NOVATEUR PUBLICATIONS
INTERNATIONAL JOURNAL OF INNOVATIONS IN ENGINEERING RESEARCH AND TECHNOLOGY [IJIERT]
ISSN: 2394-3696
VOLUME 4, ISSUE 6, June-2017

DISCOVERY OF RANKING FRAUD FOR MOBILE APPS

NAVEEN IJERI
Students, Department of CSE,KLS Gogte Institute Of Technology,Belagavi

PREETIGANAGI
Students, Department of CSE,KLS Gogte Institute Of Technology,Belagavi

PRIYANKA RAMBAN
Students, Department of CSE,KLS Gogte Institute Of Technology,Belagavi

PROF. N. V. KAREKAR
Assistant Professor, Department of CSE,KLS Gogte Institute Of Technology,Belagavi

ABSTRACT
Ranking fraud in the mobile App market refers to fraudulent or deceptive activities which have a purpose of bumping up the Apps in the popularity list. It becomes more and more frequent for App developers to use shady means such as inflating their Apps' sales or posting phony App ratings to commit ranking fraud. While the importance of preventing ranking fraud has been widely recognized. There is limited understanding and research in this area. In this project, we provide a holistic view of ranking fraud and propose a ranking fraud detection system for mobile Apps. We investigate two types of evidences i.e. ranking based evidences, rating based evidences by modelling Apps' ranking and rating behaviours through statistical hypotheses tests. We evaluate the proposed system with real-world App data collected from the App Store for a long time period. In the experiments we validate the effectiveness of the proposed system and show the scalability of the detection algorithm as well as some regularity of ranking fraud activities.

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

INTRODUCTION

The number of mobile Apps has grown at a breath taking rate over the past few years. For example, as of the end of April 2013, there are more than 1.6 million Apps at Apple's App store and Google Play. Many App stores launched apps daily. Leader boards which demonstrate the ranking chart of most popular Apps. The App leader board is one of the most important ways for promoting mobile Apps. A higher rank on the leader board usually leads to a huge number of downloads and million dollars in revenue. Therefore, App developers tend to explore various ways such as advertising campaigns to promote their Apps in order to have their Apps ranked as high as possible in such App leader boards.

As a recent trend instead of relying on traditional marketing solutions shady App developers resort to some fraudulent means to deliberately boost their Apps and eventually manipulate the chart rankings on an App store. This is usually implemented by using so-called "*bot farms*" or "*human water armies*" to inflate the App downloads and ratings in a very short time. For example, an article from Venture Beat reported that when an App was promoted with the help of rankingmanipulation it could be propelled from number 1,800 to the top 25 in Apple's top free leader board and more than 50,000-100,000 new users could be acquired within a couple of days. In fact, such ranking fraud raises great concerns to the mobile App industry. For example, Apple has warned of cracking down on App developers who commit ranking fraud in the Apple's App store.

In the literature, while there are some related work, such as web ranking spam detection online review spam detection [11] and mobile App recommendation [12], the problem of detecting ranking fraud for mobile Apps is still under-explored. To fill this crucial void in this project we propose to develop a ranking fraud detection system for mobile Apps. We identify several important challenges. First, ranking fraud does not always happen in the whole life cycle of an App, so we need to detect the time when fraud happens. Second, due to the huge number of mobile Apps it is difficult to manually label ranking fraud for each App so it is

important to have a way to automatically detect ranking fraud without using any benchmark information. Finally, due to the dynamic nature of chart rankings it is not easy to identify and confirm the evidences linked to ranking fraud [1].

