IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.53

Volume 4, Issue 1, March 2024

Fraud App Detection using Sentiment Analysis

Mr. Revgade Rohit[1], Mr. Salunkhe Pramod[2], Mr.Waychale Aniket[3], Mr. Uday Bajirao[4]
Prof. Mahesh P. Bhandakkar[5]
Department of Information Technology[1,2,3,4,5]
Matoshri Aasarabai Polytechnic, Eklahare, Nashik, Maharashtra, India

Abstract*: With the proliferation of mobile applications in everyday life, ensuring their safety has become paramount. Relying solely on user reviews to gauge an app's trustworthiness is often inadequate. Thus, there is a pressing need to implement a system that can differentiate between genuine and fraudulent applications. The aim is to develop a web-based solution capable of detecting fraudulent apps before users download them, leveraging sentiment analysis and support vector machine (SVM) technology.*

Sentiment analysis plays a crucial role in discerning the emotional undercurrents embedded within online content. By scrutinizing social media platforms, this method offers insights into public sentiment on various subjects. However, due to the prevalence of unreliable or biased reviews, users cannot always make informed decisions based on online feedback alone. By analyzing both user and administrator comments, it becomes possible to ascertain the authenticity of an application.

Employing sentiment analysis in conjunction with SVM, the system can learn and evaluate the sentiments and emotions expressed in reviews and other textual data. Notably, the manipulation of reviews constitutes a significant component of app ranking fraud. Through the combined use of sentiment analysis and SVM, the system can effectively detect such fraudulent activities, thereby assisting users in identifying trustworthy applications across both Android and iOS platforms.

Keywords: Mobile applications Safety, Fraud detection, Sentiment analysis, Support vector machine (SVM), User reviews, Authenticity, Web-based system

I. INTRODUCTION

With the advancement of technology, the usage of mobile devices has significantly increased. This surge has led to a substantial growth in the development of mobile applications across various platforms, notably the popular Android and iOS. As mobile usage continues to expand for everyday tasks, sales, and advancements, it poses a significant challenge in the business intelligence market, fueling competition among companies and application developers.

In this competitive landscape, developers invest considerable effort into showcasing the quality of their products and attracting customers to ensure future progress. Our webpage aims to display customer reviews for specific applications, providing developers with insights into their strengths and weaknesses and guiding the development of new solutions tailored to users' needs.

However, amidst this competition, some developers resort to deceitful practices, such as artificially inflating their app's popularity or using it as a platform to disseminate malware. Techniques like "bot farms" or "human click armies" are employed to rapidly increase application downloads, ratings, and reviews. Additionally, developers may engage in "crowdsurfing," wherein teams of workers collectively provide false comments and ratings to boost an app's reputation.

Given these challenges, it's crucial to ensure that users have access to genuine and reliable comments before installing an app, thereby mitigating potential risks. An automated solution is necessary to systematically analyze the multitude of comments and ratings associated with each application, facilitating informed decision-making and safeguarding users from potential mishaps.

II. PURPOSE

The primary purpose of fraud app detection is to safeguard users from malicious or deceptive mobile applications that may pose security risks or deceive users. By employing various techniques such as sentiment analysis, machine learning algorithms, and behavioral analysis, fraud app detection systems aim to identify and flag

DOI: 10.48175/568

suspicious applications before users download or interact with them. This helps in maintaining the integrity and security of app marketplaces, protecting users' personal data and devices from potential threats posed by fraudulent apps. Additionally, effective fraud app detection contributes to fostering trust and confidence among users, ensuring they can confidently engage with mobile applications without fear of falling victim to scams or malware.

III. OBJECTIVE OF SYSTEM

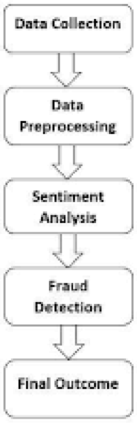
- Enhancing security: Detecting and blocking malicious apps to protect users from potential security threats such as malware, phishing, and data breaches.
- Ensuring trust: Establishing trustworthiness in app marketplaces by filtering out fraudulent apps, thereby maintaining user confidence and loyalty.
- Protecting user privacy: Safeguarding sensitive user data from being compromised or misused by fraudulent apps.
- Preventing financial loss: Mitigating the risk of users falling victim to fraudulent schemes, such as scams or unauthorized charges, through early detection and intervention.
- Promoting fair competition: Creating a level playing field for legitimate app developers by minimizing the influence of fraudulent apps that engage in unfair practices such as fake reviews or ratings manipulation.

IV. PROPOSED SYSTEM

The administrator has the authority to add and create new applications, along with providing links to the respective app stores such as Google Play or Apple App Store. Specific data pertaining to each application is collected from these stores and stored in the database for a designated period. Various data pre-processing techniques are employed to cleanse the user-provided data. Within the architecture, tokenization, stop word removal, and stemming algorithms are logically visualized.

