IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-3, Issue-5 E-ISSN: 2347-2693

Analysis of Android app Permissions for User's Privacy Preservation

Supriya S. Shinde[1*] and Santosh S. Sambare[2]

[1*,2]*Department of Computer Engineering, Pimpri Chinchwad College of Engineering, Savitribai Phule Pune University, India,*

www.ijcseonline.org

Received: May/05/2015 Revised: May/12//2015 Accepted: May/25/2015 Published: May/30/ 2015

***Abstract*—** The total number of consumers that are using smartphones has increased in the past year and continue to grow. Mobile users are concerned about their sensitive data, but often do not understand the security risks involved while performing financial transactions through a mobile application. This research work mainly focused on application permissions and whether they are categorized as dangerous or normal as per the Android developer guidelines. These two types of permissions help to compute the possible danger of each mobile application. Results showed that risky permissions apps are harmful for user's data preservation and classification of normal and dangerous apps clearly. Our work proposes a system which would help the users in analyzing and removing harmful apps and thereby protecting their security and privacy. This is achieved by analyzing the various permissions used by an application that it has requested during installation. The overall process of analyzing apps is done using weka data mining tool and classification techniques. The major objective of the proposed system is to detect and remove the potentially risky apps that are present in the user's Android device.

***Keywords*—** Android;Classification; Dangerous Permission; Harmful Apps; Normal Permission.

I. INTRODUCTION

This section describes the various related approaches used in android permission management and harmful applications detection in detail. We have collected real data from various different android devices installed apps and based on permissions extracted from each app dataset is created and examined the classification result of dangerous/harmful app and normal app using six classifiers Bayes, Function , Lazy, Meta, Rules, Tree.

Android is an open source Linux Kernel, it gives the opportunity to the user's to develop their own app and make it available on Google play store[10]. Whenever any user installs any third party app, user has only two selections either to accept all terms and install particular application or stop the installation. Thus in order to install and use an application, user has to grant all the permissions that an app needs to work properly[8].

A user who wishes to install and use any third party app doesn't understand the significance and meaning of the permissions requested by an application, and thereby simply grants all the permissions as a result of which harmful apps also get installed and perform their malicious activity behind the scene. The user's inability of analyzing the risk of any application results in compromised security and privacy[2].

In our work we proposed a system to protect Android user's from harmful and potentially risky apps. The proposed system first extracts total installed apps with their list of permissions which they are accessing without user's knowledge. Further six listed classification algorithms applied which are used to accurately classify whether an application is benign or a harmful application. This proposed system reduces the user's problem of analyzing the risk of applications through which user can take the decision of removing an harmful application.

II. LITERATURE SURVEY

This section describes the various related approaches used in android permission management and harmful applications detection in detail.

In this approach authors have used pattern mining algorithm to identify a set of contrast permission patterns that aim to detect the difference between clean and malicious applications. A benchmark malware dataset and a dataset of 1227 clean applications has been collected by us to evaluate the performance of the proposed algorithm. Valuable findings are obtained by analyzing the returned contrast permission patterns[1].

In this research Brett Ferris, Jay Stahle, and Ibrahim Baggili studies application permissions and whether they are categorized as dangerous or normal as per the Android developer guidelines. In the absence of an existing risk index, they have created Application Danger Index based on these two types of permissions to help quantify the possible danger of each mobile banking application. Additionally a comparison was made between the percentage frequency of common permissions that occur in benign, malicious and

banking applications to further inspect the potential danger in banking applications[2].

The approach adopted in this particular app is based on application repackaging to verify the real need of requesting and granting access to all the sensitive Android's APIs. This approach requires neither access to the applications' original source code nor modification of the underlying framework. Static analysis is used to compute the (maximum) set of permissions that might be used by the examined application, and dynamic analysis to validate their use. The outcomes of both static and dynamic analysis are combined and compared with the manifest's permission set to deduce whether the application is over-privileged or not. This approach can be used in order to compute mobile applications attack surface and the risk introduced by over-privileges[3].

Felt, Porter, Greenwood and David observed the permissions of the most popular Android applications and evaluated whether they are effective at protecting users. They found that 93% of free and 86% of paid applications had one or more dangerous permission/s. However, they also concluded that, when declared upfront by the developer, permission requirements can be beneficial to system security [6].

