International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 04 | April - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

Mobile Malware Detection using Machine Learning Classifiers

Divya Sharma[1*], Jasvir Singh[2]
[1,2]*Department of Computer Science & Engineering, Punjabi University, Patiala*
[1]divusharma198@gmail.com;
[2]jassiccet@gmail.com
Corresponding author email id: [1]divusharma198@gmail.com

ABSTRACT
In today world the mobile malware shows the significant threat to the security and privacy of the society using smartphones. These malware aims to access the sensitive data and harm the devices of users. This paper conducts a comprehensive comparison between the various machine learning and traditional methods for mobile malware detection based on the research papers published by the authors. Signature-based detection depends upon the predefined and common patterns, while the anomaly based techniques analyse the deviation from the regular normal behaviour. This study discusses the strengths and limitations of different approaches and highlights the need for adopting the malware detection methods to fight the growing threats. It also examines the role of machine learning algorithms, like Decision Trees, Random Forests, Convolutional Neural Networks, Support Vector Machines, and Naïve Bayes, for better malware detection. Latest findings and research highlights the importance of the continuing innovation to fight the emerging threat to the user privacy, data and security due to malwares.

Keywords: Mobile Malware, Artificial Intelligence, Virus, Signature-based Detection, Machine Learning

1. INTRODUCTION

The malicious software that unambiguously targets the operating systems on mobile phones is mobile malware. This malicious software is specifically designed to target mobile devices (such as smartphones and tablets) with the goal of gaining access to private data. The following are examples of prevalent mobile malware variants that are adaptable in nature such as virus, worm, Trojan, rootkit, adware, spyware, botnets, ransomware, backdoors, key-loggers etc (Figure 1). Virus can be defined as the bit of code that replicate itself and spread across multiple programs on a device. When a user launches a septic program, it frequently spreads itself by attaching to various applications and then executing the code [1]. Worms are capable of replicating themselves and spread over computer networks from one device to another without any human interference. By consuming bandwidth and causing congestion on web servers, worms' "payloads" can harm host devices or even take down host networks. Payloads have the ability to build botnets, erase files from the system, and steal user data. Opening a contaminated email attachment can allow worms to propagate. Trojan is a sort of malware that attracts consumers to download and install it by presenting itself as a legitimate application. Rootkit gains the access remotely to control devices in order to exploit users. It consists of a loader, dropper and the rootkit to perform destructive actions. Administrative access is required to perform various harmful operations such as stealing information, disrupting regular system routines and many more. Check Point researchers discovered the rootkit HummingBad, which deployed a misleading mobile application to steal credentials and produce bogus advertising [2]. Botnet is a network of linked devices or computers that have been secretly contaminated with malware, also known as bots or zombies. Adware is a malware type which is sponsored by advertisements and is made especially to show consumers advertisements on their own initiative. Pop-up advertising and other adverts that appear on websites

are known as malware. Adware is typically given up for free, but occasionally advertising businesses sponsor it and make money from it. Adware is merely intended to display advertisements; when users click on them, the program is activated and can either track or steal user data. Android Adware includes programs like Judy, Skinner, LightsOut, Gunpoder, and RottenSys. It is a kind of virus that tracks user behavior without permission. These include gathering important records, keeping an eye on screens, and stealing account information. By altering the security procedures of a network, spyware can cause disruptions [1]. Ransomware is a kind of malware that demands payment in ransom before releasing computer resources. Ransomware encrypts files, locks computers, restricts access, and displays messages urging users to pay money. Malware with backdoors is designed to allow other malware to infiltrate a device by creating a backdoor. It assists other malicious activities by giving them access to a network connection so they can enter and steal data. The first malware to ever open a backdoor on Windows Mobile is called Brador. Key-logger logs every single user tap on the computer to obtain their login credentials or the sensitive data. Key-loggers are commonly employed by diverse entities to get data pertaining to computer utilization. Flexispy is one of the popular program that records smartphone usage [2].

