Parshvanath Charitable Trust's
A. P. SHAH INSTITUTE OF TECHNOLOGY
(Approved by AICTE New Delhi & Govt. of Maharashtra, Affiliated to University of Mumbai)
(Religious Jain Minority)

Android Malware Detection Using Machine learning

Group Members

Rishab Agrawal 17204006
Sonam Chavan 16104067
Vishal Shah 17204003

Project Guide & Co-guide
Prof. Ganesh Gurshete
Prof. Nahid Shaikh

Contents

- Abstract
- Introduction
- Objectives
- Problem Definition
- Existing System
- Proposed System
- Survey
- Conclusion And future Scope
- References

Abstract

Android OS experiences a blazing popularity since the last few years. This predominant platform has established itself not only in the mobile world but also in the Internet of Things (IoT) devices. This popularity, however, comes at the expense of security, as it has become a tempting target of malicious apps. Hence, there is an increasing need for sophisticated, automatic, and portable malware detection solutions.

Introduction

- Malware or Malicious Software is defined as software designed to distort and interrupt the mobile or computer applications, collect important information and hence perform malicious operations.
- These malicious operations include gaining access over private information, covertly steal this valuable information over the system, display undesirable advertisement, and spy on the activities of the users.

Objectives

- To analyze the malware from the apk files and from the applications.
- To provide security to the android user from the various malwares by analyzing the permissions given to that particular application
- to analyze the android application comments by semantic analyzing technique
- to give interactive user interface to the user to detect the malicious percentage of the application.

Literature Review

Paper title:-Android mobile security by detecting and classification of malware based on permissions using machine learning algorithms

Authors:-Varma, P. Ravi Kiran, Kotari Prudvi Raj, and KV Subba Raju

Publication:-2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC). IEEE, 2017.

Findings:-They have collected different apps from google play store and the collect the standard malware dataset then they extracted manifest.xml file then they identified the permissions given to each app and convert it to arff file

Disadvantages:-It is time taking as it is extracting manifest file and also it doesn’t have GUI

Paper title:-Android Malware Detection Using Machine Learning on Image Patterns

Authors:-Darus, Fauzi Mohd, Salleh Noor Azurati Ahmad, and Aswami Fadillah Mohd Ariffin.

Publication:- 2018 Cyber Resilience Conference (CRC). IEEE, 2018

Findings:-GIST descripter is used to extract feature from the images and classification is done using 3 different machine learning descripter (KNN) k nearest neighbor, Random Forest(RF) and decision tree

Disadvantages:-Some malware sample could not be generated into images because the APK files are either corrupted or they did not have classes.dex file

Problem Definition

- Sometimes it has been impossible for the user to identify the malware in his own system.Malware enter the system while user give permissions to application.User don’t even get to know that when the malware is entered in a system.Therefore, it also can makes the damage or loss of data from our android devices.

Existing System

In the existing system, the application permissions are extracted to detect the malware and executed through the command prompt. A proper GUI was not provided to execute the tasks . All the commands were run through the command prompt. It was difficult for the non-technical user to use the system. And also Semantic analysis was not implemented.

Proposed System

- In the proposed system, we are doing the permission-based analysis and also the semantic analysis. The permission-based analysis is been done on the web-based UI while the existing systems were just doing it all on the local machine in the command prompt.
- In our system, we have implemented an admin panel as well as a user panel. In the admin panel admin have the access to upload the apk files and its details along with its categorization and also the admin can upload the comment that can be used for semantic analysis.

