International Journal of Research
Available at https://edupediapublications.org/journals

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 22
November 2018

Discovery of Ranking Fraud for Mobile Apps

P.Vijaya kumari[1], H.C.V.Ramana Rao [2]
[1]P.G. Scholar, [2]Assistant Professor
[1,2]BRANCH: Computer Science Engineering
[1,2] SVR Engineering college .
Email: [1] vijjuroyal539@gmail.com,[2]venkataramana.h@gmail.com

Abstract

Ranking fraud in the mobile App market insinuates fraudulent or deceptive activities which have a purpose behind thumping up the Apps in the popularity list. Certainly, it ends up being progressively visit for App architects to use darken implies, for instance, growing their Apps' arrangements or posting phony App assessments, to submit ranking fraud. While the hugeness of thwarting ranking fraud has been comprehensively seen, there is obliged appreciation and research around there. To this end, in this paper, we give a widely inclusive viewpoint of ranking fraud and propose a ranking fraud detection structure for mobile Apps. Specifically, we at first propose to accurately locate the ranking fraud by mining the dynamic time periods, particularly leading sessions, of mobile Apps. Such leading sessions can be used for recognizing the close-by peculiarity instead of overall inconsistency of App rankings. Furthermore, we investigate three sorts of affirmations, i.e., ranking based affirmations, rating based affirmations and review based affirmations, by showing Apps' ranking, rating and overview rehearses through statistical hypotheses tests. Besides, we propose a progression based accumulation procedure to organize all of the affirmations for fraud detection. Finally, we evaluate the proposed system with genuine App data accumulated from the iOS App Store for a long time that's all anyone needs to know. In the tests, we endorse the practicality of the proposed structure, and show the flexibility of the detection algorithm and also some consistency of ranking fraud works out.

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

INTRODUCTION

The amount of mobile Apps has created at an astounding rate throughout ongoing years. For example, as of the complete of April 2013, there are more than 1.6 million Apps at Apple's App store and Google Play. To energize the enhancement of mobile Apps, various App stores impelled step by step App pioneer sheets, which demonstrate the outline rankings of most surely understood Apps. In actuality, the App pioneer board is a champion among the most basic courses for propelling mobile Apps. A higher rank on the pioneer board when in doubt prompts incalculable and million dollars in wage. In this way, App architects will when all is said in done explore distinctive courses, for instance, publicizing endeavors to propel their Apps with the true objective to have their Apps situated as high as possible in such App pioneer sheets. Regardless, as a progressing design, as opposed to relying upon traditional marketing courses of action, cloud App creators fall back on some fraudulent method to intentionally encourage their Apps and over the long haul control the outline rankings on an App store. This is by and large executed by using indicated "bot farms" or "human water military" to extend the App downloads and examinations in a short range. For example, an article from Venture Beat uncovered that, when an App was progressed with the help of ranking control, it could be pushed from number 1,800 to the fundamental 25 in Apple's sans best pioneer board and more than 50,000-100,000 new customers could be gotten inside a few days. As a matter of fact, such ranking fraud raises staggering stresses to the mobile App industry. For example, Apple has forewarned of making a move against App engineers who submit ranking fraud in the Apple's App store. In the composition, while there are some related work, for instance, web ranking spam detection online study spam detection and mobile App proposal the issue of recognizing ranking fraud for mobile Apps is still under-explored.

To fill this noteworthy void, in this paper, we propose to develop a ranking fraud detection structure for mobile Apps. Along this line, we perceive a couple of fundamental troubles. In any case, ranking fraud does not for the most part happen in the whole life cycle of an App, so we need to perceive the time when fraud happens. Second, as a result of the massive number of mobile Apps, it is difficult to physically name ranking fraud for each App, so it is fundamental to have a way to deal with normally perceive ranking fraud without using any benchmark data. Finally, due to the dynamic thought of framework rankings, it is hard to recognize and insist the affirmations associated with ranking fraud. Unmistakably, our attentive recognition reveals that fraudulent Apps don't by and large be situated high in the leaderboard, anyway just in some leading events, which shape differing leading sessions. Note that we will display both leading events and leading sessions in detail later. Figuratively speaking, ranking fraud generally happens in these leading sessions. Thusly, recognizing ranking fraud of mobile Apps is truly to perceive ranking fraud inside leading sessions of mobile Apps. Specifically, we at first propose an essential yet convincing algorithm