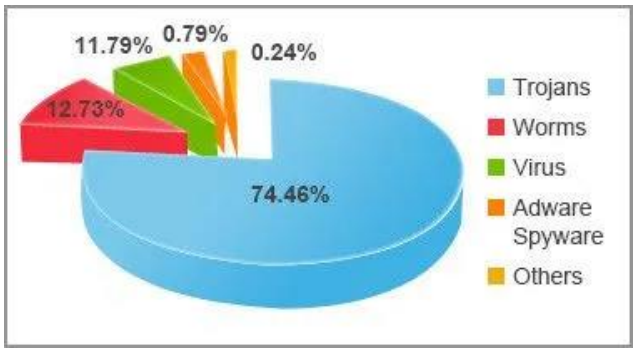

Figure 1. Mobile malware [45]

Traditional mobile malware detection techniques incorporate a variability of established methods and technologies that aim to identify and mitigate malwares targeting mobile devices (such as smartphones and tablets). There are various traditional techniques for detecting mobile malware such as Signature-based Detection, Static Analysis, Dynamic Analysis, Behavior-based Detection, Permission Analysis, Network-based Detection, Manual Analysis etc [3]. The limitations of traditional mobile malware detection include the signature dependency, traditional techniques are not effective to identify new and developing malware variants that use advanced techniques or have altered signatures. Traditional detection techniques are prone to zero-day-attacks as they could fail to detect malware that performs dynamically or utilize the system drawbacks without generating the detectable signs. The limitations of traditional malware detection methods underline the needs for more advanced techniques that can successfully address the ever-changing threat environment [4]. By overcoming the drawbacks of traditional detection techniques the Advanced mobile malware detection techniques represents the latest advancements of mobile security that uses various technologies and methods to combat more complex threats that targets the mobile devices. Various advanced mobile malware detection techniques for detecting the malware are Machine learning and Artificial Intelligence, Feature Engineering, Code Emulation and Sandboxing, Hardware-Assisted Security, Behavioral Biometrics, Zero-Day Threat Detection, Continuous Monitoring and Response, etc [5]. By addressing the limitations of the traditional detection techniques Artificial Intelligence and machine learning have changed the field of mobile malware detection. The traditional techniques struggled with zero-day attacks due to relying on the known signatures in signature-based detection technique, while the Artificial Intelligence and Machine learning algorithms identifies the patterns and anomalies in a large dataset that is associated with malicious behavior. By using the advanced feature engineering the AI and ML techniques diminishes the false positives while the traditional methods in which the malware variants that employ evasion

techniques produce the false positives [6]. The machine learning and artificial intelligence based detection techniques can automate analysis processes, ensures scalability and efficiency, learn from and adapt to new threats etc. Based on the aforementioned facts, the aim of the paper is to analyse the work of the researchers in the field of detecting and classifying Android Malware using AI based learning techniques.

2. Literature Review

This section presents the contribution of the researchers in the field of detecting mobile malware detection using machine learning classifiers. Apart from this, their work has been also compared and analysed on the basis of various attributes such as dataset, algorithms, techniques, outcomes along with the challenges in Table 1.

