

# MOBILE APP SECURITY & FEATURES LEVEL ASSESSMENT

Gayatri Shevkar, Purushottam Kale, Aasha Bhavar, Rahul Nikam

<sup>1,2,3,4</sup>*Department Of Computer Engineering, Late G. N. Sapkal College Of Engineering, Maharashtra, Nashik*

## ABSTRACT

*Fraud Ranking in the mobile App market refers to fraudulent or deceptive activities which have a purpose of bumping up the Applications in the popularity list. Indeed, it becomes more and more frequent for Application developers to use shady means, such as initiating their Applications sales or posting phony Application 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.*

*To this end, we provide a holistic view of ranking fraud and propose a ranking fraud detection system for mobile Apps. Specially, we propose to accurately locate the ranking fraud by mining the active periods, namely leading sessions, of mobile Applications. Such leading sessions can be leveraged for detecting the local anomaly instead of global anomaly of App rankings.*

*Furthermore, we 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. In addition, we introduced an optimization based aggregation method to integrate all the evidences for fraud detection.*

*Finally, we evaluate the proposed system with real-world App data collected from the IOS 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.*

**Keyword-** *Mobile apps, Ranking fraud detection, Evidence aggregation, Historical ranking records, Rating and review, Specification & feature, App sorting.*

## 1. INTRODUCTION

Over the last few years the number of mobile Apps has been growing on a very large scale. At the end of April 2018 there is number of more than 3.4 million Applications at Apples App store and Google Play. Different App stores launched their leader board on daily basis to inspire the development of mobile Apps which displays the chart rankings of most popular Apps. In fact for promoting mobile Apps, leader board of apps is the most important ways in the market. An app ranking at the top on the leader board ultimately leads to a large number of downloads and million dollars in revenue. This results in exploring of different ways by the App developers like organizing promotional drives to advertise their Apps in order to get top position in App leader boards.

The very recent trend followed in market by the corrupt App developers for bumping up of an App is to use deceptive means to intentionally boost their apps. Lastly, the chart rankings on a App store are also manipulated. 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. Venture Beat is an article that reported, using ranking manipulation when an App was promoted, in Apples top free leader board it could be push forward from number 1,800 to the up most 25 and new users more than 50,000-100,000 could be acquired within a couple of days.

It is worth noting that all the evidences are extracted by modeling application ranking, rating and review behaviors through statistical hypotheses tests. The proposed framework is scalable and can be extended with other domain generated evidences for ranking fraud detection. Finally, we evaluate the proposed system with real-world application data collected from the Apple's App store for a long time period, i.e., more than two years. Experimental

results show the effectiveness of the proposed system, the scalability of the detection algorithm as well as some regularity of ranking fraud activities.

## 2. Architectural Design

System Architecture have following modules

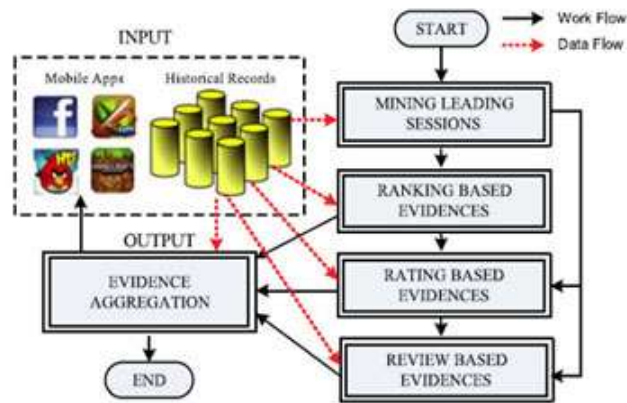
1. Mining Leading Sessions
2. Rating Based Evidences
3. Review Based Evidences
4. Evidence Aggregation

In Mining Leading Session module, we develop our system environment with the details of App like an app store. Intuitively, the leading sessions of a mobile App represent its periods of popularity, so the ranking manipulation will only take place in these leading sessions. Therefore, the problem of detecting ranking fraud is to detect fraudulent leading sessions. Along this line, the rest task is how to mine the leading sessions of a mobile App from its historical ranking records.