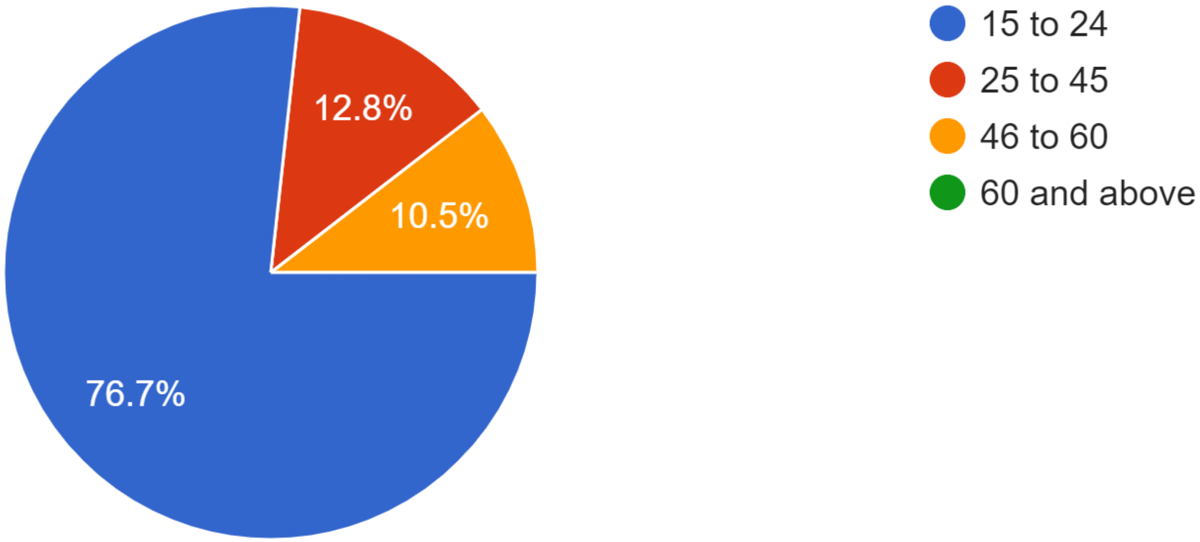
Technology stack

- Operating System: Windows10/9/8 /Ubuntu
- Database: MySql
- Database GUI: Sqlquerybrowser
- IDE: java,html,jsp
- Software: eclipse,android Sdk,web browser
- Ram :minimum 2gb