Qamar, A. et al. (2019) [1] outlines future directions for research and development, providing guidelines for both academia and industry to mitigate or prevent the harmful impacts of evolving mobile malware threats. The paper suggests future directions for researchers to enhance the development of more accurate, efficient, robust, and scalable mechanisms for Android malware detection. The aim is to stay ahead of the evolving techniques employed by malware creators and bolster the overall security of mobile devices and the community at large. Senanayake, et al. (2021) [7] aims to equip researchers with a comprehensive understanding of ML-based Android malware detection, providing insights into current methodologies and suggesting potential directions for future research and development. The highlighting on source code vulnerabilities highlights the value of taking preventative action to strengthen mobile device security against ever-evolving malware threats. In addition to code and APK analysis methods, feature extraction and analysis approaches, and the benefits and drawbacks of suggested detection methods, the study assesses machine learning (ML) and deep learning (DL) models and investigates their efficacy in Android malware detection. Given how easily vulnerabilities can be exploited by developers who make mistakes, the paper also looks at machine learning techniques for identifying source code vulnerabilities. Kouliaridis, et al. (2020) [8] highlights how outdated mobile malware research and detection techniques are in comparison to the increasing sophistication of emerging malware. The work's main goal is to provide a thorough and organized summary of the most recent findings on mobile virus detection methods. In order to meet the changing landscape of mobile threats and improve the efficacy of malware detection techniques, the study attempts to evaluate the advantages and limits of these strategies. A thorough analysis of mobile malware detection methods is presented in this extensive article, which focuses on research that was published between 2011 and 2018. The review offers an overview of the advantages and drawbacks of each detection strategy by classifying and briefly analysing them. The goal of the paper is to provide a comprehensive review of this difficult and quickly developing topic. The study also looks at how the works under examination relate to one another, identifying influential figures in the field and emphasizing the main issues that require immediate attention. Alzubaidi, A., (2021) [9] looks at the risks and difficulties involved with malware targeting smartphones in response to the increasing global use of these devices and the explosion of both free and paid applications. Due to their storage of private and sensitive data, smartphones have become popular targets for malicious software. In the context of cellphones, the article focuses on comprehending the ideas and dangers related to malware. In addition, it examines the current methods and techniques used in malware detection, exploring their workings, the datasets they make use of, and the assessment criteria they employ to gauge their efficiency. The report focuses on the dangers posed by malware that targets mobile devices. It analyses the methods, related datasets, and assessment techniques used in research on mobile malware released since 2010 in order to assess the state of the art approaches and processes for identifying this kind of malware. In closing, the study summarizes important findings, points out prospective directions for future research, and presents emerging themes in the developing field of mobile malware detection. Amro, B., (2018) [10] examines different malware detection methods utilized for each of the two main rival mobile operating systems, iOS and Android. It seeks to offer a thorough study of different methods, stressing the benefits and drawbacks of each. The work's ultimate

objective was to establish the framework for the creation of a user-profiled mobile malware detection tool, realizing the significance of customizing detection techniques to the unique features of every operating system. In addition, it looks at the methods used to distribute malware to mobile devices and provides the most recent data on malware attacks during the previous three years. Additionally, common malware detection methods for mobile applications are introduced and their advantages and disadvantages are assessed. One noteworthy feature is the identification and explanation of each detection method's shortcomings. The paper's main objective is to provide groundwork for the creation of a fresh, effective malware detection tool for mobile devices, with an emphasis on user profile as a means of boosting overall security. Mohata, et al. (2013) [11] highlights the need for effective malware detection and prevention on mobile phones, emphasizing the challenges posed by the functionality limitations of these devices. In response, the paper proposes and analyses potential limitation-oriented techniques aimed at mitigating the impact of malware on mobile phone performance. The focus is on developing strategies that balance the need for robust security with the inherent limitations of mobile devices. This paper emphasizes the vulnerability of mobile handsets to malware attacks, owing to their versatile communication and computation capabilities, along with inherent resource constraints. To ensure comprehensive protection, particularly for open-source platforms like Android, a security suite for mobile devices should incorporate a diverse set of tools with complementary capabilities. The presented detection techniques are deemed viable, but their real-world performance necessitates large-scale testing. As Android malware evolves, the effectiveness of these measures is expected to diminish, yet they still provide value by raising the entry bar for both repackaged and newly created malware, all while incurring minimal overhead. The paper underscores the need for ongoing testing and adaptation to tackle the evolving landscape of mobile malware threats. Malhotra, A. and Bajaj, K., (2016) [12] addresses the emergence of mobile platforms, with Android establishing itself as a market leader in the second quarter of 2015, according to IDC. However, the widespread adoption of Android has brought forth an escalating concern regarding malware threats and security vulnerabilities. The paper conducts a meticulous examination of terminology associated with mobile malware and delves into various techniques employed for malware detection. Additionally, the paper summarizes proposed methods and the types of approaches utilized in these methods, providing a comprehensive overview of the evolving landscape of mobile malware detection in the context of the dominant Android platform. This paper presents a comprehensive review of literature pertaining to mobile malware detection, thoroughly examining and analyzing various techniques. The advantages and disadvantages of these techniques are discussed and enumerated. The paper highlights two major approaches adopted by researchers: signature-based and anomaly-based techniques. Signature-based methods involve studying and analyzing patterns of instruction sets, while anomaly-based methods focus on detecting unusual activities. The review sheds light on existing research gaps in the field, suggesting potential areas for improvement. Riasat, et al. (2017) [13] addresses the proliferation of smartphone applications and the growing concern over malware, particularly with the increased connectivity of users to the internet. Despite advanced technology in smartphones, users remain vulnerable to malware attacks. As the functionality of smartphones continues to advance, the threat of malicious applications, malware, and adware for mobile phones is expected to rise. With Android operating systems being the most commonly used, the review highlights the challenges in distinguishing between clean and malicious applications in the Android Play Store. The paper discusses various methods for detecting Android malwares, providing a comprehensive overview of detection tools in smartphone applications. The aim is to shed light on the evolving landscape of mobile security and help users make informed decisions to safeguard their smartphones. This study delves into recent developments in Android malware detection within both official and unofficial Android Markets. The systematic analysis focuses on detecting malicious applications, exploring various detection techniques and systems employing static, dynamic, and hybrid approaches. The discussion extends to potential countermeasures against update attacks, incorporating attack tree analysis, permissions, contrasting permission patterns, and network traffic monitoring. Ashawa, et al. (2019) [14] conducts a systematic review of malware detection techniques employed for Android devices. The findings reveal that many current