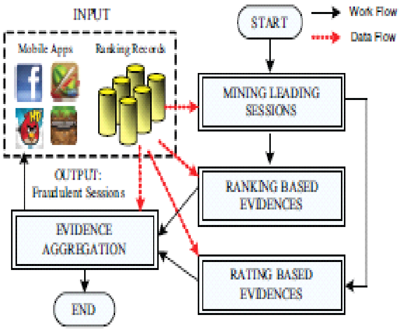


Figure 1: The framework of the ranking fraud detection system for mobile Apps.

To perceive the leading sessions of each App reliant on its credible ranking records. By then, with the examination of Apps' ranking practices, we find that the fraudulent Apps every now and again have unmistakable ranking models in each leading session differentiated and run of the mill Apps. Appropriately, we depict some fraud affirmations from Apps' evident ranking records, and make three abilities to think such ranking based fraud affirmations. Regardless, the ranking based affirmations can be affected by some real marketing endeavors, for instance, "compelled time discount". Consequently, it isn't sufficient to simply use ranking based affirmations. Thusly, we moreover propose two abilities to discover rating based affirmations, which reflect some peculiarity plans from Apps' irrefutable rating records. Similarly, we develop an unsupervised verification collection method to consolidate these two sorts of affirmations for evaluating the legitimacy of leading sessions from mobile Apps. Figure 1 exhibits the structure of our ranking fraud detection system for mobile Apps. It is imperative that all of the affirmations are removed by exhibiting Apps' ranking and rating rehearses through statistical speculations tests. The proposed structure is versatile and can be connected with other space made affirmations for ranking fraud detection. Finally, we survey the proposed structure with genuine App data accumulated from the Apple's App store for a long time period. Test outcomes exhibit the reasonability of the proposed structure, the flexibility of the detection algorithm and what's more some consistency of ranking fraud works out.

Related Works

This paper plans to recognize clients creating spam audits or survey spammers. In this recognize a few element practices of audit spammers and model these practices to identify the spammers. Specifically, this looks to display the following practices. Initially, spammers may target correct items or item bunches in request to expand their effect. Second, they probably turn from the other commentator in their appraisals of items. In this propose scoring strategies to quantify the dimension of spam for each commentator and apply them on an Amazon audit dataset. Know at that point select a sub-set of very far fetched analysts for further examination by our client evaluators with the assistance of an electronic spammer valuation programming uniquely produced for client assessment tests. Our outcomes demonstrate that our proposed positioning and administered techniques are valuable in finding spammer smooth break other benchmark technique dependent on supportiveness cast a ballot alone. In this at long last demonstrate that the identified spammers have more essential effect on appraisals thought about with the unsupportive commentators. From this paper be have alluded:- • Concept of extricating of rating and positioning. • Idea of extricating of review[1].

Advances in GPS following innovation have empowered us to introduce GPS following gadgets in city taxicabs to gather a lot of GPS follows under operational time limitations. These GPS follows give unparalleled open doors for us to reveal taxi driving extortion exercises. In this paper, be build up a taxi driving extortion discovery framework, which can methodicallly explore taxi driving extortion. In this framework, propese first give capacities to discover two parts of confirmations: travel course proof and driving separation proof. Besides, a third gathering is intended to join the two parts of confirmations in view of dempster-Shafer hypothesis. To actualize the framework, In this initially distinguish intriguing destinations from a lot of taxi GPS logs. At that point, this propose a sans parameter technique to mine the movement course confirms. Likewise, In this acquaint course check with relate to a run of the mill driving way from a fascinating site to another. In view of course stamp, this build up a generative measurable model to portray the sharing of driving separation what's more, recognize the driving separation confirmations. At long last, can this assess the taxi driving misrepresentation recognition framework with vast scale genuine taxi GPS logs. In the trial, be have find out some consistency of driving extortion exercises and research the drive of drivers to submit a driving extortion by investigating the delivered taxi extortion information. From this paper be have alluded:- • Idea of extortion location [2]

