*Machine Learning Classifier for Mobile Malware Detection*

Dissertation Chapter # 2: Literature Review

Student Name: Harjinder

Table of Contents

[2. Literature Review 3](#_Toc95487326)

[2.1 Related Work 3](#_Toc95487327)

[1. Distance Measure in K nearest Neighbor 9](#_Toc95487328)

[2. Argumentative attacks on Mobile Malware Detection 10](#_Toc95487329)

[3. Machine learning algorithm 10](#_Toc95487330)

[4. Machine learning classification malware detection using Opcode 11](#_Toc95487331)

[*Understanding of Mobile Malware* 12](#_Toc95487332)

[Reverse Engineering techniques 13](#_Toc95487333)

[Security feature in Android 14](#_Toc95487334)

[How to Secure Android Device 14](#_Toc95487335)

[Summary of Literature Review 15](#_Toc95487336)

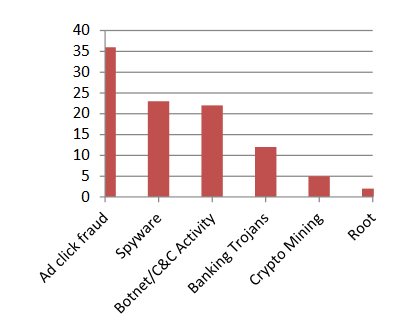
[References 16](#_Toc95487337)

# 2. Literature Review

Literature studies is part of previous research publications research finding which was formulated on mobile malware machine learning classification method. In literature the finding describes the methods and analysis including research aims & objectives. The problem statement is in view of android phone malware system to scan & predict the malware from the android device.

