PROVIDE SECURITY ABOUT RISK SCORE IN MOBILE APPLICATION'S

Bhambare Monali S[1], Kapse Poonam M[2], Gangurde Kirti S[3], Dane Tanuja S[4]

[1]*Student, Computer Engineering, SND College of Engineering, Yeola, SPPU, Maharashtra, India*
[2]*Student, Computer Engineering, SND College of Engineering, Yeola, SPPU, Maharashtra, India*
[3]*Student, Computer Engineering, SND College of Engineering, Yeola, SPPU, Maharashtra, India*
[4]*Student, Computer Engineering, SND College of Engineering, Yeola, SPPU, Maharashtra, India*

Guided By:
Prof. Shaikh I. R., Professor of Computer Engineering, SND College of Engineering Yeola, SPPU, Maharashtra, India.

Abstract

Now days as the use of mobile devices is increasing rapidly day by day, huge number of mobile apps are coming into the market. These apps ask the user access to various kinds of permissions, and also many of these perform the same task. The user comes at risk with presence of some malicious app due to access of permission it will get, as android provides a stand –alone defense mechanism with respect to malicious apps. Where it warns the user about the permissions the app requires, trusting that the user will make proper decision, which requires the user to have the technical knowledge and time, which is not user friendly for each user. Also classification of these apps can be useful in understanding the user preferences and can motivate the intelligent personalized services. But to effectively classify the app is a nontrivial task as limited contextual information is available.
To address these two issues an approach is proposed where the apps will be classified first using the enriched contextual information from web search engine, then with the contextual features from the context-rich device logs of mobile users and calculating the risk score for the app in order to generate a user friendly metric for the user to use when choosing the app. This will help us to get effective classification of the mobile apps and protect the user's mobile devices from malicious apps.

Key Words: - Mobile apps classification, risk, malware, web knowledge, enriched contextual information.

----------***----------

1. INTRODUCTION

We proposed one mobile apps which is used cover the risk of apps and classified the score. We proposed an efficient and effective approach to classify the mobile apps based on extraction of implicit and explicit real world features. Also web-based contextual information for training a multiclass mobile apps classifier with the use of risk factor score estimation. Now a day as per our observation, use of mobile devices is increasing rapidly day by day, huge number of mobile apps are coming to the market. Generally user access to various kinds of permission and also many of these perform the same task. As large number of these apps comes with similar functionality, having a proper classification of them make it easy and time efficient for user to select apps with security.

Also classification of these apps can be useful to understanding user's preferences and can motivate intelligent personalized services. Before being installed these apps ask user access to various kinds of permissions. The user comes at risk with presence of some malicious apps, due to access of permission it will get, as android provides a stand-alone defense mechanism with respect to malicious apps. Before the app is installed it just gives list of permissions the app will be accessing and leaves the decision of trusting app on user. But to make this decision it is requires that the user should have some technical knowledge and also as this request of permission comes for every app users lose interest in this warning. They ignore it and mostly make their decisions based on the reviews and ratings.

The risk score will be given in simple manner to the user just like we have rating of apps that is in easy to understand manner. So that the user will have another metric to use while selecting the app and to protect their data from malicious apps. Calculating the risk score for the app in order to generate a user to use when choosing the app. This will help us to get effective classification of the mobile apps and protect the users mobile devices from malicious apps.

2. LITERATURE SURVEY:

The Problem Automatically classify the mobile apps can also be considered as a problem or risk to classify the small and scattered text.

Now a days the smartphone users are increasing rapidly in huge manner most of android users. They will perform all the activity or regular work with android apps respect to his android smartphone. We can say the desktop or laptop will replace with smartphones but the smartphone user will look on his security concern so the need to arises security for user's data. Now a day most of the launcher provides security for android smartphone but this is not much enough to provide security for smartphone so we will go to provide

For developing proposed system we will look some related papers are as follow

- In [1] their work has presented a general framework to process the small and scattered text document on the web. The hidden topics discover from external large scale data or documentation collection that is universal data set.
- In [2] their work presented a similarity kernel function based on approach to find the similarity in between the small text. The system has searched the traditional cosine similarity calculate like cosine coefficient produce inadequate results such as suppose for the two small text like Artificial Intelligence and AI.
- In [3] classifying queries is an important task. But searched queries are mostly small, thus carry scattered information to provide correct classification. Their work have proposed a method for classify these small queries using blind feedback technique.
- In [4] Discovering the users have similar interest can be used for various applications such as recommendation, segmentation for market analysis. Their work have proposed approach which search snippets to build vector space for both usage and classifies the apps using cosine space distance.

