ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

A Survey on Recognize the Ranking Scam Occurred in Mobile Apps

Vaishali Date[1], Dipali Dongare[2], Pooja Jadhav[3], Tejal Wayal[4], Asmita Mali[5]

B.E Students, Dept. of IT, Dr. D. Y. Patil Institute of Engineering and Technology, Pimpri-411018, Savitribai Phule Pune University, Pune, India.

Assistant Professor, Dept. of IT, Dr. D. Y. Patil Institute of Engineering and Technology, Pimpri-411018, Savitribai Phule Pune University, Pune, India.

ABSTRACT - Ranking scam in mobile App refers to deceptive activities which have a purpose of raising the rank of app in leaderboard. It has becomes more frequent for App developers to use such means as inflating their Apps' sales or posting fraud ratings, to commit ranking scam. While the importance of preventing ranking fraud has been widely recognized, there has been limited research in this area. In this paper, we propose a system which discovers the presence of ranking scam in mobile applications. We are going to list the applications by finding the active period of the application named as leading session. We recognized ranking, rating and review based evidences. Using these three evidences we will calculate aggregation of them and performed hypothesis test on it to get actual rank of mobile application and authentication of user is done for further access. We will retrieve our system with data collected form application play store for long period of time.

KEYWORDS : Mobile Apps, ranking scam, ranking, rating, review, evidence aggregation, user authentication.

I. INTRODUCTION

Now a day's everyone is using smart phones. There is need of various apps to be installed on smart phone. Mobile Apps number has grown very fast over the past few years. As of the end of April 2013, there were more than 1.6 million Apps at Apple's App play store and Google Play store. To countenance the development of mobile Apps, many Application stores launched daily leader boards, which convey the chart rankings of most popular Apps. The App leader board is the important way for promoting Apps.

A favorable rank on the leader board leads to a huge downloads and million dollars in revenue. Therefore, App developers tend to explore various ways for advertising to raise their Apps in order to have their Apps ranked as high as possible. Instead of relying on traditional marketing solutions, Disreputed App developers resort to some scam means to purposely boost their Apps and eventually manipulate the chart rankings on store. This is implemented by using "boot farms" and "human water armies" to increase the App downloads ratings and reviews in a very small time. For ex, an article from Venture Beat reported that, when an Application was promoted with the help of ranking manipulation, it should be propelled from 1,800 to the top 25 in Apple's top free leader board and more than 50,000 to 100,000 new users could be acquired within a couple of days. In fact, such ranking scam raises great concerns to the mobile App industry.

Apple has recommended of cracking down the App developers who commit ranking scam in the Apple's App store. In the literature, some work is done related to web ranking spam, online review Spam detection and recommendation of mobile Application, the problem of detecting ranking scam is still under explore, To fill this we are proposing a system which discover the presence of ranking scam in mobile applications.

DOI: 10.15680/IJIRCCE.2015. 0312073

II. RELATED WORK

The related work of this study can be grouped into three categories. The first is about web ranking spam detection [1], the second is focused on online review Spam detection [2], and finally, the third includes the studies on mobile App recommendation [3].

In [1] we continue our inquiry of "web spam" introduction of artificially-created pages into the web in order influence the solutions from search engines, to drive traffic to certain pages for profit. This paper considers some prior-un described techniques for automatically detecting spam pages, examinee the effectiveness of these techniques in isolation and using grouping algorithms for aggregation. In [2] aims to detect users producing spam reviews. Different characteristic behaviors of review spammers were identified and model was done for detecting the spammers. In particular, we seek to model the behaviors spammers may target specific product groups in order to maximize their impact and they tend to deviate from the other reviewer in their ratings of products. We propose achieved method to measure the degree of spam for each reviewer and to take effect them on an Amazon review dataset. In[3] we illustrate how to extraction personal context-aware preference from the context-rich device logs for building personalized context-aware warned systems. First learn general context-aware preferences from the context logs of most of users. Then, the preference user can be represented as a distribution of these general context-aware preferences. Two approaches are there for mining general context-aware preferences based on two distinct assumptions, namely, context independent and context dependent. Finally, spacious experiments on a real-world data set that show the approaches are effectively and perform baselines with respect to mining personal context-aware preferences for mobile users. In[4] In GPS tracking technology it has enabled us to install GPS tracking devices in city taxis to collect a huge amount of GPS traces under operational time limitation. In this system, we first provide functions to find two evidences: travel route evidence and driving distance evidence and a third function is designed to combine the two evidences based on dempster-Shafer theory. Then, we propose a parameter-free method and we introduce route mark to connote a typical driving path from an interesting site to another one. Based on route mark, we use statistical model to characterize the division of driving distance and identify the driving distance evidences. We evaluate the taxi driving fraud detection system. We uncover some orderly of driving fraud activities and investigate the impetus of drivers to commit a driving fraud by analyze the produced taxi fraud data .In[5] we study issue in the context of product reviews, that are opinion rich and are vastly used by consumers and manufacturers. In the past two years, several startup companies also not disappeared which aggregate opinions from product reviews. We will see that opinion spam is as it is different from Web spam and email spam, and thus requires different quest techniques. On performing the analysis of 5.8 million reviews and 2.14 million reviewers from amazons, we see that opinion spam in reviews is large spread. This paper analyzes such spam activities and presents some techniques to detect them. In[6] Many applications in information recompense, data mining, and related fields require a ranking of instances with respect to specified criteria as opposed to a classification. Also, for such problems, established multiple ranking models have been studied and it is desirable to collect their results into a joint ranking, formalism denoted as rank aggregation. This work presents an unsupervised learning algorithm for rank aggregation (ULARA) which returns a linear cohesion of the separate ranking functions based on the principle of rewarding ordering agreement during the rankers. To present ULARA, we exhibition its effectiveness on a data fusion task across ad hoc retrieval systems.