## 2.1 Related Work

Machine learning classifier for android malware detection (M. Z. Mas'ud, S. Abdollah 2014) primarily focused on mobile application which needs security & privacy to secure personal data from unknown hacking attack. With huge number of android user various mobile user used various application for different purposes, Through operator remain nowadays competent to consumes the use of mobile applications for different purpose such as web browsing, online banking, payment and order taking purposes and various businessmen used for meetings and financial tasks and social networking with MMS. Different credential and secured applications needs security and privacy concerned, similar security solutions exists which was provided by the Google operating system, hence there is need to develop the mobile malware detection tools which provides the security to android phone user. Mobile CPU is differ from desktop, it little bit better comparatively to perform the query on demand which enables the user to connect millions of applications in real time, the best machine learning classifier, the combination of feature selection classifier, in this research five machine learning classifier has been proposed prior to do the particular analysis, calculation expected on positive false rate and positive false negative rate to capture the accuracy (Wang, L. Yang, B., 2018) machine learning based malware detection using highly imbalanced network traffic, due to increasing number of android malicious app which brings the network traffic to imbalanced the situation to combine the network capture classification analysis and mobile malware classification so the technique is used to enables the user to scan the mobile phone to detect malware from the android operating system. However the support vector machine classifier enable the user to imbalanced the malware from device using the cost sensitive technique with C4.5 cost sensitive method. The classification algorithm degrades significantly including data gravitational based classified the simplex gravitational data imbalanced classification technique, the simplex gravitational data models classified the prototype system which provides user substantial autonomy (Choi, M.J., 2013) analysis of android malware detection performance using machine learning classification method, since the mobile device support various user applications , personal information & private message has been captured due to unstable version of android operating system in 2013, since the mobile contains confidential information including sensitive data such as bank account details, emails data and personal messages in the mobile inbox. Attacker extends the attacker range not only in the desktop computing also in mobile phone network, previous studies of android malware detection present that due to instable version of android operating system needs to improve internal security structure system on the entire android telephone network, so in previous version of android phone machine learning classifier has been deployed but the detection accuracy was very low, mobile malware detection system generated the android application app scanner to do the scanning system and perform various scanning task. Preceding educations present that the mobile android to perform the machine learning classification technique to detect the various malware through collecting analyzing event and system within the android device, the understanding of android architecture with malware characteristics generate resource consumptions overhead of android device including low ratio of malware detection (White, J., 2013) applying the machine learning technique with dynamic android detection at scale the sensitive nature of android phone needs more security & user preferences the increasing concerned of smart phone malware, machine learning classifier current method of detecting malicious applications over the smart phone device, this research present evaluation of number of machine learning classifier using dataset containing thousands of real time applications including offline and online applications, since the stream framework of developed large scale validation of mobile malware detection including machine learning classification technique (Vaglini, G., 2020) model checking and machine learning technique for humming bad malware detection and extenuation, since the android operating system created with various programing technique and tools, java programming used backend and front end to proceed the interface application environment of android phone ,this research discussing two machine learning classifier techniques hamming bad malware detection methods the aggressive behavior of android applications to detect various malicious applications (M. Al-Janabi, A. M. Altamimi 2020) comparative analysis of machine learning classifier to detect and remove the malware from the android operating system since the most harmful threats produced by the developer community to demolished the android operating system various cyber-attacks and security tools & techniques enable the users to gaining access to computer system, various malware comes with different version and functions depending on the goals of the developer. Since the virus and spyware bots and Ransomware was example of malware. Though persons labelled overhead originate themselves producing subjects through chance, though, they altogether part unique object hip shared, hurting the scheme. Machine learning classifier method utilize to delete the malware from the operating system, zero signature based detection method currently used to delete the malware hence the method cannot provides the accurate result on zero day attack including polymorphic attack, machine learning classification technique is most modern and advance method to predict and scan and delete the malware from the system. The purpose of this research is going to present the best feature extraction method and classification method to analysis the static and dynamic framework of feature extraction & feature selection technique, the accuracy of detection method to classify best accuracy method of detect malware system the J48 algorithm with hybrid analysis perform the 100% accuracy of malware detection and preventions system, the deep learning decision tree method including dynamic malware detection system perform the good accuracy of android malware detection, it was believe that the machine learning classifier technique perform the malware analysis machine learning classifier method. (Uppin, C., & George, G. 2019) analysis of android malware using data replication feature extracted by machine learning tools. The era of smart phone technology plays essential roles in the business communities and student community. In these days the use smart phone has been rapidly increasing due to emerging IT technology has been introduced various desktop applications available on demands on smart phone. Android is most preferred type of operating system storing critical information including emails records banking details transaction history and other personal picture and video. Since the android phone is increasing the consumer buying interest due in convenience, equability, equivalence and emerging IT apps. The vulnerability was main targeting attack over the android phone user malware attack capture the user sensitive information because the third party customization support including various identity theft links Denial of service attack, Ransomware attack was common malware attack over the android phone user. This research present the android malware known as MysteryBot identification system including static & dynamic analysis result. MysteryBot was banking Trojan attack which capture the sensitive banking details over the android application, so the upgradation of android release operating system to update the security features and update the banking applications, so the banking application is much secure now to capture the secret information, which provides the virtual private network to the mobile user within the application to secure the user information. (Narudin, F.A., Feizollah, A 2016) mobile devices increasing number of users experiences with the technology, android part of Google operating system which contains various flexibility and smart computing features by sending email, online payment, business meetings and other benefits over the internet, users relying on mobile applications devices by sending and receiving the confidential data, intelligent malware detection keeps modifying to detect and update the security features of the mobile