ISSN (online) : 2277-5390
ISSN (Print): 2277-5382

# An improvement of finding fraud ranking of mobile apps using proportional reversed hazard model

L. Velmurugan

*Department of Computer Science, AMBO University, Ethiopia.*
velmuruganphd15@gmail.com

## Abstract

**Objective:** To predict the fraudulent ranking behaviour for mobile apps in which the fraudulent evidences are generated by thew mobile app developers for providing the top ranking for them.
**Methods:** In mobile app development, the greatest challenge is ranking the mobile app by fraudulent behaviour. The fraudulent behaviour is performed because of the degradation of significant level of the mobile apps. In previous work, to leverage the fraudulent ranking behaviours, Leading Session Methodology based Evidence Aggregation (LSMEA) and Concept Vector based Review Evidence Analysis (CVREA) are developed. These methods consist of ranking based evidences, rating based evidences and review based evidences. Then, these evidence results are aggregated to detect the fraudulent ranking behaviour of mobile apps. In which, rating based evidence is described based on the user rating for corresponding mobile app. User rating is the most significant features for advertising the mobile apps. In previous analysis, user rating is analyzed by using a Gaussian distribution for computing p-value of the statistical hypotheses which is used to define the probability of user rating based on leading sessions.
**Findings:** The rating based evidences analysis based on the Gaussian distribution suffers from some important limitations. For large dimensions, the total number of parameters is increased quadratically and the manipulation and inversion process of large matrices may become prohibitive. In addition, Gaussian distribution is intrinsically uni-modal. Therefore, a better approximation is not provided for multimodal distributions. Such limitations are removed by introducing Proportional Reversed Hazard Model (PRHM). In this paper, an improvement of finding fraud ranking of mobile apps (IFFR) is proposed by using PRHM and the three evidence outcomes are combined for detecting the fraudulent ranking behaviour for mobile apps.
**Applications/Improvements:** Mostly, the proposed approach is useful for mobile app markets for developing more number of apps for the specific purpose. Therefore, the accuracy and reputation level are required for further improvement. Thus, the reputation level and accuracy is improved and the fraudulent ranking behaviour of mobile apps is removed by the proposed approach.

**Keywords:** Mobile apps, Fraudulent ranking behaviour, Evidence analysis, Rating evidences, Proportional reversed hazard model.

## 1. Introduction

In modern years, the mobile apps usages are increased because of the increased amount of smart phones. Mobile app is a software application which is designed for running on the smart phones and released by several industries in different forms. Among several mobile apps, some apps are released for the same purpose or process. In this situation, mobile apps require their ranking level for providing the high flexibility to the users for selecting the most wanted mobile apps. For example, for chatting with other peoples, there are lots of mobile apps are available to the users such as Whatsapp, Hike, ChatON, Way2sms and etc. Due to the developed number of mobile apps, ranking fraudulent behaviours are increased. The ranking of the mobile apps are generally based on their rating and utilization of that certain app by the users. This ranking of the mobile apps are regularly changed since the improvement of the software platforms. Due to the regular basis of ranking, the fraudulent behaviours are increased. Hence, the detection of fraudulent ranking behaviour is the most important for mobile apps ranking accurately.

The ranking of the different mobile apps are explored by the app leader board. The ranking is provided according to the number of users, percentage of the rating, popularity level of the mobile apps and etc. Therefore, in this paper, the fraudulent ranking behaviour for mobile apps is detected based on the analysis of rating based evidences by using PRHM approach.

The mobile apps were modelled [1] based on the sequential approach such as Hidden Markov Model (HMM) for different mobile apps services. The sequences of the heterogeneous popularity observations of modelled for mobile apps by using popularity based HMM. Moreover, the bipartite based method was introduced for pre-clustering the popularity observations. This approach was modelled for the database which is gathered from the Apple app store and evaluated for illustrating the effectiveness. The fraudulent activities were detected and prevented by [2] using optimal aggregation approach. The ranking fraud was perfectly identified by mining the active time durations through a leading session algorithm. In addition, three types of evidences were investigated via learning historical records. All evidences were combined together by means of an optimal aggregation method. This fraud detection and prevention system was evaluated for the data gathered from the Google app store for a long duration.