Survey

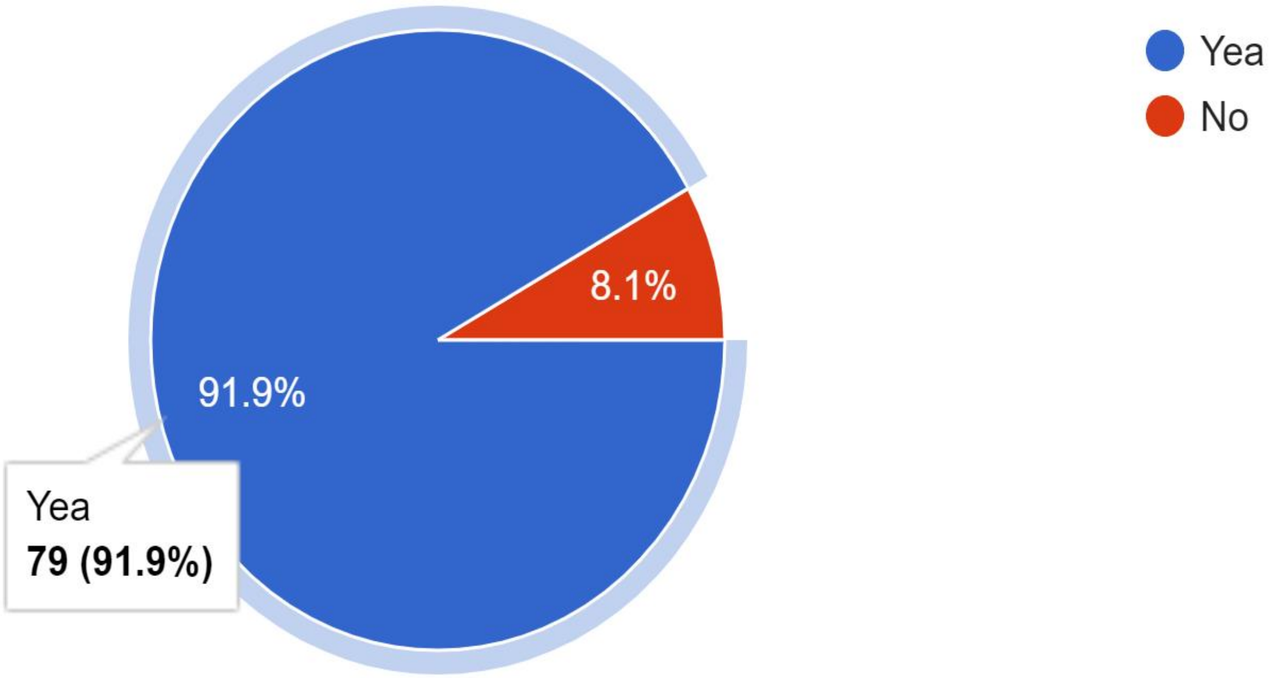
Age groups

86 responses



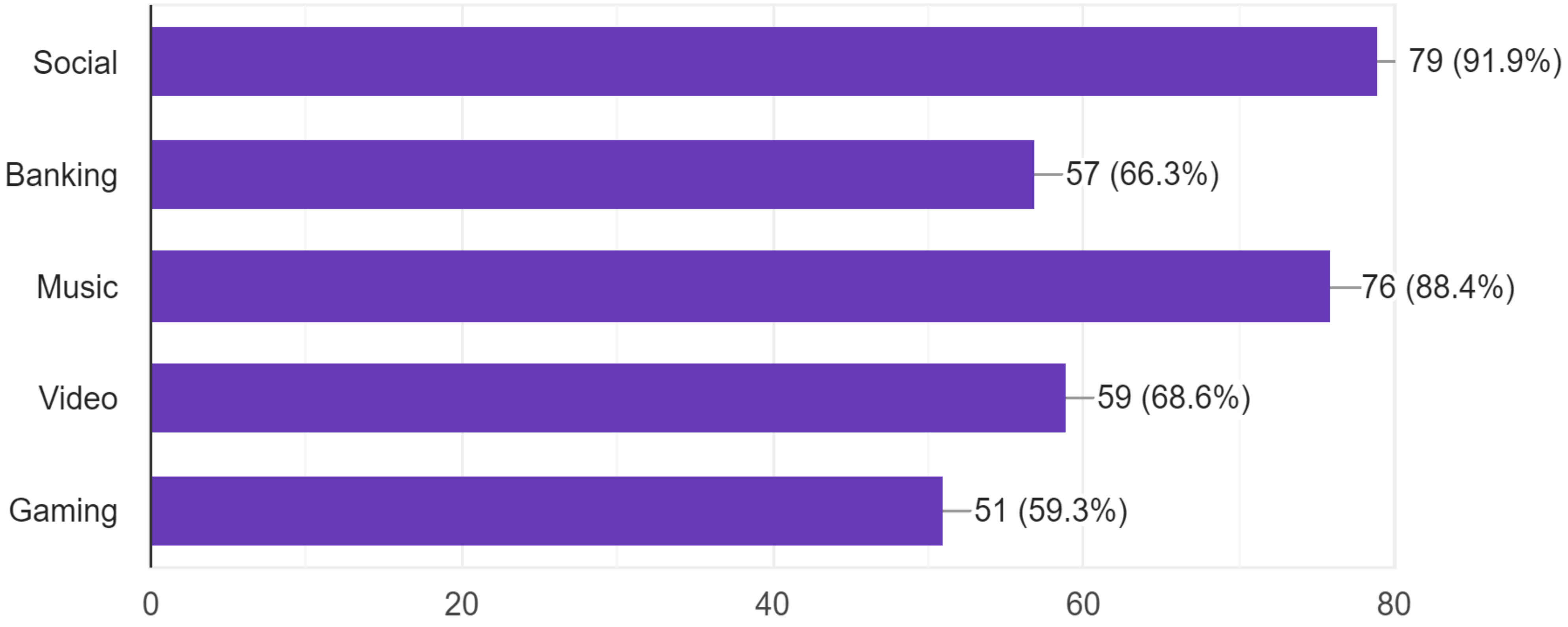
Are you an android user

86 responses



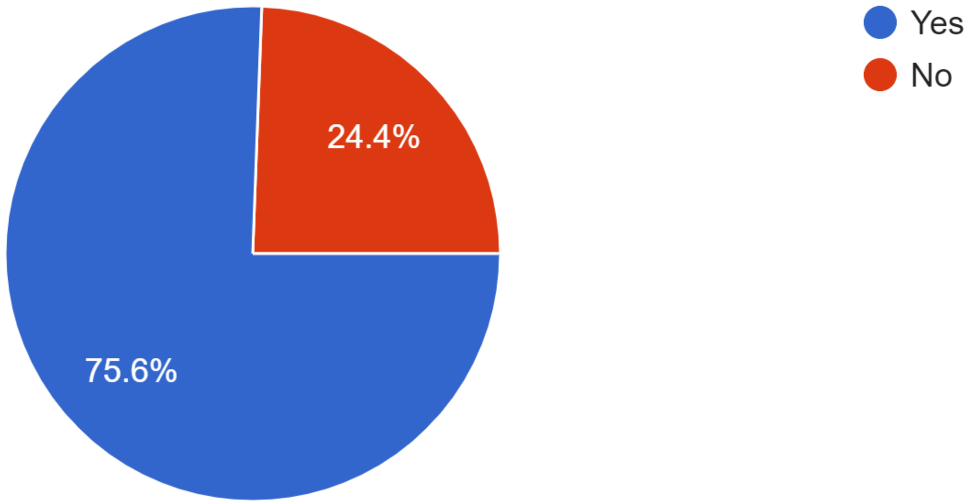
What are the types of application which are there on your android phone

86 responses



