FUZZY ANALYTICAL HIERARCHY PROCESS BASED RISK ASSESSMENT FOR MALWARE DETECTION IN ANDROID MOBILE SYSTEM

JULIZA BINTI MOHAMAD ARIF

MASTER OF SCIENCE

UNIVERSITI MALAYSIA PAHANG

SUPERVISOR'S DECLARATION

We hereby declare that we have checked this thesis and in our opinion, this thesis is adequate in terms of scope and quality for the award of the degree of Master of Science.

DR. MOHD. FAIZAL BIN AB RAZAK
SENIOR LECTURER
FACULTY OF COMPUTER SYSTEMS & SOFTWARE ENGINEERING
UNIVERSITI MALAYSIA PAHANG
LEBUHRAYA TUN RAZAK, 26300 GAMBANG, KUANTAN
PAHANG DARUL MAKMUR
TEL : 09-549 2217 FAX : 09-549 2144

_____

(Supervisor's Signature)

Full Name : DR MOHD FAIZAL BIN AB RAZAK

Position : SENIOR LECTURER

Date : 14 JUNE 2022

DR. SURYANTI BINTI AWANG
SENIOR LECTURER
FACULTY OF COMPUTER SYSTEMS
& SOFTWARE ENGINEERING
UNIVERSITI MALAYSIA PAHANG
LEBUHRAYA TUN RAZAK, 26300 GAMBANG KUANTAN
TEL:09-549 2120 FAKS:09-549 2144

_____

(Co-supervisor's Signature)

Full Name : DR SURYANTI BINTI AWANG

Position : SENIOR LECTURER

Date : 14 JUNE 2022

STUDENT'S DECLARATION

I hereby declare that the work in this thesis is based on my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree at Universiti Malaysia Pahang or any other institutions.

_____

(Student's Signature)

Full Name : JULIZA BINTI MOHAMAD ARIF

ID Number : MCN19002

Date : 14 JUNE 2022

FUZZY ANALYTICAL HIERARCHY PROCESS BASED RISK ASSESSMENT FOR MALWARE DETECTION IN ANDROID MOBILE SYSTEM

JULIZA BINTI MOHAMAD ARIF

Thesis submitted in fulfillment of the requirements
for the award of the degree of
Master of Science

Faculty of Computing

UNIVERSITI MALAYSIA PAHANG

JUNE 2022

ACKNOWLEDGEMENTS

I would like to begin by expressing my thankfulness to Allah swt for bestowing upon me the wellness necessary to accomplish this proposal.

I take this opportunity to thank gratefulness to Ts. Dr. Mohd Faizal bin Ab Razak and his supervisors for providing invaluable guidance, supervision, and encouragement throughout this study. His direction, kindness, and encouragement have all contributed significantly to my motivation to complete this study. He taught me how to conduct research and present findings in the shortest amount of time possible. It is an extraordinary privilege and honour to work and study under his direction. I owe him gratitude for what he has given me. Additionally, I'd like to convey my gratefulness to Dr. Suryanti binti Awang, my co-supervisor, for assisting me with this study.

I owe a debt of gratitude to my parents for constantly encouraging me and praying for me to complete my studies. I owe gratitude to my husband (Tc. Mohd Shahrul Pidaus b Ab Razak), my father (Mohamad Arif b Bidin), my mother (Siti Rahmah binti Yahya), my siblings (Juliana binti Mohamad Arif, Junaidah binti Mohamad Arif, Aliff bin Mohamad Arif, Jasarina binti Mohamad Arif and Azrul bin Mohamad Arif), my daughters (Dhiya Nur aira and Adelia Nur Aafiya) and my son (Muhammad Yusuf Qarizh) for their diligence, prayers, and respect in assisting me in completing this research work. Not to be forgotten is a heartfelt thank you to my HLP colleagues (Sharfah Ratibah binti Tuan Mat, Nurfateha binti Mohd Yamikazam, Norita binti Ahmad, and Halimah binti Ab Rahim), who provided invaluable advice and shared their expertise throughout this study.

Finally, I'd like to convey my gratefulness to everyone who assisted me, directly or indirectly, in making this research a success.

