Identification of Fraud Apps Using Sentiment Analysis Techniques

https://doi.org/10.3991/ijim.v15i23.27361

Abeer Aljumah, Amjad Altuwijri, Thekra Alsuhaibani(✉), Afef Selmi, Nada Alruhaily
Qassim University, Buraydah, Saudi Arabia
iofaausat@gmail.com

Abstract—Considering that application's security is an important aspect, especially nowadays with the increase in technology and the number of fraudsters. It should be noted that determining the security of an application is a difficult task, especially since most fraudsters have become skilled and professional at manipulating people and stealing their sensitive data. Therefore, we pay attention to spot insecure apps by analyzing user feedback on Google Play platform using sentiment analysis. As it is known, user reviews reflect their experiments and experiences in addition to their feelings and satisfaction with the application. But unfortunately, not all of these reviews are real, fake reviews do not reflect the sincerity of feelings, so we have been keen in our work to filter the reviews and deliver accurate and correct results. This tool is useful for both users wanting to install an android app and for developers interested in app's optimization.

Keywords—sentiment analysis, android, google play, user review, mining threat, security

1 Introduction

With the rapid development of technologies, mobile applications are widely used in people's daily life. The increase in the number of applications makes it difficult for users to choose the appropriate application for them in several aspects, the most important of which is the safety of that application. By some estimates, one out of every 36 mobile devices have high-risk apps installed [1]. Determining an application's security is not easy, especially for those who do not have any technological knowledge, so we decided to determine the level of security for the application by analyzing user reviews using sentiment analysis, which studies have proven successful in many areas.

To analyze data, we needed an organized step—by—step methodology. So, Data Analysis Life Cycle is the chosen method as it is often used for big data analysis and helps to eliminate problems in data science projects. Basic DALC phases are discovery, data preparation, model planning, model building, operationalization, and communicating results.

- Discovery: In this phase, we discover the resources that we need such as the availability of data and technology. Search in the related previous work to investigate the problem and learn from their experience.
- Data preparation: Explore, preprocess, clean, and normalize the data before modeling and analysis.
- Model planning: Select the most suitable model based on data structure and volume.
- Model building: We will consider whether the existing tools will suffice for running the model or if we need a more robust environment. We will use Python language to train and test our model.
- Operationalize: Check if our goals are met by the tests we were run in the previous phase. compare outcomes to criteria established for success and failure. Considers how best to articulate findings and outcomes.
- Communicate results: Communicates benefits of the project more broadly, delivers final reports, briefings, codes. deploy work in a controlled way.

The proposed tool contributes in some key points:

- All previous studies of identifying apps security issues through user reviews have assumed that all the reviews are genuine and written by authentic users. In fact, the proliferation of spams dramatically depresses the accuracy of opinion mining and sentiment analysis results. So, we have been keen in our work to filter the reviews to get more accurate and correct results.
- For the extraction of security-related reviews we have constructed a new list of keywords based on two researches [2][3] to increase the number of extracted reviews and improve the assessment of an application.

The rest of this paper is organized as follows. Section 2 discusses related works. Section 3 about results and discussion. Section 4 discusses experiments related to the study. At the end section 5 explains the conclusions.

2 Related work

Sentiment analysis is a text analysis technique that detects people's emotions polarity (e.g., a positive or negative opinion) within the text, as a whole document, paragraph, sentence, or clause. Also, machine learning now is a common social media analysis tool [4]. [5] Use two approaches for performing sentiment analysis: statistical model-based approaches and Natural Language Processing (NLP). It clearly shows that rule-based models outperformed the statistical models for both apps with an Overall Precision of 92% for rule-based models and 81% for a statistical model. Sentiment analysis has many types, such as Fine-grained, Emotion detection, Aspect-based, and Multilingual sentiment analysis. For Aspect-Based Sentiment Classification, [6] achieved the best performance using NBM. It achieved 88.08% classification accuracy on the restaurant's dataset and 90.53% on the hotel's dataset. Opinion spam detection has become a major challenge in sentiment analysis. Opinion spams, often known as false or fake reviews, are well-written comments that support or criticize a product. Opinion spam detection seeks to spot three distinct characteristics of a spam review: review content,