phone, user activities and location sensing which enable the attacker and spammer to access the real time location and get the secret information by the user, so implementation of machine learning models which used to protect the malware attack and suspension attacks over the internet. (Lin, H, Liu, Y., 2020) this paper present the Google play store market data, while detecting the mobile malware attacks with android permission access, baseline dataset has been used to detect and predict the malware attacks over the android phone, feature selection algorithm does not classify the classification algorithm improvement results show the prediction accuracy of models by implementing the market meta data model with 86% accuracy by using KNN and SVM algorithm demonstrated in experiment results unit. (Firdaus, A., 2021) android mobile malware detection by using the fuzzy AHP, mobile phone contains various vulnerable attack which uses to prevent the risk based fuzzy analytical approach to evaluate the android application 10,000 samples has been taken drebin and Androzoo and classify the accuracy of machine learning algorithm by determining the android application risk level detection. (Mercaldo, F. Santone, A., 2021) deep learning models for android mobile malware detection and family identification method each day users stores overabundance of subtle material and preventing the everyday life, hackers may writes harmful codes of programming for android operating system which generates automatically malware script for stealing the sensitive information from mobile devices. The vulnerable attacked information has been planned to capture the essential mobile data which based on current malware signature based detection the research present the machine learning application that represent the explained deep learning based modeling features based on android malware detection and family detection system. family detection based on convolutional neural network which founded on image dataset and image is connected with email id’s that get the family user information in real time scanning and prediction algorithm of deep learning method. Additionally the research present the various prediction and analysis method of malware attack which present the proposed deep learning based strategies founded on 0.96 to 0.97 accuracy & validate the 8446 android samples dataset of six different malware families which interpreted the results. (Kambourakis, G., 2021) machine learning based method to predict and detect the malware attack, android operating system considering open source which designed by Google operating system constructed on Java programming. Literature present the solution of malware detection system created on machine learning and deep learning method. Various android users download untrusted and unreliable mobile application from Google Play store which might be consist of malware based pattern constructed on fake advertisements and spam texts which might be engaged the user to click on certain promotional fake links and redirect to the spam server and capture the sensitive information from the mobile gallery. Yet, research answers obviously designate that the mainstream of current everything apply dissimilar metrics and replicas then service varied datasets then organization topographies stopping after dissimilar examination methods, i.e., stationary, lively, or cross. Additionally the machine learning method predict the state of the art regularization method of mobile malware detection system which organized on various feature detection based system and yet to be designed on several deep learning random forest tree and decision tree method which separate the spam and ham data from the mobile devices. (Sangal, A.L., 2021) android malware detection system constructed on machine learning method, this research present the MLDroid web based framework which helps in detect the malware from the android phone, due to increasing number of android popularity, malware developer develops malware on daily basis to capture the sensitive information from the mobile devices. To detect the malware in real time by using the MLDroid app which is available at Google play store system it works on machine learning parameters to detect the spam app’s and spam and ham user data from the mobile device. The selected features proposed on machine learning method, designed on various pattern of deep learning decision tree nonlinear approach which formally detect the malware from the system about 98% accuracy. Beside this naïve bays classifier develop by various research to detect the malware from the android device with accuracy of 76%. Practical tests on dataset of Automaton malware folks (reaching since 2010 to 2018) settle the efficiency of the future technique trendy moveable malware discovery and domestic documentation. (Jiang, P., 2021) one dimensional convolutional neural networks approach classify the spam malware images which attract the android user to click on certain link to proceed the malware executions for sending the data into remote location. Autoencoder and Self-governing Recurring Neural Network for Mobile Malware Detection system constructed on deep learning discovery method, in order to proceed the malware detection system, with softmix function include ReLu method of accuracy in order to achieve the outcome of recurrent neural network with highest accuracy rates, (Rashid, Z.N. Haji, L.M., 2021) efficiency of malware detection based on machine learning method Android remains additional susceptible and unstable due to malware attack, the classification of malware system in android phone by deploying the Bayesian algorithm Ada and grid algorithm, naïve bays algorithm and hybrid multinomial algorithm with support vector machine classifier which enables the user to detect and clean the malware from the android operating system, decision tree classifier and random forest classifier produce the highest accuracy rates for detection of malware attack in the android phone. (Mercaldo, F., Santone, A., 2021) dynamic image call based segmentation method mobile malware detection through the machine learning discovery develop the harmful code to caught the sensitive information from mobile phone which causes certain problem, recent literature present the malware detection system which constructed on various method to achieve the great outcomes by deploying the algorithm, various online web application framework downloaded from Google play store which formally used for malware scanning and detection prevent the spam attack safely. Feature extraction and build the classification models of naïve bays and support vector machine classifier to predict and detect the malware from the mobile device. Convolutional neural network and random forest tree method produces the highest accuracy rates for deploying the malware system. Genetic algorithm with SVM technique after preparing the input dataset, where missing values have been filled and clean, genetic algorithm used to reduce the number of input by determining the detection of malware attack. (Chen, S., 2020) mobile malware detection technique designed on various machine learning and deep learning methods, aim of this research is to provide the machine learning models by using the python programing machine learning algorithm to classify the android mobile malware which possibly used by various online web based application to reduce the risk of certain data hacking techniques. Recent research show that mobile malware develop to increase the rates of business revenue by capturing the business secret confidential data without permission of Google API so the issues still remain and challenging for other research to deploy the comprehensive research works to plan effective technique of machine learning algorithm to detect and capture the malware from the android operating system. Present methods to mobile malware examination and discovery cannot continuously save up through upcoming malware complexity. So future research works require to protect the android device from unknown user activities, recent android 11 version is stable and secured it does not allow location sharing information to unknown WIFI and suspicious user, recent android operating system security features enhance with rich segments of data protection and user application layers. Various Google online API works with Google play store to protect the android operating system by malware attack and hacking attack, malware is critical issues in the android previous releases, so the issues has been resolved in current android version and updated operating system features.



