 3, 4] School of Information Technology and EngineeringVIT University

Abstract-*Now Days, Ranking fraud plays major role in mobile applications store like play store and IOS store. Applications Developer gives fake ranking to their applications to rank up their apps in top most list of application market. Surely it turns out to increase number downloads to their applications. In this paper I am going to analysis the ranking fraud and what are the proposes of ranking fraud detection system for mobile applications store. First of all we find positioning misrepresentation by some mining techniques on static period namely leading season of mobile applications. That time frame can be utilized for detecting the irregularity of applications ranking. In this research I am going to investigate three type of data i.e., information based on ranking, information based on rating and information based on reviews, Likewise I will propose an improvement based on aggregation algorithm by using all the data or information that are misinterpreting users. Finally I examine the proposed system with real-world applications data collected from different-different applications store. I am validating the adequacy of proposed algorithm, and show how it will detects some regularity of fraud activities.*

Keywords-Ranking Fraud, Mobile Applications, Aggregation.

I. INTRODUCTION

In Today's world the demand of the mobile applications market is continually increasing at a very fast rate from last few year. For an example, as of the end of April 2012, there're over sixteen Million applications at mobile application stores like Google play, windows, and apple app store. Many applications store developed/build their own daily applications leader board to track them the most popularity which help to show the chart rankings. This leader board helps applications of their development. Applications leader board is the best way for promoting mobile applications the more you get ranked in leader board, the more you get a number of downloads which leads to earning of million dollars revenue. Such that Developers do some various tricks like advertising to promote their applications in order to keep application ranking higher as much as possible in various leader boards, but this is a traditional method, now days they are doing some kind of frauds that they are forcefully boost their applications and easily manipulate of ranking of their charts on an applications store. This is implemented using virtual human armies to increase the number of downloads like giving fraud ratings and fake reviews is limited time. As an e.g., some articles was published in that article applications was promoted for helping the ranking fraud in the ranking charts because of that article it could crawled from 2000 to the top of twenty-five in Application's Store top baton board that are free and added than 100000 new users can be acquired within the same day. Indeed, such positioning misrepresentation raises awesome worries to some versatile Applications industry. Such instance, Application's Store like Apple cautioned about getting serious about application developers who submit positioning extortion in their Application's store. In this thesis report we are going to study how fraud is to be done in the mobile application market. How developers giving a fake ranking of their applications, giving fake comments and so on. We are implementing applications to track how much time users or developers has given ratings, ranking and comments.

Table 1.1 Mobile Applications Fraud (Examples)

	Technical Fraud	**Compliance Fraud**
Impression Fraud	**Stacking Advertisements** It is a process which developers place various types of banners on top of the other developer's applications.	**View ability** Advertising their applications where it can see sometimes a day.
Click Fraud	**Fraud Clicks** Generating false transactions id through some websites that having no relationship with advertised applications, but when user download that applications revenue is automatically credited into developer's account.	**Miss usage Of Creative Design** Example: Displaying fake promise or displaying different applications than one of the advertisement actually they leads to.

Post install Fraud	**Faked Post Backs** Post Back events to fake either an install or post install event.	**Un Disclosed Rebrokering** Rebroking promoting offers starting with one distributer then onto the next makes for an extremely cloudy publicizing biological community, as promotes wind up without knowing where the introduce originates from

II. LITERATURE REVIEW

The Existing system works on past data of historical data it takes reviews, rating and results given by market user. The major disadvantages of the current system can be used for detection of fraud applications based on historical rating and historical reviews and past records. They cannot extract fraud evidences for a particular period of time. We are not able to find fraud applications on based on historical data. There is no existing bookmark which helps to decide which applications is fraud and which one are genuine.

On The main drawback of an existing system is that it works only on historical data. It cannot work on leading sessions (Particular time frame). No bookmark is available in existing systems so we are not able to decide which applications are fake and which one is genuine.

Identify Leading Sessions

Mobile applications ranking fraud happens only in some limited time period (leading sessions). When developers upload applications in the cloud/server after uploading at that time leading session starts, Firstly, we are proposing an algorithm to identify where leading sessions start. Each application based on its previous data. Now we are doing analysis of ranking behaviors of applications, by doing this we can find that fraud applications have different-different raking patterns as compared with other normal applications.

Analyzing some major sessions

There are two major steps to mine the time frames (leading sessions) i.e. to discover the events from the applications generated from the usage of applications over the years and to merge the events that are adjacent of building the sessions together.

