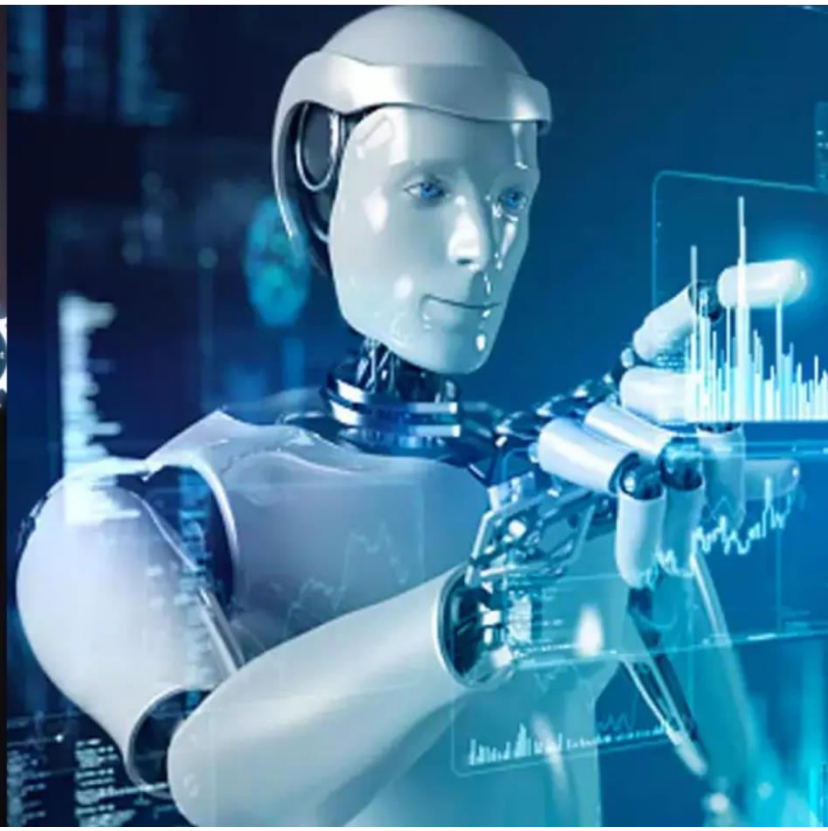
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 9.935

Volume 15, Issue 5, May 2026

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 5, May 2026

|DOI: 10.15680/IJIRSET.2026.1505077|

Fraud Apps Detection using Sentiment Analysis and Deep Learning: A Review

Chetana Nimba Patil, Prof. Nilesh Mali

Department of Computer Engineering, Ajeenkya DY Patil School of Engineering, Pune, India

ABSTRACT: The act of acting dishonestly or deceitfully in order to artificially raise an app's ranking on a popularity list in the mobile app market is known as fraud. Actually, rating fraud is becoming more and more common among app developers. Posting phone app reviews or inflating app revenues are examples of these behaviors. Despite the long-standing recognition of the significance of preventing ranking fraud, there is a dearth of study and publications in this field. In order to do this, we present a method for detecting fraud in mobile apps and provide a comprehensive analysis of fraud app detection in this work using sentiment analysis and spam filtering. To properly identify the ranking fraud in the first place, we recommend mining the active times, or leading sessions, of mobile apps.

KEYWORDS: Mobile Apps, Fraud Detection, Rating and Review, sentiment analysis.

I. INTRODUCTION

Over the past several years, there has been a significant increase in the quantity of smartphone apps. For example, the Google Play and Apple App Store have over 1.6 million apps accessible as of the end of April 2013. Many app stores created daily app leaderboards, which show the chart ranks of the most popular apps, to encourage the creation of mobile apps. The App Leader Board is without a doubt one of the most crucial tools for advertising mobile apps. In order to get their apps rated as highly as possible on these app leader boards, app developers regularly investigate various strategies, such as advertising campaigns, to promote their apps.

However, unethical app developers are increasingly using a range of dishonest tactics to intentionally promote their programs and eventually influence their chart positions on an app store, rather than depending on conventional marketing techniques. "bot farms" or "human water armies" are commonly employed to quickly inflate the number of app downloads, ratings, and reviews.