2.1. Research Methodology:

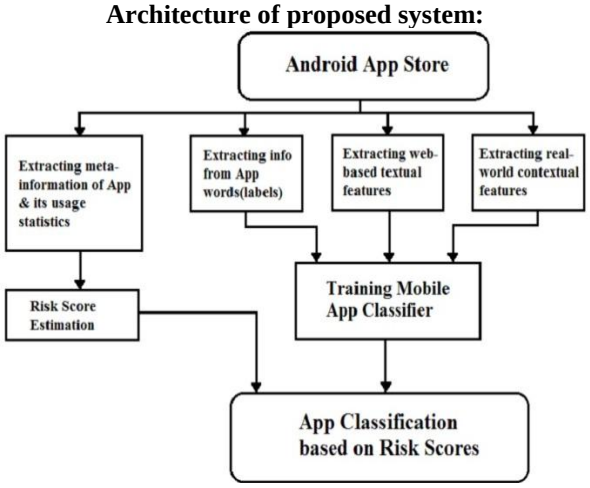
- To exploit the relevancy between App name and category labels, here the information about the app will be extracted using the app words (labels). what happens here is suppose given an App a and its category label c, the basic features that can react the relevance between a and c are considered. The weights of these features can be learned in the training process of the machine learning model.
- For extracting the web based textual features, two kind of specific features will be considered i.e. explicit feedback of vector space model and implicit feedback of semantic topics, they will be used to capture the relevance between the apps and there corresponding category labels.
- Three types of contextual features which are used to extract the real world contextual features will be considered. Pseudo feedback will be taken i.e. here for a pre-selected and labeled app; contextual record of the usage of the app is collected from the context logs of mobile user. In implicit feedback latent semantic meaning behind the collected contextual information will be considered. Then at last frequent context patterns will be used i.e here the mutually related context-value pair for the apps will be exploited, for that mining algorithm like GCPM or BP-Growth can be used.
- For classifying the app we need to train the classifier to integrate multiple effective features, for this supervised classification models like naive bayes , SVMs, decision tree or maximum entropy can be used.
- To make this classification of the app more efficient and effective we will be extracting the meta information of the apps like the list of permissions they request to access from the user and also the usage statistics. Here using the rarity of the critical permission and the pairs of critical permissions used we will calculate the risk of the app in a simple user-friendly manner. Using the machine learning technique and heuristics, technique can be presented to generate the risk signals and risk score. Naive Bayes has been extensively used both in the context of spam detection and anomaly detection in network traffic flows. In the context of Android, however, there has been limited work. So using this will improve the classification of app as we will get a strong defense against the malicious application. The figure given below explains the improved classification of the app with the risk score, i.e. here inside the app store after extracting and integrating all the features we will get the app classified in its accurate category along with its risk score.

3. PROPOSED SYSTEM:

In our proposed system have classification of the mobile apps, we will be collecting information from various methods such as web search engine, real world contextual data, contextual log information of users etc. From this data, we obtain the features for the mobile apps appearing in these logs. Then with the help of machine learning model available, we will have train data to the classifier give us the appropriate classification of the app.

To explain this in a more systematic way, consider given taxonomy T, and an app A and specified system parameter S, according to our approach, which will be extracted from the relevant web search and the contextual information about the app. To be more specific suppose we have app 'A' and then it will be classified into the S which consist of list of categories in order like {c1,c2,c3....cS}. Here for the effective feature selection an important task, is to train the machine learning model because the names of the apps are short and sparse as a result when a new app comes, whose partial or all the words present in the name are not present in the training data then the app will not be properly classified, so to overcome this we are extracting the features from different sources so that the relevance between this app and the categories can be obtained from these features. The system implemented will act as a standardization which can be used for various systems like app stores, target advertising, recommendation system, user segmentation etc. The system works according to the following phases.

Architecture of proposed system:



4. CONCLUSIONS

We discuss the main things of communicating the risk of an application to users, and propose several methods to rating this risk for security of mobile apps. We test these methods on big real-world data sets to understand each method's ability to assign risk score to the mobile apps. One effective method is the RSS method which has several advantages. It is monotonic, and it can provide feedback as to why risk is high for a specific app and how a developer could reduce that risk for mobile apps security. It performs well in identifying most current malware mobile apps as high risk score for security. This method allows for highly-critical and less-critical permissions to affect the all overall risk score of apps in an easy to understand way for user's , making it more secure as well as difficult to hack when compared with other models.

REFERENCES

[1]. "Generating Summary Risk Score for Mobile Application" – Christopher S. Gates. IEEE Transaction On Dependable And Secure Computing. May-June 2014.
[2]. "Mobile App Classification with Enriched Contextual Information" – Hengshu Zhu. IEEE Transaction On Mobile Computing. May-June 2014.
[3]. "Classifying the mobile application with risk score by using enriched information of App context. – Journal Paper ISO – 2015.
[4]. "Naïve Bayes vs Decision Trees in Intrusion Detection Systems" – Nahla Ben Amor. 2004 ACM Symposium on Applied Computing.

BIOGRAPHIES

Monali S. Bhambare.
Computer Department
SND College of Engineering & Research Center. Yeola Dist. : Nashik

Poonam M. Kapse.
Computer Department
SND College of Engineering & Research Center. Yeola Dist. : Nashik

Kirti S. Gangurde.
Computer Department
SND College of Engineering & Research Center. Yeola Dist. : Nashik

Tanuja S. Dane
Computer Department
SND College of Engineering & Research Center. Yeola Dist. : Nashik