Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 4, April : 2023

ANDROID MALWARE DETECTION USING MACHINE LEARNING

Mr B S Venkata Reddy Associate Professor, Department of Computer Science Engineering, Raghu Engineering College, Visakhapatnam, Andhra Pradesh.

venkatareddy.bs@raghuenggcollege.in

S Praveen Kumar[2], R Jyosna, L Upendra Students, Department of Computer Science Engineering, Raghu Engineering College, Visakhapatnam, Andhra Pradesh.

19981a05f7@raghuenggcollege.in, 20985a0517@raghuenggcollege.in, *17981a0596@raghuenggcollege.in*

Abstract: The prevalence of Android malware has been sharply rising, along with the variety and cooperation of their development methods. Currently, to model the patterns of static characteristics and dynamic behaviours of Android malware by using machine learning techniques. Instead of discovering dangerous patterns, our categorization technique establishes valid static properties for benign apps inside a certain category. We use the characteristics of the best-rated applications in that category to build a malware detection classifier. Android app shops categorize apps into many groups, For instance. Because every category has its own unique characteristics, the applications that fall under that category are comparable in terms of both dynamic and static features. Normally, good apps in a certain category tend to have similar characteristics. On the other hand, harmful applications frequently require unusual functionality, either less or more than is typical for the category to which they belong. The aim of this work is to improve the efficiency of classification model at identifying dangerous applications inside a given category by introducing category-based machine learning classifiers. The extensive machine learning tests showed that category-based classifiers perform noticeably better on average than non-category-based classifiers.

Keywords: MLP Classifier, SVM, Android malware

I. INTRODUCTION:

Malicious software created to infect Android-powered smartphones, pills, and other cellular gadgets is referred to as Android malware. International Data Corporation (IDC) reports that Android OS has 82.2% of the smartphone market share, compared to iOS Apple's 13.9% share in the second quarter of 2015 [3]. Malware has the potential to follow user activities, scouse borrows confidential information, display intrusive adverts, or even take whole manage of a tool.

Attackers can spread malicious apps to the Android market thank to the vulnerabilities [6]. The quantity of malware threats focused on Android smartphones is rising at the side of their reputation. consequently, it is essential to find and take away such spyware in an effort to defend Android customers' privacy and safety.

The number of published Android apps has increased significantly as a result of the openness of the Android ecosystem. In 2014, there were around 1,500,000 applications

available for download in Google Play shops, according to data [2]. One billion active users worldwide are concerned about the security of Android apps, according to statistics [7]. Android malware detection involves locating and examining questionable packages or styles of pastime on an Android device. several methods, along with system gaining knowledge of-based totally detection, behavior-based totally detection, and signature-primarily based detection, can be used to try this. The technique of signature-primarily based detection is comparing a report's or software's homes to a database of recognized malware signatures. analysing an app's behaviour as a way to find any suspicious or malicious activities is known as behavior-based totally detection. gadget studying-based totally detection identifies sparkling and undiscovered threats through using algorithms which have been skilled on massive datasets of malware.

II. OBJECTIVES

The primary objective of Android malware detection is to discover and mitigate malware threats that could compromise the security and privateness of Android users. below are some specific targets of Android malware detection:

- discover recognized malware: discover and block malware this is already recognized and has a regarded signature within the malware database.
- discover new malware: stumble on and block newly developed malware that has no longer been diagnosed earlier than by using the usage of behavior-based totally or machine studying-based totally detection strategies.
- Mitigate malware effects: locate and prevent malware from stealing sensitive information, tracking consumer pastime, showing undesirable commercials, or taking full control of a device.
- beautify Android safety: improve the general security of Android gadgets by means of detecting and preventing malware threats that might compromise the safety of the working device and different apps.

III. LITERATURE REVIEW:

In Literature [9], the article was published in 2018. In order to build a classification model by using different machine learning techniques, they have suggested an Android malware detection system that makes advantage of aspects like permissions, APIs, and the existence of different important apps. This system can automatically differentiate between legitimate and malicious Android apps (malware).

In literature [6], the article was published in the year 2021. Due to the widespread use of Android smartphones nowadays, there are now millions of free applications available. Users can engage in a variety of activities using some of these programmes. The most popular cell phones are increasingly being targeted by dangerous malicious software because they store critical employee data. The technique, relevant datasets, and evaluation metrics of the various methodologies and mechanisms currently in use to identify malware are all examined in this study. It concentrates on the concepts and dangers associated with malware.

Liu et al. (2020) [1] evaluate in element different strategies and studies repute from unique views like pattern acquisition, facts pre-

processing, characteristic choice, gadget learning algorithm, and performance evaluation.

In Literature [2], the article discusses about the vulnerability of Android smartphones to malware and the efforts made by researchers to identify permissions that could lead to malware detection. The importance of identifying conspicuous permissions that can lead to malware detection.

Jiang et al. (2020) [5] have a look at the permissions regularly utilized by malicious applications and become aware of permissions they name risky satisfactory-grained permissions, which higher differentiate benign and malicious packages.

IV. ANDROID MALWARE TYPES

Rootkits:

A form of malware that conceals its presence on the target device and grants the attacker privileged access. Without the user's knowledge, it can also carry out a number of malicious actions and install additional malware.

Trojan:

pretends to be a helpful programme in order to hide its dangerous nature. Although it gives the user useful features, it secretly performs harmful actions on their computer's history without their knowledge.

trojan horse:

without needing to be released by the owner of a device, copies and spreads throughout a network node.