ABSTRAK

Peranti mudah alih Android merekodkan sejumlah besar pengguna dan boleh diakses melalui sumber terbuka. Keterbukaan peranti mudah alih Android sangat terdedah kepada serangan perisian hasad. Walaupun pelbagai antivirus atau peranti keselamatan dipasang dalam peranti mudah alih, pengguna masih terdedah kepada serangan perisian hasad. Penyerang sentiasa membuat perubahan mengikut trend semasa. Penyelesaian sebelumnya tidak mencukupi untuk mengurangkan serangan dengan ketara, kerana perisian hasad yang lebih baharu mahir mencari kelemahan Android. Kaedah pengesanan perisian hasad Google Play tidak mencukupi untuk mengimbas aplikasi pihak ketiga yang mungkin melanggar kerahsiaan pengguna. Mekanisme keselamatan Android, yang berdasarkan kebenaran, juga tidak mencukupi, mendedahkan pengguna mudah alih kepada persekitaran yang tidak selamat dan menjadikan mereka terdedah kepada serangan luaran. Pengguna mudah alih biasanya mengabaikan senarai kebenaran yang panjang kerana ketidakfahaman mereka. Oleh itu, aplikasi Android perlu dianalisis untuk memastikan aplikasi jinak atau perisian hasad dapat dibezakan serta risiko setiap permintaan kebenaran diketahui. Dalam pengesanan perisian hasad mudah alih, terdapat dua jenis analisis perisian hasad, yang termasuk analisis statik dan dinamik. Kajian ini memanfaatkan ciri kebenaran dan menekankan teknik analisis statik. Analisis statik meneliti program tanpa pelaksanaan aplikasi dan memberitahu kelakuannya. Kelebihan analisis statik ialah pengesanan pantas, keperluan sumber minimum dan ketepatan tinggi dalam mengesan perisian hasad. Matlamat penyelidikan ini adalah untuk mencadangkan penilaian risiko berasaskan proses hierarki analisis kabur untuk pengesanan perisian hasad dalam sistem mudah alih Android. Penilaian risiko digunakan untuk mendidik pengguna mudah alih tentang bahaya yang berkaitan dengan pemberian permintaan kebenaran. Bilangan permintaan kebenaran oleh setiap aplikasi Android diambil kira dalam menilai risiko serangan perisian hasad. Tiga teknik pengoptimuman seperti Particle Swarm Optimization (PSO), Information Gain dan Evolutionary Computational digunakan untuk memilih ciri kebenaran terbaik. Setiap kebenaran dibahagikan kepada kumpulan, dan skala perbandingan berpasangan kabur digunakan untuk menentukan wajaran setiap kumpulan kebenaran. Proses penilaian menggunakan 10,000 set data yang diperoleh daripada Drebin dan Androzoo. Selain itu, dapatan menunjukkan kadar ketepatan yang dicapai ialah 90.54% untuk pengesanan perisian hasad. Penilaian risiko secara berkesan mengkategorikan aplikasi Android kepada empat tahap risiko yang berbeza (sangat rendah, rendah, sederhana dan tinggi). Menurut analisis risiko, keluarga perisian hasad yang mempunyai tahap risiko tinggi ialah Plankton, ExploitLinuxLotoor dan SMSreg. Sifat dan kumpulan kebenaran mesej menunjukkan wajaran tertinggi dengan nilai 0.274 dan 0.273, masing-masing. Penemuan cemerlang kajian mengesahkan bahawa ciri kebenaran adalah penting untuk menilai perisian hasad serta analisis risiko pada aplikasi Android. Penilaian risiko dapat menemui pendedahan risiko kepada aplikasi Android dan memberikan pengetahuan kepada pengguna dengan menyediakan tahap risiko untuk meminimumkan serangan.

Kata kunci: Aplikasi Android, Analisis Statik, Sistem Pengesanan Perisian Hasad Mudah Alih, Penilaian Risiko.

ABSTRACT

Android mobile devices record a large number of users and are accessible via open source. The openness of the Android mobile devices is extremely vulnerable to malware attacks. Even though various antivirus or security devices are installed in the mobile device, users are still exposed to malware attacks. Attackers are constantly making changes according to current trends. Previous solutions are insufficient to significantly reduce attacks, as newer malware is skillful at finding Android vulnerabilities. Google Play's malware detection method is insufficient to scan third-party applications that may violate user confidentiality. Android security mechanism, which is based on permissions, is also insufficient, exposing mobile users to non-secure environments and making them susceptible to external attacks. Mobile users typically disregard lengthy lists of permissions due to their incomprehensibility. Therefore, Android applications need to be analysed to ensure that benign or malware applications can be distinguished as well as the risk of each permission request being known. In mobile malware detection, there are two types of malware analysis, which include static and dynamic analysis. This study leverages permission features and emphasises static analysis techniques. Static analysis examines programs without execution of the application and notifies its behaviour. The advantages of static analysis are fast detection, minimal resource requirements, and high accuracy in detecting malware. The goal of this research is to propose a fuzzy analytical hierarchy process based risk assessment for malware detection in Android mobile systems. Risk assessment is applied to educate mobile users about the dangers associated with granting permission requests. The number of permission requests by each Android application is taken into account in assessing the risk of malware attacks. The three optimization techniques such as Particle Swarm Optimisation (PSO), Information Gain and Evolutionary Computational are applied to select the best permission features. Each permission was divided into groups, and fuzzy pairwise comparison scale was applied to determine each permission group's weightage. The assessment process applied 10,000 datasets retrieved from Drebin and Androzoo. In addition, the findings show the accuracy rate achieved was 90.54% for malware detection. Risk assessment effectively categorised the Android application into four distinct risk levels (very low, low, medium, and high). According to risk analysis, the malware families with the high risk level are Plankton, ExploitLinuxLotoor, and SMSreg. Properties and message permission group indicate the highest weightage with value 0.274 and 0.273, respectively. The study's excellent findings confirmed that permission features are important for evaluating malware as well as risk analysis on an Android application. Risk assessment able to discover risk exposure to Android applications and provide knowledge to users by providing risk levels to minimize the attacks.