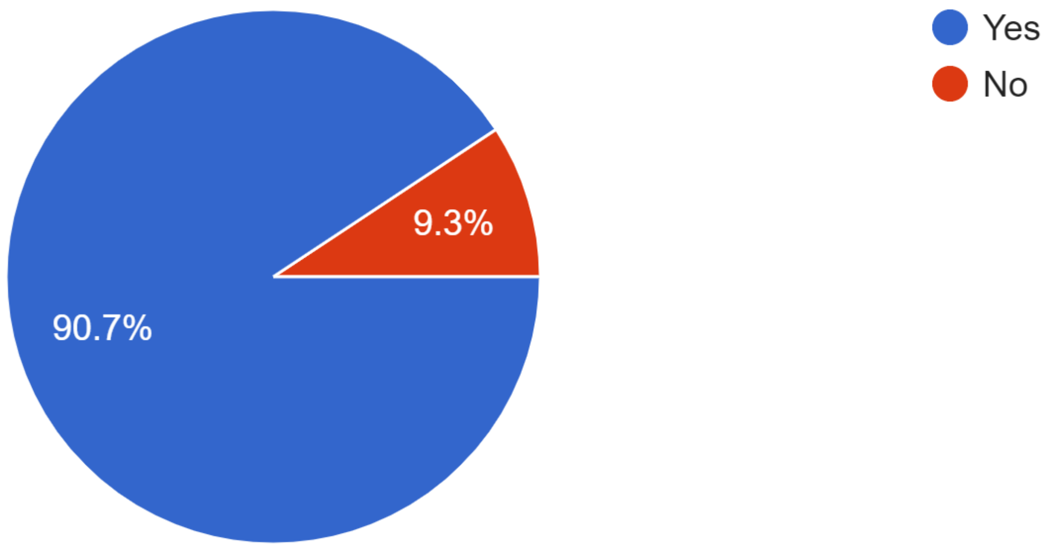
While installing any application, have you ever clicked on "Accept" button without actually reading the permissions ?

86 responses



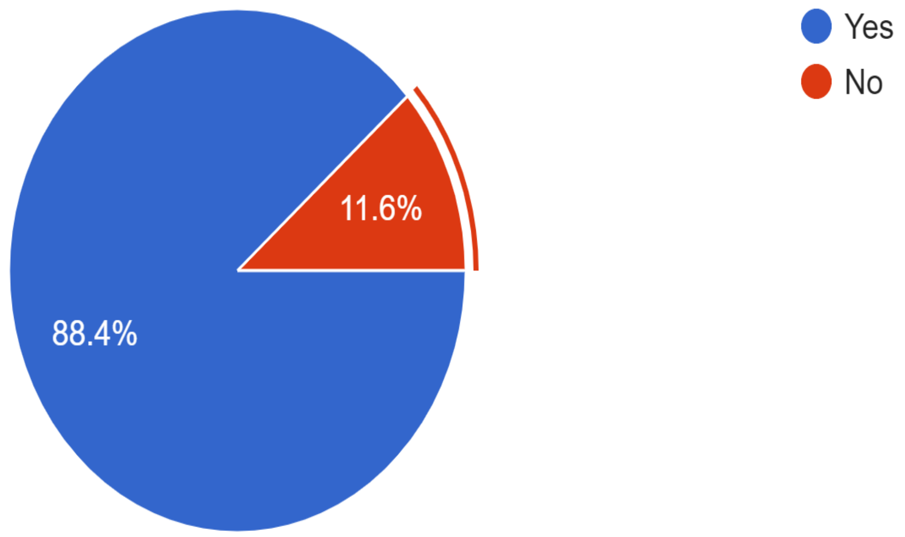
Do you get unnecessary pop-ups for permissions while using certain application?