metadata of review, and real-life knowledge about the product [7]. Several techniques and methods are suggested to help detect fake reviews with greater accuracy. One of the most effective ways is the process of extracting features from the text, that can be categorized into two main groups: Features related to review content and the second method focuses on the features of reviewers [8][9]. Android is the most popular mobile operating system due to its open-source nature. The security of Android is provided by techniques require prior installation and are based on app features. In contrast, we want to stop installation by analyzing reviews. [2] Provides a framework called CIAA-RepDroid, a fine-grained security-related reputation based on security-related sentiment analysis and probabilistic classification model. [10] Has developed the AUTOREB framework, as compared to the other approaches, AUTOREB excels a large margin with 51.36% in accuracy.

3 Results and discussion

The practical implementation of this tool is composed of data preprocessing, reviews filtering, aspect-based sentiment analysis, and finally the risk assessment results and presentation.

3.1 Filtering

This step aims to gather reviews about security problems. Manually checking all of the reviews to identify security-related ones will be time-consuming and error-prone. Several ML algorithms have been proposed to extract useful reviews in many different ways. On the other hand, those intelligent algorithms need a huge volume of annotation data, and manual annotation has a significant effect on the performance. As a result, we extract security-related reviews using a keyword-based technique. We have constructed our list of security-related keywords based on the two lists of CIAA-RepDroid [2] and SRR-Miner [3].

3.2 Spam detection

We can say that user ratings are no longer considered a reliable metric for determining quality, except if we detect and exclude these spam reviews. Two main approaches are being used for spam detection: behavioral and textual features. Behavioral features correspond to features such as review date, rating, and geo-location of the reviewer. Textual features refer to methods, such as part-of-speech patterns, word frequency, n-grams, and cosine similarity to find linguistic clues of deception. As an optimized choice for this task, we used the SpEagle tool [11].

3.3 Preprocessing

Data preprocessing is a crucial step in sentiment analysis. It prepares the raw data to make it suitable for building and training Machine Learning models. For our model,

we applied Tokenization and Lemmatization. We did not remove stopwords, punctuation and lowercase because VADER (more about Vader in the next section) does not handle stop words [12] and can very well understand the sentiment of a text containing capital words and punctuations. Usually, preprocessing is the first step in any natural language processing project. But, in our case we needed to perform filtering and spam detection steps before. Because, those steps need to work with the raw data with no changes at all. Otherwise, the results will be negatively affected.

3.4 Aspect-based sentiment analysis

In this step, we compared NLTK, TextBlob, Flair, and VADER, which are some of the most popular sentiment analysis models, to determine the best one for our work. When it comes to analyzing comments or reviews from social media, the received emotional feeling changes based on the used icons and emojis. VADER has the advantage of considering emojis and some essential points such as punctuation, capitalization, grade point average, inflections, grammar, and colloquial [13]. That is why VADER is the best choice for us to work with.

3.5 Risk assessment and results presentation

To assess security for an app, reviews for each application will be analyzed independently, and deliver an assessment of each one of the four security aspects of the app: confidentiality, integrity, availability, and authentication (CIAA) to recommend where improvements should hold exactly. and finally deliver a global assessment for the app as a whole.

4 Experiments

This section presents the main findings from applying the proposed model to real applications in the Google Play Store. This section includes four experiments:

4.1 Why do we filter the reviews?

Most people care about the functional aspects of the application, forgetting the security aspects. Despite the rampant attacks and the spread of malicious applications. As Figure 1 shows that reviews related to security are few compared to other reviews. Because our focus is on those related to security, the first step was filtering reviews. This step saves a lot of time and effort. The time spent on the rest of the steps will be greatly affected by this step, which speeds up the work and reduces the use of space and processor.