EXISTING SYSTEM

3.1. DISADVANTAGES OF EXISTING SYSTEM:

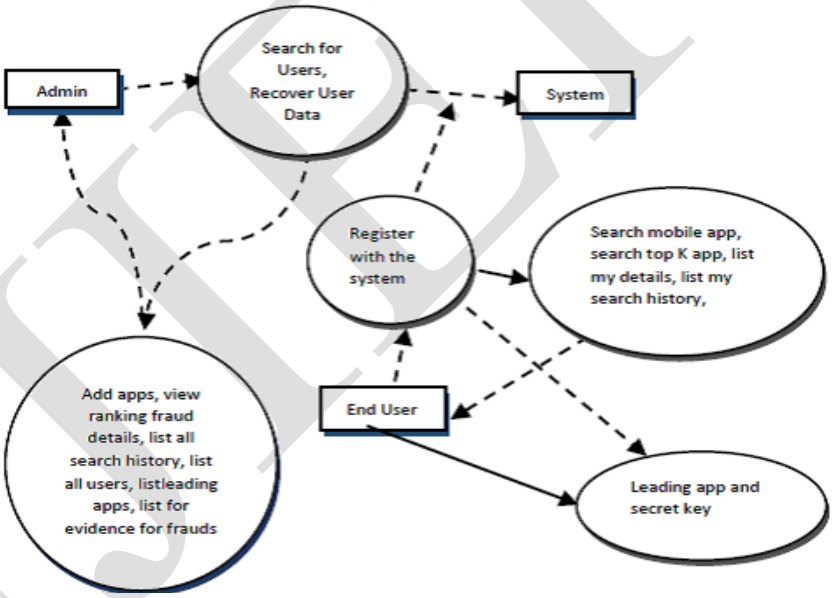
- Although some of the existing approaches can be used for anomaly detection from historical rating and review records, they are not able to extract fraud evidences for a given time period.
- Cannot able to detect ranking fraud happened in Apps' historical leading sessions.
- There is no existing benchmark to decide which leading sessions or Apps really contain ranking fraud.

PROPOSED SYSTEM

We proposed 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 behaviours.We find that the fraudulent Apps often have different ranking patterns in each leading session compared with normal Apps. Thus we characterize some fraud evidences from Apps historical ranking records and develop two functions to extract such ranking based fraud evidences. In Ranking Based Evidences by analysing the Apps historical ranking records. In Rating Based Evidences user rating is one of the most important feature 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.

SYSTEM DESIGN

4.1 DATA FLOW DIAGRAM



IMPLEMENTATION

5.1. IMPLEMENTATION DETAILS

The implementation phase of any project development is the most important phase as it yields the final solution, which solves the problem at hand. The implementation phase involves the actual materialization of the ideas, which are expressed in the analysis document and developed in the design phase.

Implementation should be perfect mapping of the design document in a suitable programming language in order to achieve the necessary final product. Often the product is ruined due to incorrect programming language chosen for implementation or unsuitable method of programming.

It is better for the coding phase to be directly linked to the design phase in the sense, if the design is in terms of objects oriented then implementation should be preferably carried out in an object oriented way.

5.2. MODULES

5.2.1. ADMIN LOGIN

In this module the Admin has to login by using valid user name and password. After login successful he can do some operations such as add apps, view all applications, view ranking fraud details view all search history, lists all users, list leading applications, view evidence for the frauds and logout[2].

5.2.2. ADD APP

In this module, the admin can add the applications. If the admin want add the new app, he will enter application name, app description, mobile type, users, file name, application images and click on register. The details will be stored in the database.

5.2.3. VIEW APPLICATION

In this module, when the admin clicks on view application, application name, app description, mobile type, users, file name, application images will be displayed.

5.2.4. RANKING FRAUD DETAILS

In this module, when admin clicks on ranking fraud details, ranking fraud count, user name, mobile type, application name, application ID, date and time will be displayed[2].

5.2.5. EVIDENCE FOR FRAUDS

In this module, when admin clicks on evidence for fraud details, user name, mobile type, application name, application ID, fraud IP address, fraud system name, date and time will be displayed [3].

5.2.6. USER LOGIN

In this module, there are n numbers of users are present. User should register before doing some operations. After registration successful he has to login by using authorized user name and password. Login successful he will do some operations like search mobile apps, search top K apps, view my details, list my search history, request for secret key, logout. If user clicks on my details button, then the server will give response to the user with their tags such as UID, user name, password, e-mail, contact no, location, DOB, gender, pin code details.

5.2.7. SEARCH AND DOWNLOAD MOBILE APPS

In this module user can search the mobile app type and click on search then he will enter application name, application images, view details of mobile app, enters application ID enter the secret key and download the file and send response to user[4].

5.2.8. SEARCH FOR TOP K APPLICATIONS

In this module user enter the application name and select the top N details then leading app details will be displayed such as application name, app description, mobile type, users, file name, application images and ratings will be displayed.