86 responses



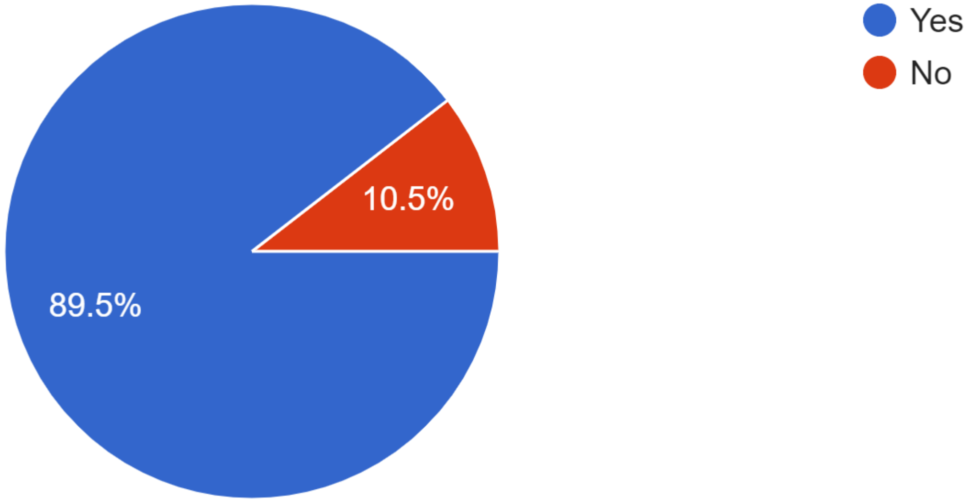
Have you ever faced situation where a particular application may not require certain permissions but still it asks ?

