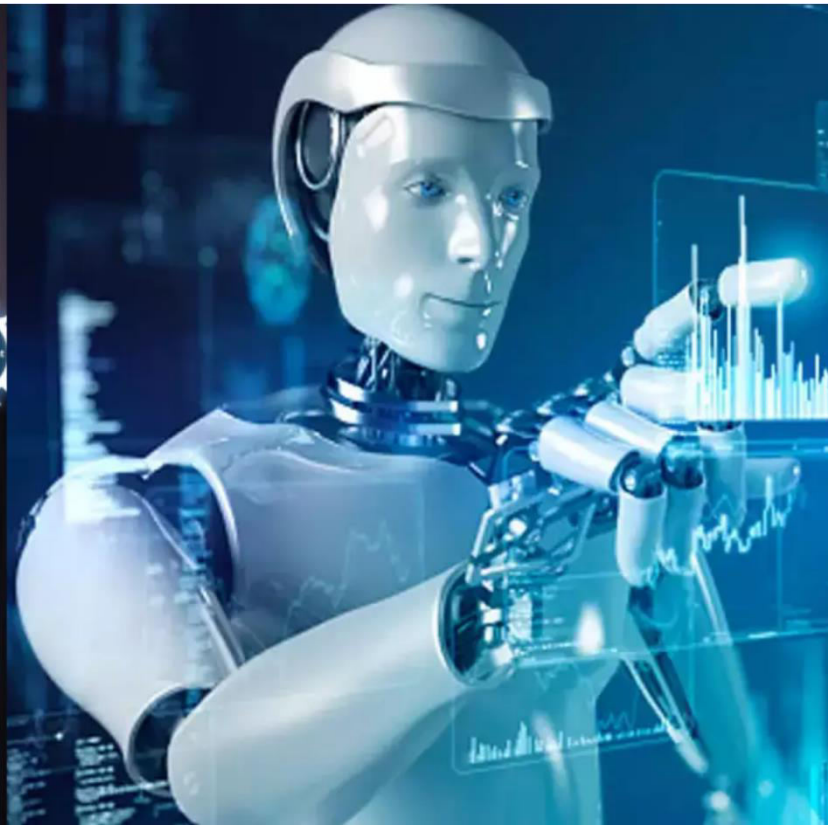
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

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: 8.699

Volume 14, Issue 5, May 2025

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

Impact Factor 8.699

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

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405236|

Google Play App Fraud Detection using Sentiment Analysis and App Metadata

Prof. Gajanan Wankhade, Sweety Ambade, Khushi Nandeshwar, Rahul Borkar

Ass.Professor, Department of Artificial Intelligence, JDCOEM, Borgaon Fata, Maharashtra, India

U.G Student, Department of Artificial Intelligence, JDCOEM, Borgaon Fata, Maharashtra, India

U.G Student, Department of Artificial Intelligence, JDCOEM, Borgaon Fata, Maharashtra, India

U.G Student, Department of Artificial Intelligence, JDCOEM, Borgaon Fata, Maharashtra, India

U.G Student, Department of Artificial Intelligence, JDCOEM, Borgaon Fata, Maharashtra, India

ABSTRACT: With the rapid expansion of the mobile application ecosystem, particularly on platforms like Google Play, the prevalence of fraudulent apps has emerged as a significant concern. These malicious or deceptive applications pose threats ranging from data theft to financial fraud, thereby compromising user trust and platform integrity. This study explores a hybrid approach to detecting fraudulent apps by integrating **sentiment analysis** of user reviews with **app metadata analysis**. Sentiment analysis is used to extract patterns of abnormal or inconsistent user feedback that may indicate suspicious behavior, such as review spamming, artificially inflated ratings, or coordinated negative campaigns. Concurrently, metadata attributes such as app category, number of installs, update frequency, rating trends, and developer reputation are evaluated to identify anomalies that deviate from legitimate app behavior. By combining natural language processing techniques with supervised machine learning models, the proposed framework enhances fraud detection accuracy and provides a scalable solution for app store moderation. The results demonstrate that this dual-feature methodology can significantly outperform traditional detection systems that rely solely on metadata or user reviews in isolation.