Evaluative messages on the Web have turn into a profitable premise of conclusions on items, administrations, occasions, people, and so forth. As of late, numerous scientists have contemplated such feeling sources as item surveys, meeting posts, and websites. Notwithstanding, existing exploration has been centered around association and rundown vzation of conclusions utilizing ordinary dialect preparing and information mining strategies. A vital subject that has been dismissed so far is judgment spam or trust value of online feelings. In this paper, be think about this issue with regards to item surveys, which are assessment rich and are extensively utilized by customers and item producers. In the recent years, a few new businesses additionally showed up which aggregate sentiments from item audits. It is in this manner high time to consider spam in audits. To the best of our insight, there is still no distributed examination on this theme, in spite of the fact that Web spam and email spam have been explored expansively. In this will see that sentiment spam is fairly unique in relation to organize spam furthermore, email spam, and hence requires diverse location systems. In view of the investigation of 5.8 million audits and 2.14 million analysts from amazon.com, in this demonstrate feeling spam in audits is across the board. This paper dissects such spam exercises and shows some crisp procedures to identify them [3].

Numerous applications in data recovery, common dialect handling, information mining, and related fields require a positioning of cases as for indicated criteria instead of a grouping. Besides, for some such issues, numerous perceived positioning models have been very much considered and it is alluring to join their outcomes into a joint positioning, formalism meant as rank collection. This work introduces a novel invalid learning calculation for rank accumulation (ULARA) which restores a direct blend of the individual positioning capacities based on the standard of remunerating requesting assention between the rankers. In adding to exhibiting ULARA, we demonstrate its prosperity on an information association assignment crosswise over specially appointed recovery frameworks [4].

PURPOSE OF THE PROJECT

We first propose a fundamental yet feasible algorithm to perceive the leading sessions of each App reliant on its chronicled ranking records. By then, with the examination of Apps' ranking practices, we find that the fraudulent Apps frequently have unmistakable ranking models in each leading session differentiated and run of the mill Apps. In this way, we depict some fraud affirmations from Apps' legitimate ranking records, and make three abilities to think such ranking based fraud affirmations. We furthermore propose two sorts of fraud affirmations subject to Apps' assessing and study history, which reflect some variation from the norm structures from Apps' evident rating and review records.

In Ranking Based Evidences, by separating the Apps' chronicled ranking records, we see that Apps' ranking practices in a leading event reliably satisfy a specific ranking precedent, which includes three unmistakable ranking stages, to be particular, rising stage, keeping up stage and withdraw organize.

In Rating Based Evidences, especially, after an App has been appropriated, it might be assessed by any customer who downloaded it. In all actuality, customer rating is a champion among the most basic features of App take note. An App which has higher rating may attract more customers to download and can similarly be situated higher in the pioneer board. In this way, evaluating control is also a basic perspective of ranking fraud.

PROBLEM IN EXISTING SYSTEM

- In the composition, while there are some related work, for instance, web ranking spam detection, online review spam detection and mobile App proposition, the issue of recognizing ranking fraud for mobile Apps is still under-examined.
- Generally, the related works of this examination can be gathered into three characterizations.
- The top notch is about web ranking spam detection.
- The below average is fixated around recognizing on the web review spam.
- Finally, the second rate class consolidates the examinations on mobile App proposition

SOLUTION OF THESE PROBLEMS

Yet a bit of the present systems can be used for peculiarity detection from irrefutable rating and review records, they are not prepared to expel fraud affirmations for a given period (i.e., leading session). Can't prepared to recognize ranking fraud happened in Apps' chronicled leading sessions There is no present benchmark to pick which leading sessions or Apps really contain ranking fraud.

PLAN OF THESE PROBLEMS

- We first propose a direct yet effective algorithm to perceive the leading sessions of each App subject to its chronicled ranking records. By then, with the examination of Apps' ranking practices, we find that the fraudulent Apps frequently have unmistakable ranking precedents in each leading session differentiated and normal Apps. Thusly, we depict some fraud affirmations from Apps' bona fide ranking records, and make three abilities to think such ranking based fraud affirmations.

- We moreover propose two sorts of fraud affirmations reliant on Apps' assessing and overview history, which reflect some anomaly structures from Apps' chronicled rating and review records.