detection techniques struggle to effectively identify zero-day malware and other variants that employ obfuscation to evade detection. The critical appraisal of the study identifies limitations in existing detection techniques, emphasizing the need for improvements to enhance overall detection efficacy. The paper underscores the urgency of developing more robust and adaptive techniques to counter the evolving threats faced by Android devices. The paper highlights the need for further research, expressing an intention to explore methods for establishing a security perimeter defense around Google Bouncer. This defence aims to enhance the efficiency of reviewing Android applications from third parties before they are uploaded to the Play Store. The study contributes to advancing the understanding of Android malware detection and paves the way for future research in the field.

Table 1: Analysis of the existing techniques used for malware detection

Author	Dataset	Algorithm	Technique	Outcome	Strength	Limitation
Nur Syuhada Selamat and Fakariah Hani Mohd Ali(2019) [15]	305 types of malware 236 types of benign	Decision tree(DT)	N/A	Accuracy 99%	Effective detection, comparative analysis, non-intrusive approach	Small dataset, overfitting risk, complexity of malware
Fairuz Amalina Narudin, et al.(2014) [16]	1260 types of malware 20 benign application	Bayes network, MLP, Decision Tree, KNN Random Forest	N/A	Accuracy 99%	High accuracy, Use of diverse features, Comparison of multiple classifiers	Processing time, low KNN performance, dependency on dataset
P Sumalathaand G.S. Mahalakshmi (2023) [17]	Android malware dataset **(**CICAndMal2017) 426 malware and 5,065 benign	Random Forest, Decision Tree, Multi- layer Preceptron (MLP)	Stacking Ensemble for Automatic Android Malware Detection (SE-AAMD) algorithm	Accuracy 96.72%	High accuracy, improved security, ensemble approach	Dataset influence, model complexity, training time
Fabio Martinelli , et al.(2017) [18]	3564 malware 3536 benign	Convolutional Neural Network (CNN)	N/A	N/A	Dynamic analysis, large dataset	Exact accuracy not provided, evaluation metrics, less dataset coverage, resource intensive

