*Machine Learning Classifier for Mobile Malware Detection*

Dissertation Chapter # 5: Discussion & Conclusion

Student Name: Harjinder

# Chapter # 5 Discussion & Conclusion

Mobile android phone various (Sangal, A.L., 2021) malware detection has been proceed from the machine learning technique, due to increasing popularity of android phone, various developer develop malware on daily basis to destroy the android operating system and applications. This research proposed framework detect mobile malware from the android phone and prevent them and the proposed framework supporting dynamic analysis by performing machine learning strategies, the mobile system able to detect real time android application by scanning various mobile phone applications with the help of android malware detection system of advance machine learning technique, by gaining the feature selection approach it has been addressed to solves the various feature selection problem by training and testing the dataset of android application. Additionally the following feature used to detect the android applications by performing the 500, 000 android apps still the android applications is not secured there is need to improve them. User is protected to installed third party software from other sources, so there is need to facilitate them additionally by supporting various android applications scanning. Empirical results revealed presented various machine learning technique which process parallel machine learning and deep learning algorithm performed the furthest principal gathering technique Y-MLP and nonlinear ensembles decision tree approach by selecting feature selection approach and detect the highest detection rate of 98% to detect and prevent malware from android phone in real world apps. (Mesleh, A., Awajan, A., 2020) intelligent mobile malware detection using permission request and API calls. Malware is serious threats that posing to threat the android phone user badly, two types of android malware attacked on android operating system fraudulent mobile app and injected malicious mobile app. Android mobile phones uses various amount of three dimensional grouping targeting strategies to group the dataset. The valuable mobile API calls to maximize the likelihood to maximize the likelihood to identifying the mobile malware application, since the android malicious applications invoke on different API calls which mobile malware often used to scan the risky apps. Android app using the ambiguous group and risky group to scan the android malware app with various framework scanning feature. (Canfora, G. Cimitile, A., 2016) mobile malware detection in the real world to detect and prevent the real world mobile application by installing the user in real instance various machine learning algorithm has been predicted by various researcher in the past, several feature has been tested and predicted and prevented by the machine learning algorithm. Various researcher addressed mobile malware technique and addressed the solution in the literature, the studies addressed the different mobile malware detection technique, and several problem has been classified mobile malware detection problems by addressing the solution towards the leading goal of machine learning detection classification, K nearest neighbors does not provides the great accuracy due to the hyperplanes was not reflected the target variable on the prediction discovery of mobile malware security permission apps. Various researcher published empirical studies aimed at accessing the quality of set of feature, different researcher addressed proposed the quality behavior of machine learning algorithm and the discriminant a trusted applications by malicious one extracting opcode-based feature since the android application variant open source ended the application is open and accessible across the leading network correspondence. The mobile security feature applications has been classified on different mobile security feature detection, it can be used & classified on starting point to define the classification approach to detect the real time mobile application which has been classified and addressed the solution. the experiment result present the accuracy prediction rate which has been classified and prevented on support vector machine classifier and decision tree with random forest classifier method. (Sahs, J. Khan, L., 2012) machine learning based approach has been deployed previously on the classification of mobile malware detection. The recent emergence of mobile platform which capable of executing the increasing complex solution of software solutions has been suggested and organized the sensitive applications such as banking applications associated with the malware targeted application at mobile device. The problem has been detected and classified due to limited resource available and limited privileges granted to the user the studies preset the unique idea of machine learning detection discovery which has been analyzed in the past since the application contains adware advertisement and backdoor advertisement which cause problematic situation on the android device since the various third party mobile applications was not reflected due to instability of various mobile applications the machine learning based approach has been used in the past which proposed on unique property of required meta data and scan the real application of android phone since the mobile applications was not secured due to the instability of other applications. The problem has been detected and identified on various mobile permission dataset which does not reflect the applications due to the limited resources available on privileges granted to the user the information has been passed out and prevented which based on the application scanning the target application which was attached on each application by using the Meta data application. Since the android phone application connected with backend Google API based on Meta data information searching information. The research has been presented the various state of the art machine learning method based system which discovered the android app permission access, the previous android release contains various issues and problem which extract the various malware information contains the different attribute of dataset. The application has been monitored and prevented on the discovery of android malware detection & prevention since the machine learning based system for the detection of malware detection discovery which based on malware on android device. The proposed system based on extract the number of feature by training and testing the dataset, because the training and testing feature extract the target applications on the basis of different set of attributes which related to the attribute classification techniques has been monitored and classified on advance machine learning classification techniques. Since the offline classification method proposed on support vector classification technique which was classified on number of feature selection based approach. (Lin, H. Liu, Y., 2020) experiencing of machine learning onto the market scale mobile malware detection. Since the application is stable due to the latest release of android operating system which contains the different feature classification method. Mobile eco system has become the natural classification method proposed on machine learning classification malware detection prevention channel has been actually classified & prevented on different mobile attributes classification. It is suggested that the Google updates on update of security feature has been proposed on different classification technique of mobile classification method which has been proposed on the basis of mobile android machine learning based method proposed on classification technique.

