IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 11, Issue 5, May 2022

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.118

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 5, May 2022||

| DOI:10.15680/IJIRSET.2022.1105065 |

Implementation towards Malware Detection on Android Smartphones

Kokane Sakshi Balasaheb, Khule Vaishnavi Dhananjay, Katore Aishwarya Vilas,

Thorat Rutuja Rajendra

U.G.Students, Department of Information Technology, Amrutvahini College of Engineering, Sangamner, Maharastra, India

ABSTRACT: With Modern era of mobile applications, thousands and millions of apps are available for each and every application. These apps are freely available on popular app market such as play store. For a common person it becomes difficult to judge a fraud app in these many available. Fraudulent behaviors in Google Play and malware detection is need for this. how to effectively detect the new malwares and malicious software variants has been a difficult problem. In view of the traditional feature extraction method based on binary program, this system presents a method for fea-ture extraction of JAVA source code. The method uses the Keywords Correlation Distance to compute the correlation between key codes such as API calls, Android permissions, the common parameters, and the common key words in Android mal-ware source code. Then SVM is applied to make the system gain to accommodate the function of the new malicious software sample, so as to detect new malicious software and existing malwares. This method combines the characteristics of the malicious software categories and operating environment to record the behaviour of the malicious software.

KEYWORDS: Text detection, Inpainting, Morphological operations, Connected component labelling.

I. INTRODUCTION

Android malwares have increased significantly in recent years. Smartphone is performing a more and more important role in daily life. There is no doubt that Android has become the most popular platform for smart phone today. This trend has attracted attention of attackers, more and more malicious applications emerged in the official and alternative Android marketplaces. Malware is an abbreviation for two words malicious and software. Actually, it is software that included in the computer system for malicious purposes, without any knowledge from the computer owner. It may be used to collect important information, or gain access to computer systems. The seriousness of malicious software ranges from hurt the users with annoying Ads to steal important data. With the advent of the Internet era, the smart phones in the world are also getting more and more popular, especially the smart phone with Android operating system with its excellent performance.

Android malwares have increased significantly in recent years. It has been high-lighted that among all mobile malware, the share of Android based malware is higher than 46 percent and still growing rapidly Given the rampant growth of Android mal-ware, there is a pressing need to effectively mitigate or defend against them.

To develop a system which effectively mitigate malware detection focus on identifying the features of malicious apps by using machine learning techniques to recognize and model the malicious patterns of static features and dynamic behaviours of malware.

Paper is organized as follows. Section II describes about the related work done earlier for the system to be developed. Section IIIpresentsmethod used and algorithms used for the detection.Section IV presents experimental results showing results of images tested. Finally, Section V presents conclusion.

II. RELATED WORK

Examining Features for Android Malware Detection [1]Author:M. Leeds, M. Keffeler,T.Atkison Mobile malware is a constant threat for Android users.As these devices become increasingly important in our daily lives, it is of the utmost importance to ensure their safety and security.Android Malware Detection and Protection: A Survey[2] Author: Saba

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 5, May 2022||

| DOI:10.15680/IJIRSET.2022.1105065 |

Arshad, Abid Khan, Munam Ali Shah, Mansoor Ahmed. A detailed performance evaluation of these antimalware techniques is also provided and the benefits and limitations of these antimalware are deduced comprehensively. An Intelligent Methodology for Malware Detection in Android Smart-phones Based Static Analysis[3] Author: Ahmed H.Mostafa, Marwa M. A.Elfattah and Aliaa A. A. Youssif It takes into account various features based on permissions declared in android-Manifest.xml file and methods and APIs used in the applications.Authors extracted the features from 650 application divided into 325 for malware representing 89 malware families and 325 benign applications. Smartphone Applications, Malware and Data Theft [4]Author:Lynn M. Batten,Veelasha Moonsamy and Moutaz Alazab Authors introduced a new Application Programming Interface (API) as well as two additional permissions and applied a method known as privilege separation, which extracts the advertising component from the main functionality component of the Application. Detection, Classification and Characterization of Android Malware Using API Data Dependency[5] Author: Yongfeng Li, Tong Shen, Xin Sun, Xuerui Pan, and Bing Mao Authors proposed DroidADDMiner,an efficient and precise system to detect, classify and characterize Android malware DroidADDMiner is a machine learning based system that extracts features based on data dependency between sensitive APIs. It extracts API data dependence paths embedded in app to construct feature vectors for machine learning.