Keyword: Android applications, Static Analysis, Mobile Malware Detection System, Risk Assessment.

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

REFERENCES

Abawajy, J., Darem, A., & Alhashmi, A. A. (2021). Feature subset selection for malware detection in smart iot platforms. *Sensors (Switzerland)*, *21*(4), 1–19. https://doi.org/10.3390/s21041374

Abhijit Sarmah. (2019). *Intrusion Detection Systems: Definition, Need and Challenges*. https://www.sans.org/reading-room/whitepapers/detection/intrusion-detection-systems-definition-challenges-343

Abijah Roseline, S., & Geetha, S. (2021). A comprehensive survey of tools and techniques mitigating computer and mobile malware attacks. *Computers and Electrical Engineering*, *92*(March), 107143. https://doi.org/10.1016/j.compeleceng.2021.107143

Adebayo, O. S., & Aziz, N. A. (2019). Improved Malware Detection Model with Apriori Association Rule and Particle Swarm Optimization. *Security and Communication Networks*, *2019*. https://doi.org/10.1155/2019/2850932

Afifi, F., Anuar, N. B., Shamshirband, S., & Choo, K. K. R. (2016). DyHAP: Dynamic Hybrid ANFIS-PSO approach for predicting mobile malware. *PLoS ONE*, *11*(9), 1–21. https://doi.org/10.1371/journal.pone.0162627

Alali, M., Almogren, A., Hassan, M. M., Rassan, I. A. L., & Bhuiyan, M. Z. A. (2018). Improving risk assessment model of cyber security using fuzzy logic inference system. *Computers and Security*, *74*, 323–339. https://doi.org/10.1016/j.cose.2017.09.011

Alam, S., Alharbi, S. A., & Yildirim, S. (2020). Mining nested flow of dominant APIs for detecting android malware. *Computer Networks*, *167*, 107026. https://doi.org/10.1016/j.comnet.2019.107026

Alazab, M., Alazab, M., Shalaginov, A., Mesleh, A., & Awajan, A. (2020). Intelligent mobile malware detection using permission requests and API calls. *Future Generation Computer Systems*, *107*, 509–521. https://doi.org/10.1016/j.future.2020.02.002

Allix, K., Bissyandé, T. F., Jérome, Q., Klein, J., State, R., & Le Traon, Y. (2016). Empirical assessment of machine learning-based malware detectors for Android: Measuring the gap between in-the-lab and in-the-wild validation scenarios. *Empirical Software Engineering*, *21*(1), 183–211. https://doi.org/10.1007/s10664-014-9352-6

Altaher, A. (2017). An improved Android malware detection scheme based on an evolving hybrid neuro-fuzzy classifier (EHNFC) and permission-based features. *Neural Computing and Applications*, *28*(12), 4147–4157. https://doi.org/10.1007/s00521-016-2708-7

Alzaylaee, M. K., Yerima, S. Y., & Sezer, S. (2020). DL-Droid: Deep learning based android malware detection using real devices. *Computers and Security*, *89*. https://doi.org/10.1016/j.cose.2019.101663

Amin, M., Tanveer, T. A., Tehseen, M., Khan, M., Khan, F. A., & Anwar, S. (2020). Static malware detection and attribution in android byte-code through an end-to-end deep system. *Future Generation Computer Systems*, *102*, 112–126. https://doi.org/10.1016/j.future.2019.07.070

Ananya, A., Aswathy, A., Amal, T. R., Swathy, P. G., Vinod, P., & Mohammad, S. (2020). SysDroid: a dynamic ML-based android malware analyzer using system call traces. *Cluster Computing*, *23*(4), 2789–2808. https://doi.org/10.1007/s10586-019-03045-6

