ANDROID MOBILE MALWARE DETECTION MODEL BASED ON PERMISSION FEATURES USING MACHINE LEARNING APPROACH

SHARFAH RATIBAH BINTI TUAN MAT

MASTER OF SCIENCE

UNIVERSITI MALAYSIA PAHANG

Universiti Malaysia PAHANG
Engineering • Technology • Creativity

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 : TS. DR. MOHD FAIZAL BIN AB RAZAK
Position : SENIOR LECTURER
Date : 18 JANUARY 2022

(Co-supervisor's Signature)

Full Name : DR. MOHD NIZAM BIN MOHMAD KAHAR
Position : ASSOCIATE PROFESSOR
Date : 18 JANUARY 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 : SHARFAH RATIBAH BINTI TUAN MAT

ID Number : MCN19003

Date : 18 JANUARY 2022

ANDROID MOBILE MALWARE DETECTION MODEL BASED ON PERMISSION FEATURES USING MACHINE LEARNING APPROACH

SHARFAH RATIBAH BINTI TUAN MAT

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

Faculty of Computing

UNIVERSITI MALAYSIA PAHANG

JANUARY 2022

ACKNOWLEDGEMENTS

Praise and thanks be to Allah for His grace and love. The endurance, blessing, perseverance from Him is my main pillar to start and went through this tough journey to end.

I'd like to convey my sincere gratitude to my supervisors, Dr. Mohd Faizal b Ab Razak and Professor Madya Dr. Mohd Nizam b Mohmad Kahar for the constant guidance, patience, encouragement throughout this study, and uncountable knowledge for my learning in the University Malaysia Pahang. Their leadership supported me in my study, publishing and thesis writing. Their countless efforts have further encouraged me to work hard so as to achieve the milestones in a defined time limit.

I would like to thank scholarship program, Hadiah Latihan Persekutuan (HLP) that support my study. Great appreciation also to Ministry of Higher Education for funding via FRGS under project ID: RACER/1/2019/ICT03/UMP//2(RDU192613).

I would like to express my deepest appreciation to my family for their unconditional love and encouragement completely my life. My heartfelt gratitude goes to my husband (Mohd Zulkifli Amin b Salleh), my mother (Rahimah bt Hassan), my daughters (Syafiqah Alyaa, Syakirah Auni) and my sons (Syakir Alif, Syareef Aqeef and Syahir Aqil). Their understanding and supporting during the journey of my study are very meaningful. Also dedicated to my late father (Tuan Mat @Syed Ali) who ever gave me motivations, taught and showed the reality sense of life.

Last, but, not least, I'd like to share my gratitude to my lab partner (Juliza bt Mohamad Arif), who had a stimulating discussion and working together before the deadline. Also, I’d like to thank my HLP friends (Nurfateha, Norita and Halimah) for always being there for me and inspiring me when I was stuck. We started this study together at the beginning and I wish them happiness and success.

Finally, I would like to thank the Faculty of Computing for its help in enabling me to deal with all sorts of matter during my studies.