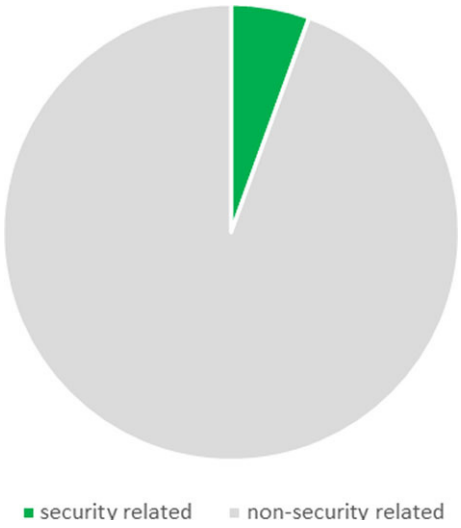

Fig. 1. The percentage of security-related reviews and the non-security related reviews

4.2 Why do we focus on the security aspect?

As shown in Figure 2, WeChat has a high Google Play rating, and many people have installed it. But this doesn't mean that the app is secure enough, as most users rate the app according to the functions and services it provides, without shedding light on the security aspects. Figure 3 shows the assessment results related to this application when our model is applied to it. Which appear to have a 56% of risk, that is considered high, especially in terms of availability.

Fig. 2. WeChat in google play

Fig. 3. Risk assessment for WeChat

4.3 Why do we exclude spam reviews?

Reviews are an important source in the application's reputation. But, evaluating an application through raw comments and ratings is an inaccurate way. After we filtered the spam reviews, we got very little results. There are several reasons for this first, because we only filtered the reviews related to the security, as shown previously in Figure 4, their number is small compared to the other aspects. Secondly, Google Play has made efforts to remove fake reviews and claimed to have removed millions of fake reviews in 2018 but, they were not 100% successful [14].

4.4 Why did we use a keywords list combined from two researches?

Our tool is to assess the security of applications by analyzing the reviews, so we are trying to collect as many reviews related to security as possible to get the correct evaluation of the application. As shown in Figure 4, when we filtered reviews based on security words in [3], we got approximately 3594 reviews, while in [2] we got 4698 reviews. Based on a goal to collect the largest amount of reviews. We constructed our list of security-related keywords based on the two lists of CIAA-RepDroid [2] and SRR-Miner [3], which gave us a larger amount of reviews.

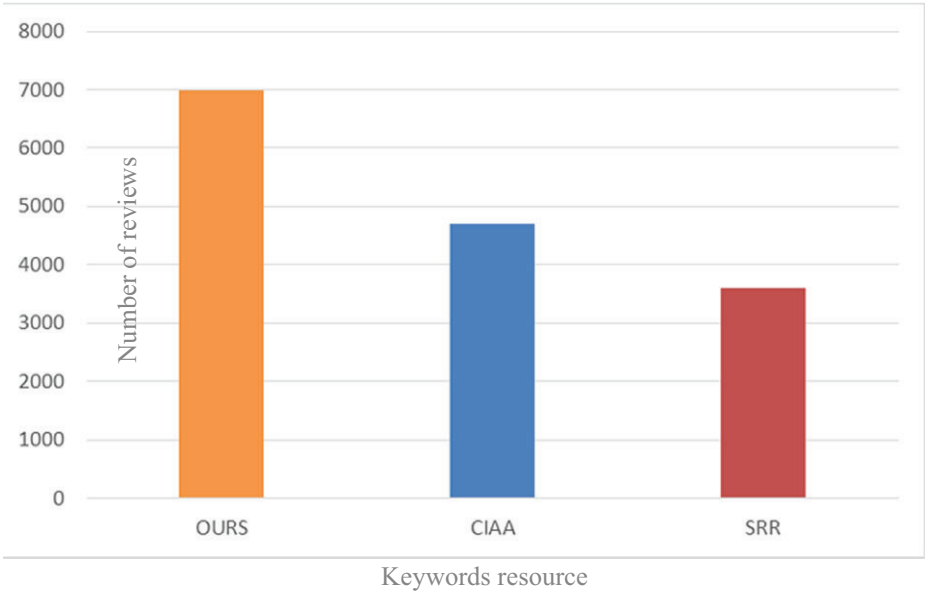

Fig. 4. The result of filtering the reviews based on keywords from each resource

5 Conclusion

This tool is useful for users who are willing to install an android app and for developers interested in making an app better. It helps to increase the awareness of users

to combat suspicious apps, increase the security level in google play and reduce the incidence of attacks, present users with a detailed overview of security issues that have been exposed, and provide developers with a specific knowledge about the vulnerabilities and misbehaviors of the app as user-generated report.