The different approach for detecting the fraud ranking [3] was discussed for mobile apps. In this paper, the complete positioning misrepresentation and the ranking fraud detection scheme were provided. Three processes such as detecting the web ranking spam, detecting online review spam and recommending mobile apps were combined. The fraud ranking detection for mobile apps was achieved based on the leading events and combining of neighbouring events [4] was detected from the historical records of the mobile apps. This prevention system was evaluated for the data which is gathered from the App storeroom for various services which are related to the recommendation of mobile apps to the user.

By using different opinion mining approaches [5] the detection of fraudulent ranking were studied. The opinion mining approaches [6] were provided for mining the leading sessions of mobile apps which are utilized in order to detect the ranking fraud accurately wherein the local anomaly was detected instead of a global anomaly of app rankings. This fraud detection system was evaluated for App store data with long duration. The holistic view of ranking fraud and a ranking fraud detection system [7] was provided for mobile apps. Two types of evidences were investigated such as ranking based and rating based evidences through modelling the mobile apps ranking and rating behaviours by using statistical hypotheses analysis. Furthermore, for integrating all evidences for fraud detection, an aggregation approach based on the optimization was introduced. This detection system was evaluated for real world mobile app data which is gathered from the Apple's app store along with the long time period.

The product review spammers [8] were detected based on the behaviour of the rating. The degree of spam was computed based on the scoring method for every reviewer. Then the subset of highly suspicious reviewers was collected by using web based spammer. This detection method was evaluated for the data which is collected from an Amazon review database. The fraud detection for financial statements [9] was developed for the fuzzy ranking approach. The fraud classification rules which are learned from the genetic algorithm were converted into the fuzzy score for representing the degree where the company's financial statements were matched with the rules.

The novel method was developed for predicting the click frauds in mobile advertising [10]. The fraud prediction was performed based on the Hellinger Distance Decision Tree (HDDT) which consists of feature selection by using Recursive Feature Elimination (RFE) and classification. The efficiency of the fraud detection was evaluated for the database which is provided by Buzzcity. A semi-supervised hybrid shilling attack detector [11] was developed fro recommending the trustworthy products. MC-Relief was introduced by this approach for selecting the effective detection metrics. The semi-supervised Naive Bayes was also introduced for separating the Random-Filler model attackers and Average-Filler model attackers. This method was evaluated for the database which is collected from Netflix.

## 2. Detection of fraudulent ranking behaviour

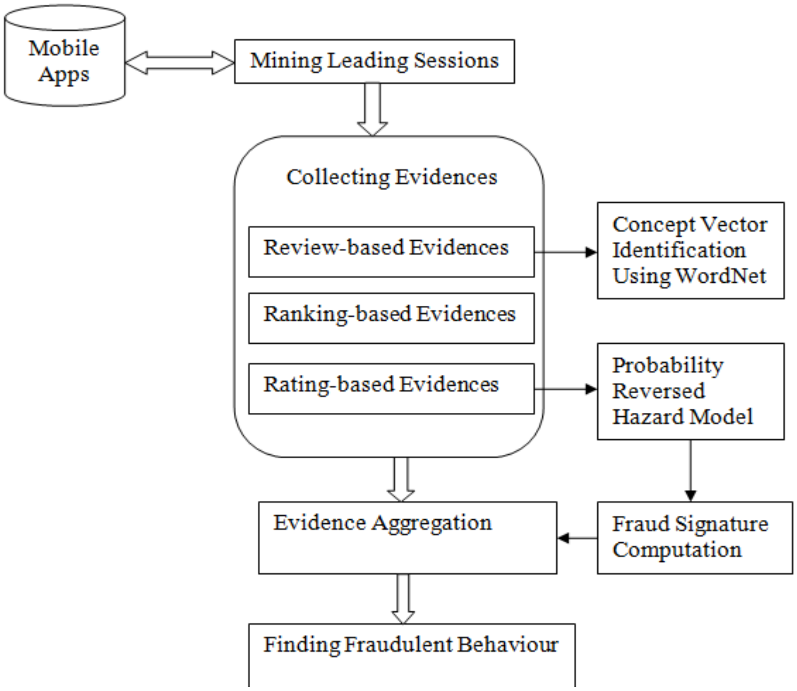
In this paper, the detection of fraudulently ranked mobile apps is achieved by proposed fraudulent behaviour detection approach and the mobile users are prevented from installing the worst mobile apps. The fraudulent behaviour detection for mobile app is achieved by collecting the evidences which is utilized for finding the fraudulent signature such as,