RESULTS

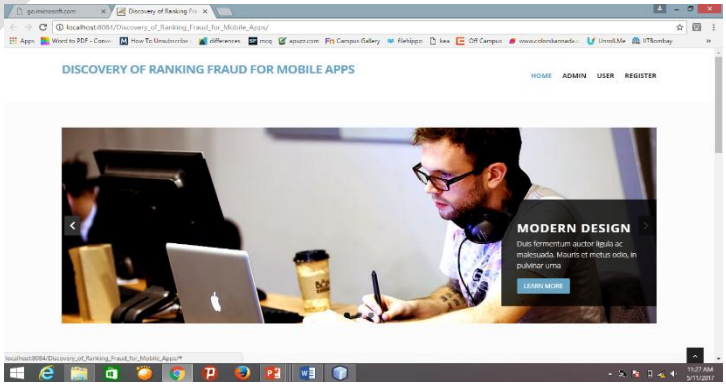


Fig 6.1. Home page

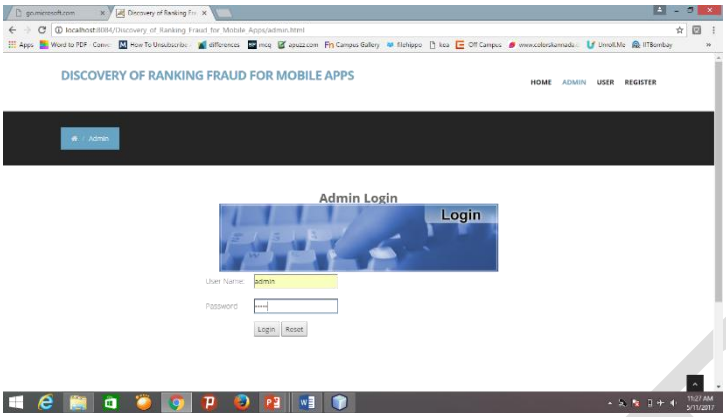


Fig 6.2. Admin login page

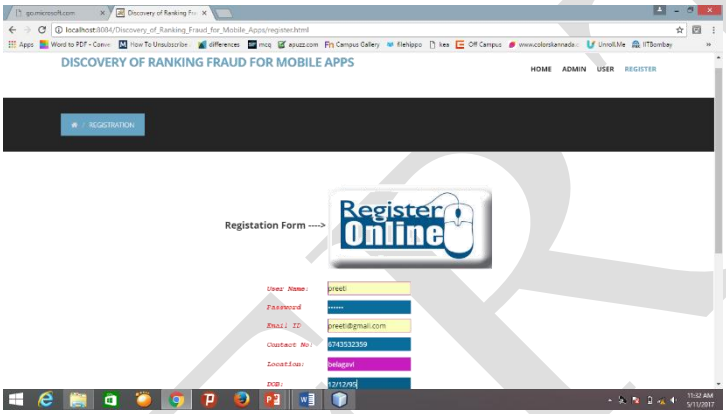


Fig 6.3. User registration

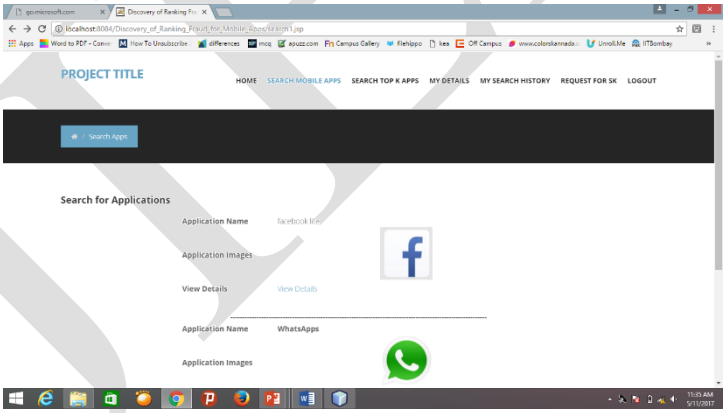


Fig 6.4. Apps Listing

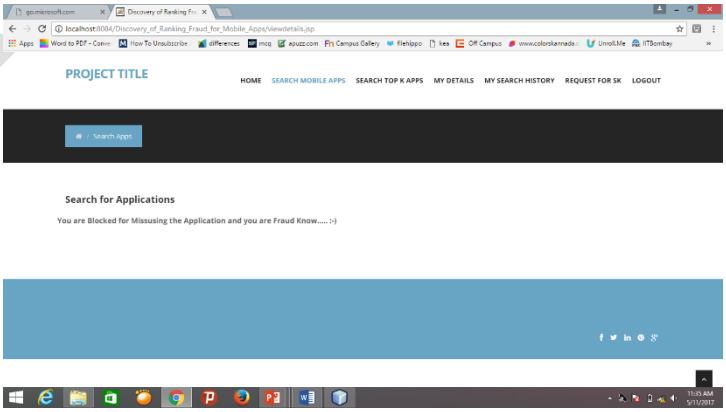


Fig 10.9. Fraud user

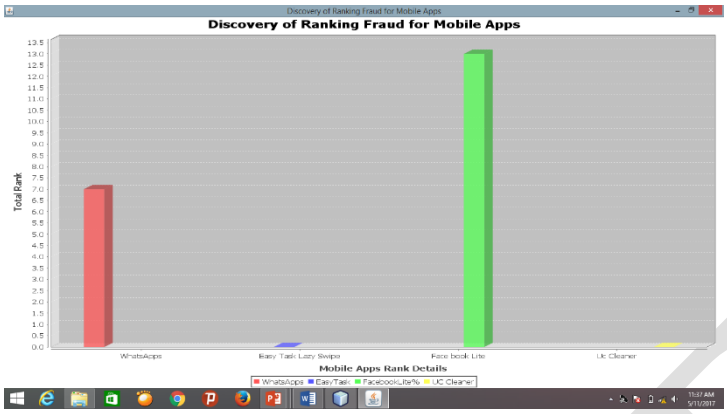


Fig 10.10. Ranking results

CONCLUSION

In this project, 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 based evidences and rating based evidences for detecting ranking fraud. We proposed an optimization based aggregation method to integrate all the evidences for evaluating the credibility of leading sessions from mobile Apps. An unique perspective of this approach is that all the evidences can be modelled by statistical hypothesis tests, thus it is easy to be extended with other evidences from domain knowledge to detect ranking fraud. Finally, we validate the proposed system with extensive experiments on real-world App data collected from the App store. Experimental results showed the effectiveness of the proposed approach.Besides ratings, most of the App stores also allow users to write some textual comments as App reviews [1]. Such reviews can reflect the personal perceptions and usage experiences of existing users for particular mobile Apps. Specifically, before downloading or purchasing a new mobile App user sees the reviews. Therefore, fake users 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 leaderboard.

REFERENCES

1) Hengshu Zhu, Hui Xiong, Senior Member, IEEE, Yong Ge, and Enhong Chen, Senior Member, IEEE*"detection of fraud ranking for mobile apps", IEEE Transaction and data engineering, vol 27,No 1, January 2015.*

2) https://developer.apple.com/news/index.php?id=0- 2062012a.

3) http://venturebeat.com/2012/07/03/apples-crackdown-on- app-ranking-manipulation/.

4) http://www.ibtimes.com/apple-threatens-crackdown-biggest-app-store-ranking-fraud-406764.