Yuan, et al. (2016) [19]	Various android apps	Multi-layer perceptron, Naïve Bayes and Logistic regression	Hybrid	Accuracy 94.60%	Deep learning techniques, online detection engine (DiorDetector)	No dataset information, scalability, algorithm details, generalization
Anusha Damodaran, et al.(2017) [20]	Harebot, Security Shield, SmartHDD, Zbot, Winwebsec, ZeroAccess	N/A	Hybrid	N/A	Comprehensive review, insights into dataset	Accuracy not provided, temporal limitation, algorithm and technique details
Shifu Hou, et al.(2016) [21]	Real sample collection from Comodo Cloud Security Center.	Neural Network	Hybrid	Accuracy 92.66%	Malware image recognition, Real Sample Collection	Dataset size & diversity, comparative analysis, Generalization
Majid Salehi and Morteza Amini(2017) [22]	4034 malware 10024 benign	Random forest, Markov chain	Dynamic	Accuracy 96%	RF classifications, high accuracy, low overhead	Training data quality, mimicry attacks, root access requirement
Ankita Kapratwar, et al. (2017) [23]	103 Malware 97 Benign	Naïve Bayes, simple logic	Static	Accuracy 96.6%	Efficiency of static analysis, robustness	Dataset size, dynamic feature collection, complexity
Matthew Leeds, et al.(2017) [24]	Andrototal.org	Machine learning algorithm	Hybrid	Accuracy 80% (permission request) 60% (system calls)	Reliability of permission data	Small dataset, limited features, complexity of malware behavior
McLaughlin, et al.(2017) [25]	3 datasets were used 863 benign, 1260 malware; 3627 benign, 2475 malware; 9268 benign, 9902 malware	Convolutional neural network (CNN)	Static	Accuracy 87%	Large dataset, end-to-end training, efficiency, comparative performance	Network complexity, platform specificity

Guozhu Meng, et al.(2016) [26]	223170 real world applications	Random Forest, Naïve Bayes, AdaBoost, Linear SVM	Static	Accuracy 87.0%	Efficiency and scalability, good performance	Training data quality, need for regular updates, resource intensive
Arvind Mahindruand Paramvir Singh (2017) [27]	11000 android applications	Naive Bayes, Simple Logistic	Dynamic	Accuracy Simple Logistic 84.08%, Naïve Baiyes 67.64%	Large dataset, dynamic permissions, scalability	Dependency on permission model, overfitting, complexity of malware
Jyoti Malik and Rishabh Kaushal (2016) [28]	N/A	N/A	Content based	63%	Pattern based detection, semi-automated approach	Dependency and complexity of network traffic, generalizability
Hui-Juan Zhu, et al.(2018) [29]	1065 malware 1065 benign	Random forest	Static	Accuracy 89.9%	Fast and cost effective	Bias and variance in features detection
Muhammad Aamir, et al.(2024) [30]	5560 malware 9476 benign	Convolutional neural network (CNN)	N/A	Accuracy 99.92%	High accuracy, comprehensive evaluation, dataset size	Model complexity, interpretability, dependency on parameters
Catarina Palma, et al.(2023) [31]	Derbin, CICAndMal2017, AMSF	Support vector machine, Random Forest, KNN, Naïve Bayes, MLP	N/A	SVM and RF shows the higher accuracy with promising results	Real world application, generalization ability, high dimensionality reduction	Dataset standardization, future dataset usage, evaluation challenges
S. Poornima and R. Mahalakshmi (2024) [32]	CICAndMal2017	Deep Belief Network, Artificial Neural Networks , Generative Adversarial Network , and	N/A	Accuracy DBN-99.83% ANN-93.11% GAN-96.75% LSTM-	Hybrid analysis framework, reliable dataset, dynamic with reinforcement learning	System complexity, limited dataset, interpretability

		Long Short-Term Memory Network		94.42%		
Hamid Bostani and Veelasha Moonsamy (2024) [33]	Approx 17,000 samples were collected from different platforms	EvadeDroid	N/A	80% to 95% evasion rate	Effective evasion, query-efficient optimization, real-world feasibility	Dependency on opcode-level similarity, limited access to target classifiers
Mohamad Arif et al.(2021) [34]	Drebin and AndroZoo	Fuzzy AHP (Analytical Hierarchy Process)	N/A	Accuracy 90.54%	Risk-based approach, multi-criteria decision making, static analysis	Limited to permission based features, dependence on the quality of the dataset
Sharfah Ratibah Tuan Mat, et al(2022) [35]	Drebin and AndroZoo	Naïve Bayes	Static	Accuracy 91.1%	Permission based approach, optimized feature selection	Dependency on static analysis, feature selection trade-offs
Lu and Wang(2022) [36]	Drebin and CICMalDroid	CNN	N/A	N/A	Application protocol independent, encryption-agnostic	Dataset limitation, lack of specific accuracy value, complexity
Yang et al.(2022) [37]	Drebin and AMGP	Contrastive Learning	N/A	Accuracy 96%	Impact reduction, token free encoding, variable feature extraction	Gaps in research, performance variability, computational complexity
Ibrahim, et al.(2021) [38]	CTU-13	KNN	Dynamic	Accuracy 80%	Use of real-world dataset, structure and protocol independence	Ineffectiveness of oversampling technique
Colin Galen and Robert	Elastic Malware Benchmark for	AdaBoosted LightGBM,	Static	Accuracy 94%,	Large dataset usage,	Model variability,