### Research Finding

This research finding presented and suggested the android application contains various malware and contain with virus information. Since the research finding present the android permission application based dataset which has been analyzed and predicted on research method. This research fill the gap in between the mobile releases and latest version of android operating system, because stable release of android operating system has been analyzed on different parameter of malware detection & prevention discovery. The bogus advertisements presented on insecure website which has been access by the android operating system and monitored on different parameter. Google platform is much secure and providing Google API layers functionality to the android user which extracted the useful information without any hurdles and malware. Various banking applications is secured and stable which proposed their own private network which classified and administered on different parameter of mobile malware detection and prevention based discovery. It is suggested and presented through the research finding the machine learning method has been used by the Google to protect the android operating system from the outside malware and third party illegal software discovery. The better understanding of machine learning discovery which proposed on various machine learning based method proposed & analyzed on different scales of machine learning algorithm discovery. Mobile malware detection has been classified & administered on different parameter of various mobile method technique since the modern and advance machine learning algorithm discovered the various features of malware detection & prevention.

## Research Outcome

Since the mobile T-market evaluated and discussed on different mobile communication channels (Vakalis, I., 2018) dynamic permission based android malware detection technique using machine learning method the android based application contains malware and different insecure advertisements which cause problematic situation the android phone not secured in previous mobile version because of low security feature and low API interface of over the android phone. Android application needs the number of sensitive permission during their installation and runtime. Various android running and execution application required user permission to execute and retrieve them on real time internet interface. The contribution of this research based on android permission dataset of APK file and other mobile android dataset which proposed the solution by scanning the different features and parameter of android phone and discovered and suggest the solution to protect the third party application from unknown user. This research evaluate the number of parameter of dataset by selecting the feature selection and selecting the parameter of training and testing the dataset to predict and validate the dataset the 123 dynamic permission based security feature solved the execution level of API layer functionality to predict and prevent the malware from the android phone. Since the machine learning classifier method predict on various algorithm based strategies such as naïve bays classifier and support vector machine classifier and decision tree classifier method proposed to predict the android permission dataset, since the model tuning and training to predict the Relu functionality of machine learning algorithm which founded on the parameter of classification techniques. The experiment result present that the malware classification prediction accuracy proposed on RF, J48 and SL are comparable the performance of marginal techniques has been actively analyzed based on the training the dataset feature. (Zhao, Y., Li, L., Wang. 2021) the impact of sample duplication in machine learning method discovery proposed on the parameter classification of android malware detection and removal method, android operating system is stable and accurate because of various operating system secured API layer functionality protect the mobile application from unknown access the duplication of attribute changing which needs to change the parameter of mobile and APK attribute, so there is need to fix the attribute parameter of APK which would be secured techniques to secure the app from the malware attack. The experiment result show the sample space of malware detection, the duplication of application installation with minor changing of attribute which cause problem on android phone due to non-secure installation featured on different classification techqnieu parameter which reflect the base of malware attack. The distribution of third party layer functionality which proposed on designing the app which are not reliable.

## About the APP on Google Play store

About this app present the application detail which is presented currently in Google play store this method is very useful to identify the app from malware and security prevention. Such as the detail of Netflix app presented in Google play store with great description “Netflix is the leading subscription service for watching TV episodes and movies on internet in real time” this elaboration is very useful before installing this app in android phone. Various android based LED TV does not detect malware due to poor quality of operating system interface and previous versions of android is part of android TV. Since the Google is providing the security to the android phone user which is remarkable discovery of the internet.