III SCOPE OF RESEARCH

To detect the scam occurred in ranking of mobile application. Improve the ranking based system using evidences Ranking, Rating, Review and providing authentication to user for futher access.

IV PROPOSED METHODOLOGY AND DISCUSSION

We are developing a system which discovers the presence of ranking scam in mobile applications. In this system we locate the ranking scam by mining the active period's mainly leading session and collect three evidences ranking, rating and review. Using these three evidences we are calculating aggregation and performed hypothesis test on it to get actual rank of mobile app and authentication of user is done for further access.

SYSTEM FLOW

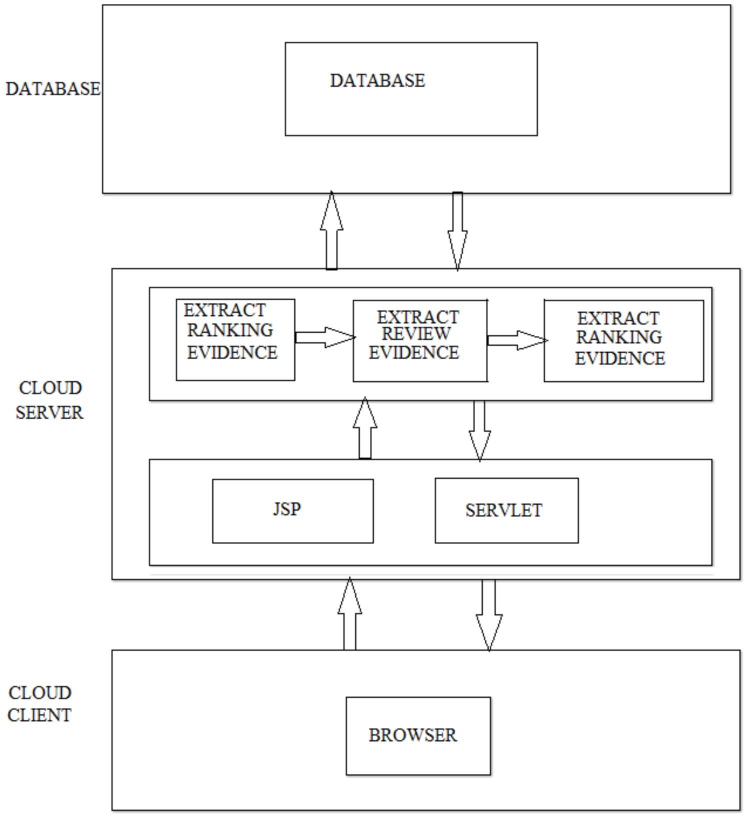

Fig No 01 Architecture framework

This figure implies the framework of our ranking scam detection system for mobile apps. We are gathering historical records of some mobile apps from this records we will identify leading sessions with help of algorithm. Then we will extract the evidences of ranking based, rating based, review based. Then combine these evidences by aggregation method and on that we will perform a statistical hypothesis test which tends to actual ranking of the applications, then for futher access user authentication will be done.

V.CONCLUSION

We are developing a system which discovers the presence of ranking scam in mobile applications. Specifically, we first displayed that ranking scam happened in leading sessions and provided a method for mining leading sessions for each Application from its historical ranking records. Then, we recognized ranking, rating and review based evidences for ascertaining ranking scam. More we proposed an optimized based aggregation method to integral all the evidences. A perspective of this approach is that all the evidences can be modeled by hypothesis tests, thus it is comfortable to be extended with other evidences from domain knowledge to unripe ranking scam. Finally, we will validate the proposed system with extensive experiments on real-world App data collected from the Play store.

REFERENCES

1. 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.
2. 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.
3. H. Zhu, E. Chen, K. Yu, H. Cao, H. Xiong, and J. Tian, "Mining personal context-aware preferences for mobile users," in Proc. IEEE 12th Int. Conf. Data Mining, 2012, pp. 1212–1217.
4. Y. Ge, H. Xiong, C. Liu, and Z.-H. Zhou, "A taxi driving fraud detection system," in Proc IEEE 11th Int. Conf. Data Mining, 2011, pp. 181–190.
5. Jindal and B. Liu, "Opinion spam and analysis," in Proc. Int.Conf. Web Search Data Mining, 2008, pp. 219–230.
6. Klementiev, D. Roth, and K. Small, "An unsupervised learning algorithm for rank aggregation," in Proc. 18th Eur. Conf. Mach. Learn., 2007, pp. 616–623.
7. Hengshu Zhu, Hui Xiong, Yong Ge, and Enhong Chen "Discovery of Ranking Fraud for Mobile Apps"in Proc IEEE Jan 2015.