International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 07 | July - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

FRAUD APP DETECTION USING SENTIMENT ANALYSIS

[1] YASHODHA P G,[2] SACHIN S M

[1]Assistant Professor. Department of MCA, BIET, Davangere
[2]Student, Department of Master of Computer Applications, BIET, Davangere

Abstract

The swift expansion of smartphone apps has resulted in a surge in fraudulent programs, endangering users and the reliability of app stores. Conventional techniques for app appraisal frequently fall short in distinguishing between real and fake applications. This study presents a thorough method for spotting phony mobile apps by employing sentiment analysis and data mining. The system examines user evaluations and comments and uses LSTM (Long Short-Term Memory) models to discern between genuine and fraudulent opinions. Sentiment analysis integration improves the identification of questionable app activity by offering greater insights into user comments. By reducing the quantity of fraudulent programs, improving app store integrity, and giving users accurate results, this strategy seeks to create a mobile app ecosystem that is more dependable and safe.

Keywords: Fraudulent mobile applications, app store integrity, data mining, sentiment analysis, Long Short-Term Memory (LSTM) models.

I.INTRODUCTION

Mobile applications are now widely used, outpacing traditional internet access as customers' preferred method of digital connection due to the explosive growth of mobile phone users. However, the growth in fraudulent applications that have been brought about by this explosion in the use of mobile apps poses a severe threat to consumers' security and confidence. This project intends to use data mining and methods of sentiment analysis to create a sophisticated system that can detect fraudulent programs before users download them to react to this growing problem. Sentiment analysis is essential to this project because it allows the system to decipher the psychological undertones of user-generated content posted on different websites, such comments and reviews. Sentiment analysis tracks public opinions and attitudes regarding a variety of subjects, including mobile applications, by observing social media platforms and other digital channels. Differentiating real user opinions from possibly fraudulent ones becomes crucial in a world where consumers can't always rely on the veracity or validity of internet reviews. The suggested method uses data mining techniques in addition to sentiment analysis to look through the enormous volumes of textual data associated with mobile apps, including ratings, administrator comments, and user reviews. The technology looks at behavior patterns and sentiment to identify which apps are authentic and which are fake. Manipulation of reviews is a crucial component of app ranking fraud, highlighting the necessity for strong analytical methods to effectively counteract fraudulent activity.The study uses Long Short-Term Memory (LSTM) models, which are particularly good at learning and processing sequential data, along with other cutting-edge machine learning models to accomplish this goal. The technique can determine the probability of an app being fake based on labeled datasets that include both authentic and fraudulent app behavior, which the LSTM model is trained on. To put this idea into practice, an online program that offers two separate roles—administrator and user—has been built. The platform allows the super user Admin to register, view analysis of user feedback, upload

datasets, and look through a list of all users who have registered. Users have the option to register and provide reviews for the applications they select in the interim. In order to successfully stop fraudulent app actions, this online application offers an intuitive interface for sentiment research, community participation, and data-driven insights surrounding app sentiments.

II.LITERATURE SURVEY

Users are depending more and more on crowdsourced information, like reviews on Yelp and Amazon, liked posts and adverts on stolen accounts, and collusion networks, according to a [1] report. Current methods for identifying this kind of activity mostly rely on learning over known or suspected attacks through supervised or semi-supervised learning. They are not able to identify attacks when the attacker modifies their approach or when the operator misses them during labeling. Sentiment analysis is used to identify fraudulent apps.

Spam campaigns that have been discovered on well-known product review websites (like the Google Play Store) have drawn increasing attention from academics and industry [2] article, where a team of online posters is employed to work together to create false evaluations for certain target products. Targets' perceived reputations are to be manipulated in order to serve their objectives.

Online product reviews have grown in importance as a form of user feedback, according to the [3] paper. Imposters have been posting false or misleading reviews to promote and/or denigrate specific target goods or services because of their notoriety. Review spammers are the term for these imposters. Over the previous few years, a number of strategies have been put up to address the issue. This paper adopts an alternative strategy that takes advantage of the burrstones.

Online reviews of apps and services can be very helpful to clients, but they must be safeguarded against manipulation, according to the [4] study. The majority of research to date has concentrated on examining internet reviews from a single hosting website. How might information from several review hosting sites be used? This is our work's central query. As a reaction, create a methodical approach to combine, analyze, and assess reviews from various hosting sites. Pay particular attention to reviews and make use of over 15 million reviews from over 3.5 million people.