## Ratings & Reviews on Google Play store

Rating & reviews presented on Google play store which is very useful for the determination and prediction of android application. Review based on 3 star 2 star and 5 star this application rating is very helpful before installing the android app on the android phone. Since in windows operating system Avast, AVIRA, AVG is well recognized virus name it’s not antivirus. Microsoft updated the security features in new release operating system which was introduced in 2015 with the name of windows 10 operating system which contains built in anti-virus, so there is no need to install the third party anti-virus software, since the anti-virus software itself is virus.

## Editor Choice APP

Editor choice app presented on Google play store which is secured application suggested by the reliable authoritative members of developer which does not contain virus. Google suggested that the rotating selection of the best apps, which handpicked by the play store editor. Editor choice app functionality works on machine learning prediction based on user choice of interest application interest so the editor choice app automatically generate the suggestion list based on machine learning programming prediction which already secured from malware attack.

## Mobile Malware Discovery

Android phone was not performing well in the previous releases of android phone, due to insecure and instable android operating system since the upgradation appear in 2017 and 2018 year, Google planned to update the android phone security features followed by the third party API layers of Google service layer. Google in these days much secured operating system for the android family and so the question of malware is now out of question due to the reliability exists in 2021, this research finding and discovery present that the android phone is stable and reliable in year 2021 because of reliable applications installation parameter based on user permission choice. It is suggested that the Google built in machine learning feature are updated and processed on different parameter. Google operating system are updated and revised the security feature which are much reliable and needful. Android 11 version are more stable and reliable because of application permission installation performed on user permission if the user allow to add the new app based on the user selection and user choice it is recommended and otherwise the application is not add in android phone. Since the previous android version contains various malware attack attribute which was connected in real time web application portal and interact the virus to installed the software automatically in the android phone and some application in android phone are automatically remove after some period of time due to the malware attack happened in before 2017 these types of issues appear commonly in the android phone. Software are installed automatically and software are removed automatically in previous android releases now the issue has been resolved and updated, this research review the basic research gap from 2011 to 2017 in literature review section and after update of android operating system release which is considered much reliable operating system because 86% market share of android phone due to its popularity. Since the mobile malware attacked happened on adware based, backdoor and ransomeware attack happened on android phone but these issues resolved by using the machine learning algorithm discovery parameter detecting the malicious app and malicious malware from the android operating system.

# References

Mahindru, A. and Sangal, A.L., 2021. MLDroid—framework for Android malware detection using machine learning techniques. *Neural Computing and Applications*, *33*(10), pp.5183-5240.

Alazab, M., Alazab, M., Shalaginov, A., Mesleh, A. and Awajan, A., 2020. Intelligent mobile malware detection using permission requests and API calls. *Future Generation Computer Systems*, *107*, pp.509-521.

Mercaldo, F., Visaggio, C.A., Canfora, G. and Cimitile, A., 2016, May. Mobile malware detection in the real world. In *2016 IEEE/ACM 38th International Conference on Software Engineering Companion (ICSE-C)* (pp. 744-746). IEEE.

Sahs, J. and Khan, L., 2012, August. A machine learning approach to android malware detection. In *2012 European Intelligence and Security Informatics Conference* (pp. 141-147). IEEE.

Gong, L., Li, Z., Qian, F., Zhang, Z., Chen, Q.A., Qian, Z., Lin, H. and Liu, Y., 2020, April. Experiences of landing machine learning onto market-scale mobile malware detection. In *Proceedings of the Fifteenth European Conference on Computer Systems* (pp. 1-14).

Geneiatakis, D., Baldini, G., Fovino, I.N. and Vakalis, I., 2018, February. Towards a mobile malware detection framework with the support of machine learning. In *International ISCIS Security Workshop* (pp. 119-129). Springer, Cham.

Zhao, Y., Li, L., Wang, H., Cai, H., Bissyandé, T.F., Klein, J. and Grundy, J., 2021. On the impact of sample duplication in machine-learning-based android malware detection. *ACM Transactions on Software Engineering and Methodology (TOSEM)*, *30*(3), pp.1-38.