86 responses

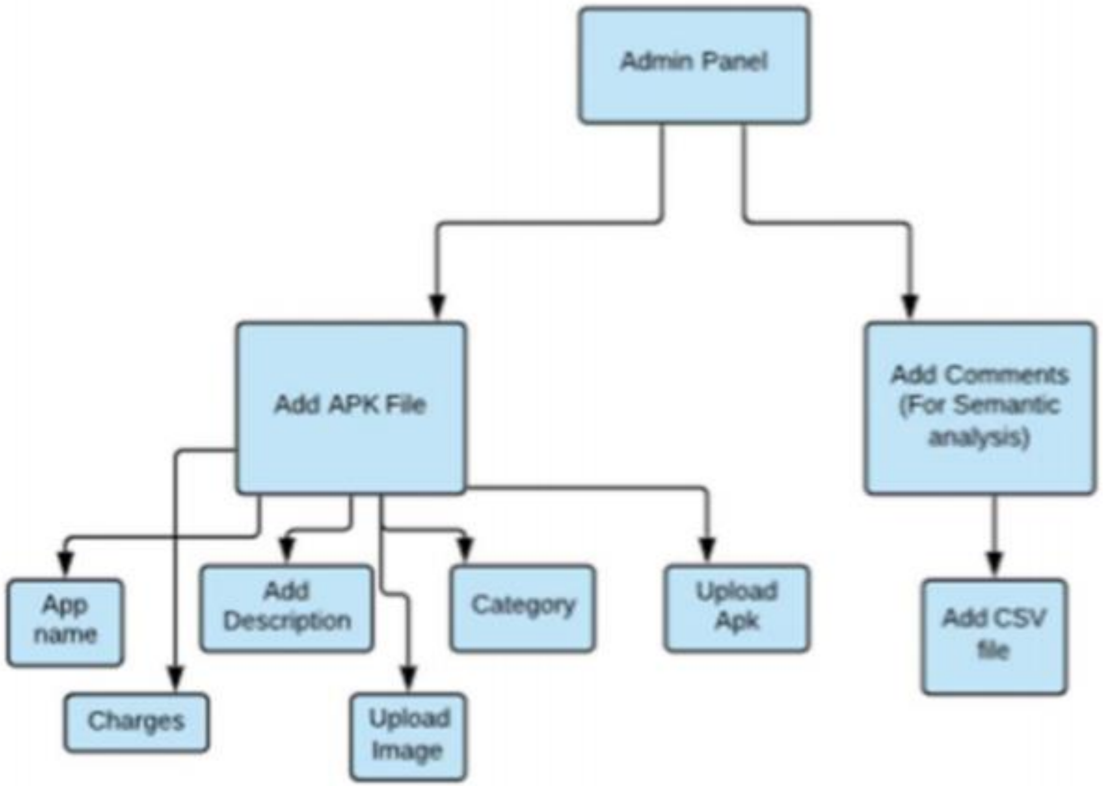


Will it be helpful for you if you get a analysis report for a particular application ,i.e. how malicious that application is on the basis of its permission access from the user.