Online reviews have grown in importance as a tool for decision-making and product design, according to a [5] paper. But opinion spamming frequently targets review systems. While supervised learning has been used for years to study fake review identification, large-scale datasets' ground truth is still lacking. Real false reviews are not the foundation of most supervised learning systems currently in use; instead, pseudo-fake reviews are. Presenting the first work on Chinese fake review identification with filtered reviews from Damping's fake review detection system, in collaboration with Dianping1, the biggest Chinese review hosting site.

Online reviews are fast emerging as one of the most significant sources of knowledge for customers on a variety of apps and services, according to the [6] paper. As a result of their growing significance, spammers and unethical business owners have more chances to fabricate evaluations in order to defame their rivals or artificially promote their own apps and services. Numerous studies have been conducted in response to this expanding issue on the best methods for identifying review spam using different machine learning algorithms. Converting reviews to word vectors, which has the ability to provide hundreds of thousands of features, is a common thread among most of these experiments.

Based on the two suppositions that people are more likely to view reviews from those who are connected to them as reliable and that review spammers are less likely to maintain a large relationship network with regular users, [7] paper provides an efficient and effective method to identify review spammers by incorporating social relations. This paper makes two contributions: (1) describes how social relationships can be used to predict review ratings and suggests a model for rating prediction based on trust that uses proximity as trust weight; and (2) creates a model for

trust-aware detection based on rating variance that iteratively determines the spam city indicator based on user-specific overall trustworthiness scores.

The language and rating properties of a review can be used in the [8] article to identify phony reviews for an app. To put it succinctly, the suggested system (ICF++) will assess an application's dependability, the trustworthiness of the reviewers, and the honesty of the review. A review's honesty value will be calculated. The experiment's outcome demonstrates that, in comparison to the iterative computation framework (ICF) method's result, the suggested system is more accurate.Online social networks, or OSNs, are used for a variety of purposes in commerce, education, telemarketing, medical, and entertainment, according to the [9] article. OSNs encapsulate the structure and dynamics of person-to-person and person-to-technology interaction. Additionally, this technology makes illegal activity easier to carry out. In this new view of social life that articulates and reflects the connections that occur offline, spotting anomalies is crucial because they may indicate a serious issue or contain information that the analyst finds valuable.

In the [10] paper, they present a novel, all-encompassing method called SpEagle, which employs cues from relational data (network) and all metadata (text, timestamp, and rating) to identify products targeted by spam and suspicious users and reviews. Using information to estimate the class distribution of the nodes, SpEagle uses a review-network based classification task that takes into account prior knowledge. It works quite well.

III. METHODOLOGY

A multi-step procedure that integrates data collecting, preprocessing, sentiment analysis, feature extraction, model training, and deployment is used in the methodology for identifying fraudulent mobile applications. The following steps are how the system uses user-generated content—mainly reviews and comments—to flag questionable applications:

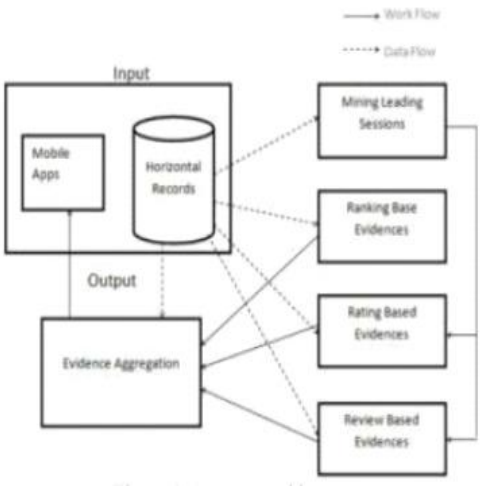

Figure3: architecture diagram

1. Data Gathering

- Determine the source: Look for social media sites and app stores (App Store, Google Play, Apple App Store) that have a lot of user ratings and comments.
- Data Collection: To gather user reviews, ratings, comments, and relevant metadata for different mobile applications, employ web scraping tools and APIs.

2. Processing Data

- Cleaning: To guarantee clear content, eliminate extraneous information such as HTML tags, special characters, and duplication.
- Normalization is the process of changing text to a standard format by applying stemming and lemmatization procedures, converting to lowercase, and eliminating stop words.
- Tokenization: For simpler processing and analysis, divide text into tokens, or individual words or phrases.
- Labeling: To help train the model, manually annotate a portion of data to identify reviews and comments that pertain to legitimate vs fraudulent applications.