- In Ranking Based Evidences, by separating the Apps' chronicled ranking records, we see that Apps' ranking practices in a leading event reliably satisfy a specific ranking precedent, which contains three different ranking stages, to be particular, rising stage, keeping up stage and subsidence organize.

- In Rating Based Evidences, especially, after an App has been conveyed, it might be assessed by any customer who downloaded it. In actuality, customer rating is a champion among the most essential features of App business. An App which has higher rating may pull in more customers to download and can moreover be situated higher in the pioneer board. Subsequently, assessing control is similarly a fundamental perspective of ranking fraud.

- In Review Based Evidences, other than assessments, most of the App stores similarly empower customers to stay in contact with some printed comments as App studies. Such reviews can reflect the individual observations and use experiences of existing customers for particular mobile Apps.

PROPOSED SYSTEM

- Three sorts of data including content, customer demography, and casual network features are every now and again used in advanced pestering detection. Since the substance is the most tried and true, our work here spotlights on substance based advanced tormenting detection.
- In development, each auto encoder layer is intended to take in an

unquestionably one of a kind depiction of the data.

- In this paper, we develop another substance depiction show reliant on a variety of SDA: thought little of stacked de noising auto encoders (m SDA), which gets straight instead of nonlinear projection to enliven planning and limits boundless tumult spread with the true objective to take in more healthy depictions.

- In this paper, we investigate one significant learning procedure named stacked de noising auto encoder (SDA). SDA stacks a couple of de noising auto encoders and interfaces the yield of each layer as the insightful depiction. Each de noising auto encoder in SDA is set up to recover the data from a debased adjustment of it. The information is polluted by discretionarily setting a segment of the commitment to zero, which is called dropout uproar. This de noising process urges the auto encoders to learn solid depiction.

- We utilize semantic data to develop m SDA and make Semantic-redesigned Marginalized Stacked De noising Auto encoders (smS DA). The semantic data contains hassling words. A customized extraction of tormenting words reliant on word embeddings is proposed so the included human work can be diminished. In the midst of getting ready of smSDA, we try to change tormenting features from other run of the mill words by finding the lethargic structure, i.e. relationship, among tormenting and normal words. The sense behind this musing is that some tormenting messages don't contain pestering words. The association data found by smSDA changes tormenting features from customary words, and this consequently empowers detection of bothering messages without containing hassling words.

NEED FOR COMPUTERIZATION

We overall know the essentialness of computerization. The world is progressing at helping rate and everyone is running short of time. One for the most part needs to get the data and play out an endeavor he/she/they desire(s) inside a concise time allotment and too with proportion of profitability and precision. The application regions for the computerization have been picked dependent on following segments:

- Minimizing the manual records kept at different regions.

- There will be more data genuineness.

- Facilitating distinctive statistical data which helps in essential authority?

- To diminish manual undertakings in activities that included repetitive work.

Data DESIGN

The information setup is the association between the data structure and the customer. It incorporates the making point of interest and methodologies for data preparation and those methods are imperative to put trade data in to a usable shape for getting ready can be expert by surveying the PC to scrutinize data from a made or printed report or it can occur by having people entering the data direct into the system. The arrangement of data revolves around controlling the proportion of data required, controlling the oversights, avoiding deferment, keeping up a vital separation from extra means and keeping the method direct. The data is organized in such a course along these lines, to the point that it outfits security and ease of use with holding the insurance. Data Design pondered the going with things:

- What data should be given as data?
- How the data should be planned or coded?
- The talk to deal with the working personnel in giving data.
- Methods for arranging input endorsements and dares to seek after when bungle occur.

Goals

1.Input Design is the route toward changing over a customer arranged depiction of the commitment to a PC based structure. This structure is basic to keep up a vital separation from bungles in the data input process and exhibit the correct bearing to the organization for getting right data from the electronic system.

2. It is expert by making straightforward screens for the data segment to manage tremendous volume of data. The goal of arranging input is to make data entry less complex and to be free from bungles. The data segment screen is organized with the goal that all of the data controls can be performed. It also gives record seeing workplaces.