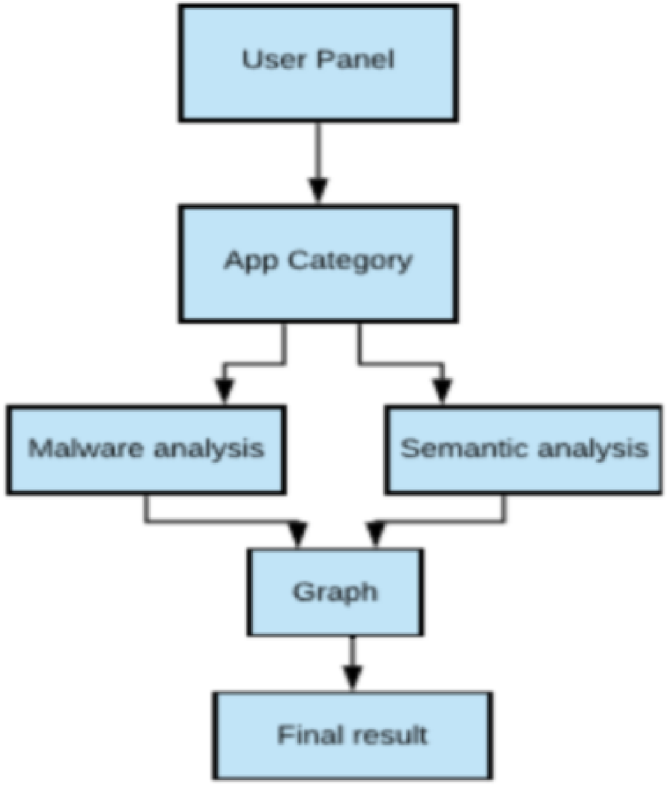
86 responses



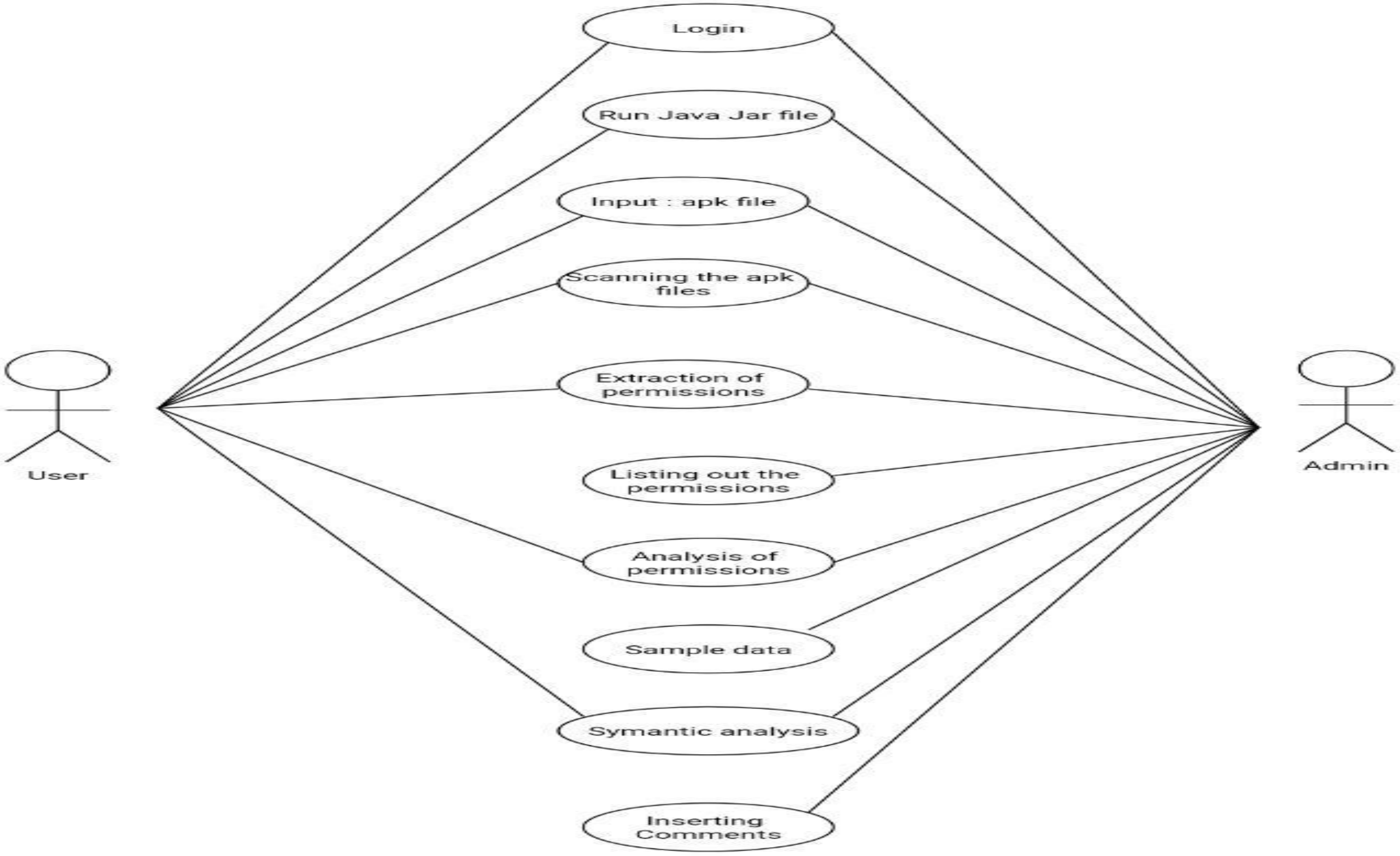
Admin Panel Flowchart



User Panel Flowchart



Usecase Diagram



Module1
Admin Module

- In admin module admin can upload the apk
- Admin can upload the apk on the basis of their category
- As soon as the apk is add the permission is extracted from that apk
- Admin can also upload the comments of that apk

Module 2
user Module

- In user modul user can select the category of the apk

- And then user can select the apk from that category

- User can able to view the malicious percentage of that apk

- User can also view the semantic analysis of that apk with the help of graph

Conclusion and Future Scope

In our work, we propose a system for permission analysis and semantic analysis. Our system is also used to detect malware permissions based on an application by comparing it with a dataset. This proposed system can be applied in the fields of the security system and also for the n users like a malware detection software. However, there are limitations in our system. The permissions which we are defining are as per our but it can differ from users to users. The permissions which the user likes that it is not a malware-based can be malware for any other user. Future works will contain the improvement of that.

References

- Varma, P. Ravi Kiran, Kotari Prudvi Raj, and KV Subba Raju. "Android mobile security by detecting and classification of malware based on permissions using machine learning algorithms." 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC). IEEE, 2017.

- Darus, Fauzi Mohd, Salleh Noor Azurati Ahmad, and Aswami Fadillah Mohd Ariffin. "Android Malware Detection Using Machine Learning on Image Patterns." 2018 Cyber Resilience Conference (CRC). IEEE, 2018.

- Chang, Wei-Ling, Hung-Min Sun, and Wei Wu. "An Android Behavior-Based Malware Detection Method using Machine Learning." 2016 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC). IEEE, 2016.

THANK YOU!!