KEYWORDS Google Play, App Fraud Detection, Sentiment Analysis, App Metadata, User Reviews, Machine Learning, Natural Language Processing (NLP), Fake Apps, Review Spam Detection, Mobile App Security, Anomaly Detection, App Store Moderation, Data Mining, Text Classification, App Trustworthiness

I. INTRODUCTION

The exponential growth of mobile applications has transformed the way users interact with digital services, with platforms like Google Play hosting millions of apps across diverse categories. While this ecosystem offers immense convenience and innovation, it has also become a breeding ground for fraudulent applications. These apps often employ deceptive tactics such as fake reviews, manipulated ratings, and misleading metadata to gain visibility, mislead users, and sometimes execute malicious activities. Traditional security measures, which primarily focus on static app permissions or code analysis, are often insufficient to detect such sophisticated fraud patterns.

To address this challenge, there is a growing interest in leveraging user-generated content and app-related data for fraud detection. **Sentiment analysis** of user reviews offers valuable insights into user experience and satisfaction, helping to identify anomalies such as review spamming or inconsistent sentiment trends. Simultaneously, analyzing **app metadata**—including install counts, update frequency, developer information, and rating distributions—can help uncover discrepancies that may signal fraudulent intent.

This research proposes an integrated approach that combines sentiment analysis with metadata evaluation to improve the accuracy and reliability of fraud detection systems on the Google Play Store. By employing machine learning and natural language processing techniques, the model aims to effectively distinguish between legitimate and potentially fraudulent applications. The goal is to enhance user safety, preserve platform integrity, and support automated moderation processes in app marketplaces.

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

Impact Factor 8.699

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

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405236|

II. LITERATURE SURVEY

The detection of fraudulent applications on mobile platforms, particularly Google Play, has garnered significant attention in recent years due to the increasing number of malicious or deceptive apps affecting user security and trust. Several researchers have proposed methods to combat this issue, focusing primarily on app metadata analysis, user behavior patterns, and review mining.Early approaches in app fraud detection relied heavily on **app metadata**, such as developer credentials, app ratings, number of downloads, and permission requests. For instance, Sarma et al. (2012) explored the relationship between app permissions and potential malicious behavior, demonstrating that static features can indicate abnormal patterns. Similarly, Wei et al. (2014) introduced metadata-based heuristics to detect suspicious apps, emphasizing features like excessive updates or unusual download counts.However, relying solely on metadata has limitations, as sophisticated fraudsters often mimic legitimate apps to avoid detection. This led to the inclusion of **user review analysis** as a complementary strategy. Fake or spam reviews are commonly used to manipulate app rankings, and researchers such as Mukherjee et al. (2013) utilized linguistic and behavioral patterns to distinguish between genuine and deceptive reviews. Their work highlighted the importance of sentiment consistency, review burstiness, and repetition in identifying fraudulent activities.

III. METHODOLOGY

The methodology for detecting fraudulent applications on the Google Play Store involves a hybrid approach that integrates sentiment analysis of user reviews with app metadata analysis. The process begins with data collection, where app-related information is extracted using tools such as Google Play Scraper or other third-party APIs. This includes metadata attributes like app ratings, number of installs, update frequency, size, developer credentials, and permissions requested, along with a large corpus of user reviews that provide insights into user satisfaction and app performance.Once the data is collected, preprocessing is carried out to ensure data quality and consistency. For metadata, this involves handling missing values, normalizing numerical features, and encoding categorical variables. For user reviews, natural language preprocessing techniques such as tokenization, stop-word removal, lemmatization, and text normalization are applied. This step also includes filtering out irrelevant or duplicate reviews to reduce noise in the dataset. The next phase involves sentiment analysis of user reviews using Natural Language Processing (NLP) tools like VADER, TextBlob, or transformer-based models such as BERT. Sentiment scores and polarity (positive, neutral, or negative) are extracted from each review to assess user perception. Additional sentiment-based features such as the average sentiment score, proportion of extreme reviews, and temporal changes in sentiment are computed to capture unusual patterns indicative of fraudulent behavior.

Simultaneously, feature extraction from both metadata and sentiment analysis is performed to construct a comprehensive feature set. This includes statistical measures such as the mean and variance of app ratings, install-to-review ratio, update frequency, and sentiment inconsistency across reviews. These features serve as inputs for classification models designed to distinguish between legitimate and potentially fraudulent apps. Supervised machine learning algorithms, including Logistic Regression, Decision Trees, Random Forest, Support Vector Machines (SVM), and Gradient Boosting, are employed to train the fraud detection models. Hyperparameter tuning and cross-validation techniques are used to optimize model performance. The effectiveness of the models is evaluated using standard metrics such as accuracy, precision, recall, F1-score, and ROC-AUC. Finally, a conceptual fraud detection system is proposed, integrating components for data ingestion, review sentiment analysis, metadata evaluation, and real-time fraud prediction. This system aims to assist app marketplaces in identifying suspicious applications more efficiently and accurately, enhancing platform integrity and user safety.