Arif, J. M., Faizal, M., Razak, A., Ratibah, S., Mat, T., Awang, S., Syahidatul, N., Ismail, N., & Firdaus, A. (2021). Android mobile malware detection using fuzzy AHP. *Journal of Information Security and Applications*, *61*(July), 102929. https://doi.org/10.1016/j.jisa.2021.102929

Arif, J. M., Razak, M. F. A., Awang, S., Tuan Mat, S. R., Ismail, N. S. N., & Firdaus, A. (2021). A static analysis approach for Android permission-based malware detection systems. *PLOS ONE*, *Idc*. https://doi.org/10.1371/journal.pone.0257968

Arslan, R. S., Dogru, I. A., & Barisci, N. (2019). Permission-Based Malware Detection System for Android Using Machine Learning Techniques. *International Journal of Software Engineering and Knowledge Engineering*, *29*(1), 43–61. https://doi.org/10.1142/S0218194019500037

Arzt, S., Rasthofer, S., Fritz, C., Bodden, E., Bartel, A., Klein, J., Le Traon, Y., Octeau, D., & McDaniel, P. (2014). FLOWDROID: Precise context, flow, field, object-sensitive and lifecycle-aware taint analysis for Android apps. *ACM SIGPLAN Notices*, *49*(6), 259–269. https://doi.org/10.1145/2594291.2594299

Baraiya, D., & Diwanji, P. H. (2017). A Survey on Android Malware Detection Techniques. *DEStech Transactions on Computer Science and Engineering*, *3*(wcne), 143–147. https://doi.org/10.12783/dtcse/wcne2016/5088

Bharathi, S. V. (2019). Forewarned is forearmed: Assessment of IoT information security risks using analytic hierarchy process. *Benchmarking*, *26*(8), 2443–2467. https://doi.org/10.1108/BIJ-08-2018-0264

Blanco-Mesa, F., Merigó, J. M., & Gil-Lafuente, A. M. (2017). Fuzzy decision making: A bibliometric-based review. *Journal of Intelligent and Fuzzy Systems*, *32*(3), 2033–2050. https://doi.org/10.3233/JIFS-161640

Burguera, I., Zurutuza, U., & Nadjm-Tehrani, S. (2011). Crowdroid: Behavior-based malware detection system for android. *Proceedings of the ACM Conference on Computer and Communications Security*, *May*, 15–25. https://doi.org/10.1145/2046614.2046619

Chebyshev, V. (2021a). *IT threat evolution Q1 2021. Mobile statistics.* https://securelist.com/it-threat-evolution-q1-2021-mobile-statistics/102547/

Chebyshev, V. (2021b). *Mobile malware evolution 2020*. https://securelist.com/mobile-malware-evolution-2020/101029/

Chen, S., Xue, M., Fan, L., Hao, S., Xu, L., Zhu, H., & Li, B. (2018). Automated poisoning attacks and defenses in malware detection systems: An adversarial machine learning approach. *Computers and Security*, *73*, 326–344. https://doi.org/10.1016/j.cose.2017.11.007

Chouhan, R. R. (2017). A Preface on Android Malware : Taxonomy , Techniques and Tools. *International Journal on Recent and Innovation Trends in Computing and Communication*, *June*, 1111–1117.

D'Angelo, G., Ficco, M., & Palmieri, F. (2020). Malware detection in mobile environments based on Autoencoders and API-images. *Journal of Parallel and Distributed Computing*, *137*, 26–33. https://doi.org/10.1016/j.jpdc.2019.11.001

De Lorenzo, A., Martinelli, F., Medvet, E., Mercaldo, F., & Santone, A. (2020). Visualizing the outcome of dynamic analysis of Android malware with VizMal. *Journal of Information Security and Applications*, *50*(2020), 102423. https://doi.org/10.1016/j.jisa.2019.102423

Dovom, E. M., Azmoodeh, A., Dehghantanha, A., Newton, D. E., Parizi, R. M., & Karimipour, H. (2019). Fuzzy pattern tree for edge malware detection and categorization in IoT. *Journal of Systems Architecture*, *97*(December 2018), 1–7. https://doi.org/10.1016/j.sysarc.2019.01.017

Edjossan-Sossou, A. M., Galvez, D., Deck, O., Al Heib, M., Verdel, T., Dupont, L., Chery, O., Camargo, M., & Morel, L. (2020). Sustainable risk management strategy selection using a fuzzy multi-criteria decision approach. *International Journal of Disaster Risk Reduction*, *45*(January), 101474. https://doi.org/10.1016/j.ijdrr.2020.101474