3.When the data is entered it will check for its authenticity. Data can be entered with the help of screens. Legitimate messages are given as when required with the objective that the customer won't be in maize of minute. Thus the objective of data setup is to make a data plan that is definitely not hard to seek after

YIELD DESIGN

A quality yield is one, which meets the essentials of the end customer and presents the data indisputably. In any structure eventual outcomes of getting ready are passed on to the customers and to other system through yields. In yield structure it is settled how the data is to be ousted for incite require and besides the printed rendition yield. It is the most indispensable and direct source data to the customer. Compelling and adroit yield design improves the structure's relationship to help customer fundamental authority.

1. Arranging PC yield should proceed in a dealt with, well completely thought about way; the right yield must be made while ensuring that each yield part is organized with the objective that people will find the structure can use easily and reasonably. Exactly when examination plan PC yield, they should Identify the specific yield that is relied upon to meet the requirements.

2.Select techniques for demonstrating data.

3.Create record, report, or diverse arrangements that contain data made by the structure.

The yield kind of a data structure should accomplish no less than one of the going with goals.

- Convey data about past activities, current status or projections of the
- Future.
- Signal basic events, openings, issues, or advices.
- Trigger a movement.
- Confirm a movement.

MODULES DESCRIPTION

Mining Leading Sessions

In the essential module, we develop our structure condition with the purposes of enthusiasm of App like an application store. Naturally, the leading sessions of a mobile App address its seasons of reputation, so the ranking control will simply happen in these leading sessions. Along these lines, the issue of recognizing ranking fraud is to perceive fraudulent leading sessions. Along this line, the key task is the way by which to mine the leading sessions of a mobile App from its bona fide ranking records. There are two essential steps for mining leading sessions. To begin with, we need to discover leading events from the App's chronicled ranking records. Second, we need to join bordering leading events for creating leading sessions.

Ranking Based Evidences

In this module, we make Ranking based Evidences system. By looking at the Apps' evident ranking records, web serve that Apps' ranking practices in a leading event reliably satisfy a specific ranking model, which involves three various ranking stages, specifically, rising stage, keeping up stage and subsidence arrange. Specifically, in each leading event, an App's ranking first augmentations to an apex position in the leaderboard (i.e., rising stage), by then keeps such zenith position for a period (i.e., caring for stage), in conclusion reduces till the complete of the event (i.e., subsidence organize).

Rating Based Evidences

In the third module, we redesign the system with Rating based evidences module. The ranking based evidences are useful for ranking fraud detection. In any case, a portion of the time, it isn't sufficient to simply use ranking based evidences. For example, some Apps made by the prevalent planners, for instance, Gameloft, may make them lead events with broad estimations of u1 in view of the designers' credibility and the "casual" publicizing sway. Moreover, a part of the real marketing organizations, for instance, "obliged time discount", may in like manner result in colossal ranking based evidences. To understand this issue, we in like manner consider how to remove fraud evidences from Apps' valid rating records.

Review Based Evidences

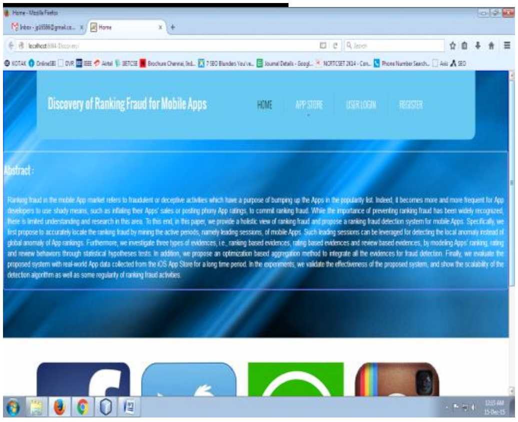
In this module we incorporate the Review based Evidences module in our structure. Other than evaluations, an extensive part of the App stores furthermore empower customers to think about some printed comments as App reviews. Such reviews can reflect the individual observations and utilize experiences of existing customers for particular mobile Apps. Truth be told, review control is a champion among the most basic perspective of App ranking fraud. Specifically, before downloading or securing another mobile App, customers as often as possible previously scrutinized its undeniable reviews to encourage their essential administration, and a mobile App contains more positive reviews may pull in more customers to download. In this way, fakers every now and again post fake overviews in the leading sessions of a specific App with the ultimate objective to extend the App downloads, and in this way push the App's ranking position in the pioneer board.