II. RELATED WORK

Detailed The pair wise features are first explicitly utilized to detect group colluders in online product review spam campaigns, which can reveal collusions in spam campaigns from a more fine-grained perspective. In [1] paper, Spam campaigns spotted in popular product review websites (e.g., amazon. com) have attracted mounting attention from both industry and academia, where a group of online posters are hired to collaboratively craft deceptive reviews for some target products. The goal is to manipulate perceived reputations of the targets for their best interests.

In [2] paper, Online product reviews have become an important source of user opinions. Due to profit or fame, imposters have been writing deceptive or fake reviews to promote and/or to demote some target products or services. Such imposters are called review spammers. In the past few years, several approaches have been proposed to deal with the problem. In this work, take a different approach, which exploits the burrstones nature of reviews to identify review spammers.

In [3] paper, Online reviews on products and services can be very useful for customers, but they need to be protected from manipulation. So far, most studies have focused on analyzing online reviews from a single hosting site. How could one leverage information from multiple review hosting sites? This is the key question in our work. In response, develop a systematic methodology to merge, compare, and evaluate reviews from multiple hosting sites. focus on hotel reviews and use more than 15million reviews from more than3.5million users spanning three prominent travel sites.

In [4] paper, Users increasingly rely on crowd sourced information, such as reviews on Yelp and Amazon, and liked

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 5, May 2026

|DOI: 10.15680/IJIRSET.2026.1505077|

post sand ads on Facebook. This has lento market for black hat promotion techniques via fake (e.g., Sybil) and compromised accounts, and collusion networks. Existing approaches to detect such behavior relies mostly on supervised (or semi-supervised) learning over known (or hypothesized) attacks. They are unable to detect attacks missed by the operator while labeling, or when the attacker changes strategy.

In [5] paper, Online reviews have become an increasingly important resource for decision making and product designing. But reviews systems are often targeted by opinion spamming. Although fake review detection has been studied by researchers for years using supervised learning, ground truth of large scale datasets is still unavailable and most of existing approaches of supervised learning are based on pseudo fake reviews rather than real fake reviews. Working with Dianping1, the largest Chinese review hosting site, present the first reported work on fake review detection in Chinese with filtered reviews from Damping's fake review detection system.

In [6] paper, Online reviews are quickly becoming one of the most important sources of information for consumers on various products and services. With their increased importance, there exists an increased opportunity for spammers or unethical business owners to create false reviews in order to artificially promote their goods and services or smear those of their competitors. In response to this growing problem, there have been many studies on the most effective ways of detecting review spam using various machine learning algorithms. One common thread in most of these studies is the conversion of reviews to word vectors, which can potentially result in hundreds of thousands of features.

In [7] paper, it providing an efficient and effective method to identify review spammers by incorporating social relations based on two assumptions that people are more likely to consider reviews from those connected with them as trustworthy, and review spammers are less likely to maintain a large relationship network with normal users. The contributions of this paper are two-fold: (1) elaborate how social relationships can be incorporated into review rating prediction and propose a trust based rating prediction model using proximity as trust weight; and (2) design a trust-aware detection model based on rating variance which iteratively calculates user-specific overall trustworthiness scores as the indicator for spam city.

In [8] paper, to detect fake reviews for a product by using the text and rating property from a review. In short, the proposed system (ICF++) will measure the honesty value of a review, the trustiness value of the reviewers and the reliability value of a product. The honesty value of a review will be measured by utilizing the text mining and opinion mining techniques. The result from the experiment shows that the proposed system has a better accuracy compared with the result from iterative computation framework (ICF) method.

In [9] paper, Online Social Networks (OSNs), which captures the structure and dynamics of person-to-person and person-to-technology interaction, is being used for various purposes such as business, education, telemarketing, medical, entertainment. This technology also opens the door for unlawful activities. Detecting anomalies, in this new perspective of social life that articulates and reflects the off-line relationships, is an important factor as they could be a sign of a significant problem or carrying useful information for the analyzer.