Enck, W., Gilbert, P., Chun, B. G., Cox, L. P., Jung, J., McDaniel, P., & Sheth, A. N. (2010). Taint droid: An information flow tracking system for real-time privacy monitoring on smartphones. *Communications of the ACM*, *57*(3), 99–106. https://doi.org/10.1145/2494522

Enck, W., Ongtang, M., & McDaniel, P. (2009). On lightweight mobile phone application certification. *Proceedings of the ACM Conference on Computer and Communications Security*, *May*, 235–245. https://doi.org/10.1145/1653662.1653691

Faruki, P., Ganmoor, V., Laxmi, V., Gaur, M. S., & Bharmal, A. (2013). AndroSimilar: Robust statistical feature signature for android malware detection. *SIN 2013 - Proceedings of the 6th International Conference on Security of Information and Networks*, *September 2015*, 152–159. https://doi.org/10.1145/2523514.2523539

Feizollah, A., Anuar, N. B., Salleh, R., Suarez-Tangil, G., & Furnell, S. (2017). AndroDialysis: Analysis of Android Intent Effectiveness in Malware Detection. *Computers and Security*, *65*, 121–134. https://doi.org/10.1016/j.cose.2016.11.007

Felt, A. P., Chin, E., Hanna, S., Song, D., & Wagner, D. (2011). Android permissions demystified. *Proceedings of the ACM Conference on Computer and Communications Security*, *October*, 627–636.

https://doi.org/10.1145/2046707.2046779

Firdaus, A., Anuar, N. B., Karim, A., & Razak, M. F. A. (2018). Discovering optimal features using static analysis and a genetic search based method for Android malware detection. *Frontiers of Information Technology and Electronic Engineering*, *19*(6), 712–736. https://doi.org/10.1631/FITEE.1601491

Firdaus, A., Anuar, N. B., Razak, M. F. A., & Sangaiah, A. K. (2018). Bio-inspired computational paradigm for feature investigation and malware detection: interactive analytics. *Multimedia Tools and Applications*, *77*(14), 17519–17555. https://doi.org/10.1007/s11042-017-4586-0

Garg, S., & Baliyan, N. (2019). Data on Vulnerability Detection in Android. *Data in Brief*, *22*, 1081–1087. https://doi.org/10.1016/j.dib.2018.12.038

Garg, S., & Baliyan, N. (2021). Android security assessment: A review, taxonomy and research gap study. *Computers and Security*, *100*, 102087. https://doi.org/10.1016/j.cose.2020.102087

Goyal, R. K., Kaushal, S., & Sangaiah, A. K. (2018). The utility based non-linear fuzzy AHP optimization model for network selection in heterogeneous wireless networks. *Applied Soft Computing Journal*, *67*, 800–811. https://doi.org/10.1016/j.asoc.2017.05.026

Grace, M., Zhou, Y., Zhang, Q., Zou, S., & Jiang, X. (2012). RiskRanker: Scalable and accurate zero-day android malware detection. *MobiSys'12 - Proceedings of the 10th International Conference on Mobile Systems, Applications, and Services*, 281–293. https://doi.org/10.1145/2307636.2307663

Gyamfi, N. K. (2018). *Survey of Mobile Malware Analysis, Detection Techniques and Tool*. 1101–1107.

Hornyack, P., Han, S., Jung, J., Schechter, S., & Wetherall, D. (2011). "These aren't the droids you're looking for": Retrofitting android to protect data from imperious applications. *Proceedings of the ACM Conference on Computer and Communications Security*, *May*, 639–651. https://doi.org/10.1145/2046707.2046780

IDC. (2019). *Smartphone Market Share*. https://www.idc.com/promo/smartphone-market-share/os

Imtiaz, S. I., Rehman, S. ur, Javed, A. R., Jalil, Z., Liu, X., & Alnumay, W. S. (2021). DeepAMD: Detection and identification of Android malware using high-efficient Deep Artificial Neural Network. *Future Generation Computer Systems*, *115*, 844–856. https://doi.org/10.1016/j.future.2020.10.008

Irolla, P., & Dey, A. (2018). The duplication issue within the Drebin dataset. *Journal of Computer Virology and Hacking Techniques*, 1–5. https://doi.org/10.1007/s11416-018-0316-z

Jablonský, J. (2017). Mathematical Methods in Economics (MME 2017) international conference. *Statistika*, *97*(4), 283–288.