3. Sentiment Analysis

- Sentiment Categorization: Use Natural Language Processing (NLP) methods to divide reviews and

comments' sentiments into groups like favorable, unfavorable, and neutral.
- Aspect-Based Sentiment Analysis: To obtain in-depth sentiment insights, identify sentiments associated with particular application elements, such as performance, security, and usability.

4. Extraction of Features

- Sentiment Features: Determine the emotional tone of the reviews by highlighting sentiment scores and patterns from the analysis.
- Behavioral Features: Look for irregularities that point to fraudulent activity by analyzing user behavior patterns, such as the timing and frequency of reviews.
- Textual Features: To find recurring themes in fake reviews, extract keywords, phrases, and writing styles from the text.

5. Model Development

- Algorithm Selection: Because LSTM networks can handle sequential data and capture temporal connections in text, they should be prioritized when choosing machine learning algorithms.
- Training: Using the labeled dataset, train the LSTM model such that it can differentiate between authentic and fraudulent app activities using features that have been extracted.
- Validation: To increase the model's predicted performance and fine-tune its parameters, validate it using an independent dataset.

6. Implementation of a Fraud Detection System

- Integration: Incorporate the LSTM model that has been trained into an online application to analyze fresh app reviews and comments in real-time.
- Real-Time Monitoring: Generate warnings and insights for administrators and users by continuously monitoring incoming data for indications of fraud.

7. Evaluation and Improvement

- Performance measures: Use measures like accuracy, precision, recall, and F1 score to assess how well the system is performing.
- User input: To determine areas of strength and potential improvement, get input from users and administrators.
- System Updates: To preserve and improve fraud detection capabilities, the system should be updated on a regular basis with fresh data and improved models.

3.1 DATA SET USED

Several important datasets are used by the fraud app detection system to train and evaluate its models, guaranteeing precise and trustworthy predictions. Gathered from app shops such as the Google Play Store and the Apple App Store, user reviews and ratings offer insightful information on the opinions and experiences of users. App names, developer information, download counts, release dates, and update histories are just a few of the elements found in app metadata, which is taken from official websites and app store listings. This context is crucial for determining the validity of an app. Furthermore, the analysis goes beyond app stores to include social media comments from sites like Facebook, Twitter, and Reddit that capture general popular sentiment and opinions about the apps. The official responses from developers are provided by administrator comments, which are sourced from app stores and developer websites. They offer further context and define official positions on app performance and concerns. In order to teach the machine learning models, a portion of user reviews and comments are manually classified as authentic or fraudulent. This process produces labeled datasets, which allow the model to identify patterns linked to fraudulent activity. Metrics like review frequency and timeliness, which are obtained from user interactions on social media and app stores, are examples of behavioral data that can be used to spot odd activity that could be a sign of fraud. Finally, the detection model's accuracy and robustness are improved by using past fraud data from cybersecurity reports and databases tracking known fraudulent apps.

3.2 DATA PREPROCESSING

User ratings and comments are analyzed by the fraud app detection system to identify counterfeit mobile applications. Initially, it gathers information from social media and app stores. Preprocessing is the next step in cleaning and preparing this data. It involves deleting unnecessary information, normalizing the text, and segmenting it into individual words. The system then uses sentiment analysis to ascertain if the reviews are neutral, negative, or positive. To assist in identifying fraud, it extracts important information including sentiment ratings and user behavior patterns. A Long Short-Term Memory (LSTM) model is trained with these features in order to identify trends in both authentic and fraudulent reviews. An online platform that examines fresh reviews in real-time and notifies administrators and users of possible fraud uses the trained model. To increase the accuracy and efficacy of the system, fresh data and user comments are added on a regular basis.

3.3 ALGORITHM USED:

Long Short-Term Memory (LSTM) Networks

The fraud app detection system employs the Long Short-Term Memory (LSTM) network as its principal algorithm. Recurrent neural networks (RNNs) of the long short-term memory (LSTM) variety are especially well-suited for processing sequential data and identifying long-term dependencies. LSTM networks find use in many different fields, including as natural language processing, speech recognition, and finance. LSTM networks, for instance, can be applied to text-to-speech transcription or stock price prediction using historical data.