*Figur1: threat targeting Google play breakdown the last year (Geneiatakis, D., 2019)*

## Distance Measure in K nearest Neighbor

MysteryBot was discovered in 2018, by ThreatFabric, it was the capability to combine the Ransomware keylogger and banking Trojan. MysteryBot was similar characteristics of LokiBot with C&C server. (Geneiatakis, D., 2019) performance evaluation of distance measures in KNN for mobile malware detection, related work was described with various mobile malware detection for android operating system which often based on machine learning classification technique, the approach is understandable to provide the valuable results to configure the technique, K nearest neighbors considering the different hyper techniques with different hyper parameter to emphasis the different measurement technique, the research proposed the various machine learning malware detection method over the android phone user by using the K Nearest neighbor.

## Argumentative attacks on Mobile Malware Detection

Recent research show that (Xue, M., 2019) machine learning classification techniques has been widely used for computer security task including mobile malware detection & prevention, malware was global issue over the smart phone communication various competitor planned to create malware to capture the sensitive data of the competitor organization, malware was patent threat needs to improve the Google operating system which cause the serious issue. Capability of adversarial network, hence the machine learning detection solution deployed over the android operating system which needs some additional cost with Google API to plan the online analytics technique to capture the online malware attack which was major discovery with the Google operating system. This research effectively designed machine learning technique to generate the generative adversarial networks, by use of effective adversarial method the thresholds distortion method technique enable the developer the scan the real time malware capturing the real time sensitive information. Android dataset used and capture the 98% scanning accuracy to detect the malware from the android operating system. The generated samples dataset detect the malware from the android phone and report them.

## Machine learning algorithm

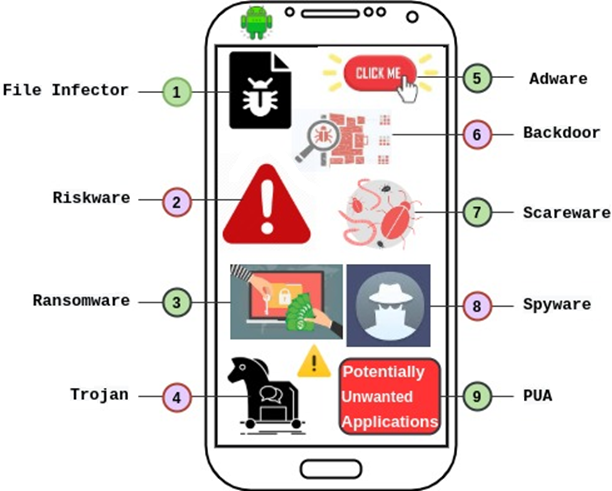
Machine learning classifier for android malware detection (Agrawal, P. Trivedi, B., 2021) the growing popularity of android devices, it is also prone to malware attack, so there are various malware tools are available to scan the malware from android phone, but the most effective and static analysis technique used lot of resources to build the machine learning model to enable the user to detect various resources and manual overhead. By using of advance machine learning method enable the organization to deploy the employee’s real time mobile telecommunication malware detection system to protect the organization data. This research analyze the different malware detection technique which was based on machine learning classifier method, this research also highlights the research strength and weaknesses including future scope. The outcome of research present the various machine learning classification technique,

1. Random forest classifier
2. Naïve Bays
3. Support vector machine
4. Decision tree

Since the naïve bays classifier produced the highest accuracy rates and detection to scan and predict the malware from the android phone.