Jaiganesh, M., Sivakami, R., & Kumar, A. V. A. (2019). Secure isolation of cloud consumers legitimacy using fuzzy analytical hierarchy process (AHP). *The Journal of Analysis*, *27*(2), 311–326. https://doi.org/10.1007/s41478-018-0127-0

Jerlin, M. A., & Marimuthu, K. (2018). A New Malware Detection System Using Machine Learning Techniques for API Call Sequences. *Journal of Applied Security Research*, *13*(1), 45–62. https://doi.org/10.1080/19361610.2018.1387734

Kaganski, S., Majak, J., & Karjust, K. (2018). Fuzzy AHP as a tool for prioritization of key performance indicators. *Procedia CIRP*, *72*, 1227–1232. https://doi.org/10.1016/j.procir.2018.03.097

Kakavand, M., Dabbagh, M., & Dehghantanha, A. (2018). Application of machine learning algorithms for android malware detection. *ACM International Conference Proceeding Series*, 32–36. https://doi.org/10.1145/3293475.3293489

Karbab, E. M. B., Debbabi, M., Derhab, A., & Mouheb, D. (2018). MalDozer: Automatic framework for android malware detection using deep learning. *DFRWS 2018 EU - Proceedings of the 5th Annual DFRWS Europe*, *24*, S48–S59. https://doi.org/10.1016/j.diin.2018.01.007

Karimi, H., Sadeghi-Dastaki, M., & Javan, M. (2020). A fully fuzzy best–worst multi attribute decision making method with triangular fuzzy number: A case study of maintenance assessment in the hospitals. *Applied Soft Computing Journal*, *86*, 105882. https://doi.org/10.1016/j.asoc.2019.105882

Khan, A. A., Shameem, M., Kumar, R. R., Hussain, S., & Yan, X. (2019). Fuzzy AHP based prioritization and taxonomy of software process improvement success factors in global software development. *Applied Soft Computing Journal*, *83*, 105648. https://doi.org/10.1016/j.asoc.2019.105648

Khariwal, K., Singh, J., & Arora, A. (2020). IPDroid: Android malware detection using intents and permissions. *Proceedings of the World Conference on Smart Trends in Systems, Security and Sustainability, WS4 2020*, 197–202. https://doi.org/10.1109/WorldS450073.2020.9210414

Kim, H., Cho, T., Ahn, G. J., & Hyun Yi, J. (2018). Risk assessment of mobile applications based on machine learned malware dataset. *Multimedia Tools and Applications*, *77*(4), 5027–5042. https://doi.org/10.1007/s11042-017-4756-0

Kim, K., Kim, J., Ko, E., & Yi, J. H. (2020). Risk Assessment Scheme for Mobile Applications Based on Tree Boosting. *IEEE Access*, *8*, 48503–48514. https://doi.org/10.1109/ACCESS.2020.2979477

Kouliaridis, V., Kambourakis, G., Geneiatakis, D., & Potha, N. (2020). Two anatomists are better than one-Dual-level android malware detection. *Symmetry*, *12*(7), 1–21. https://doi.org/10.3390/sym12071128

Kumar, K. A., Raman, A., Gupta, C., & Pillai, R. R. (2020). The recent trends in malware evolution, detection and analysis for android devices. *Journal of Engineering Science and Technology Review*, *13*(4), 240–248. https://doi.org/10.25103/jestr.134.25

Li, H., Shen, L., Wang, Y., Feng, J., Tan, H., & Li, Z. (2021). Risk Measurement Method of Collusion Privilege Escalation Attacks for Android Apps Based on Feature Weight and Behavior Determination. *Security and Communication Networks*, *2021*. https://doi.org/10.1155/2021/8814844

Li, J., Sun, L., Yan, Q., Li, Z., Srisa-An, W., & Ye, H. (2018). Significant Permission Identification for Machine-Learning-Based Android Malware Detection. *IEEE Transactions on Industrial Informatics*, *14*(7), 3216–3225. https://doi.org/10.1109/TII.2017.2789219

Li, L., Bissyandé, T. F., Papadakis, M., Rasthofer, S., Bartel, A., Octeau, D., Klein, J., & Traon, L. (2017). Static analysis of android apps: A systematic literature review. *Information and Software Technology*, *88*, 67–95. https://doi.org/10.1016/j.infsof.2017.04.001

Liu, K., Xu, S., Xu, G., Zhang, M., Sun, D., & Liu, H. (2020). A Review of Android Malware Detection Approaches Based on Machine Learning. *IEEE Access*, *8*, 124579–124607. https://doi.org/10.1109/ACCESS.2020.3006143

Liu, X., Lin, Y., Li, H., & Zhang, J. (2020). A novel method for malware detection on ML-based visualization technique. *Computers and Security*, *89*. https://doi.org/10.1016/j.cose.2019.101682

