AUTOMATED ANDROID MALWARE DETECTION USING OPTIMAL ENSEMBLE LEARNING APPROACH FOR CYBER SECURITY

A. Durga Devi [1], K.Siva Sai Krishna[2],

[1]**Assistant professor of PG Department,** Dantuluri Narayana Raju College**, Bhimavaram, Andhrapradesh**

Email:- adurgadevi760@gmail.com

[2]**PG Student of MCA, Dantuluri** Narayana Raju College**, Bhimavaram, Andhrapradesh**

Email:- k.sivasainaidu143@gmail.com

ABSTRACT

Android malware growth has been increasing dramatically along with increasing the diversity and complicity of their developing techniques. Machine learning techniques are the current methods to model patterns of static features and dynamic behaviors of Android malware. Whereas the accuracy rates of the machine learning classifiers increase with increasing the quality of the features, we relate between the apps' features and the features that are needed to deliver its category's functionality. Differently, our classification approach defines legitimate static features for benign apps under a specific category as opposite to identifying malicious patterns.We utilize the features of the topratedapps in a specific category to train a malware detection classifier for that given category. Android apps stores organize apps into different categories, for instance,26 categories on Google Play Store. Each category has its distinct functionalities which means the apps under a specific category are similar in their static and dynamic features. Ingeneral, benign apps under a certain category tend to share a common set of features. On the contrary, malicious apps tend to request abnormal features, less or more than what is common for the category that they belong to.This study proposes category-based machine learning classifiers to enhance the performance of classification models at detecting malicious apps under a certain category. The intensive machine learning experiments proved that category-based classifiers report a remarkable higher average performance compared to non-category based.

1 INTRODUCTION

According to International Data Corporation (IDC), Android OS is the most popular smart phone platform with 82.2% of the market share of smart phones, while 13.9% for iOS apple in the second quarter of 2015 [3].Statistically speaking, it is also the first targeted platform by malware authors seeking to take the control over millions of Android smart phones over the world. Due to the popularity of Android's smart phones, its apps' security is a serious issue concerning 80% of smart phone susers.

Android is an open source development environment that offers a rich SDK that enables developers to deploy their own apps and distribute them through Android apps centers. Android's popularity is a result of being an open source, third-party distribution centers, a rich

SDK, and the popularity of Java as a programming language. Importantly, due to this open environment, malware authors can develop malicious apps that abuse the features that the platform offers or pack a legitimate app with a piece of malicious code; besides, exploiting vulnerabilities in the platform, hardware, or other installed apps to lunch malicious behaviors.

Literature Survey

The initial studies on smart phone malware were chiefly targeted on understanding the threats behaviors of rising malware. There has been vital work on the matter of police work malware on mobile devices. Many approaches monitor the facility usage of applications and report abnormal consumption. Others monitor system calls and arrange to discover uncommon system call patterns. Different approaches additional ancient comparison with acknowledged malware or different heuristics. Signatures primarily based ways, introduced within the mid-90s area unit ordinarily employed in malware detection. The main weakness of this kind of approach is its weakness in police work metamorphic and unseen malware. Rather than victimization predefined signatures for malwaredetection, data processing and machine learning techniques give a good thanks to dynamically extract malware patterns. For smart phone-based mobile computing platforms, recent years have witnessed an increasing range of additional sophisticated malware attacks like repackaging.

3 IMPLEMENTATION STUDY

EXISTING SYSTEM:

One existing work has used data processing and options generated from windows workable API calls. They achieved sensible leads to a really giant scale dataset with concerning 35,000 transportable workable files. Another activity foot printing methodology additionally provides a dynamic approach to discover self-propagating malware. All these existing ways have basically advanced the mechanical man malware detection; however, the misuse detection isn't reconciling to the novel mechanical man malware and continually needs frequent change of the signatures.