In Rating Based Evidences module, we enhance the system with Rating based evidences module. The ranking based evidences are useful for ranking fraud detection. However, sometimes, it is not sufficient to only use ranking based evidences. For example, some application created by the famous developers, such as Gameloft, may have some leading events with large values of u1 due to the developer's credibility and the 'word-of-mouth' advertising effect. Moreover, some of the legal marketing services, such as 'limited-time discount', may also result in significant ranking based evidences. To solve this issue, we also study how to extract fraud evidences from application historical rating records.

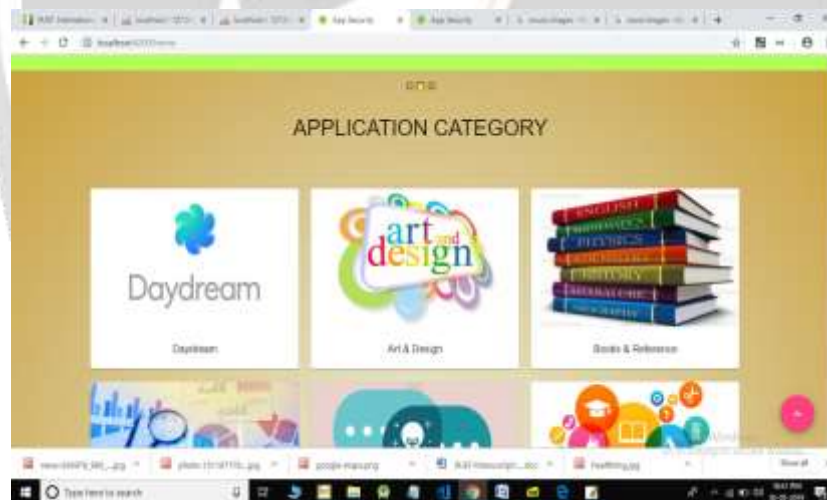
In Review Based Evidences module we add the Review based Evidences module in our system. Besides ratings, most of the App stores also allow users to write some textual comments as App reviews. Such reviews can reflect the personal perceptions and usage experiences of existing users for particular mobile applications. Indeed, review manipulation is one of the most important perspectives of application ranking fraud. Specifically, before downloading or purchasing a new mobile application, users often first read its historical reviews to ease their decision making, and a mobile application contains more positive reviews may attract more users to download. Therefore, imposters often post fake reviews in the leading sessions of a specific application in order to inflate the application downloads, and thus propel the application ranking position in the leader-board.

**Architectural Design.**



**Fig -1** System Architecture

In Evidence Aggregation module we develop the Evidence Aggregation module to our system. After extracting three types of fraud evidences, the next challenge is how to combine them for ranking fraud detection. Indeed, there are many ranking and evidence aggregation methods in the literature, such as permutation based models score based models and Dumpster-Shafer rules. However, some of these methods focus on learning a global ranking for all candidates. This is not proper for detecting ranking fraud for new Apps. Other methods are based on supervised learning techniques, which depend on the labelled training data and are hard to be exploited. Instead, we propose an unsupervised approach based on fraud similarity to combine these evidences.