ABSTRAK

Penggunaan peranti mudah alih Android telah meningkat dengan pesat dan meraih populariti yang besar dalam pasaran peranti mudah alih. Ia telah menjadi barang paling berharga di seluruh dunia. Populariti dan sistem operasi utama peranti mudah alih Android telah menimbulkan kebimbangan terhadap ancaman perisian hasad. Pengarang yang tidak bertanggungjawab dengan sengaja menggunakan perisian berbahaya seperti root exploit, botnet, Trojan horse, dan spyware dan diterbitkan di Google Play untuk memperoleh keuntungan khusus untuk diri mereka sendiri. Perisian hasad Android ini mempunyai kecekapan untuk mencuri maklumat sulit pengguna dan mengubah sumber maklumat pengguna. Pelbagai teknik yang berbeza telah diadaptasi untuk mengesan dan mencegah penyebaran malware Android, termasuk teknik pengesanan anomali, berdasarkan tanda tangan, dan teknik pengesanan hibrid. Walaupun begitu, teknologi terkini menunjukkan bahawa penyerang perisian hasad Android menemui kaedah yang lebih canggih untuk mengelak daripada dikesan. Kajian ini bertujuan untuk mencadangkan sistem pengesanan perisian hasad Android menggunakan pengelas Bayesian dan pengelas Multilayer perceptron melalui teknik analisis statik untuk memerangi masalah perisian hasad Android. Kajian ini memfokuskan ciri kebenaran pada peranti mudah alih Android. Di samping itu, kajian ini menggunakan dua jenis set data yang diambil daripada Androzoo untuk aplikasi baik dan Drebin untuk aplikasi hasad. Set data pertama mengandungi 10,000 sampel, dan kumpulan data kedua mengandungi 96,074 sampel. Dalam kajian ini, beberapa eksperimen dilakukan untuk mempelajari tingkah laku ciri kebenaran dan mencari ketepatan terbaik mengikut pendekatan yang digunakan. *Chi-square* dan *information gain* adalah dua algoritma yang digunakan dalam pemilihan ciri. Ini bertujuan untuk mengetahui tingkah laku ciri kebenaran yang bertindak balas terhadap ketepatan mengikut bilangan ciri. Kedua-dua sampel set data kemudiannya akan dinilai menggunakan pendekatan pembelajaran mesin dan pembelajaran mendalam dipilih untuk mendapatkan ketepatan terbaik dalam proses pengesanan perisian hasad. Pengesanan melalui pembelajaran mesin memperoleh ketepatan sebanyak 85.4% bagi 96,074 sampel dan 91.1% bagi 10,000 sampel. Manakala pengesanan menggunakan pembelajaran mendalam memperolehi ketepatan sebanyak 98.02% bagi 96,074 sampel dan 98% bagi 10,000 sampel. Kesimpulannya, ketepatan pembelajaran mendalam sesuai bagi set data yang besar dan juga set data yang kecil manakala pembelajaran mesin menghasilkan pengesanan yang baik dalam set data yang lebih kecil.

ABSTRACT

The use of Android mobile devices has increased exponentially and gained massive popularity in the mobile market. It has become the most valuable item to humans across the world. The popularity and primary operating system of the Android mobile device have raised concerns over malware threats. Unscrupulous authors have deployed malicious software such as root exploit, botnet, Trojan horse, and spyware and published it on Google Play to gain profits. Android malware has the ability to abduct user credentials and cause a resource to maltreat. Different techniques have been adopted to detect and prevent the spread of Android malware, including anomaly, signature-based, and hybrid detection techniques. Nevertheless, current technologies indicate that Android malware attackers have find novel ways to avoid detection. This study aims to propose an Android malware detection model using Bayesian classifier and Multilayer perceptron classifier via static analysis technique to address the Android malware issue. This study focused on the permission feature of Android mobile devices. This study obtained two types of datasets which were retrieved from Androzoo and Drebin database. The first dataset contains 10,000 samples, and the second dataset contains 96,074 samples. Several experiments were conducted to learn the permission features' behaviour and find the best accuracy for the approaches used. Chi-square and information gain algorithms were used for features selection. The aim is to learn the behaviour of permission features that react to the accuracy according to the number of features. Both samples of datasets then were evaluated using machine learning and deep learning approaches to analyse the best accuracy of malware detection. The validation of machine learning obtained 85.4% accuracy for 96,074 samples and 91.1% accuracy for 10,000 samples. The validation in deep learning obtained 98.02% accuracy for the 96,074 samples and 98% accuracy for the 10,000 samples. These best achievements for both datasets were from the deep learning approach. In conclusion, the accuracy of deep learning is always greater in smaller or larger datasets, and machine learning produces great detection in smaller datasets.