III. PROPOSED WORK

The overall design of the proposed system is given in following fig. 1 and each of these components is addressed in the following sections briefly.

- Enlist all installed third party applications and their permissions will be extracted and applications permission dataset prepared.
- Android permission app dataset is pre-processed and classification algorithms applied using weka data mining tool.
- Total number of normal and harmful applications is classified and performance of each classifier evaluated using six classifiers.

Fig. 1 shows architecture and Fig. 2 gives brief idea about overall flow of proposed work. This approach is useful for all the users to protect their sensitive data from being misused by third party apps.

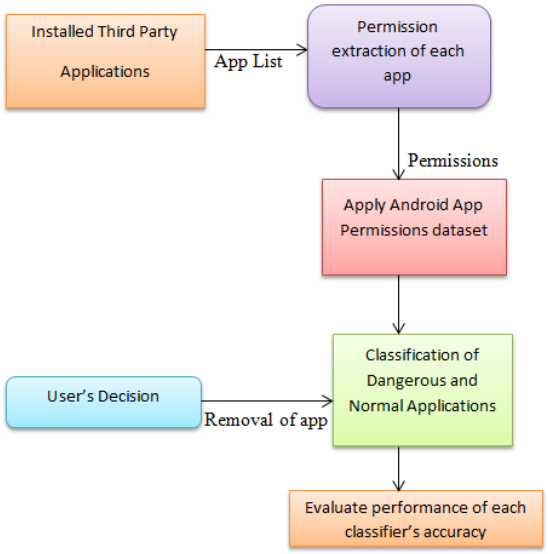

Fig. 1 Architecture Design of Proposed System

A. *Workflow of proposed system*

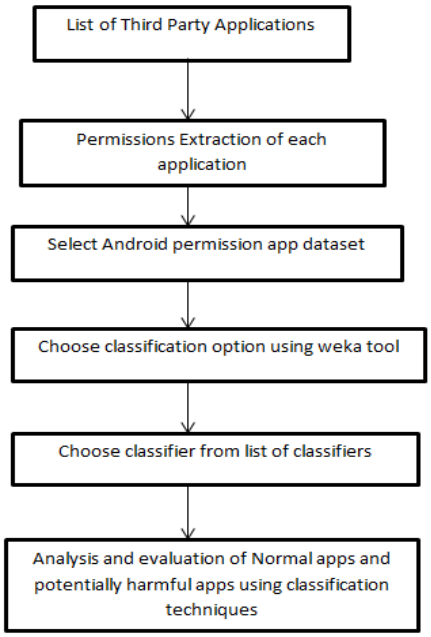

Fig. 2 Workflow of proposed system.

Workflow steps are as follows:

1. Identify the list of third party installed applications.
2. Extract the complete list of permissions of each application.
3. Identify android: protection level of each permission, i.e. Normal or Dangerous of each app
4. Take android app permissions dataset. To identify the harmful applications apply classification algorithms.

5. Note the accuracy of spam classification given by it and time required for execution
6. Results as accuracy among different harmful and normal apps Classifiers are analysed.

B. Dataset Used:

The android permission dataset was created by real time collected data from various third party apps. This dataset contains 16 instances and 8 attributes (7 continuous input attribute and 1 nominal class label target attribute.)

The data set has 16 instances. Among them, 9 instances are harmful applications which are risky for user's sensitive data preservation and 7 instances are normal applications. For each instance, there are 8 attributes. The first 8 attributes are all continuous real number ranging from 0 to 7. The last attribute is a nominal class attribute. 1 denotes that the harmful application, 0 denotes that the normal application.

C. Multiple classification Algorithms Used:

1. Bayes Classifier

Bayes method is also used for classification in data mining .There are six Bayesian method such as AODE, ADOEsr, Naive Bayes, Bayesian Net, Naive Bayes Simple, Naive Bayes updatable. In our work we have used Naive Bayes classification method. Naive Bayes classifier makes assumption about independence of the attributes. Bayes Rules are used to predict the class with some feature values [4].

2. Function Classifier

Neural Network and regression are the concepts used by Function Classifier. Function classifier can be written down as mathematical equation in natural way.The various methods of function classifier are Linear Regression, Logistic, FunctionsLogistic, RBNFNetwork, etc. For our experiment we have used FunctionsLogistic. FunctionsLogistic builds logistic models, fitting them using LogitBoost with simple regression function base learner as base learner and determining how many iterations to perform using cross validation, which supports automatic attributes selection[7].