Disadvantages:

- Misuse detection isn't reconciling
- Accuracy is less
- Mechanical man malware detection

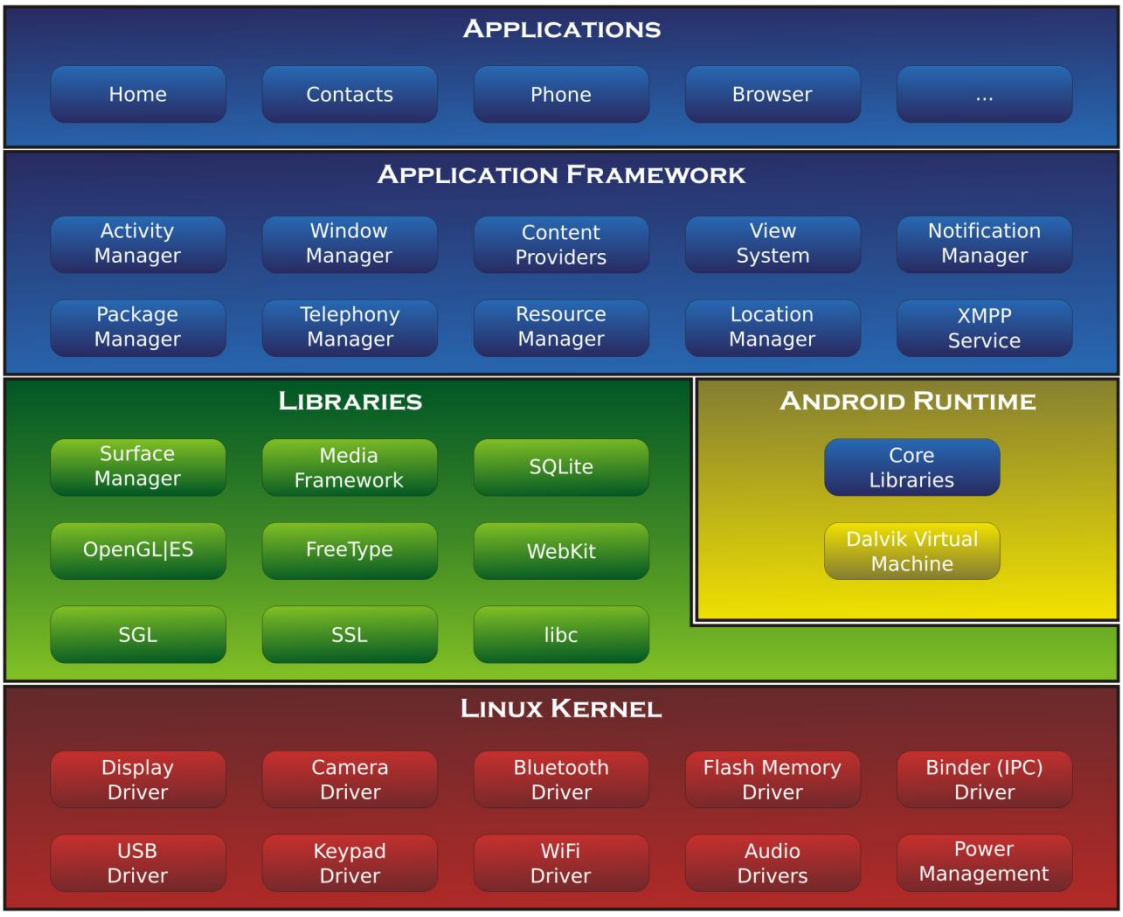
Proposed System & alogirtham

In the proposed system we implement a better feature extraction techniques and then we apply the genetic algorithm forfeature extraction and then we use two machine learning model called as SVM

4.1 Advantages:

1. Easy to identify and block malware
2. Accuracy is more
3. Dynamic feature extraction using genetic algorithm

Fig:3.1 System Architecture



IMPLEMENTATION

1Modules:-

(Data Collection and Feature Filtering)

Collect all applications in separate folders which contain benign as well as suspicious applications respectively.

Using “Glob” frame work in python create an array offiles is for further processing.

Analyze each application in the array using “pyaxmlparser”and“androguard”framework.