Spyware:

Sends a person's data, including contacts, location, messages, and other personal records, to a distant server, and uses the programme and gathers data.

Ransomware:

The user's data is encrypted, and a fee is then demanded to receive the decryption key. The user's data may also be threatened with publication or destruction if payment is not received.

V. EXISTING SYSTEM

Data processing and working choices created by Windows have been employed in one previous work. API requests. They were able to provide useful results that led to a pretty large dataset with about 35,000 portable usable files. Another activity foot printing methodology offers a dynamic way to find malware that spreads on its own. All of these methods now in use have essentially increased the detection of mechanical man malware; nevertheless, abuse detection is incompatible with newly discovered mechanical man malware and requires periodic signature changes. The analytical gap is present here. They used decision trees and naïve bayes classifiers, which have low accuracy, in the current system.

VI. PROPOSED SYSTEM

Inside the proposed system we implement a

better characteristic extraction techniques and then we observe the genetic set of rules for characteristic extraction and then we use system gaining knowledge of version referred to as SVM and multi perceptron classifier for

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 4, April : 2023

classification of android malware detection which gives the higher accuracy ratio whilst evaluate to existing machine.

VII. ALGORITHMS

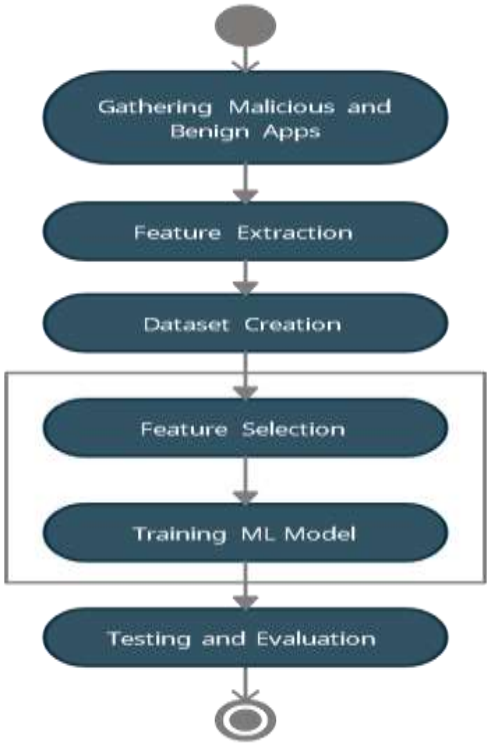
- SVM (Support Vector Machine):

A supervised machine learning technique called SVM is utilised for regression and classification analysis. Finding a hyperplane that best divides data points into discrete classes according to their attributes is how the algorithm operates. SVM seeks to optimise the distance between each class's closest data points and the hyperplane.

- MLP (Multi Perceptron Classifier):

A MLP classifier is a type of neural network used for classification tasks. It consists of multiple layers of interconnected nodes that apply nonlinear transformations to their inputs before passing them on to the next layer. The output layer produces the final classification decision based on the activations of the neurons in the previous layers. MLP classifiers are trained using backpropagation to adjust the weights of the connections between neurons.

FLOW CHART



- first of all, we acquire a number of malicious and benign android packages with the aid of retrieving their APKs on-line.
- next, we put into effect feature extraction by means of enumerating the API calls, permissions and activity of the APKs to get an honest concept of the behavior of the specific apps.
- Then we create a dataset primarily based on the extracted features by using compiling them into CSV documents for destiny use and reference.
- After that we pick unique capabilities which appear to be an anomaly or a red flag, accumulate and store them in new CSV documents and educate our system getting to know version according to them.
- in the end, our remaining phase is to test our model with the statistics and examine our findings in step with the consequences.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 4, April : 2023

VIII. RESULTS

Fig 1: Output1

Fig 2: Output2

IX. CONCLUSION

In our study, we suggest a category-based system that learns classifiers to enhance the functionality of class models. System studying algorithms were utilised to train classifiers using harmful app functions during static and dynamic analysis of malicious applications in order to create models that could recognise malicious patterns. In other words, our categorization system creates valid static functions for benign apps rather than detecting dangerous styles. We build a profile of the common functional units of a class using the characteristics of the top-rated applications in that class. In other words, we connect between the app's features and the functions required to provide the functionality of the class to which the app belongs in order to determine whether or not the app exhibits the qualities of benignity.

X. REFERENCES

[1] Liu et al Nature 2020, Ji dong yu, Yoko katayama, Thomas Warshcied

https://www.researchgate.net/publication/350278658_Liu_et_al_Nature_2020

[2] Arora, A., Peddoju, S.K., Conti, M. Permpair Accessed April 19, 2015.

[3] Research_gate:

https://www.researchgate.net/publication/328495819_Android_Malware

[4] http://developer.android.com/. Accessed April 19, 2015.

[5] Xujaing, baolei mao, xingly hyung: https://www.researchgate.net/figure/The-top-20-used-permissions-of...

[6] Alzubaidi, IEEE Access **9** (2021):

https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=%20&arnumber=9585476

[7] GOOGLE: We Have 1 Billion Monthly Active Android Users | Business Insider India Accessed April 19, 2015.

[8] Forbes-Report 97 http://www.forbes.com/sites/gordonkelly/2014/03/24/

[9] J. D. "RanDroid, Koli: Android malware detection using random machine learning classifiers." 2018 (ICSESP). IEEE,2018.