Evidence Aggregation

In this module we develop the Evidence Aggregation module to our structure. In the wake of evacuating three sorts of fraud evidences, the accompanying test is the best approach to go along with them for ranking fraud detection. Doubtlessly, there are many ranking and confirmation add up to methods in the composition, for instance, change based models

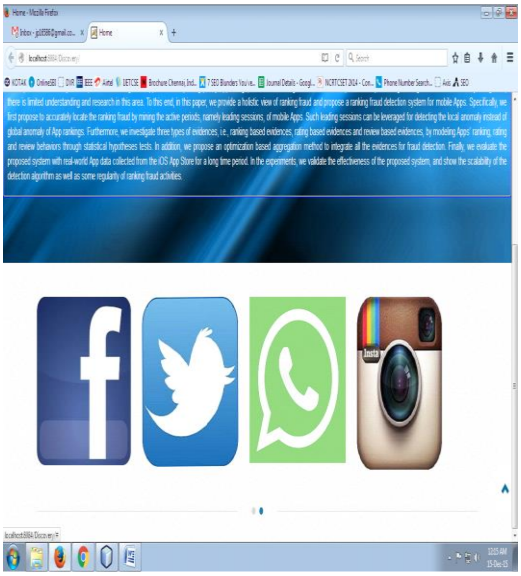
score based models and Dempster-Shafer rules . Nevertheless, a segment of these procedures revolve around taking in an overall ranking for all candidates. This isn't real to perceive ranking fraud for new Apps. Distinctive systems rely upon directed learning methods, which depend upon the named getting ready data and are hard to be manhandled. Or maybe, we propose an unsupervised strategy subject to fraud comparability to combine these evidences.

SCREEN SHOTS

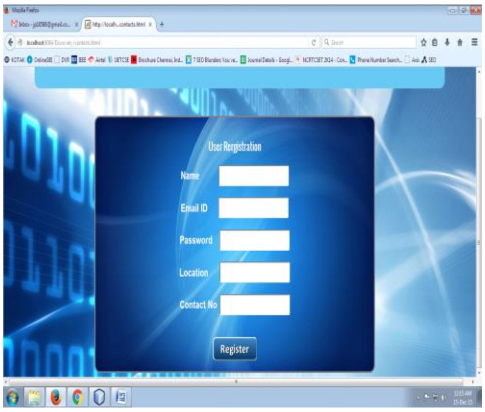


Abstract :

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. Indeed, 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. To this end, in this paper, we provide a holistic view of ranking fraud and propose a ranking fraud detection system for mobile Apps. Specifically, we first propose to accurately locate the ranking fraud by mining the active periods, namely leading sessions, of mobile Apps. 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 propose 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.

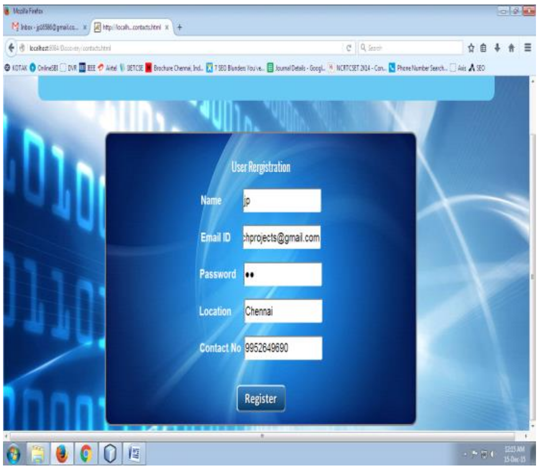


there is limited understanding and research in this area. To this end, in this paper, we provide a holistic view of ranking fraud and propose a ranking fraud detection system for mobile Apps. Specifically, we first propose to accurately locate the ranking fraud by mining the active periods, namely leading sessions, of mobile Apps. 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 propose 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.