5) Y. Ge, H. Xiong, C. Liu, and Z.-H. Zhou. *A taxi driving fraud detection system. In Proceedings of the 2011 IEEE 11th International Conference on Data Mining, ICDM '11,pages 181{190, 2011.*

6) D. F. Gleich and L.-h. Lim. Rank *aggregation via nuclear norm minimization. In Proceedings of the 17th ACM SIGKDD international conference on Knowledge discovery and data mining, KDD '11, pages 60{68, 2011.*

7) J. Kivinen and M. K. Warmuth. *Additive versus exponentiated gradient updates for linear prediction. In Proceedings of the twenty-seventh annual ACM symposium on Theory of computing, STOC '95, pages 209{218, 1995.*

8) A. Klementiev, D. Roth, and K. Small. *An unsupervised learning algorithm for rank aggregation. In Proceedings of the 18th European conference on Machine Learning, ECML '07, pages 616{623, 2007.*

9) A. Klementiev, D. Roth, and K. Small. *Unsupervised rank aggregation with distance-based models. In Proceedings of the 25th international conference on Machine learning, ICML '08, pages 472{479, 2008.*

10) E.-P. Lim, V.-A. Nguyen, N. Jindal, B. Liu, and H. W. Lauw. *Detecting product review spammers using rating behaviors. In Proceedings of the 19th ACM international conference on Information and knowledge management, CIKM '10, pages 939{948, 2010.*

11) 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.*

12) K. Shi and K. Ali. Getjar *mobile application recommendations with very sparse datasets. In Proceedings of the 18th ACM SIGKDD international conference on Knowledge discovery and data mining, KDD '12, pages 204{212, 2012.*

13) N. Spirin and J. Han. *Survey on web spam detection: principles and algorithms. SIGKDD Explore. Newsl., 13(2):50{64, May 2012.*

14) Z. Wu, J. Wu, J. Cao, and D. Tao. Hysad*: a semi-supervised hybrid shilling attack detector for trustworthy product recommendation. In Proceedings of the 18th ACM SIGKDD international conference on Knowledge discovery and data mining, KDD '12, pages 985{993, 2012.*

I.