Extract the following things in the analysis phase:

a. Permissions

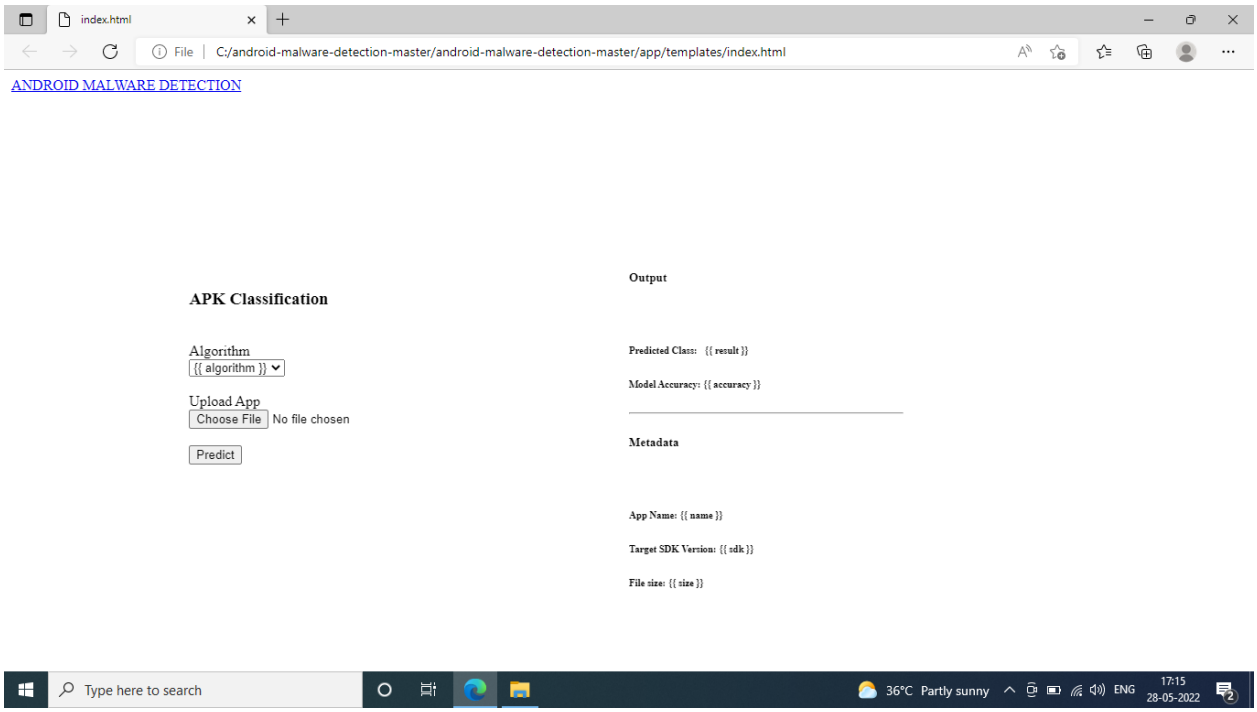
b. Activities

c. Intents

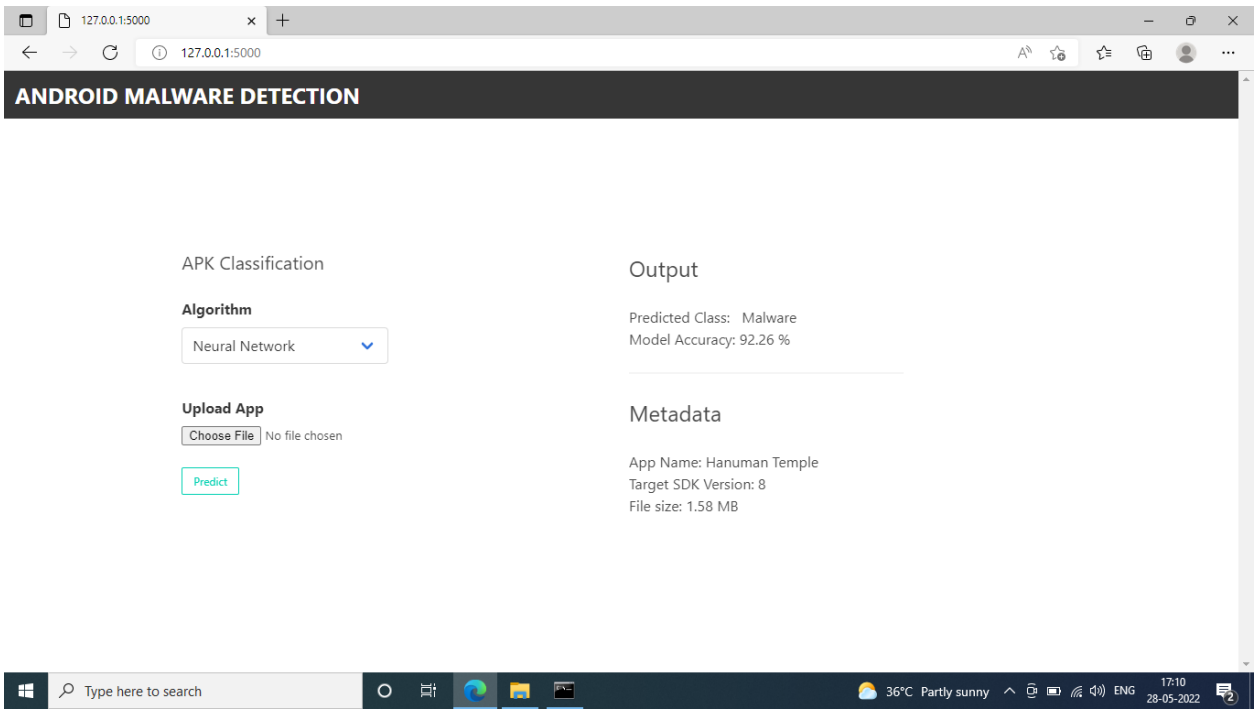
d. APIcalls

5 RESULTS AND DISCUSSION

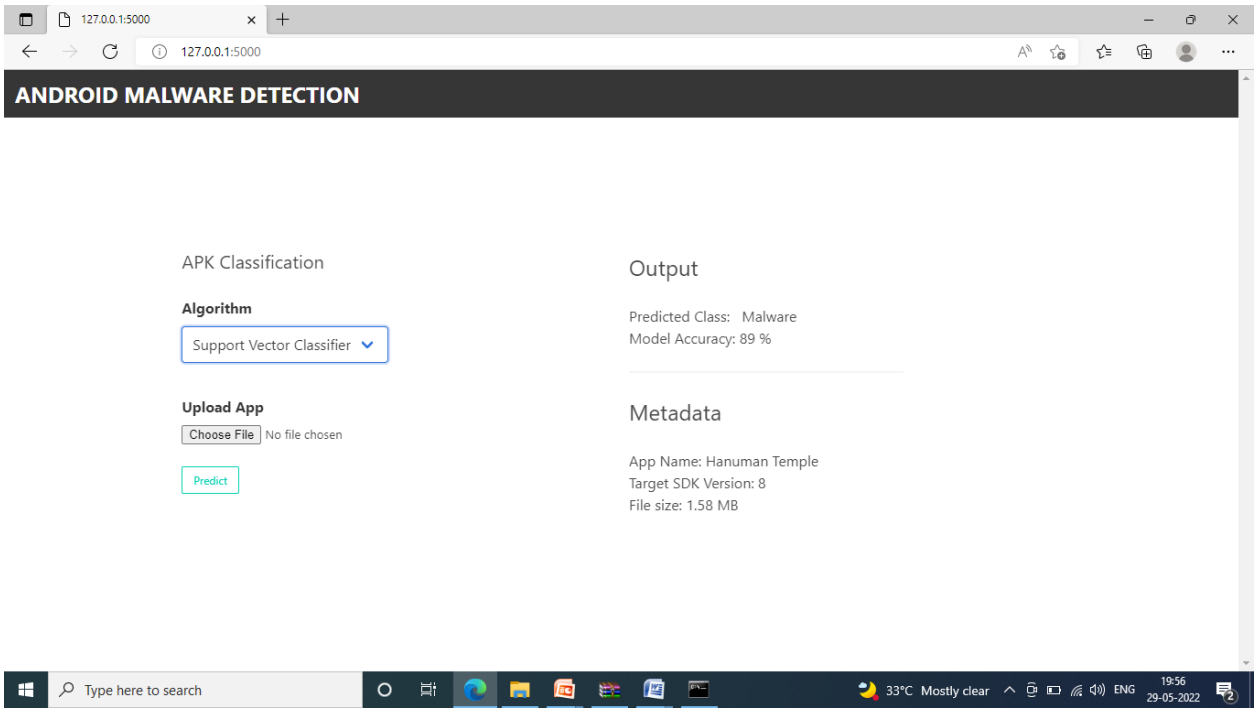
Screen shots



5.1 HOME PAGE



5.2 SELECT AN ALGORITHM



5.3 UPLOAD A FILE

6. CONCLUSION AND FUTURE WORK

CONCLUSION

In our study, we propose category-based machine learning classifiers to improve the performance of the classification models. In static analysis of Android malware, machine learning algorithms have been used to train classifiers with features of malicious apps tobuild models that capable of detecting malicious patterns. Differently, our classification approach defines legitimate static features for benign apps as opposite to identifying malicious patterns.We utilize the features of the toprated apps in a specific category to define a profile of the common sets of features for that category. In other words, to detect whether or not the app