Lubuva, H., Huang, Q., & Msonde, G. C. (2019). A Review of Static Malware Detection for Android Apps Permission Based on Deep Learning. *International Journal of Computer Networks and Applications*, *6*(5), 80. https://doi.org/10.22247/ijcna/2019/187292

Mahbub, T. N., Hossain, S. S., Akash, R. A., Reza, S. M. S., & Tasnim, Z. (2021). Implementing Fuzzy Analytical Hierarchy Process (FAHP) to Measure Malicious Behaviour of Codes in Smart Meter. *International Conference on Robotics, Electrical and Signal Processing Techniques*, 90–94. https://doi.org/10.1109/ICREST51555.2021.9331027

Malleswari, D. N., Dhavalya, A., Sai, V. D., & Srikanth, K. (2018). A detailed study on risk assessment of mobile app permissions. *International Journal of Engineering and Technology(UAE)*, *7*(1.1 Special Issue 1), 297–300. https://doi.org/10.14419/ijet.v7i1.1.9706

Mat, S. R. T., Razak, M. F. A., Kahar, M. N. M., Arif, J. M., Mohamad, S., & Firdaus, A. (2021). Towards a systematic description of the field using bibliometric analysis: malware evolution. In *Journal of Scientometrics* (Issue 0123456789). Springer International Publishing. https://doi.org/10.1007/s11192-020-03834-6

Mathur, A., Podila, L. M., Kulkarni, K., Niyaz, Q., & Javaid, A. Y. (2021). NATICUSdroid: A malware detection framework for Android using native and custom permissions. *Journal of Information Security and Applications*, *58*(January), 102696. https://doi.org/10.1016/j.jisa.2020.102696

Mehtab, A., Shahid, W. Bin, Yaqoob, T., Amjad, M. F., Abbas, H., Afzal, H., & Saqib, M. N. (2020). AdDroid: Rule-Based Machine Learning Framework for Android

Malware Analysis. *Mobile Networks and Applications*, *25*(1), 180–192. https://doi.org/10.1007/s11036-019-01248-0

Muylkens, E. (2019). Nokia Threat Intelligence Report – 2019. *Network Security*, *2019*(12), 4. https://doi.org/10.1016/s1353-4858(18)30122-3

Narudin, F. A., Feizollah, A., Anuar, N. B., & Gani, A. (2016). Evaluation of machine learning classifiers for mobile malware detection. *Soft Computing*, *20*(1), 343–357. https://doi.org/10.1007/s00500-014-1511-6

Naway, A., & Li, Y. (2018). A Review on The Use of Deep Learning in Android Malware Detection. *International Journal of Computer Science and Mobile Computing*, *7*(12), 42–58.

Pan, Y., Ge, X., Fang, C., & Fan, Y. (2020). A Systematic Literature Review of Android Malware Detection Using Static Analysis. *IEEE Access*, *8*, 116363–116379. https://doi.org/10.1109/ACCESS.2020.3002842

Patade, A., & Shekokar, N. (2019). An architecture for analysis of mobile botnet detection using machine learning. In *Communications in Computer and Information Science* (Vol. 1045). Springer Singapore. https://doi.org/10.1007/978-981-13-9939-8_12

Peiravian, N., & Zhu, X. (2013). Machine learning for Android malware detection using permission and API calls. *Proceedings - International Conference on Tools with Artificial Intelligence, ICTAI*, 300–305. https://doi.org/10.1109/ICTAI.2013.53

Portokalidis, G., Homburg, P., Anagnostakis, K., & Bos, H. (2010). Paranoid android: Versatile protection for smartphones. *Proceedings - Annual Computer Security Applications Conference, ACSAC, May 2014*, 347–356. https://doi.org/10.1145/1920261.1920313

Potha, N., Kouliaridis, V., & Kambourakis, G. (2020). An extrinsic random-based ensemble approach for android malware detection. *Connection Science*. https://doi.org/10.1080/09540091.2020.1853056

Qamar, A., Karim, A., & Chang, V. (2019). Mobile malware attacks: Review, taxonomy & future directions. *Future Generation Computer Systems*, *97*, 887–909. https://doi.org/10.1016/j.future.2019.03.007

Rabbani, M., Wang, Y. L., Khoshkangini, R., Jelodar, H., Zhao, R., & Hu, P. (2020). A hybrid machine learning approach for malicious behaviour detection and recognition in cloud computing. *Journal of Network and Computer Applications*, *151*(May 2019), 102507. https://doi.org/10.1016/j.jnca.2019.102507