In this setup, user comments and reviews stored in the database serve as input for the algorithm. The algorithm then calculates the frequency of positive and negative words appearing in the reviews. If the count of positive words exceeds that of negative words, the system returns a positive sentiment; conversely, if the count of negative words is higher, a negative sentiment is returned. In cases where the counts are equal, the system indicates a neutral sentiment.

SYSTEM ARCHITECTURE



Attackers target data sources because they have the most valuable and sensitive information. Every cloud user’s privacy and security are affected if data is lost. Insider threats are harmful operations carried out by people with authorization. With the fast growth of networks, many companies and organizations have established their internal networks.The malicious insider becomes a crucial threat to the organization since they have more access and opportunity to produce significant damage. Unlike outsiders, insiders possess privileged and proper access to information and resources.Insider

DOI: 10.48175/568

risks may be defined and addressed using criteria including insider indications, detection approaches, and insider kinds. There are two sorts of analysis intervals: real-time, which may identify malicious activity in real-time, and offline anomaly detection, which gathers log data and looks for certain patterns

V. CONCLUSION

This paper introduces a methodology for detecting fraudulent applications through the integration of support vector machine and sentiment analysis techniques. The approach is elucidated through an architecture diagram illustrating the underlying algorithms and processes employed in the project. Data is gathered and stored in a database, where it undergoes evaluation using the specified algorithms.

This methodology offers a novel approach by consolidating evidence to produce a unified outcome. The proposed framework demonstrates scalability and can be expanded to encompass evidences from various domains for fraud detection in reviews. Experimental findings indicate the effectiveness of the system, highlighting the scalability of the detection algorithm and revealing patterns in ranking fraud activities.

VI. ACKNOWLEDGMENT

We express our heartfelt gratitude to our esteemed mentors and professors, especially, for their invaluable guidance in our academic and project endeavours. We also extend our thanks to the *Information Technology*Department and its staff for their continuous support. Our sincere thanks go to Dr.S.J.BagulPrincipal of MatoshriAasarabai Polytechnic, Eklahare, Nashikfor his support and permission to complete this project. We appreciate the assistance of our department's support staff, and we're grateful to our parents, friends, and all those who supported usthroughout this project.

REFERENCES

[1] Daniel A. Keim, “Information Visualizing and Visual Data Mining” IEEE Trans. Visualization and Visual Data Mining, vol. 8,Jan-Mar 2002.

[2] FuzailMisarwala, KausarMukadam, and Kiran Bhowmick, “Applications of Data Mining in Fraud Detection”, vol. 32015.

[3] Esther Nowroji., Vanitha., “Detection Of Fraud Ranking For Mobile App Using IP Address Recognition Technique”, International Journal for Research in Applied Science & Engineering Technology, vol. 4, 2016.

[4] Ahmad FIRDAUS, Nor Badrul ANUAR, Ahmad KARIM, MohdFaizal Ab RAZAK, “Discovering optimal features using static analysis and a genetic search based method for Android malware detection” Frontiers of Information Technology and Electronic Engineering, 2018.

[5] JavvajiVenkataramaiah, BommavarapuSushen, Mano. R, Dr.GladispushpaRathi, “An enhanced mining leading session algorithm for fraud app detection in mobile applications” International Journal of Scientific Research in Engineering., April2017.

[6] Avayaprathambiha. P, Bharathi. M, Sathiyavani. B, Jayaraj. S “To Detect Fraud Ranking For Mobile Apps Using SVM Classification” International Journal on Recent and Innovation Trends in Computing and Communication, vol. 6, February2018.

[7] Suleiman Y. Yerima, SakirSezer, Igor Muttik, “Android Malware Detection Using Parallel Machine Learning Classifiers”, 8th International Conference on Next Generation Mobile Applications, Services and Technologies,Sept.2014.

[8] SidharthGrover,“Malware detection: developing a system engineered fair play for enhancing the efficacy of stemming search rank fraud”, International Journal of Technical Innovation in Modern Engineering &Science,Vol. 4, October2018.

[9] PatilRohini, Kale Pallavi, JathadePournima, KudaleKucheta, Prof. Pankaj Agarkar, “MobSafe: Forensic Analysis For Android Applications And Detection Of Fraud Apps Using CloudStack And Data Mining”, International Journal of Advanced Research in Computer Engineering & Technology, Vol. 4, October2015. [10] Neha M. Puram, Kavita R. Singh, “Semantic Analysis of App Review for Fraud Detection using Fuzzy Logic”, International Journal of Computer & Mathematical Sciences, Vol. 7, January2018.

DOI: 10.48175/568