6 References

[1] Imran, K., Anjum, N., Alghamdi, A., Shaikh, A., Hamdi, M., and Mahfooz, S. (2022). A secure and efficient cluster-based authentication scheme for internet of things (IoTs). Computers, Materials & Continua, 70(1), 1033–1052. https://doi.org/10.32604/cmc.2022.018589

[2] Tchakounté, F., Yera Pagor, A. E., Kamgang, J. C., and Atemkeng, M. (2020). CIAA-RepDroid: a fine grained and probabilistic reputation scheme for android apps based on sentiment analysis of reviews. Future Internet, 12, 145. https://doi.org/10.3390/fi12090145

[3] Tao, C., Guo, H., and Huang, Z. (2020). Identifying security issues for mobile applications based on user review summarization. Information and Software Technology, 122, 106290. https://doi.org/10.1016/j.infsof.2020.106290

[4] Nilashi, M., Minaei-Bidgoli, B., Alrizq, M., Alghamdi, A., Alsulami, A. A., Samad, S., and Mohd, S. (2021). An analytical approach for big social data analysis for customer decision-making in eco-friendly hotels. Expert Systems with Applications, 186, 115722. https://doi.org/10.1016/j.eswa.2021.115722

[5] Liu, J., Sarkar, M. K., and Chakraborty, G. Feature-based sentiment analysis on android app reviews using SAS® text miner and SAS® sentiment analysis studio. In Proceedings of the SAS Global Forum 2013 Conference, May 2013, (Vol. 250).

[6] Afzaal, M., Usman, M., and Fong, A. (2019). Tourism mobile app with aspect-based sentiment classification framework for tourist reviews. IEEE Transactions on Consumer Electronics, 65, 233–242. https://doi.org/10.1109/TCE.2019.2908944

[7] Quasim, M. T., Alkhammash, E. H., Khan, M. A. et al. (2021). Emotion-based music recommendation and classification using machine learning with IoT Framework. Soft Computing, 25, 12249–12260. https://doi.org/10.1007/s00500-021-05898-9

[8] Etaiwi, W., and Awajan, A. The effects of features selection methods on spam review detection performance. International Conference on New Trends in Computing Sciences (ICTCS), October 2017, IEEE, pp. 116–120. https://doi.org/10.1109/ICTCS.2017.50

[9] Hassan, R., and Islam, M. R. Detection of fake online reviews using semi-supervised and supervised learning. International Conference on Electrical, Computer and Communication Engineering (ECCE), February, IEEE, pp. 1–5.

[10] Kong, D., Cen, L., and Jin, H. Autoreb: Automatically understanding the review-tobehavior fidelity in android applications. 22nd ACM SIGSAC Conference on Computer and Communications Security, October 2015, pp. 530–541. https://doi.org/10.1145/2810103.2813689

[11] Shebuti, R., and Akoglu, L. Collective opinion spam detection: bridging review networksand metadata. 21th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, August 2015, pp. 21–28.

[12] Gustafsson, M. (2020). Sentiment analysis for tweets in Swedish: using a sentiment lexicon with syntactic rules. Computer Science, 1–40.

[13] Hutto, C., and Gilbert, E. Vader: A parsimonious rule-based model for sentiment analysis of social media text. International AAAI Conference on Web and Social Media, May 2014.

[14] Fernandez. N. (2020). It's 2020 and the google play store still has a major fake review problem. Accessed: 22.8.2021. [Online]. Available: https://www.androidauthority.com/play-store-fake-review-problem-1082191/

7 Authors

Abeer Aljumah, Department of Information Technology, College of Computer, Qassim University, Buraydah, Saudi Arabia.

Amjad Altuwijri, Department of Information Technology, College of Computer, Qassim University, Buraydah, Saudi Arabia.

Thekra Alsuhaibani, Department of Information Technology, College of Computer, Qassim University, Buraydah, Saudi Arabia.

Afef Selmi, Department of Information Technology, College of Computer, Qassim University, Buraydah, Saudi Arabia.

Nada Alruhaily, Department of Information Technology, College of Computer, Qassim University, Buraydah, Saudi Arabia.

Article submitted 2021-09-06. Resubmitted 2021-10-16. Final acceptance 2021-10-21. Final version published as submitted by the authors.