Rajak, M., & Shaw, K. (2019). Evaluation and selection of mobile health (mHealth) applications using AHP and fuzzy TOPSIS. *Technology in Society*, *59*(August), 101186. https://doi.org/10.1016/j.techsoc.2019.101186

Ramík, J., & Korviny, P. (2010). Inconsistency of pair-wise comparison matrix with fuzzy elements based on geometric mean. *Fuzzy Sets and Systems*, *161*(11), 1604–1613. https://doi.org/10.1016/j.fss.2009.10.011

Rashidi, B., Fung, C., & Bertino, E. (2017). Android resource usage risk assessment using hidden Markov model and online learning. *Computers and Security*, *65*, 90–107. https://doi.org/10.1016/j.cose.2016.11.006

Razak, M. F. A., Anuar, N. B., Othman, F., Firdaus, A., Afifi, F., & Salleh, R. (2018). Bio-inspired for Features Optimization and Malware Detection. *Arabian Journal for Science and Engineering*, *43*(12), 6963–6979. https://doi.org/10.1007/s13369-017-2951-y

Razak, M. F. A., Anuar, N. B., Salleh, R., & Firdaus, A. (2016). The rise of "malware": Bibliometric analysis of malware study. *Journal of Network and Computer Applications*, *75*, 58–76. https://doi.org/10.1016/j.jnca.2016.08.022

Razak, M. F. A., Anuar, N. B., Salleh, R., Firdaus, A., Faiz, M., & Alamri, H. S. (2018). "Less Give More": Evaluate and zoning Android applications. *Measurement: Journal of the International Measurement Confederation*, *133*, 396–411.

Salah, A., Shalabi, E., & Khedr, W. (2020). A lightweight android malware classifier using novel feature selection methods. *Symmetry*, *12*(5), 1–16. https://doi.org/10.3390/SYM12050858

Salah, Y., Hamed, I., Nabil, S., Abdulkader, A., & Mostafa, M. M. (2019). Mobile Malware Detection : A Survey. *International Journal of Computer Science and Information Security*, *17*(1).

Sharma, A., Gandotra, E., Bansal, D., & Gupta, D. (2019). Malware Capability Assessment using Fuzzy Logic. *Cybernetics and Systems*, *50*(4), 323–338. https://doi.org/10.1080/01969722.2018.1552906

Shiqi, L., Shengwei, T., Long, Y., Jiong, Y., & Hua, S. (2018). Android malicious code classification using deep belief network. *KSII Transactions on Internet and Information Systems*, *12*(1), 454–475. https://doi.org/10.3837/tiis.2018.01.022

Sihag, V., Vardhan, M., & Singh, P. (2021). A survey of android application and malware hardening. *Computer Science Review*, *39*, 100365. https://doi.org/10.1016/j.cosrev.2021.100365

Taheri, R., Ghahramani, M., Javidan, R., Shojafar, M., Pooranian, Z., & Conti, M. (2020). Similarity-based Android Malware Detection Using Hamming Distance of Static Binary Features. *Future Generation Computer Systems*, *105*, 230–247. https://doi.org/10.1016/j.future.2019.11.034

Thapa, S. (2017). *Fuzzy Based DBSCAN Text Mining Technique for Malware Detection*. *8*(5).

Tuan Mat, S. R., Razak, M. F. A., Kahar, M. N. M., Arif, J. M., & Zabidi, A. (2021). Applying Bayesian probability for Android malware detection using permission features. *2021 International Conference on Software Engineering & Computer Systems and 4th International Conference on Computational Science and Information Management (ICSECS-ICOCSIM)*, 574–579. https://doi.org/10.1109/icsecs52883.2021.00111

Wang, G., & De Baets, B. (2018). *Advances in Fuzzy Logic and Technology 2017*. *641*. https://doi.org/10.1007/978-3-319-66830-7

Xu, R., Saïdi, H., & Anderson, R. (2012). Aurasium: Practical policy enforcement for android applications. *Proceedings of the 21st USENIX Security Symposium, January 2012*, 539–552.

Yan, L. K., & Yin, H. (2012). DroidScope: Seamlessly reconstructing the os and dalvik semantic views for dynamic android malware analysis. *Proceedings of the 21st USENIX Security Symposium, January 2012*, 569–584.

Yan, P., & Yan, Z. (2018). A survey on dynamic mobile malware detection. *Software Qual J*, *May 2017*, 891–919. https://doi.org/10.1007/s11219-017-9368-4

Zaburko, J., & Szulzyk-Cieplak, J. (2019). Information security risk assessment using the AHP method. *IOP Conference Series: Materials Science and Engineering*, *710*(1). https://doi.org/10.1088/1757-899X/710/1/012036