Steele(2021) [39]	Research 2018 (EMBER2018)	Optimized LightGBM, LightGBM		94.1%, 91%	implication for real-world system	dependency on training data, computational cost.
Y. Fu and Q. Lan(2020) [40]	Chinese security company	Bayesian and Gaussian	Static	Accuracy 80% to 85%	Use of deep generative models, efficient handling of large dataset	Unspecified dataset usage fir experiments, lack of research challenges.
B. Ramadhan, et al.(2020) [41]	VirusShare, portablcapps.com and windows7 ultimate 32-bit directory	Naive Bayes	Hybrid	Accuracy 93% (static) 85% (dynamic)	Automatic malware detection, efficient and simple algorithm used.	Evasion technique can reduce detection accuracy, dependency on analysis technique
Oneil B. Victoriano (2019) [42]	HelDroid	Decision Tree, Naïve Bayes, Random Forest	N/A	Acuracy 98.08%	High accuracy, multiple classifiers, complement to anti-virus	Dataset dependency, limited unknown features, inference speed
Yuan Yang, et al.(2018) [43]	MALICA(Real world malware samples)	Bayesian	Hybrid	Precision 97.41%, recall rate 97.21%	Probabilistic approach, high precision and recall rate, novel and light weight method	Computational complexity, single dataset evaluation
Esraa Odat and Qussai M. Yaseen (2023) [44]	Drebin, Malgenome, and MalDroid2020	Random Forest, Decision Tree, Logistic Regression, SVM, KNN	N/A	Accuracy98%	High Accuracy, multiple dataset creation, utilizing co-existence of static features	Dataset specificity, dependency on dataset quality, computational resources for training and evaluation

3. Conclusion

The findings of this study provide insights into the need for the application of varied datasets, algorithms, and techniques to ensure effective mobile-based malware detection. Although each of the identified techniques exhibits some strengths and weaknesses, a comprehensive understanding of each would assist ultimately in the development of effective and adaptive malware detection systems. No single technique is uniformly superior, and the choice of approach is largely decided by individual application demand. Among the possible directions for future research, there exist addressing the limitations identified in this study such as dataset quality and quantity, algorithm scalability, or computational resource demands. Additionally, efforts directed towards developing techniques based on hybrid or ensemble systems show promise for improved malware detection effectiveness. To conclude, the issue of the increased prevalence of mobile malware is an important challenge for smartphone users and security experts. The variety of detection methods described in the paper is an indicator of continuous efforts to overcome continuing threats and prevent malicious attacks. Signature-based methods can be utilized to identify well-known malware; meanwhile, anomaly-based can offer more freedom to identify new threats. The use of machine learning algorithms is feasible for improving the effectiveness of detection. They can be adapted with labeled and unlabelled data to identify patterns and anomalies potentially associated with malicious activities.