- Ranking-based Evidences
- Review-based Evidences
- Rating-based Evidences

Among these evidences, rating-based evidences are estimated based on the user rating, which increases the attractiveness of the mobile apps in order to download it. In this proposed methodology, Proportional Reversed Hazard Model (PRHM) is introduced for analyzing the rating-based evidence in order to detect the fraudulent activities. The proposed research methodology is shown in Figure 1. The detection of fraudulent ranking behaviour is performed by the following processes:

- Mining leading sessions
- Gathering evidences
- Proportional Reversed Hazard Model (PRHM)

*Figure 1. Flow of process*



### 2.1. Mining leading session

The time sequence of leading events or attempts are called as leading sessions. By using the analysis of the historical data of the mobile apps which are available in online, the leading sessions are extracted. The mining of leading sessions is performed by following steps:

- Discovering the leading events
- Combining adjacent leading events to generate leading sessions

The time duration spent for each mobile task are extracted during the process of discovering the leading events. Then, the discovered leading events are merged together for generating the leading sessions.

**Algorithm 1:** Mining Leading Sessions

**Input 1:** Historical ranking records, $R_A$ for Mobile app $A$

**Input 2:** Ranking Threshold, $K^*$

**Input 3:** Combining Threshold, $\phi$

**Output:** Set of leading sessions, $S_A$ for $A$

**Initialization:** $S_A = \emptyset$

```
1. $E_s = \emptyset$; $e = \emptyset$; $s = \emptyset$; $t_{start}^e = 0$;
2. For each $i \in [1, |R_A|]$ do
3. If ($r_i^A \leq K^*$ and $t_{start}^e == 0$) then
4. $t_{start}^e = t_i$
5. Else if ($r_i^A > K^*$ and $t_{start}^e \neq 0$) then
```

```
//Discovered one event
$t_{end}^{e} = t_{i-1}; e =< t_{start}^{e}, t_{end}^{e} >$
If ($E_s == \emptyset$) then
$E_s \cup= e;\ t_{start}^{s} = t_{start}^{e};\ t_{end}^{s} = t_{end}^{e};$
Else if (($t_{start}^{e} - t_{end}^{s}) < \emptyset$) then
$E_s \cup= e;\ t_{end}^{s} = t_{end}^{e};$
Else then
//Discovered one session
$s =< t_{start}^{s}, t_{end}^{s}, E_s >$
$S_A \cup= s; s = \emptyset$ is a new session
$E_s = \{e\};\ t_{start}^{s} = t_{start}^{e};\ t_{end}^{s} = t_{end}^{e};$
$t_{start}^{e} = 0; e = \emptyset$ is a new leading event
Return $S_A$
```

### 2.2. Gathering evidences

The evidences related to the fraudulent behaviour of mobile apps are predicted after leading sessions are mined. This prediction is utilized for finding the fraudulently ranked mobile apps. Three behaviours of mobile apps like ranking based, review based and rating based evidences are collected along with the consideration of various time sessions. By using the app leader board, ranking based evidences are gathered in order to provide the best review of apps to the mobile users.

Three phases are considered in the ranking of the mobile apps such as rising phase, maintenance phase and recession phase. In rising phase, the ranking value is increased rapidly and in maintenance phase, the ranking value is maintained without any degradation. In recession phase, the ranking value of the mobile apps is degraded rapidly from higher level to lower level in recession phase. These three ranking phases are varied in various time sessions. Hence, the fraudulent behaviour is detected by discovering the unexpected rising of ranking level or detected in recession phase.

The product comments or reviews are referred as review based evidences which are provided by the users about the particular mobile app. The comments or reviews may be either positive or negative, in which the fraudulent industries may neglect many negative comments in order to increase their developed mobile apps. The fraudulent activities are identified by extracting the user reviews through analyzing verbs which are used frequently according to the fraud signature. Here, Concept Vector based Review Evidence Analysis [12] (CVREA) is utilized where the concepts of user comments are identified based on the computation of fraudulent signature. This concept vector identification is achieved by using WordNet tool which provided various comments with different syntactic meanings and then filtered the significant concepts by conceptual term frequency.