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

REFERENCES

Abri, F., Siami-Namini, S., Khanghah, M. A., Soltani, F. M., & Namin, A. S. (2019). Can Machine/Deep Learning Classifiers Detect Zero-Day Malware with High Accuracy? *Proceedings - 2019 IEEE International Conference on Big Data, Big Data 2019*, 3252–3259. https://doi.org/10.1109/BigData47090.2019.9006514

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

Agrawal, A. (2015). *Android Application Security Part 2-Understanding Android Operating System*. Manifestsecurity. https://manifestsecurity.com/android-application-security-part-2/

Ali, W. (2019). *Hybrid Intelligent Android Malware Detection Using Evolving Support Vector Machine Based on Genetic Algorithm and Particle Swarm Optimization*. *19*(9), 15–28.

Allix, K., Bissyandé, T. F., Klein, J., & Le Traon, Y. (2016). AndroZoo: Collecting millions of Android apps for the research community. *Proceedings - 13th Working Conference on Mining Software Repositories, MSR 2016*, 468–471. https://doi.org/10.1145/2901739.2903508

Almin, S. B., & Chatterjee, M. (2015). A novel approach to detect Android malware. *Procedia Computer Science*, *45*(C), 407–417. https://doi.org/10.1016/j.procs.2015.03.170

Alzaylaee, M. K., Yerima, S. Y., & Sezer, S. (2020). DL-Droid: Deep learning based android malware detection using real devices. *Computers and Security*, *89*, 101663. https://doi.org/10.1016/j.cose.2019.101663

Amin, M., Shehwar, D., Ullah, A., Guarda, T., Tanveer, T. A., & Anwar, S. (2020). A deep learning system for health care IoT and smartphone malware detection. *Neural Computing and Applications*, *0123456789*. https://doi.org/10.1007/s00521-020-05429-x

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

An, N., Duff, A., Naik, G., Faloutsos, M., Weber, S., & Mancoridis, S. (2018). Behavioral anomaly detection of malware on home routers. *Proceedings of the 2017 12th International Conference on Malicious and Unwanted Software, MALWARE 2017*, *2018-Janua*, 47–54. https://doi.org/10.1109/MALWARE.2017.8323956

Anwar, S., Zain, J. M., Zolkipli, M. F., Inayat, Z., Khan, S., Anthony, B., & Chang, V. (2017). From intrusion detection to an intrusion response system: Fundamentals, requirements, and future directions. *Algorithms*, *10*(2). https://doi.org/10.3390/a10020039

Awareness, S. (2020). *6 Common Phishing Attacks and How to Protect Against Them*. Tripwire. https://www.tripwire.com/state-of-security/security-awareness/6-common-phishing-attacks-and-how-to-protect-against-them/

Belaoued, M., Boukellal, A., Koalal, M. A., Derhab, A., Mazouzi, S., & Khan, F. A. (2019). Combined dynamic multi-feature and rule-based behavior for accurate malware detection. *International Journal of Distributed Sensor Networks*, *15*(11). https://doi.org/10.1177/1550147719889907

Besharati, E., Naderan, M., & Namjoo, E. (2018). LR-HIDS: logistic regression host-based intrusion detection system for cloud environments. *Journal of Ambient Intelligence and Humanized Computing*, *0*(0), 0. https://doi.org/10.1007/s12652-018-1093-8

Betacrash. (2018). *The App Store Celebrates 10 Years and 2 Million Apps*. Betacrash. http://betacrash.com/app-store/

Bhatt, D. (2019). Machine Learning versus Deep Learning. *Studytonight.Com*. https://www.studytonight.com/post/machine-learning-versus-deep-learning

Borges, E. (2021). *Top 10 Common Network Security Threats Explained*. Securitytrails. https://securitytrails.com/blog/top-10-common-network-security-threats-explained

Cecere, G., Corrocher, N., & Battaglia, R. D. (2015). Innovation and competition in the smartphone industry: Is there a dominant design? *Telecommunications Policy*, *39*(3–4), 162–175. https://doi.org/10.1016/j.telpol.2014.07.002

Cen, L., Gates, C. S., Si, L., & Li, N. (2015). A Probabilistic Discriminative Model for Android Malware Detection with Decompiled Source Code. *IEEE Transactions on Dependable and Secure Computing*, *12*(4), 400–412. https://doi.org/10.1109/TDSC.2014.2355839

Chandler, C. L., & E, B. S. E. (1990). *CERTAINTY FACTOR DETERMINATION IN A RULE-BASED EXPERT by IN Submitted to the Graduate Faculty of Texas Tech University in the Requirements for IN*.