III. METHODOLOGY

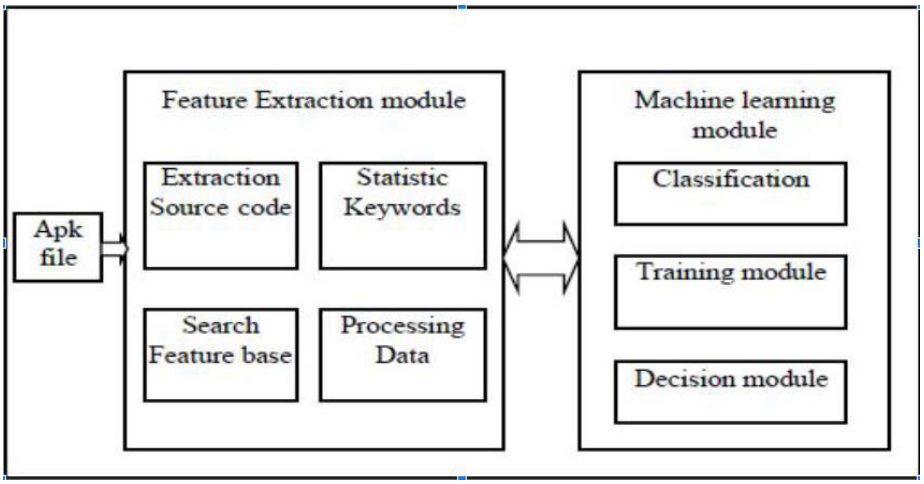
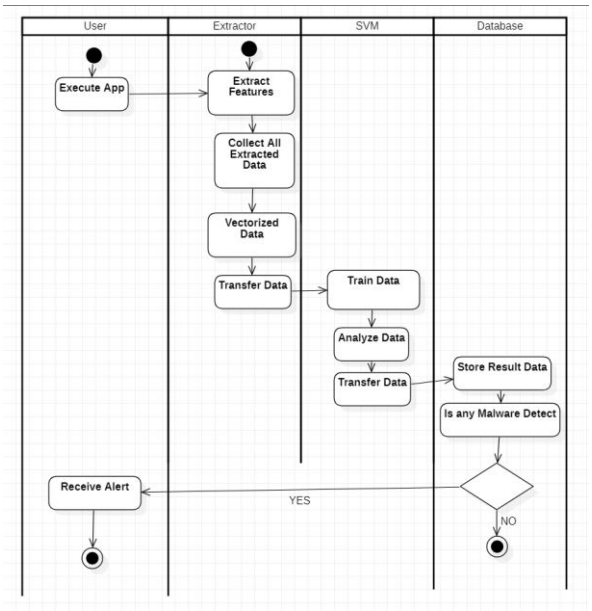


Fig. 1.System Architecture



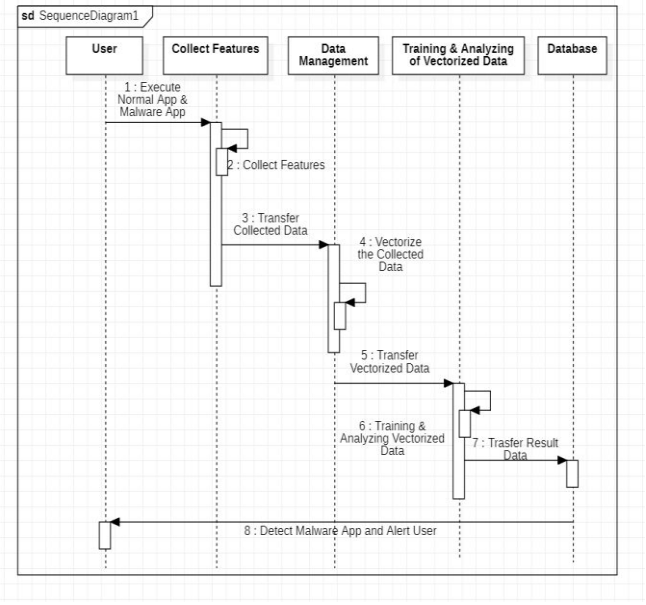


Fig 2. . Activity Diagram Fig3. . Sequence Diagram

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 5, May 2022||

| DOI:10.15680/IJIRSET.2022.1105065 |

MODULES:

1. Feature Extraction:
   The feature extraction module is responsible for the feature extraction

   (a) Decompiling: In this module we unzip Android application package(APK)to get the Mani-fest.xml file in the root directory then we use the opensource software dex2jarand jadnt158 to decompile the classes.dex in thedirectory.
   (b) Selection of Keywords : We select five representative keywords set according to the observation of malwares

      i. Android Permission
      ii. Activity Action Intent Parameter
      iii. Broadcast Intent Action Constant
      iv. The commonly Package Name
      v. API Call

   (c) Statistic keywords : In this module we record the frequency and locationof every keyword in class of APK and in the configuration file, to storagethe information using matrix then use Keywords Correlation Distancealgorithm calculated the distance be-tween the two keywords.
2. Machine Learning
   Machine learning module is responsible for classification and decisionmaking.
   (a) Classification : We present a classification method based on SVM(SupportVector Machine).SVM is a supervised learning model with associatedlearning algorithms that analyze data used for classification and regression analysis
   (b) Training module : We use LIBSVM is a library for Support Vector Machines to train. The steps of training are shown as follows:
      (a) Prepare training samples and testing samples.
      (b) Build java project, import LibSVM jars.
      (c) Put the training samples and testing samples under the project directory,also you can build a directory by yourself.
3. Decision
   This module we classify the keyword sets as seven types:
   (a) NETWORK
   (b) PHONESTATE
   (c) SYSTEMINFO
   (d) GPSLOCATION
   (e) WRITESTORAGE
   (f) BULETOOTN
   (g) SMS

ALGORITHM

• Input: D data set, on-demand features, aggregation-based features,
• Output: Classification of Application
1. for each application App id in D do
2. Get on-demand features and stored on vector x for App id
3. x.add (Get Features(app id));
4. end for
5. for each application in x vector do
6. Fetch first feature and stored in b, and other features in w.
7. hw,b (x) = g (z) here z=(wTx + b)
8. if(z ≥ 0)
9. assign g(z)= 1;
10. else g(z) = -1;
11. end if
12. end for