The other significant evidence is rating based evidences which are prepared anonymously to increase the reputation level of the mobile apps and prevent the web pages from fraudulent ranking. This is achieved by analyzing the extracted leading session. In previous work, rating based evidences are extracted based on the computation of the p-value of statistical hypotheses for defining the leading sessions in order to detect the fraudulent ranking behaviour by using the Gaussian approximation. However, Gaussian distribution has some limitations such as manipulation and inversion of large matrices is prohibitive. In addition, it is intrinsically uni-modal and so it is unable to provide the best approximation for multimodal distributions. Therefore, these limitations are removed by using the Proportional Reversed Hazard Model (PRHM) which is explained in below.

### 2.3. Proportional reversed hazard model (PRHM)

One of the most significant features is rating the records for advertising the mobile apps. The rating of the mobile apps is provided by the user who has downloaded the specific mobile app. More users can download the mobile apps with higher rating probability and such mobile apps are ranked higher level on the leader board. Therefore, the rating manipulation is the most important perspective of ranking fraud. If an app has ranking fraud in the leading session $s$, then the ratings in the time duration of $s$ may have anomaly patterns compared to its historical ratings which are utilized for generating the rating based evidences. Normally, the common mobile apps are received equivalent average ratings for each day, whereas the fraudulent apps are received higher average ratings during leading sessions compared with other time durations. Hence, two rating fraud evidences are described based on the user rating behaviours.

Evidence 1: Compared to normal mobile apps, the app with rating manipulation may have higher ratings in the fraudulent leading sessions related to its historical ratings. For each leasing sessions, the fraud signature $\Delta R_s$ is defined as follows:

$$\Delta R_s = \frac{\bar{R}_s - \bar{R}_A}{\bar{R}_A}, (s \in A) \qquad (1)$$

In equation (1), $\bar{R}_s$ is the average rating in leading session $s$ and $\bar{R}_A$ is the average historical rating of mobile app $A$. Hence, if the value of $\Delta R_s$ in leading session is higher than the other leading sessions of apps on the leader board, then it has a high probability of having ranking fraud. The detection of higher probability of having ranking fraud is performed based on the two statistical hypotheses which is used for computing the importance of $\Delta R_s$ for all leading sessions. The two statistical hypotheses are defined as follows:

- The signature $\Delta R_s$ of leading session $s$ is not helpful for ranking fraud detection.
- The signature $\Delta R_s$ of leading session $s$ is much higher than the expectation level.

In this proposed approach, the Proportional Reversed Hazard Model (PRHM) is used for computing the p-value of the above hypotheses. The PRHM is performed based on the reversed hazard function which is the fraction of the density function to its distribution function. The evidence is computed based on the PRHM as follows:

Consider the probability density function $f_R(\cdot)$ and the distribution function $F_R(\cdot)$ for a random variable $R$. The following notations are utilized in PRHM.

$$\text{Reversed Hazard function, } rh_R(r) = \frac{f_R(r)}{F_R(r)} \qquad (2)$$

The above notation for random variable $S$ is also similar to those of $R$ except replacing $R$ by $S$. Assume, $\Delta R_s$ follows the PRHM distribution with a proportionality constant or exponential parameter, $\alpha > 0$, if,

$$rh_S(r) = \alpha rh_R(r)\ for\ all\ r > 0 \qquad (3)$$

If the equation (6) is satisfied by the two random variables $S$ and $R$, then the distribution and density functions are defined as,

$$F_S(r) = \left(F_R(r)\right)^{\alpha} \text{ And } f_S(r) = \alpha\left(F(r)\right)^{\alpha-1} f_R(r) \qquad (4)$$

The proportional hazard model is defined from the distribution function as follows,

$$F_R(r) = \frac{r^c}{1+r^c}\ for\ r > 0, c > 0 \qquad (5)$$

Hence, $\Delta R_s$ follows the PRHM, $\Delta R_s \sim \mathcal{N}(\hat{\alpha})$ where $\hat{\alpha}$ is obtained by the Maximum Likelihood Estimation (MLE) method from the observations of $\Delta R_s$ in all mobile app's historical leading sessions.