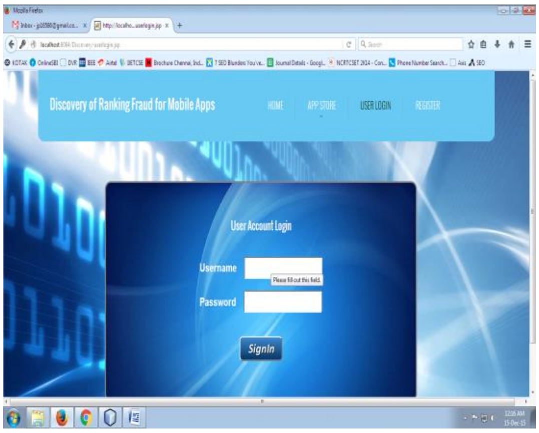
User Regsitration

Name
Email ID
Password
Location
Contact No



User Regsitration

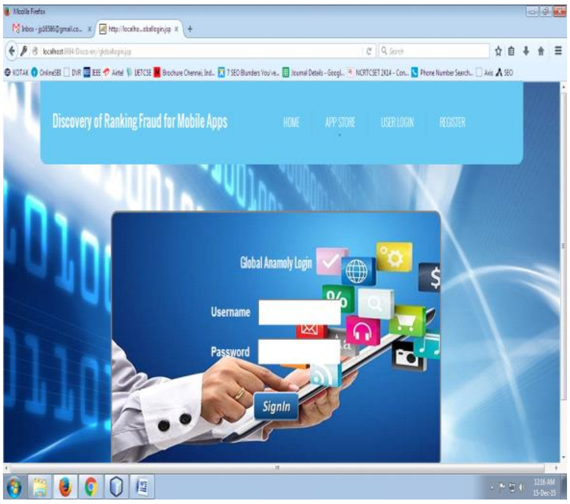
Name jp
Email ID hprojects@gmail.com
Password ••
Location Chennai
Contact No 9952649690

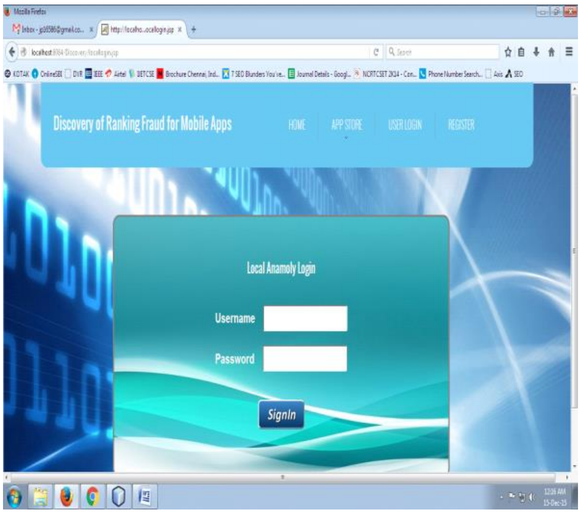


User Account Login

Username
Please fill out this field.
Password

.





CONCLUSION

In this paper, we developed a ranking fraud detection system for mobile Apps. Specifically, we recently shown that ranking fraud happened in leading sessions and gave a procedure to burrowing leading sessions for each App from its genuine ranking records. By then, we recognized ranking based evidences, rating based evidences and overview based evidences for distinguishing ranking fraud. Furthermore, we proposed a streamlining based combination system to facilitate all of the evidences for surveying the acceptability of leading sessions from mobile Apps. An extraordinary perspective of this technique is that all of the evidences can be shown by statistical hypothesis tests, along these lines it is definitely not hard to be connected with various evidences from space data to distinguish ranking fraud. Finally, we favor the proposed structure with wide preliminaries on obvious App data accumulated from the Apple's App store. Preliminary outcomes exhibited the sufficiency of the proposed technique. Later on, we plan to analyze all the more ground-breaking fraud evidences and dismember the inert relationship among rating, review and rankings. Likewise, we will grow our ranking fraud detection approach with other mobile App related organizations, for instance, mobile Apps recommendation, for enhancing customer experience.

Reference:-

1. 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.

2. 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.

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

4. 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. 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.

6. https://developer.apple.com/news/index.php ?id=0- 2062012a. 3)

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

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

9. 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.

10. 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.

11. 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

12. 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.

13. 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.

14. 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.

15. 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.

16. 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.

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

18. 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.