Claris. (2018). *Newzoo: Smartphone users will top 3 billion in 2018, hit 3.8 billion by 2021*. Dean Takahashi. https://venturebeat.com/2018/09/11/newzoo-smartphone-users-will-top-3-billion-in-2018-hit-3-8-billion-by-2021/

Clausing, J. (2021). *5-ways-hackers-get-to-your-mobile-device*. AT&T Business. https://www.business.att.com/learn/tech-advice/5-ways-hackers-get-to-your-mobile-device.html

Clemens, J. (2015). Automatic classification of object code using machine learning. *Proceedings of the Digital Forensic Research Conference, DFRWS 2015 USA*, *14*, S156–S162. https://doi.org/10.1016/j.diin.2015.05.007

Computer Hope. (2019). *Computer vs. smartphone*. Computer Hope. https://www.computerhope.com/issues/ch001398.htm

Curry, D. (2021). *Android Statistics (2021)*. Business of Apps. https://www.businessofapps.com/data/android-statistics/

Dassanayake, D. (2021). *Millions of Android phones infected by dangerous malware, these phones are at risk*. Express25. https://www.express.co.uk/life-style/science-technology/1527645/Millions-Android-phones-infected-dangerous-malware-these-phones-at-risk

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*, 102423. https://doi.org/10.1016/j.jisa.2019.102423

Deshpande, P., Sharma, S. C., Peddoju, S. K., & Junaid, S. (2018). HIDS: A host based intrusion detection system for cloud computing environment. *International Journal of Systems Assurance Engineering and Management*, *9*(3), 567–576. https://doi.org/10.1007/s13198-014-0277-7

Deviceatlas. (2020). *15 Mobile Web Predictions for 2020*. Deviceatlas. https://deviceatlas.com/blog/15-mobile-web-predictions-2020

Employee, N. (2017). *5 mobile security threats you can protect yourself from*. Norton. https://us.norton.com/internetsecurity-mobile-types-of-common-mobile-threats-and-what-they-can-do-to-your-phone.html

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

Feizollah, A., Anuar, N. B., Salleh, R., & Wahab, A. W. A. (2015). A review on feature selection in mobile malware detection. *Digital Investigation*, *13*, 22–37. https://doi.org/10.1016/j.diin.2015.02.001

Felt, A. P., Finifter, M., Chin, E., Hanna, S., & Wagner, D. (2011). A survey of mobile malware in the wild. *Proceedings of the ACM Conference on Computer and Communications Security*, 3–14. https://doi.org/10.1145/2046614.2046618

Feng, R., Chen, S., Xie, X., Meng, G., Lin, S. W., & Liu, Y. (2021). A Performance-Sensitive Malware Detection System Using Deep Learning on Mobile Devices. *IEEE Transactions on Information Forensics and Security*, *16*(XX), 1563–1578. https://doi.org/10.1109/TIFS.2020.3025436

Georgiev, D. (2021). *39+ Smartphone Statistics You Should Know in 2020*. Review42. https://review42.com/smartphone-statistics/

Guanghui Sun. (2020). Thiết kế và triển khai hệ thống quản lý thể thao trường học dựa trên WEB. In *Springer Nature Thụy Sĩ AG 2020*. Springer International Publishing. https://doi.org/10.1007/978-3-030-15235-2

Haider, W., Creech, G., Xie, Y., & Hu, J. (2016). Windows based data sets for evaluation of robustness of Host based Intrusion Detection Systems (IDS) to zero-day and stealth attacks. *Future Internet*, *8*(3). https://doi.org/10.3390/fi8030029

Hootsuite. (2020). *Digital Around The World*. Datareportal. https://datareportal.com/global-digital-overview

Hu, X. L., Zhang, L. C., & Wang, Z. X. (2018). An adaptive smartphone anomaly detection model based on data mining. *Eurasip Journal on Wireless Communications and Networking*, *2018*(1). https://doi.org/10.1186/s13638-018-1158-6