Evidences Based on Rankings

In Evidences based on rankings time frame is compared with several time frames. So first of all we have to analyze the same characteristics of time frame (that is called leading sessions) for identifying fraud users who are doing fake rankings. By studying the Apps historic ranking facts, we take a look at that Apps rating behaviors in a leading session is continually fulfill a particular rating sample, which comprises of three diverse positioning stages, to be specific, rising stage, keeping up stage and subsidence stage. In particular, in each driving occasion, an App's positioning first increment to a pinnacle position on the Leaderboard (i.e., rising stage), then keeps such pinnacle position for a period (i.e., looking after stage), lastly diminishes till the end of the occasion (i.e., retreat stage).

Aggregation Evidence

After mining on previous evidences (Rating based, Ranking Based, Review based), next move is to how to join them for identifying ranking fraud detection. Surely, there are many positioning and confirmation accumulation strategies in the writing, However, a number of those techniques, awareness about getting to know an international ranking of all candidates. for example, change based models, models based on score and DSR(Dempster-!Shafer rules). This is not appropriate for recognizing positioning misrepresentation for fresh out of the box new Apps. Some different strategies are constructing absolutely with respect to administered becoming acquainted with methods, which depend upon the sorted tutoring records and are difficult to be misused. We recommend a freely techniques depends on the parallel of fraud to use all these evidences at the same time.

Evidences Based on Ratings

The positioning based confirmations are valuable for positioning extortion identification. But on a daily basis, it isn't sufficient to simplest use evidences based on the ranking given by the developer or user. . Specifically, after an application has been posted, it is able to be routed via any person who use it or download it. Indeed, person or use's review/ratings are one of the most important functions on a play store in the mobile application market. An Application which has better score or ranking in the play store may

additionally appeal or attract more customers to download and can also be ranked better inside the Leaderboard. Thus, rating control is likewise a very crucial aspect in ranking fraud which is done by the developers. Naturally, if an Application has positioned misrepresentation in a main session (leading sessions s), the evaluations for the length of the day and age of us can likewise have peculiarity styles contrasted and its memorable scores.

Evidences Based on Reviews

Rather than Ranting and ranking many applications store play store, IOS store and other permit applications, users or application downloads to give their view in textual format (comments). Such assessments can mirror the non-open recognitions and use investigations of present clients for specific mobile applications. Certainly evaluate manipulation is one of the very critical aspect of mobile Applications ranking fraud. But when new applications, user download application from play store by IOS store, they often go through historic reviews, this will help downloaders that applications is useful or not this review also helps applications owners to attract more number of users. Subsequently, con artists consistently submit fake audits inside the leading themes of a particular Application keeping in mind the end goal to rank up the Applications downloads, and as needs to drive the Applications positioning position on the top of the chart. The bother of distinguishing the neighborhood inconsistency of audits inside the main classes and catching them as confirmations for positioning extortion identification are still under-investigated. In this quiet end, right here we endorse or proposed some fraud evidences based on Applications reviews behaviors in main periods for detecting ranking fraud. In this quiet end, right here we endorse or proposed some fraud evidences based on Applications comments or reviews behaviors in main periods(leading time ofs applications) for detecting ranking fraud..

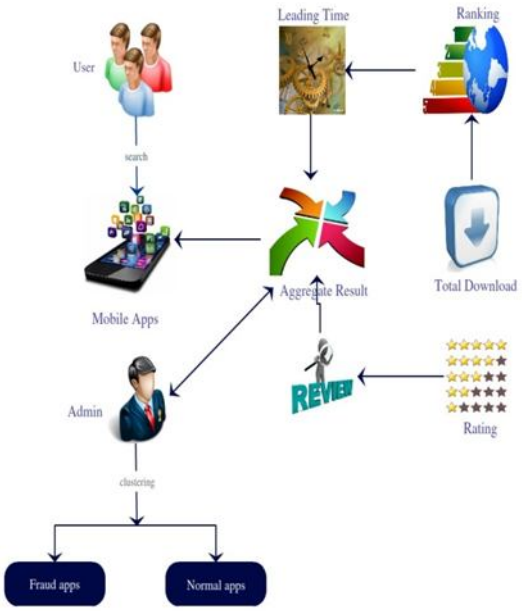

Figure.1 Proposed System Architecture

Figure.1 shows that admin can do data analysis on mobile applications and find whether application is fraud apps or the normal one. When user downloads mobile applications the number of download will increase if number of download is higher the aggregate results appear on mobile application's store. Admin find aggregate results appear based on based on number of reviews; number of ratings, total number of downloads.