References

1. Qamar, A., Karim, A. and Chang, V., 2019. Mobile malware attacks: Review, taxonomy & future directions. Future Generation Computer Systems, 97, pp.887-909.
2. Tahir, R., 2018. A study on malware and malware detection techniques. International Journal of Education and Management Engineering, 8(2), p.20.
3. Bayazit, E.C., Sahingoz, O.K. and Dogan, B., 2020, June. Malware detection in android systems with traditional machine learning models: a survey. In 2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA) (pp. 1-8). IEEE.
4. Kim, Y.K., Lee, J.J., Go, M.H., Kang, H.Y. and Lee, K., 2022. A systematic overview of the machine learning methods for mobile malware detection. Security and Communication Networks, 2022.
5. Avasarala, B.R., Day, J.C. and Steiner, D., Northrop Grumman Systems Corp, 2016. System and method for automated machine-learning, zero-day malware detection. U.S. Patent 9,292,688.
6. Ali, S., Rehman, S.U., Imran, A., Adeem, G., Iqbal, Z. and Kim, K.I., 2022. Comparative evaluation of ai-based techniques for zero-day attacks detection. Electronics, 11(23), p.3934.
7. Senanayake, J., Kalutarage, H. and Al-Kadri, M.O., 2021. Android mobile malware detection using machine learning: A systematic review. Electronics, 10(13), p.1606.
8. 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.
9. Alzubaidi, A., 2021. Recent advances in android mobile malware detection: A systematic literature review. IEEE Access, 9, pp.146318-146349.
10. Amro, B., 2018. Malware detection techniques for mobile devices. arXiv preprint arXiv:1801.02837.
11. Mohata, V.B., Dakhane, D.M. and Pardhi, R.L., 2013. Mobile malware detection techniques. Int J Comput Sci Eng Technol (IJCSET), 4(04), pp.2229-3345.
12. Malhotra, A. and Bajaj, K., 2016. A survey on various malware detection techniques on mobile platform. Int J Comput Appl, 139(5), pp.15-20.
13. Riasat, R., Sakeena, M., Wang, C., Sadiq, A.H. and Wang, Y.J., 2017. A survey on android malware detection techniques. DEStech Trans. Comput. Sci. Eng.

14. Ashawa, M.A. and Morris, S., 2019. Analysis of android malware detection BJKL;'techniques: a systematic review.
15. Selamat, N. and Ali, F., 2019. Comparison of malware detection techniques using machine learning algorithm. Indones. J. Electr. Eng. Comput. Sci, 16, p.435.
16. Narudin, F.A., Feizollah, A., Anuar, N.B. and Gani, A., 2016. Evaluation of machine learning classifiers for mobile malware detection. Soft Computing, 20, pp.343-357.
17. Sumalatha, P. (2023), 'Machine Learning Based Ensemble Classifier for Android Malware Detection', International Journal of Computer Networks & Communications (IJCNC) 15 (4), 111-122.
18. Martinelli, F., Marulli, F. and Mercaldo, F., 2017. Evaluating convolutional neural network for effective mobile malware detection. Procedia computer science, 112, pp.2372-2381.
19. Yuan, Z., Lu, Y. and Xue, Y., 2016. Droiddetector: android malware characterization and detection using deep learning. Tsinghua Science and Technology, 21(1), pp.114-123.
20. Damodaran, A., Troia, F.D., Visaggio, C.A., Austin, T.H. and Stamp, M., 2017. A comparison of static, dynamic, and hybrid analysis for malware detection. Journal of Computer Virology and Hacking Techniques, 13, pp.1-12.
21. Hou, S., Saas, A., Ye, Y. and Chen, L., 2016. Droiddelver: An android malware detection system using deep belief network based on api call blocks. In Web-Age Information Management: WAIM 2016 International Workshops, MWDA, SDMMW, and SemiBDMA, Nanchang, China, June 3-5, 2016, Revised Selected Papers 17 (pp. 54-66). Springer International Publishing.
22. Salehi, M. and Amini, M., 2017. Android malware detection using Markov Chain model of application behaviors in requesting system services. arXiv preprint arXiv:1711.05731.
23. Kapratwar, A, Di Troia, F & Stamp, M. 2017. Static and Dynamic Analysis of Android Malware. doi.org/10.5220/0006256706530662.
24. Leeds, M., Keffeler, M. and Atkison, T., 2017, April. A comparison of features for android malware detection. In Proceedings of the SouthEast Conference (pp. 63-68).
25. McLaughlin, N., Martinez del Rincon, J., Kang, B., Yerima, S., Miller, P., Sezer, S., Safaei, Y., Trickel, E., Zhao, Z., Doupé, A. and Joon Ahn, G., 2017, March. Deep android malware detection. In Proceedings of the seventh ACM on conference on data and application security and privacy (pp. 301-308).
26. Meng, G., Xue, Y., Xu, Z., Liu, Y., Zhang, J. and Narayanan, A., 2016, July. Semantic modelling of android malware for effective malware comprehension, detection, and classification. In Proceedings of the 25th International Symposium on Software Testing and Analysis (pp. 306-317).
27. Mahindru, A. and Singh, P., 2017, February. Dynamic permissions based android malware detection using machine learning techniques. In Proceedings of the 10th innovations in software engineering conference (pp. 202-210).
28. Malik, J. and Kaushal, R., 2016, July. CREDROID: Android malware detection by network traffic analysis. In Proceedings of the 1st acm workshop on privacy-aware mobile computing (pp. 28-36).
29. Zhu, H.J., Jiang, T.H., Ma, B., You, Z.H., Shi, W.L. and Cheng, L., 2018. HEMD: a highly efficient random forest-based malware detection framework for Android. Neural Computing and Applications, 30, pp.3353-3361.
30. Aamir, M., Iqbal, M.W., Nosheen, M., Ashraf, M.U., Shaf, A., Almarhabi, K.A., Alghamdi, A.M. and Bahaddad, A.A., 2024. AMDDLmodel: Android smartphones malware detection using deep learning model. Plos one, 19(1), p.e0296722.
31. Palma, C., Ferreira, A. and Figueiredo, M., 2023. Explainable Machine Learning for Malware Detection on Android Applications. Information, 15(1), p.25.
32. Poornima, S. and Mahalakshmi, R., 2024. Automated malware detection using machine learning and deep learning approaches for android applications. Measurement: Sensors, 32, p.100955.