$$\hat{\alpha} = -\frac{n}{\sum_{i=1}^{n} \ln F(r_i)} \qquad (6)$$

Where, $n$ is the amount of all ranking records. Then, the evidence can be computed as,

$$\psi_1(s) = 1 - P(\mathcal{N}(\hat{\alpha}) \geq \Delta R_s) \qquad (7)$$

Evidence 2: Compared with the other leading sessions of mobile apps on the leader board if the discovered leading session has lower rate, then the probability of having ranking fraud is high. Here, the fraud signature $\mathcal{D}(s)$ is computed using Cosine similarity method as follows,

$$\mathcal{D}(s) = \frac{\sum_{i=1}^{|L|} P(l_i|R_{s,A}) \times P(l_i|R_A)}{\sqrt{\sum_{i=1}^{|L|} P(l_i|R_{s,A})^2} \times \sqrt{\sum_{i=1}^{|L|} P(l_i|R_A)^2}} \qquad (8)$$

In equation (8), $P(l_i|R_{s,A})$ is the normal distribution with respect to the rating level $l_i$ and the mobile app $A$'s leading session $s$ and $P(l_i|R_A)$ are the normal distribution with respect to $l_i$ and the mobile app $A$'s historical rating records.

$$P(l_i|R_{s,A}) = \left(\frac{N_{l_i}^s}{N_{(\cdot)}^s}\right) \qquad (9)$$

Where, $N_{l_i}^s$ refers the number of ratings in $s$ and the ratings at level $l_i$ and $N_{(\cdot)}^s$ refers the total number of ratings in $s$. Similarly, $P(l_i|R_A)$ is also computed. To identify the ranking fraud two hypotheses are defined for computing the importance of $\mathcal{D}(s)$ for every leading session. The two hypotheses are as follows:

- The signature $\mathcal{D}(s)$ of leading session $s$ is not helpful for ranking fraud detection.
- The signature $\mathcal{D}(s)$ of leading session $s$ is much lower than the expectation level.

Therefore, the p-value for these hypotheses is computed based on the PRHM distribution. Consider, $\mathcal{D}(s)$ follows the PRHM distribution, $\mathcal{D}(s) \sim \mathcal{N}(\hat{\alpha})$ where $\hat{\alpha}$ is obtained by the Maximum Likelihood Estimation (MLE) method from the observations of $\mathcal{D}(s)$ in all mobile app's historical leading sessions. Then, the evidence is computed as follows:

$$\psi_2(s) = 1 - P(\mathcal{N}(\hat{\alpha}) \leq \mathcal{D}(s)) \qquad (10)$$

The values of two computed evidences $\psi_1(s)$ and $\psi_2(s)$ are in the range of $[0,1]$. Therefore, the leading session with higher evidence value has the high probability of having the ranking fraud activities. Then, the different evidences are aggregated based on the unsupervised approach based on weight function as given below.

The final evidence score is given as,

$$\psi^*(s) = \sum_{i=1}^{N_\psi} w_i \times \psi_i(s) \qquad (11)$$

$$\text{Subject to, } \sum_{i=1}^{N_\psi} w_i = 1 \qquad (12)$$

In the above equations, $N_\psi$ is the number of evidences and weight $w_i \in [0,1]$ is the aggregation parameter of evidence $\psi_i(s)$.

**Algorithm 2:** Fraudulent ranking behaviour detection with PRHM based Rating Evidence Analysis

**Input:** Different mobile apps

**Output:** Fraudulent ranking behaviour of mobile apps

1. Gather the user ratings of different mobile apps
2. Mine the leading sessions as given in algorithm 1
3. For each leading sessions $S_i \in S_a$
4. Compute the ranking based evidences
5. Compute the review based evidences using CVREA
6. PRHM ()
7. End for
8. Aggregate the different evidences based on unsupervised approach
9. Find the fraudulent ranking behaviour of mobile apps

//PRHM ()