LSTM networks are capable of digesting sequential input, retaining significant information over extended periods of time, and producing precise predictions based on this knowledge. The long-term information storage capacity of memory cells and gates that control the information flow into and out of these cells allow LSTMs to accomplish this.

Goal: By analyzing and learning patterns from user reviews and comments, LSTM networks let the system differentiate between the actions of legitimate and fraudulent apps.

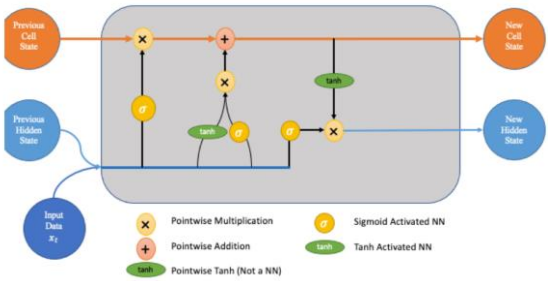

Figure 3.3: architecture diagram

Function:

- Sequential Data Handling: Because LSTMs are able to process data in sequences, they are perfect for text analysis applications where word and phrase order is important.
- Long-Term Dependencies: Their ability to retain knowledge for extended periods of time is useful for deciphering the subtleties and context of user reviews.
- Pattern Recognition: LSTMs are trained to identify intricate patterns and nuanced signs of fraud using labeled datasets containing reviews that are both real and fraudulent.
- Accuracy: By using textual analysis of reviews and comments, LSTMs enhance the system's capacity to predict with greater accuracy whether an app is authentic or counterfeit.

3.4 Techniques Used

LSTM networks use a variety of strategies to manage and process data sequences efficiently. They make use of specialized long-sequence long-term memory (LSTM) cells that selectively update memory states using information-flow-controlling gates. Based on current inputs and previous states, sigmoid activation functions in these gates control the amount of information that is stored or discarded. Tanh activation functions provide the proper scaling of new data added to the memory state. In order to improve prediction accuracy over time, backpropagation through time techniques are used during training to modify network parameters depending on error

gradients derived across sequences. Gradient clipping is a technique that limits the amount of gradients to minimize unstable training, whereas dropout regularization randomly deactivates connections between LSTM units to prevent overfitting.

When combined, these techniques improve LSTM networks' capacity to recognize intricate patterns in sequential data, which makes them useful for applications such as time series analysis and natural language processing.

IV. RESULT AND DISCUSSION

Sentiment analysis-based fraud app detection system has shown encouraging results in detecting possibly fraudulent mobile applications. The technology accurately discerns between authentic user interactions and those that suggest fraudulent activity through the analysis of user evaluations and comments. The technology employs sophisticated methods such as LSTM networks and natural language processing to detect anomalous review trends and strange sentiment patterns, which enable it to reliably identify suspicious app actions.

Discussion: This system's capacity to decipher the emotional tone and contextual significance of user feedback from a variety of channels is what makes it successful. It keeps an eye on user behavior patterns and sentiment trends to identify potentially dangerous apps, such as ones that receive negative comments or excessively positive evaluations from dubious sources. Over time, the incorporation of LSTM networks improves its capacity to identify subtle indications of fraud, enabling administrators and users to receive timely alerts to prevent installing counterfeit applications. refined cybersecurity and user trust in mobile app settings are facilitated by machine learning models that are continuously refined to ensure they can react to changing fraudster techniques.

4.1 Graph

Figure 4.1 : fraud app using sentiment analysis

V. CONCLUSION

In conclusion, by examining user reviews and comments, the sentiment analysis-based fraud app detection system successfully detects possibly counterfeit mobile applications. Through the use of cutting-edge methods such as LSTM networks and natural language processing, the system is able to discern between the activities of legitimate and questionable apps with high accuracy. By providing proactive safeguards to shield users from fraudulent activity and encouraging confidence and safety in the use of mobile apps, this improves security throughout the app ecosystem. Continued advancements in sentiment analysis techniques and machine learning models will fortify the system's defenses against changing app fraud risks.

VI.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 business 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 fake reviews 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 Arti?cial Intelligence Research Society Conference, 2016.

[7] H. Xue, F. Li, H. Seo, and R. Pluretti," Trust-Aware Review Spam Detection",IEEE Trustcom/ISPA.,2015.

[8] E. D. Wahyuni , A. Djunaidy," Fake Review Detection From a ProductReview Using Modi?ed 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.

****