III. PROPOSED SYSTEMS

As a proposal we are proposing a system which detects fraud applications for mobile stores. Usually ranking does not appear in the accomplished in time application so we charge to ascertain that time usually when fraud happens. This time frame is also called as leading sessions or high time. Firstly, we propose an algorithm to analyze arch seasons of every application. Then it analysis the behavior of applications based on ranking, rating, and reviews. The proposal is that the user should need permission from admin to access applications. What admin do is that admin gives an access key to a particular device to particular user so it helps from fraud applications.

Advantages of Proposed Systems

- The main advantage of proposed algorithm is that it will show only those applications that are genuine.
- The admin of mobile application market can easily track which applications are getting fake review, ranking, and ratings,

- It helps to save lots of money on mobile applications markets like play store and IOS store.
- Giving all rights to admin only. Admin will decide which applications should be on the leader board.

IV. CONCLUSIONS

In this research, we have designed a ranking fraud applications system for mobile applications. Categorically, are detection systems shows that when ranking and rating fraud is happening in a particular time frame so we are providing a methods to mine all the time frame for each and every applications from its previous ranking and rating records. Then, we found evidences based on ranking, evidences based on rating and evidences based on reviews for searching fraud in ranking of mobile applications. Now I am proposing an optimization techniques depends on aggregation algorithm for using all the records for measuring the reliability of a particular time frame (leading sessions), for mobile applications. An different angle of this access is that all the evidences should be designed by statistical antecedent tests, appropriately it is simple to be continued with added evidences from area ability to ascertain baronial fraud applications. In last, we are validating the system which we are proposing with some effective experiments on the real-time applications which we are collecting from the play store. The results which we got in experiments are very effective by using proposed approach.

FUTURE RESEARCH RECOMMENDATIONS

For future work we are planning to study more evidences based on fraud and we will do analysis on the relationship between all the major aspects for promoting mobile applications like ranking, rating, reviews. Additionally we are planning to enhance our fraud detection systems for with added accompanying applications services for eg. We will recommend mobile applications for user's better experience.

REFERENCES

[1] Ge, Yong, Hui Xiong, Chuanren Liu, and Zhi-Hua Zhou. "A taxi driving fraud detection system." In Data Mining (ICDM), 2011 IEEE 11th International Conference on, pp. 181-190. IEEE, 2011.

[2] Gleich, David F., and Lek-heng Lim. "Rank aggregation via nuclear norm minimization." In Proceedings of the 17th ACM SIGKDD international conference on Knowledge discovery and data mining, pp. 60-68. ACM, 2011.

[3] Griffiths, T.L. and Steyvers, M., 2004. Finding scientific topics. Proceedings of the National academy of Sciences, 101(suppl 1), pp.5228-5235.

[4] Mukherjee, Arjun, Abhinav Kumar, Bing Liu, Junhui Wang, Meichun Hsu, Malu Castellanos, and Riddhiman Ghosh. "Spotting opinion spammers using behavioral footprints." In Proceedings of the 19th ACM SIGKDD international conference on Knowledge discovery and data mining, pp. 632-640. ACM, 2013.

[5] Ntoulas, Alexandros, Marc Najork, Mark Manasse, and Dennis Fetterly. "Detecting spam web pages through content analysis." In Proceedings of the 15th international conference on World Wide Web, pp. 83-92. ACM, 2006.

[6] Spirin, Nikita, and Jiawei Han. "Survey on web spam detection: principles and algorithms." ACM SIGKDD Explorations Newsletter 13, no. 2 (2012): 50-64.

[7] Volkovs, Maksims N., and Richard S. Zemel. "A flexible generative model for preference aggregation." In Proceedings of the 21st international conference on World Wide Web, pp. 479-488. ACM, 2012.

[8] Mukherjee, Arjun, Abhinav Kumar, Bing Liu, Junhui Wang, Meichun Hsu, Malu Castellanos, and Riddhiman Ghosh. "Spotting opinion spammers using behavioral footprints." In Proceedings of the 19th ACM SIGKDD international conference on Knowledge discovery and data mining, pp. 632-640. ACM, 2013.

[9] (2012), (Online).Available: https://developer.apple.com/news/index.php?=02062012abc.

[10] 2012[Online]., Available: http://venturebeat.com/2012/07/03/ apples- crackdown-on-app ranking-manipulation/

[11] 2012 [Online]. index.html Available at: http://www.lextek.com/manuals/ /onix

[12] (2012). [Online]. Available at: http://www.ling.gu.se/lager/ porter-stemmer/mogul