## Machine learning classification malware detection using Opcode

Analysis of machine learning classifier proposed on (Ariff, N.A.M., 2020,) android malware detection tool using the Opcode mechanism. Android devices continuous to rise with more reliable application were introduced to make the daily routine task much easier and efficiently, mobile application framework uses the social media networking sites, including various other application technique including online banking, payment, online shopping web browsing, and other application and activities. Most of the application required user to provide private credential including private browsing experience to protect data from unknown sources, in the past various detection technique has been introduced to make daily task much easier. Therefore the enhance mobile detection used to enhance the security features which used against the malicious attack. Most of the android application provides the user permission to do the effective planning task to scan & capture the application in real time and detection various internal security credentials features to capture the advance problem of the android detection discovery. Hence the advance mobile malware detection techniques required to improve the malware detection system of the android phone. Machine learning classifier evaluated and validated based on the discovery of false positive and true positive rate, false positive rate classify the malicious mobile application. Mobile malware detection by using the method of opcode to classify the mobile operating system security several machine learning classifier method has been deployed to enhance the machine learning classification techniques with malware application detection discovery.



*Figure 2: android malware families (source IT world Canada)*

## *Understanding of Mobile Malware*

Android mobile is one of common threats over the globe (IT World 2020) various e-commerce site and mobile banking applications needs security and protection to prevent from the malware attack beside this the hacking attack is also very common issues in central America. The common mobile malware is known as adware, which has been used some additional features to deploy with organized approach of mobile malware detection system. Since the number of android app is rise due to equitability and equivalence applications interface. The affected sector includes healthcare, finance, transportation, government, and various e-commerce platform various mobile attacker uses the techniques to capture the sophisticated intrusion detection system which was follows on different category, the understanding of malware detection system including series detection system. Adware present the spam and fake advertisements over the android phone application and redirect the user on the given link to capture the user data. Some common adware advertisement techniques based on weight loss, making money in less time, and bogus virus warning on screen. These given links are provided on real time internet web links and user experience to click on these links to redirect them on certain sites and scan the user data on the particular given link. Some common malware adware family are as follows:

1. Gexin
2. Batmobi
3. Ewind
4. Shedun
5. Pandaad
6. Appad
7. Dianjin
8. Gmobi
9. Hummingbird
10. Mobisec
11. Loki
12. Kyhub

Beside the other malware known as backdoor which might be exploits the device covertly by hiding in the background, and file infector contains which contaminate the file specially the executable APK file. PUA acts as unwanted interruption to normal activities perform by the device, since the Ransomware acts as crypto locker that encrypts the files and directories and demand the ransom from the user to access the his own data. Riskware, poses the risk to the potential vulnerability on the smart phone. Scareware serves as fear coaxer that ignites fear in the user mind and forces them to download malicious apps. Spyware indulges into spying activities to capture the useful information from the android phone and send them to remotely by using the internet service and controlled the server. Since the Trojan acts like imitator in the background android application which keeps stealing the application information on the running background task and send them directly on the other server on backend.

## Reverse Engineering techniques

Reverse engineering is the process to determine the functionality of any object it used to obtain source code of the mobile app from the APK file. Various reverse engineering tools has been used to capture and detect the hidden malicious code inside the legitimate application various common reverse engineering tool based on android app including APK inspector APK tool, Bytecode viewer and Smali, and Jadx.

## Security feature in Android

Google update Android operating system security features in android 11 version, various permission and security features has been added on it, android user makes it use the best to do the files permission and photos and video permission over the usages on the internet. Android update the security while opening and installing the application in the android phone. Google offers the application on time permission services to access the apps such as allow meet to take pictures and record video while using the app. Auto reset permission android 11 automatically reset the permission given to it, by means of Google app permission location and recording the audio and video on the real time implementations of applications. Background locations access, permanent location access, offers the on demand location access if the user granted the location service then operating system.