posses the characteristics of benign, we relate between the app's features and the features that are needed to deliver the category's functionality that the app belongs to. Android stores organize apps into different categories; 26 categories on the Google Play Store, for example.

7. REFRENCES

[1] Androguardusage.**https://code.google.com/p/androguard/wiki/Usage**. Accessed April 24,2015.

[2] Android-statistics&facts—statistics**http://www.statista.com/topics/876/android/.**AccessedApril19,2015.

[3] Android and ios continue to dominate the worldwide smartphone market with android shipments just shy of 800 million in 2013, according to idc.**http://www.idc.com/getdoc.jsp?containerId=prUS24676414.**AccessedApril19,2015.

[4]Application fundamentals android developers. **http://developer.android.com/guide/components/fundamentals.html**. Accessed April19,2015.

[5]Aredownload/installation.**https://redmine.honeynet.org/projects/are/wiki.**AccessedApril28,2015.

[6] Dynamic analysis tools for android fail to detect malware with heuristic evasion techniques.**http://thehackernews.com/2014/05/dynamic-analysis-tools-for-android-fail.html**.AccessedApril19,2015.

[7] "global smart phones ales exceed 1.2 bunits in 2014. "gfk-wesee the big picture.**http://www.gfk.com/news-and-events/press-room/press-releases/pages/global-smartphone-sales-exceed-1-2b-units-in-2014.aspx.**AccessedApril19,2015.

[8] Google:Wehave1 billionmonthlyactive android

users**http://www.businessinsider.com/google-we-have-1-billion-monthly-active-android-users-2014-6.**AccessedApril19,2015.

[9] Report: 97-forbes. **http://www.forbes.com/sites/gordonkelly/2014/03/24/report-97-of-mobile-malware-is-on-android-this-is-the-easy-way-you-stay-safe**/AccessedApril19,2015.

[10] Smartphoneosmarketshare,q42014.**http://www.idc.com/prodserv/smartphone-os-market-share.jsp.**AccessedApril19,2015.

[11] Arp,D.,Spreitzenbarth,M.,Hübner,M.,Gascon,H.,Rieck,K.,andSiemens,C. (2014).Drebin:Effective and explainable detection of android malware in yourpocket.InProc.ofNDSS.