33. Bostani, H. and Moonsamy, V., 2024. Evadedroid: A practical evasion attack on machine learning for black-box android malware detection. Computers & Security, 139, p.103676.
34. Arif, J.M., Ab Razak, M.F., Mat, S.R.T., Awang, S., Ismail, N.S.N. and Firdaus, A., 2021. Android mobile malware detection using fuzzy AHP. Journal of Information Security and Applications, 61, p.102929.
35. Mat, S.R.T., Ab Razak, M.F., Kahar, M.N.M., Arif, J.M. and Firdaus, A., 2022. A Bayesian probability model for Android malware detection. ICT Express, 8(3), pp.424-431.
36. Lu, T. and Wang, J., 2022. F2DC: Android malware classification based on raw traffic and neural networks. Computer Networks, 217, p.109320.
37. Yang, S., Wang, Y., Xu, H., Xu, F. and Chen, M., 2022. An android malware detection and classification approach based on contrastive lerning. Computers & Security, 123, p.102915.
38. Ibrahim, W.N.H., Anuar, S., Selamat, A., Krejcar, O., Crespo, R.G., Herrera-Viedma, E. and Fujita, H., 2021. Multilayer framework for botnet detection using machine learning algorithms. IEEE Access, 9, pp.48753-48768.
39. Galen, C. and Steele, R., 2021, April. Empirical measurement of performance maintenance of gradient boosted decision tree models for malware detection. In 2021 International Conference on Artificial Intelligence in Information and Communication (ICAIIC) (pp. 193-198). IEEE.
40. Fu, Y. and Lan, Q., 2020, August. Deep generative model for malware detection. In 2020 Chinese Control And Decision Conference (CCDC) (pp. 2072-2077). IEEE.
41. Ramadhan, B., Purwanto, Y. and Ruriawan, M.F., 2020, October. Forensic malware identification using naive bayes method. In 2020 International Conference on Information Technology Systems and Innovation (ICITSI) (pp. 1-7). IEEE.
42. Victoriano, O.B., 2019, October. Exposing android ransomware using machine learning. In Proceedings of the 2019 International Conference on Information System and System Management (pp. 32-37).
43. Yang, Y., Cai, Z., Wang, C. and Zhang, J., 2018. Probabilistically inferring attack ramifications using temporal dependence network. IEEE Transactions on Information Forensics and Security, 13(11), pp.2913-2928.
44. Odat, E. and Yaseen, Q.M., 2023. A novel machine learning approach for android malware detection based on the co-existence of features. IEEE Access, 11, pp.15471-15484.
45. https://www.linuxandubuntu.com/home/difference-between-malware-viruses-worms-spyware-trojans-and-ransomware