In [10] paper, they propose a new holistic approach called SpEagle that utilizes clues from all metadata (text, timestamp, and rating) as well as relational data (network), and harness them collectively under a unified system to spot suspicious users and reviews, as well as products targeted by spam. SpEagle employs a review-network-based classification task which accepts prior knowledge on the class distribution of the nodes, estimated from metadata. Positive points are: It enables seamless integration of labeled data when available. It is extremely efficient.

In [11] this paper, mangoes are graded in four types like Green Mango, Yellow Mango and Red Mango which are based on machine learning method. This system considers RGB values size and shape of mangoes. Following analysis is used to obtain good probability. This helps to train system to identify appropriate maturity of mangoes. This research is conducted on two machine learning method i.e. Naive Byes and SVM (Support Vector Machine).

III. EXISTING SYSTEM

Lot of work has been done in this field because of its extensive usage and applications. In this section, some of the approaches which have been implemented to achieve the same purpose are mentioned. These works are majorly differentiated by the algorithm for fraud app detection.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 5, May 2026

|DOI: 10.15680/IJIRSET.2026.1505077|

IV. PROPOSED SYSTEM

The proposed system focuses on detecting fraudulent mobile applications by analyzing app ranking behavior, user reviews, ratings, and sentiment patterns. The system identifies abnormal ranking trends known as leading sessions, which indicate artificial boosting of app popularity. It integrates sentiment analysis and spam review detection to examine user feedback authenticity. Historical ranking records, review text, timestamps, and rating distributions are mined to detect suspicious patterns. By combining behavioral analytics with textual opinion mining, the system can accurately identify fraudulent apps and prevent ranking manipulation in app stores.

V. CONCLUSION

In this work, we developed a mobile app fraud detection system. To be more specific, we first showed how ranking fraud was caused by leading sessions and provided a method for mining leading sessions using sentiment analysis and spam detection from each App's historical ranking records. Then, based on a review, we found evidence for fraud-detection apps.

REFERENCES

[1]. Ch. Xu and J. Zhang," Combating product review spam campaigns via multiple heterogeneous pairwise features", In SIAM International Conference on Data Mining, 2014.
[2]. G. Fei, A. Mukherjee, B. Liu, M. Hsu, M. Castellanos, and R. Ghosh, "Exploiting bustiness in reviews for review spammer detection", In ICWSM, 2013.
[3]. A. j. Minnich, N. Chavoshi, A. Mueen, S. Luan, and M. Faloutsos, "True view: Harnessing the power of multiple review sites",In ACM WWW, 2015.
[4]. B. Viswanath, M. Ahmad Bashir, M. Crovella, S. Guah, K. P. Gummadi, B. Krishnamurthy, and A. Mislove, "Towards detecting anomalous user behavior in online social networks", In USENIX, 2014.
[5]. H. Li, Z. Chen, B. Liu, X. Wei, and J. Shao," Spotting fakereviews via collective PU learning", In ICDM, 2014.
[6]. M. Crawford, T. M. Khoshgoftaar, and J. D. Prusa," Reducing Feature Set Explosion to Faciliate Real-World Review Sapm Detection", In Proceeding of 29th International Florida Artificial Intelligence Research Society Conference, 2016.
[7]. H. Xue, F. Li, H. Seo, and R. Pluretti," Trust-Aware Review Spam Detection",IEEETrustcom/ISPA.,2015.
[8]. E. D. Wahyuni , A. Djunaidy," Fake Review Detection From a ProductReview Using Modified Method of Iterative Computation Framework", In Proceeding MATEC Web of Conferences, 2016.
[9]. R. Hassanzadeh," Anomaly Detection in Online Social Networks: Using Datamining Techniques and Fuzzy Logic", Queensland University of Technology, Nov, 2014.
[10] R. Shebuti, L. Akoglu," Collective opinion spam detection: bridging review networks and metadata", In ACM KDD, 2015.
[11] G.D. Upadhye, D.Pise,"Grading of Harvested Mangoes Quality and Maturity Based on Machine Learning Techniques",IEEE International conference on smart city and Emerging Technology,2018.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details