10. Begin
11. Load the user ratings
12. For each ratings $R_i \in R$
13. Compute the reverse hazard function, $r⍰_S(r)$
14. Compute the distribution and density function, $F_S(r)$ and $f_S(r)$
15. Compute the evidence 1,

$$\psi_1(s) = 1 - P(\mathcal{N}(\hat{\alpha}) \geq \Delta R_s)$$

```
Compute $P(l_i|R_{s,A})$ and $P(l_i|R_A)$
Compute fraud signature of each user ratings using cosine similarity
    $\mathcal{D}(s) = \frac{\sum_{i=1}^{|L|} P(l_i|R_{s,A}) \times P(l_i|R_A)}{\sqrt{\sum_{i=1}^{|L|} P(l_i|R_{s,A})^2} \times \sqrt{\sum_{i=1}^{|L|} P(l_i|R_A)^2}}$
Find the evidence 2,
    $\psi_2(s) = 1 - P(\mathcal{N}(\hat{\alpha}) \le \mathcal{D}(s))$
End for
End
```

The given pseudocode is useful for detecting the fraudulent ranking behaviour for mobile apps by using the proposed PRHM method based rating evidence analysis. This approach is useful for improving the accuracy of the fraudulent ranking behaviour detection by finding the ratings of the user based on the fraudulent signature.

## 3. Results

In this section, the performance evaluation of the proposed methodology is discussed with the previous fraudulent ranking behaviour detection approach such as LSMEA and CVREA. The experimental analysis is conducted for illustrating the improved performance of the proposed fraudulent ranking behaviour detection approach. The comparison is made in terms of parameters such as precision, recall and time complexity for different number of mobile apps. The parameter values for previous and proposed methodology are shown in Table 1.

*Table 1. Comparison analysis values*

| Number of Mobile Apps | Precision | | | Recall | | | Time Complexity (ms) | | |
|---|---|---|---|---|---|---|---|---|---|
| | LSMEA | CVREA | IFFR | LSMEA | CVREA | IFFR | LSMEA | CVREA | IFFR |
| 5 | 0.12 | 0.35 | 0.4 | 0.35 | 0.41 | 0.46 | 34 | 20 | 12 |
| 10 | 0.19 | 0.57 | 0.62 | 0.5 | 0.58 | 0.63 | 50 | 40 | 22 |
| 15 | 0.34 | 0.65 | 0.7 | 0.55 | 0.63 | 0.69 | 71 | 50 | 38 |
| 20 | 0.59 | 0.83 | 0.88 | 0.67 | 0.72 | 0.77 | 82 | 65 | 46 |
| 25 | 0.71 | 0.87 | 0.92 | 0.79 | 0.82 | 0.87 | 89 | 70 | 57 |
| 30 | 0.82 | 0.95 | 0.99 | 0.84 | 0.96 | 0.99 | 95 | 78 | 61 |

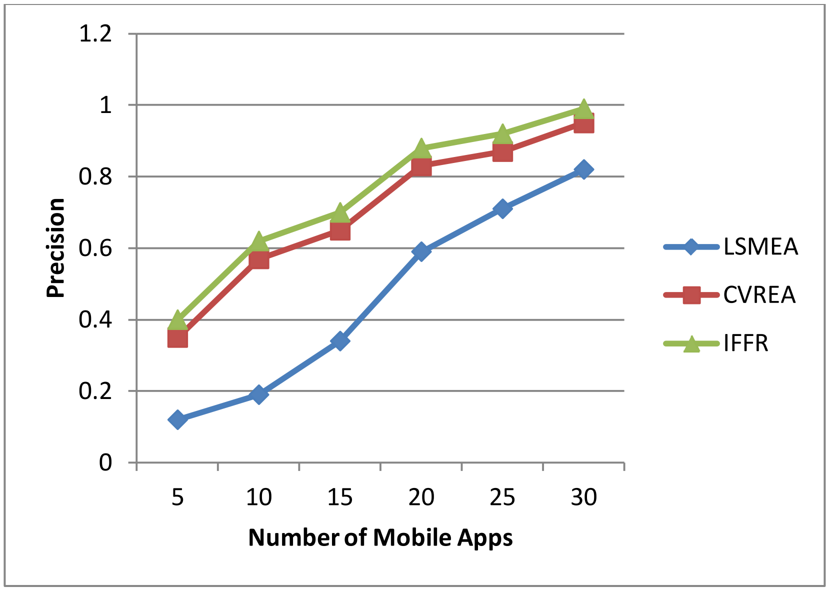
### 3.1. Precision

Precision value is provided for detecting the number of fraudulent ranking behaviour accurately. Precision is defined as the fraction of the true positives or it is evaluated based on the fraudulent ranking behaviour detection at true positive and false positive values. It is also known as positive predictive value. Precision value is computed as,

$$Precision = \frac{True\ Positive\ value\ (TP)}{True\ Positive\ value\ (TP) + False\ Positive\ value\ (FP)}$$

Figure 2 shows that the comparison of precision values made between previous approach and proposed approach which is provided for detecting the ranking fraud behaviour of mobile apps. In this figure, the number of mobile apps is taken in X-axis and the precision values are taken in Y-axis. From this comparison graph, it is demonstrated that the improved effectiveness of the proposed fraudulent ranking behaviour detection based on PRHM approach.