## How to Secure Android Device

User do not download apps from unreliable sources, user might be encountered with download any unreliable app from unknown sources, even the application in Google play store are not secure, android 11 version and 12 is updated security version operating system of mobile network which enables the user to prevent the application from hacking attack and malware attack. Avoid third part app store which might be infect from viruses and hacking links which might be redirected the user to particular running server which cause the problem and capture the real time data over the internet. Say no to clickable link and does not click on fake and spam advertisement which might be capture the user information in real time and redirect them to another link various flashing and certain links make impression over the user choice, user might be interest on buying some grocery items and buying some clothes by using the online internet application. The use of common adware attack was very common malware threats which might be able the user to redirect them on certain link and capture the information in real time. User did not install any operating system update form unknown source until the android security and operating system makes any notification over the user operating system. since the used of various 100 of mobile application which might be able to slow down the performance of android operating system since the android operating system limited processing memory and storing memory so needs to improve the processing power and storing capacity. Latest android version are updated from malware attack in 2021, so there is need to improve the malware classification technique due to less number of classification technique are used in the past so the android operating system does not perform very well, but the malware threat still remain active but the implementation of machine learning classification techniques enable the Google operating system to update the android anti malware system.

## Summary of Literature Review

Mobile malware detection and prevention system has been deployed in the past by using the various advance machine learning technique, various mobile malware attack family has been discussed and highlighted in this studies, so the research method is deeply discussed in the literature finding so there is need to implement the advance machine learning classification technique to scan and remove the malware from android phone. So literature suggested that various machine learning active algorithm deploy in the android phone to prevent from the malware attack. So the pattern of analysis followed by the python programming including jupyter notebook with anaconda IDE.

1. Support vector machine classifier
2. Naïve bays classifier
3. Decision tree classification technique
4. Multinomial classifier TFIDF Vectorizer
5. NLP technique by using Machine learning algorithm
6. Random forest classifier

Machine learning classification technique based on advance detection discovery based method which followed on dataset from the Github repository and Kaggle repository. Dataset downloaded from the above mentioned link from 3000 samples of android running application malware dataset which includes various malware and non-malware information, so the classification and detection discovery followed the pattern of machine learning algorithm classification method to suggest based on the real time detection techniques and choice. So there is need to use the latest android phone, Google operating system contains machine learning classification method.

# References

M. Z. Mas'ud, S. Sahib, M. F. Abdollah, S. R. Selamat and R. Yusof, "Analysis of Features Selection and Machine Learning Classifier in Android Malware Detection," 2014 International Conference on Information Science & Applications (ICISA), 2014

Chen, Z., Yan, Q., Han, H., Wang, S., Peng, L., Wang, L. and Yang, B., 2018. Machine learning based mobile malware detection using highly imbalanced network traffic. *Information Sciences*, *433*, pp.346-364.

Ham, H.S. and Choi, M.J., 2013, October. Analysis of android malware detection performance using machine learning classifiers. In *2013 international conference on ICT Convergence (ICTC)* (pp. 490-495). Ieee.

Amos, B., Turner, H. and White, J., 2013, July. Applying machine learning classifiers to dynamic android malware detection at scale. In *2013 9th international wireless communications and mobile computing conference (IWCMC)* (pp. 1666-1671). IEEE.

Martinelli, F., Mercaldo, F., Nardone, V., Santone, A. and Vaglini, G., 2020. Model checking and machine learning techniques for HummingBad mobile malware detection and mitigation. *Simulation Modelling Practice and Theory*, *105*, p.102169.