3. Rule Classifier

Relationships among all attributes can be found by using Association Rules. More than one conclusion is predicted by the rule classifier. The correctly predicted records are called coverage. Accuracy is total number of records correctly classified from total number of records. Support is coverage divided by total number of records. Different methods in rules classifier are Conjunctive Rule, Decision table, DTNB, PART, Zero, JRip and Rider. For our dataset we have used PART method. PART obtains rules from partial decision trees [3].It builds the tree using C4.5's heuristics with the same user defined parameters as J4.8.

4. Lazy Classifier

Lazy learners store the training instances and do no real work until classification time[7].It supports incremental learning. Different lazy classifier methods are IB1, IBK, K-Star, LWL, LBR. For our data set we have used K-Star algorithm. K-Star is a nearest neighbour method with a generalized distance function based on transformations.

5. Meta classifier

Meta classifiers operate on output of other learners and hence called as meta learners. Meta classifier includes large number of classifiers. The most important meta classifiers are Bagging, AdaBoostM1, LogitBoost, MultiClass Classifier, CVParameterSelection , Filtered Classifier. In our dataset we have used Filtered Classifier which runs on filtered data.

6. Decision Trees

Decision Trees specify the sequence of decision that need to be made along with the resulting recommendation. A Divide and Conquer approach to the problem of learning from a set of independent instances leads naturally to a style of representation called a decision tree[1].There are different methods for decision tree such as ADTree, BFTree, J48, J48graft, DecisionStump etc. For our data set we have used J48. Based on the highest value of the Information Gain and Entropy, it creates a tree of attributes which depicts the arrangement of attribute in tree structure. Improved version of C4.5 is J48.[7]

IV. RESULTS AND DISCUSSION

We have used Eclipse and java language for implementation. Initially through proposed permission extraction app, all permissions are extracted. Further based on extracted permissions real dataset of android permissions have used with weka tool and classification algorithms are applied. Based on true positive and false negative performance measures harmful and normal apps are categorized. Hence privacy of user's sensitive data will be preserved using proposed approach.

Fig. 3. List of applications using implemented PPM app.

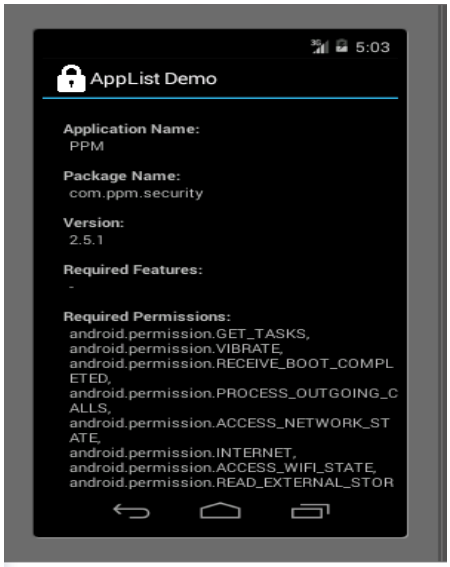

Fig. 4 List of Permissions of PPM Application .

Fig. 3 shows the overall applications list installed on your device using PPM (Privacy Permission Management)app, which we have implemented using java. Further in fig. 4. List of all the permissions particular application using is displayed. From various studies we understood that internet, call log access, account management, camera access these are few dangerous permissions which are harmful for users.

Table (a) gives brief idea about classification results of six different classifiers on android permission app dataset using weka tool and classification method of weka tool. It clearly shows that among six classifiers of weka tool Naïve Bayse and K-Star classifiers gives better performance to classify the harmful and normal applications.

Algorithms	Correctly classified Instances(%)	Incorrectly classified Instances(%)	Time taken to build model
Navie Bayse	100	0	0
Logistic	87.5	12.5	0.11
K-Star	100	0	0
Filtered Classifier	87.5	12.5	0.03
PART	87.5	12.5	0.01
J48	87.5	12.5	0

a. Result of classification algorithms

Six classification algorithms performance on android permission app dataset is shown in terms of correctly classified, incorrectly classified instances and time taken to build model is shown in terms of graphical representation below. Among the six classifiers Naïve bayes and K-star algorithms performance is accurate for classification of harmful and normal apps.