*Figure 2. Comparison of precision*



### 3.2. Recall

Recall is defined as the fraction of the mobile apps in which the fraudulent ranking behaviour is detected accurately. Recall is evaluated as follows,

$$Recall = \frac{True\ Positive\ value\ (TP)}{True\ Positive\ value\ (TP) + False\ Negative\ value\ (FN)}$$

*Figure 3. Comparison of recall*

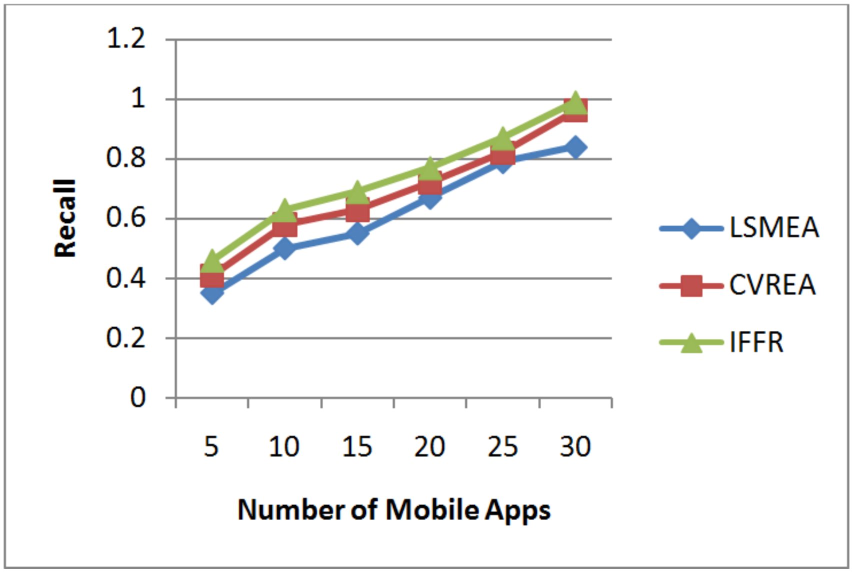


Figure 3 shows that the comparison of recall values made between previous approach and proposed approach which is provided for detecting the ranking fraud behaviour of mobile apps. In this figure, the number of mobile apps is taken in X-axis and the recall values are taken in Y-axis. From this comparison graph, it is demonstrated that the improved effectiveness of the proposed fraudulent ranking behaviour detection based on PRHM approach.

### 3.3. Time complexity

Time complexity is defined as the amount of time taken by the mobile apps for detecting the fraudulent ranking behaviour present in the user ratings for particular mobile apps. The time complexity is measured in terms of millisecond.