**Fig -2:** Result 1



Fig -3: Result 2

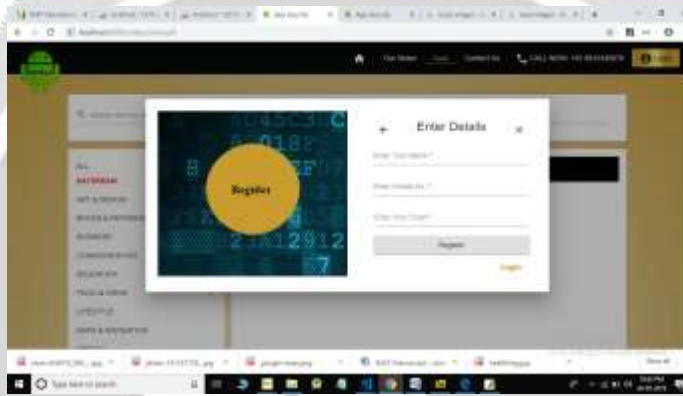


Fig -4: Result 3

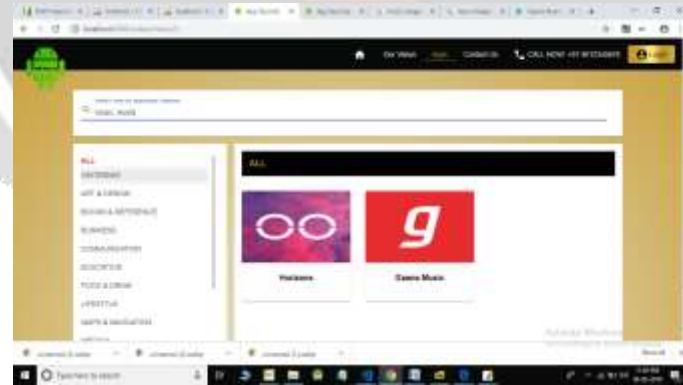
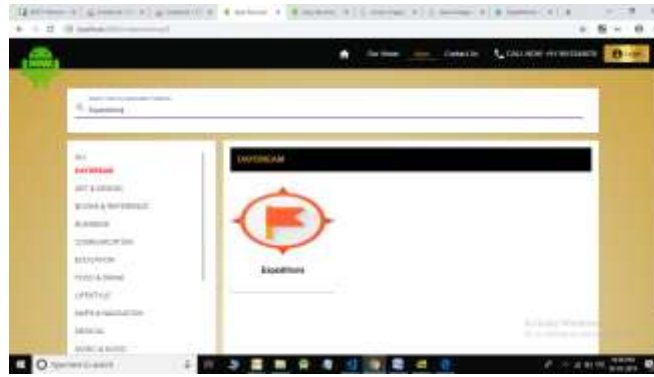


Fig -5: Result – Feature wise Search



**Fig -6:** Result – Search by App Name

#### 4. CONCLUSIONS

In this report, we developed a ranking 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, 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. 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. Experimental results showed the effectiveness, of the proposed approach. In the future, we plan to study more effective evidences and analyze the latent relationship among rating, review and rankings. Moreover, we will extend our ranking approach with other mobile App related services, such as mobile Apps recommendation, for enhancing user experience.

#### 5. REFERENCES

- [1] D. M. Blei, A. Y. Ng, and M. I. Jordan, "Latent Dirichlet allocation," *J. Mach. Learn. Res.*, pp. 993-1022, 2003. M. Young, *The Technical Writer's Handbook*. Mill Valley, CA: University Science, 1989.
- [2] E.-P. Lim, V.-A. Nguyen, N. Jindal, B. Liu, and H. W. Lauw, "Detecting product review spammers using rating behaviors," in *Proc. 19th ACM Int. Conf. Inform. Knowl. Manage.*, 2010, pp. 939-948.
- [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] 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.
- [5] D. M. Blei, A. Y. Ng, and M. I. Jordan, "Latent Dirichlet allocation," *J. Mach. Learn. Res.*, pp. 993-1022, 2003. M. Young, *The Technical Writer's Handbook*. Mill Valley, CA: University Science, 1989.
- [6] E.-P. Lim, V.-A. Nguyen, N. Jindal, B. Liu, and H. W. Lauw, "Detecting product review spammers using rating behaviors," in *Proc. 19th ACM Int. Conf. Inform. Knowl. Manage.*, 2010, pp. 939-948.