WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Identification of Harmful Apps

***Jai Surya T S*[1]**

[1]Sri Krishna Adithya College of Arts and Science, India

ABSTRACT

Nowadays, the majority of us have Android smartphones and frequently utilize the Play Store or App Store. Although both marketplaces provide a large selection of applications, sadly, not all of them are fraudulent. These apps may lead to data theft as well as harm to phones. Thus, these programs need to be branded so that customers of the shop can identify them. We provide a website for information, feedback, and application reviews because of this. As a result, determining which application is fraudulent or not gets easier. The web application can process many applications concurrently. Additionally, users may not always find accurate or genuine product reviews online.

INTRODUCTION

The quantity of mobile applications has astonishingly increased in recent years. One of the most crucial methods for promoting mobile apps is through app rating. Recently, dishonest app developers have been using dishonest methods to enhance their programs and eventually control the app store rankings, rather than depending on conventional marketing strategies. This is often accomplished by employing "bot farms" or "human water armies" to rapidly boost the number of programs downloaded, rated, and reviewed.

SCOPE OF THE PROJECT

To identify ranking fraud, we discovered rating-, ranking-, and review-based evidences in our project. Additionally, we proposed an optimization-based aggregation approach that incorporated all the information needed to evaluate the authenticity of leading sessions from mobile applications.

MODULES

- Evidence-based ranking of user interface design
- Evidence-based rating
- Review-based supporting data
- assembling of evidence
- Assessment of Performance

Modules Description:

1. Evidence-based ranking of user interface design

Users may only connect to the server by providing their login and password in order to establish a connection. In the event that the user closes the browser directly and is able to log back in, the user must register their email address, password, and username with the server. To maintain the upload and download speeds, the server will establish an account for each user. The user ID will be assigned to the name. Typically, logging in allows access to a certain page.

2. Evidence-based rating

In order to extract fraud evidence from this model, we should first examine the fundamental characteristics of leading events. Through the examination of the Apps ranking records, we can see that the ranking behaviors of the Apps during a leading event consistently meet a particular ranking pattern. This pattern indicates a significant comprehension of the leading event. The evidence based on rankings is helpful in identifying ranking fraud.

3. Review-based supporting data

Any user who downloads an app once it has been released has the option to rate it. User ratings are, in fact, among the most crucial aspects of app advertising. An app with a better rating could be downloaded by more people and show up higher on the leaderboard. Thus, another important aspect of positioning extortion is rating control.Ratings during that period may exhibit anomalous patterns as compared to the App's historical ratings, if the App has intuitively ranked fraud in a leading session. This information may be utilized to create rating-based proof.

4. Assembling of Evidence

Reviews for certain mobile applications may represent the individual opinions and experiences of current users. Certainly, one of the most important criticisms of app positioning extortion is survey manipulation. In particular, people frequently check past evaluations of a mobile app before downloading or buying it to make their decision-making process easier. A mobile app with more good ratings may draw in more users.

5. Evidence Aggregation

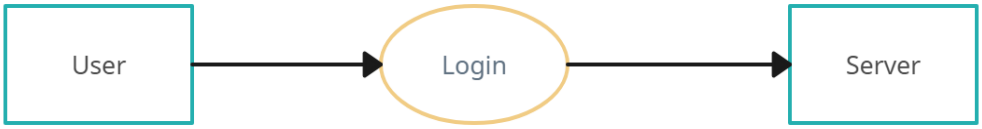
The next step is to figure out how to mix the three different sorts of fraud evidence to rank fraud detection. There are unquestionably many positioning and tested conglomeration tactics available; some of these strategies focus on teaching all applicants a global positioning. When it comes to identifying positional extortion for unused apps, this is frequently inappropriate. Some approaches rely on supervised learning strategies, which are hard to abuse and rely on labeled training data. Alternatively, we suggest combining this information using an unsupervised method based on fraud similarities.

6. Performance Evaluation:

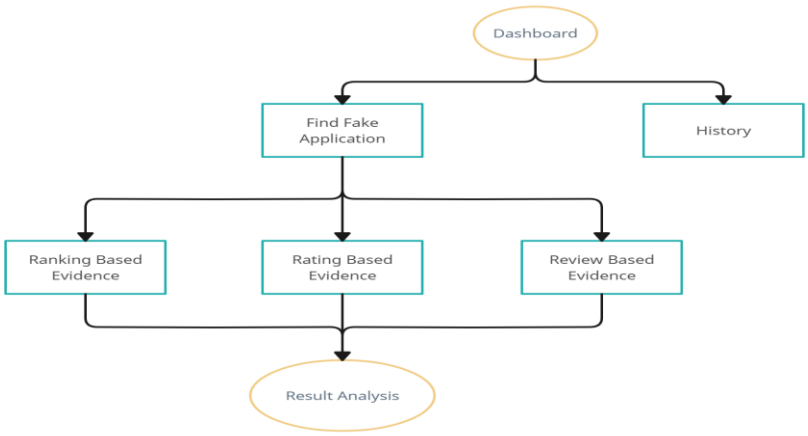
It is evident that there are more apps with moo rankings than there are tall ranks. Furthermore, there is greater rivalry between free apps than between commercial apps, especially in tall rankings where the distribution of apps based on various ratings is considered. The fact that the distribution of app ratings is not evenly distributed in the numbers suggests that a relatively small proportion of apps are highly popular.

SYSTEM ARCHITECT

DFD: Level 0 :



DFD: Level 1:



CONCLUSION :

We developed a positioning extortion location framework for portable applications in this study. Specifically, we first revealed that ranking extortion occurred during driving sessions and provided a way to extract driving session data for any App using its previous location records. By that time,

we identified positioning extortion using positioning-based confirmations, rating-based confirmations, and audit-based confirmations. Furthermore, in order to coordinate all of the confirmations for determining the legitimacy of driving sessions from portable Apps, we presented an optimization-based aggregation technique. This method's unique selling point is that all of the confirmations can be expressed as quantifiable conjecture tests, making it easy to extend with further confirmations from space data to detect positional extortion. Finally, we accept the suggested framework after extensive testing on actual app data gathered from Apple's App Store. Investigative findings revealed the suitability of the suggested strategy.