*Figure 4. Comparison of time complexity*

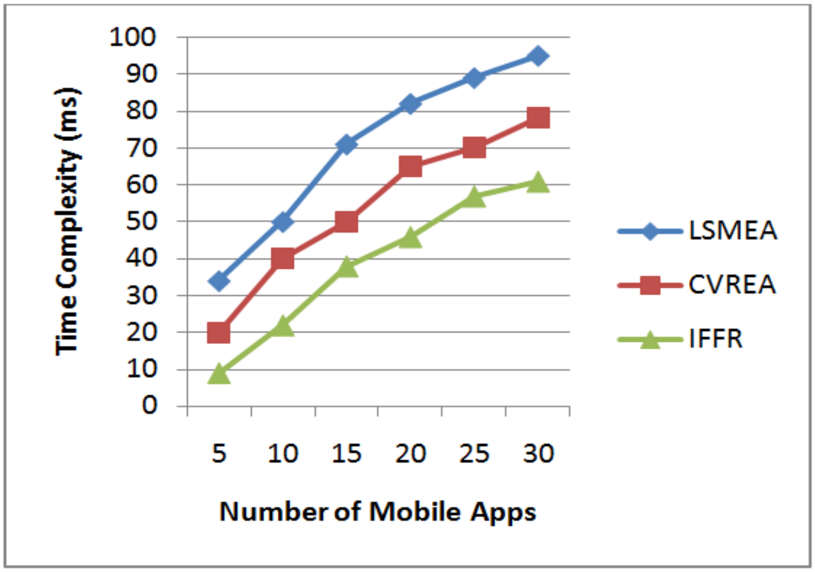


Figure 4 shows that the comparison of time values taken by the mobile apps in previous approach and proposed approach which is provided for detecting the ranking fraud behaviour of mobile apps. In this graph, the number of mobile apps is taken in X-axis and the time complexity values in millisecond are taken in Y-axis. From this comparison graph, it is demonstrated that the improved effectiveness of the proposed fraudulent ranking behaviour detection based on PRHM approach.

## 4. Conclusion

Nowadays, mobile apps are the most popular technology among the developed population which provides the development of several mobile apps for similar purpose. However, the rating of mobile apps is made by the fraudulent behaviour which requires to be avoided for filtering the unwanted mobile apps from the group of detected mobile apps. In this paper, the fraudulent ranking behaviour detection system for mobile apps is developed based on the rating based evidences by using PRHM approach. Initially, the leading sessions are mined from the historical ranking records for each mobile app. Then, the ranking based evidences and review based evidences are identified in order to detect the ranking fraud. In addition, the rating based evidences are identified based on the proposed PRHM approach. After that, the identified evidences are aggregated to evaluate the credibility of leading sessions from mobile apps. Thus, the experimental results proved that the proposed approach has better performance than previous approach.

## 5. References

1. H. Zhu, C. Liu, Y. Ge, H. Xiong, E. Chen. Popularity modeling for mobile apps: A sequential approach. *IEEE transactions on cybernetics*. 2015; 45(7), 1303-1314.
2. V. Pingale, L. Kuhile, P. Phapale, P. Sapkal, S. Jaiswal. Fraud detection & prevention of mobile apps using optimal aggregation method. *International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE)*. 2016; 6(3), 491-497.
3. M. Zende, A. Gupta. Survey on fraud ranking in mobile apps. *International Journal of Science and Research (IJSR)*. 2016; 5(2), 27-30.
4. M.P.U. Gayke, S.B. Thakare. Ranking fraud detection for mobile apps using evidence aggregation method. *International Journal of Engineering Development and Research (IJEDR)*. 2016; 4(3), 58-64.
5. T.B. Gade, N.G. Pardeshi. A survey on ranking fraud detection using opinion mining for mobile apps. *International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE)*. 2015; 4(12), 337-339.
6. J. Yesudoss, T. Banusankari. An efficient word alignment model for co-extracting opinion targets and opinion words from online reviews. *Indian Journal of Innovations and Developments*. 2015; 4(7), 1-5.

7. H. Zhu, H. Xiong, Y. Ge, E. Chen. Ranking fraud detection for mobile apps: a holistic view. In: *Proceedings of the 22nd ACM international conference on Information & Knowledge Management*. 2013; 619-628.

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

9. W. Chai, B.K. Hoogs, B.T. Verschueren. Fuzzy ranking of financial statements for fraud detection. In: *2006 IEEE International Conference on Fuzzy Systems*. 2006; 152-158.

10. M. Taneja, K. Garg, A. Purwar, S. Sharma. Prediction of click frauds in mobile advertising. In: *Contemporary computing (IC3), 2015 Eighth International Conference on IEEE*. 2015; 162-166.

11. Z. Wu, J. Wu, J. Cao, 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 ACM*. 2012; 985-993.

12. L. VelMurugan. Latent relation analysis based discovering fraudulent ranking identification on mobile web apps. *Indian Journal of Science and Technology*. 2015; 8(34), 1-8.

*The Publication fee is defrayed by Indian Society for Education and Environment (iSee). www.iseeadyar.org*

***Citation**:*

L. Velmurugan. An improvement of finding fraud ranking of mobile apps using proportional reversed hazard model. *Indian Journal of Innovations and Developments.* 2016; 5(10), October.