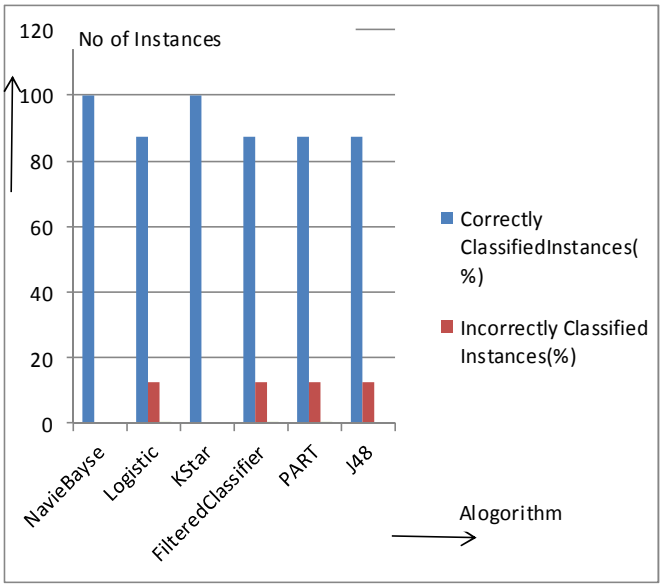

Fig. 6 Classification Algorithms graphical representation

V. CONCLUSION

This paper proposed a new approach for handling privacy permission management to android applications. The proposed system, Android Application Analyzer, allows users to identify harmful applications installed in their phone and also provides a provision to remove them. The proposed system is using a classification technique which will be helpful for user's sensitive data preservation.

A dataset is prepared consisting of applications with their permissions and categorized as harmful or normal after study of the permissions. Later this dataset is used to detect harmfulness of an application using various classification algorithms. The result showed the best classifier algorithm is Naïve Bayes for android permission app which giving 100 percent accuracy.

REFERENCES

[1] Veelasha Moonsamy, Jia Rong, Shaowu Liu, "Mining permission patterns for contrasting clean and malicious android applications", www.elsevier.com/locate/fgcs,**2014**.

[2] Brett Ferris, Jay Stahle, and Ibrahim Baggili, "Quantifying the Danger of Mobile Banking Applications on the Android Platform", 9th ANNUAL SYMPOSIUM ON INFORMATION ASSURANCE (ASIA'14), JUNE **3-4**, **2014**.

[3] Dimitris Geneiatakis ,Igor Nai Fovino , Ioannis Kounelis,Paquale Stirparo , "A Permission verification approach for android mobile applications", www.sciencedirect.com,**2015**.

[4] Christoph Stach and Bernhard Mitschang ,"Design and Implementation of the Privacy Management Platform" **2014** IEEE **15**th International Conference on Mobile Data Management

[5] Mohd Fauzi bin Othman,Thomas Moh Shan Yau,"Comparison of Different Classification Techniques Using WEKA for Breast Cancer".Control and Instrumentation Department, Faculty of Electrical Engineering, Universiti Teknologi Malaysia, Skudai, Malaysia.

[6] Felt, A. P., Greenwood, K., & Wagner, D. (**2011**, June). "The effectiveness of application permissions". In Proceedings of the 2nd USENIX conference on Web application development (pp. **7-7**).

[7] Supriya S. Shinde, Prof. Rahul Patil," Improving spam mail filtering using classification algorithms with discretization Filter" International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS), September-November, **2014**, pp. **82-87.**

[8] http://www.makeuseof.com/tag/the-seven-deadly-android-permissions-how-to-avoid-the-sin-of-slothful-preparedness/

[9] http://developer.android.com

[10] Ryan Farmer:" A Brief Guide to Android Security"(**2012**)

AUTHORS PROFILE

Supriya S. Shinde is pursuing M.E. in Computer Engineering from Pimpri Chinchwad College of Engineering. She has completed B.E. in Information Technology from Pune University . Her area of interest is Information Security, Mobile Computing.

Prof. S. S. Sambare is a senior faculty at Pimpri Chinchwad College of Engineering. He has completed M.E. in Computer Engineering and B.E. in Computer Science. He has teaching experience of 22+ years. His research area of interest is Computer Networks, Mobile Communication.