M. Al-Janabi and A. M. Altamimi, "A Comparative Analysis of Machine Learning Techniques for Classification and Detection of Malware," 2020 21st International Arab Conference on Information Technology (ACIT), 2020, pp. 1-9,

Uppin, C., & George, G. Analysis of Android Malware Using Data Replication Features Extracted by Machine Learning Tools. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 193–201. 2019

Baldini, G. and Geneiatakis, D., 2019, April. A performance evaluation on distance measures in KNN for mobile malware detection. In *2019 6th international conference on control, decision and information technologies (CoDIT)* (pp. 193-198). IEEE.

Shahpasand, M., Hamey, L., Vatsalan, D. and Xue, M., 2019, February. Adversarial attacks on mobile malware detection. In *2019 IEEE 1st International Workshop on Artificial Intelligence for Mobile (AI4Mobile)* (pp. 17-20). IEEE.

Agrawal, P. and Trivedi, B., 2021. Machine learning classifiers for android malware detection. In *Data Management, Analytics and Innovation* (pp. 311-322). Springer, Singapore.

Anuar, N.A., Mas’ud, M.Z., Bahaman, N. and Ariff, N.A.M., 2020, November. Analysis of machine learning classifier in Android malware detection through opcode. In *2020 IEEE Conference on Application, Information and Network Security (AINS)* (pp. 7-11). IEEE.

Charbuty, B. and Abdulazeez, A., 2021. Classification based on decision tree algorithm for machine learning. *Journal of Applied Science and Technology Trends*, *2*(01), pp.20-28.

Wang, P., Fan, E. and Wang, P., 2021. Comparative analysis of image classification algorithms based on traditional machine learning and deep learning. *Pattern Recognition Letters*, *141*, pp.61-67.

Kasinathan, T., Singaraju, D. and Uyyala, S.R., 2021. Insect classification and detection in field crops using modern machine learning techniques. *Information Processing in Agriculture*, *8*(3), pp.446-457.

Abdulkareem, N.M. and Abdulazeez, A.M., 2021. Machine learning classification based on Radom Forest Algorithm: A review. *International Journal of Science and Business*, *5*(2), pp.128-142.

Hani, S.I. and Sahib, N.M., 2021. Mobile Malware Detection using Anomaly Based Machine Learning Classifier Techniques. Diyala Journal For Pure Science, 17(02).

Narudin, F.A., Feizollah, A., Anuar, N.B. et al. Evaluation of machine learning classifiers for mobile malware detection. Soft Comput 20, 343–357 (2016). https://doi.org/10.1007/s00500-014-1511-6

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).

Arif, J.M., Ab Razak, M.F., Mat, S.R.T., Awang, S., Ismail, N.S.N. and . Android mobile malware detection using fuzzy AHP. Journal of Information Security and Applications, 61, p.102929.

Iadarola, G., Martinelli, F., Mercaldo, F. and Santone, A., 2021. Towards an interpretable deep learning model for mobile malware detection and family identification. Computers & Security, 105, p.102198.

Kouliaridis, V. and Kambourakis, G., 2021. A Comprehensive Survey on Machine Learning Techniques for Android Malware Detection. Information, 12(5), p.185.

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.

Mercaldo, F. and Santone, A., 2021. Formal Equivalence Checking for Mobile Malware Detection and Family Classification. IEEE Transactions on Software Engineering.

Wei, S., Zhang, Z., Li, S. and Jiang, P., 2021. Calibrating Network Traffic with One-Dimensional Convolutional Neural Network with Autoencoder and Independent Recurrent Neural Network for Mobile Malware Detection. Security and Communication Networks, 2021.

Omer, M.A., Zeebaree, S.R., Sadeeq, M.A., Salim, B.W., x Mohsin, S., Rashid, Z.N. and Haji, L.M., 2021. Efficiency of malware detection in android system: A survey. Asian Journal of Research in Computer Science, pp.59-69.

Casolare, R., De Dominicis, C., Iadarola, G., Martinelli, F., Mercaldo, F. and Santone, A., 2021. Dynamic Mobile Malware Detection through System Call-based Image representation. J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl., 12(1), pp.44-63.

Kouliaridis, V., Barmpatsalou, K., Kambourakis, G. and Chen, S., 2020.A survey on mobile malware detection techniques. IEICE Transactions on Information and Systems, 103(2), pp.204-211.