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 5, May 2022||

| DOI:10.15680/IJIRSET.2022.1105065 |

IV. EXPERIMENTAL RESULTS

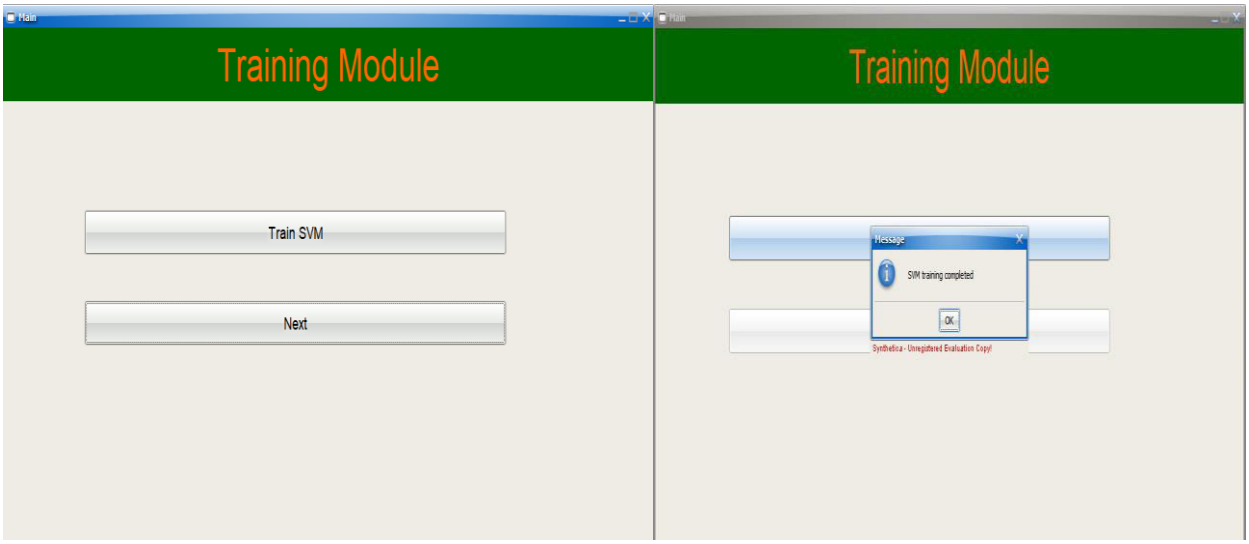


Fig 4 : Training Module

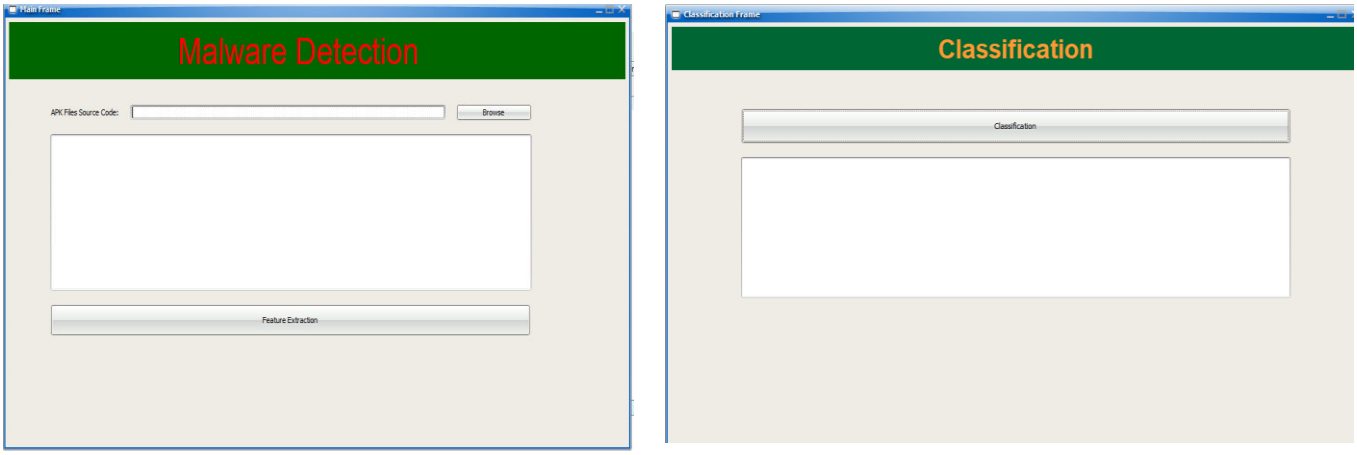


Fig 5 : Classification Module

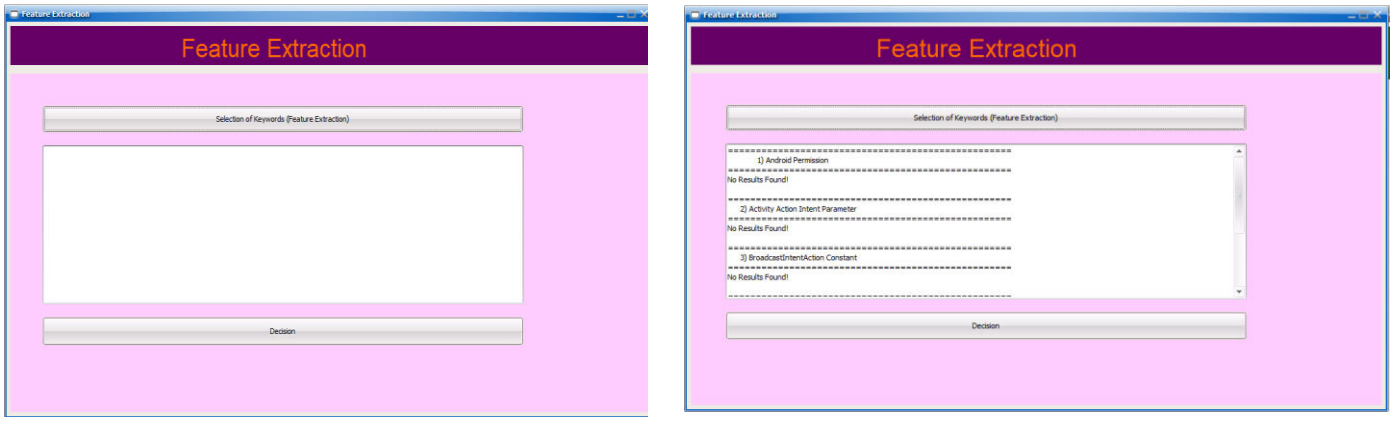
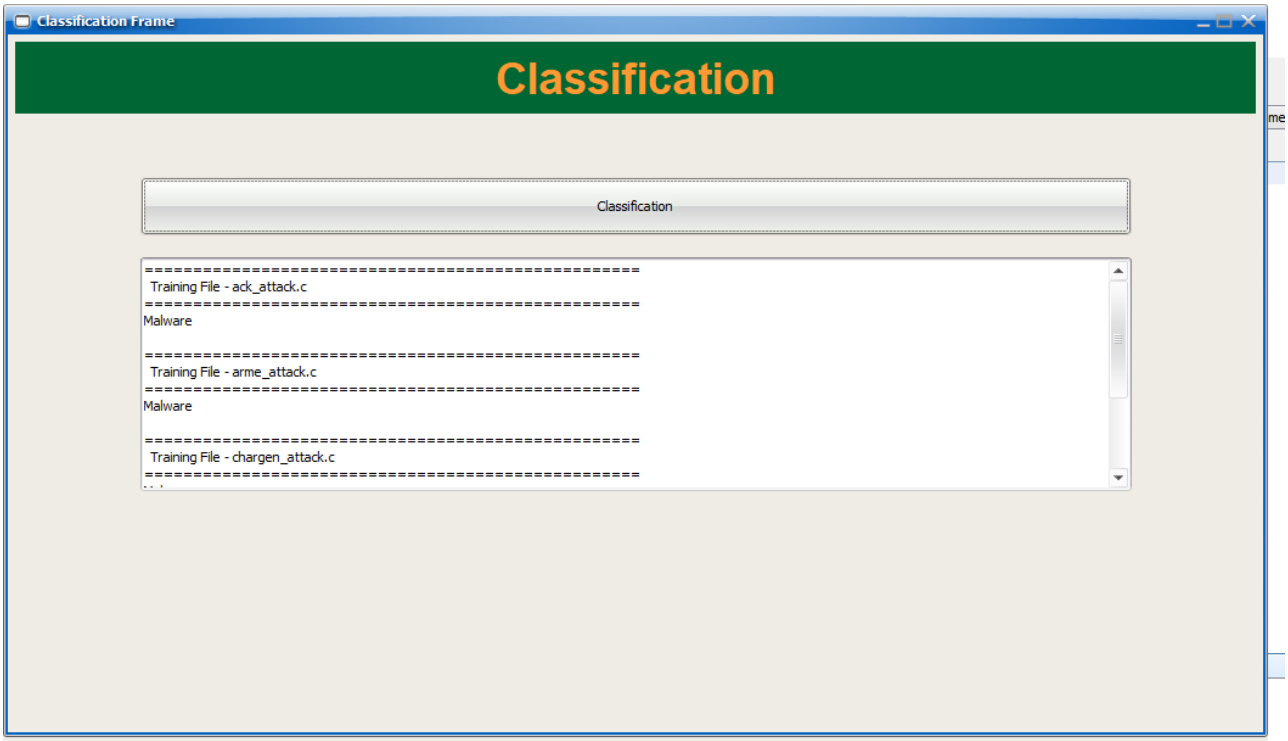


Fig 6 : Feature Extraction

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 5, May 2022||

| DOI:10.15680/IJIRSET.2022.1105065 |



V. CONCLUSION

In this system we proposed an extraction method of Android malware detection based on KCD. Then we combine the feature into keywords feature vector. Finally, learn and decision by SVM for detecting new malware and malicious variant. This system is different from conventional methods. Experiments show the method is effective and efficient in detecting malwares on Android platforms.

REFERENCES

[1] M. Leeds, M. Keffeler, T. Atkison, " Examining Features for Android Malware Detection " Computer Science Department, University of Alabama, Tuscaloosa, AL, USA Intel Conf. Security and Management SAM'17 ISBN: 1-60132-467- 7, 2017.

[2] Saba Arshad, Abid Khan, Munam Ali Shah, Mansoor Ahmed, " Android Malware Detection & Protection: A Survey" (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, No. 2, 2016.

[3] Ahmed H. Mostafa, Marwa M. A. Elfat tah and Aliaa A. A. Youssif, " An Intelligent Methodology for Malware Detection in Android Smartphones Based Static Analysis ", International Journal of Communication 2016

[4] Lynn M. Batten, Veelasha Moonsamy and Moutaz Alazab, " Smartphone Applications,Malware and Data Theft " Springer Science Business Media Singapore 2016.

[5] Yongfeng Li(B), Tong Shen, Xin Sun, Xuerui Pan, and Bing Mao, "Detection, Classification and Characterization of Android Malware Using API Data Dependency ", Institute for Computer SciencesSocial Informatics and Telecommunications Engineering 2015.

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.118

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

Scan to save the contact details