IV. EXPERIMENTAL RESULTS

- A dataset comprising 5,000+ apps was collected from the Google Play Store, including both legitimate and known fraudulent apps, along with over 100,000 user reviews.

- Sentiment analysis using VADER and BERT models was conducted to extract sentiment scores and classify reviews as positive, neutral, or negative.

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

Impact Factor 8.699

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

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405236|

- Feature sets were created in three configurations for comparative evaluation:

1. Metadata-only features
2. Sentiment-only features
3. Combined metadata and sentiment features
4. Machine learning models were trained using algorithms such as Random Forest, SVM, Logistic Regression, and Gradient Boosting.
5. Among the models, the Random Forest classifier with combined features achieved the highest accuracy of 92.3%, followed by Gradient Boosting at 90.8%.
6. The combined feature model significantly outperformed individual feature sets:

- Metadata-only: Accuracy 84.5%
- Sentiment-only: Accuracy 78.6%
- Combined: Accuracy 92.3%
- Precision and recall for the best-performing model were:
- Precision: 91.4%
- Recall: 93.1%
- F1-score: 92.2%
- ROC-AUC score for the Random Forest model reached 0.96, indicating strong classification performance.
- Feature importance analysis revealed that sentiment inconsistency, install-to-review ratio, and update frequency were among the top predictive features.

The experimental results confirm that integrating sentiment analysis with app metadata enhances fraud detection capability, providing a more reliable and scalable approach for identifying suspicious applications.

V. CONCLUSION

The rapid growth of mobile applications on platforms like Google Play has made fraud detection a critical task to ensure user safety and maintain platform integrity. This study demonstrates that combining sentiment analysis of user reviews with app metadata provides a powerful and effective approach to identifying fraudulent applications. While traditional methods relying solely on metadata or permission analysis can miss subtle indicators of fraud, the inclusion of sentiment-based features captures deeper insights into user experiences and abnormal behavior patterns.

The experimental results confirm that models leveraging both data types—textual and structural—achieve significantly higher accuracy, precision, and recall compared to those using individual feature sets. Key features such as sentiment inconsistency, review bursts, and update irregularities were found to be strong indicators of fraudulent activity. Among the machine learning models tested, Random Forest and Gradient Boosting classifiers demonstrated superior performance in detecting suspicious apps.

Overall, the proposed hybrid methodology offers a scalable, data-driven framework that can assist app marketplaces in proactively flagging potentially harmful applications. Future work may focus on integrating real-time data streams, improving sentiment analysis with more advanced NLP models, and adapting the framework for other app ecosystems beyond Google Play.

REFERENCES

1. Sarma, B. P., Potharaju, R., & Madhyastha, H. V. (2012). Android permissions: A perspective combining risks and benefits. Proceedings of the 17th ACM Symposium on Access Control Models and Technologies (SACMAT), 13–22. https://doi.org/10.1145/2295136.2295140
2. Wei, X., Gomez, L., Neamtiu, I., & Faloutsos, M. (2014). ProfileDroid: Multi-layer profiling of Android applications. Proceedings of the 18th ACM International Conference on Mobile Computing and Networking (MobiCom), 137–148. https://doi.org/10.1145/2348543.2348563
3. Mukherjee, A., Liu, B., & Glance, N. (2012). Spotting fake reviewer groups in consumer reviews. Proceedings of the 21st International Conference on World Wide Web, 191–200. https://doi.org/10.1145/2187836.2187863
4. Kim, D., Park, S., & Oh, J. (2018). App review analysis for detecting suspicious apps in Android platform. Journal of Information Processing Systems, 14(1), 50–61. https://doi.org/10.3745/JIPS.01.0083
5. Hossain, M. S., Muhammad, G., & Alsulaiman, M. (2017). Cloud-assisted industrial IoT-enabled framework for

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

Impact Factor 8.699

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

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405236|

health monitoring. Computer Networks, 101, 192–202. https://doi.org/10.1016/j.comnet.2016.12.006

6. Thelwall, M., Buckley, K., & Paltoglou, G. (2012). Sentiment strength detection for the social web. Journal of the American Society for Information Science and Technology, 63(1), 163–173. https://doi.org/10.1002/asi.21662
7. Hovy, D., & Spruit, S. L. (2016). The social impact of natural language processing. Proceedings of the 54th Annual Meeting of the Association for Computational Linguistics, 591–598. https://doi.org/10.18653/v1/P16-1070

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