Huda, S., Islam, R., Abawajy, J., Yearwood, J., Hassan, M. M., & Fortino, G. (2018). A hybrid-multi filter-wrapper framework to identify run-time behaviour for fast malware detection. *Future Generation Computer Systems, 83,* 193–207. https://doi.org/10.1016/j.future.2017.12.037

Ictbuz.com. (2021). *Top 20 Mobile Phone Brands in the World 2021*. ICTbuz. https://ictbuz.com/top-mobile-phone-brands/

IDC. (2020). *Smartphone Market Share*. IDC. https://www.idc.com/promo/smartphone-market-share/os

IDC. (2021). *Smartphone Shipments Return to Positive Growth in the Fourth Quarter Driven by Record Performance by Apple, According to IDC*. IDC. https://www.idc.com/getdoc.jsp?containerId=prUS47410621

Inayat, Z., Gani, A., Anuar, N. B., Khan, M. K., & Anwar, S. (2016). Intrusion response systems: Foundations, design, and challenges. *Journal of Network and Computer Applications*, *62*, 53–74. https://doi.org/10.1016/j.jnca.2015.12.006

JavaTpoint. (2020). *Android versions*. JavaTpoint. https://www.javatpoint.com/android-versions

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

Jha, S., Prashar, D., Long, H. V., & Taniar, D. (2020). Recurrent neural network for detecting malware. *Computers and Security*, *99*, 102037. https://doi.org/10.1016/j.cose.2020.102037

Jose, S., Malathi, D., Reddy, B., & Jayaseeli, D. (2018). A Survey on Anomaly Based Host Intrusion Detection System. *Journal of Physics: Conference Series*, *1000*(1). https://doi.org/10.1088/1742-6596/1000/1/012049

Kaspersky. (2019). *https://www.kaspersky.com/resource-center/threats/top-seven-mobile-security-threats-smart-phones-tablets-and-mobile-internet-devices-what-the-future-has-in-store*. https://www.kaspersky.com/resource-center/threats/top-seven-mobile-security-threats-smart-phones-tablets-and-mobile-internet-devices-what-the-future-has-in-store

KerdaZz. (2020). *Phone evolution*. Shutterstock. https://www.shutterstock.com/image-vector/vector-set-phone-icons-flat-design-718948519

Knowbility. (2019). *Online Native App Accessibility Workshop*. Knowbility. https://knowbility.org/services/training/ios-android-workshop/

Koucham, O., Rachidi, T., & Assem, N. (2015). Host intrusion detection using system call argument-based clustering combined with Bayesian classification. *IntelliSys 2015 - Proceedings of 2015 SAI Intelligent Systems Conference*, 1010–1016. https://doi.org/10.1109/IntelliSys.2015.7361267

Koyuncu, M., & Pusatli, T. (2019). Security Awareness Level of Smartphone Users: An Exploratory Case Study. *Mobile Information Systems*, *2019*. https://doi.org/10.1155/2019/2786913

Kumar, G. S., & Bagane, P. (2020). Detection of malware using deep learning techniques. *International Journal of Scientific and Technology Research*, *9*(1), 1688–1691.

Kumari, A., & Sood, M. (2021). Performance analysis of the ml prediction models for the detection of sybil accounts in an osn. In *Advances in Intelligent Systems and Computing* (Vol. 1166). Springer Singapore. https://doi.org/10.1007/978-981-15-5148-2_60

Lanet, J., Eds, C. T., Conference, I., & Hutchison, D. (2018). *for Information Technology*. Springer International Publishing. https://doi.org/10.1007/978-3-030-12942-2

Lemos, R. (2020). *Google Bouncer Vulnerabilities Probed by Security Researchers*. Eweek. https://www.eweek.com/security/google-bouncer-vulnerabilities-probed-by-security-researchers

Liang, J., Chen, J., Zhu, Y., & Yu, R. (2019). A novel Intrusion Detection System for Vehicular Ad Hoc Networks (VANETs) based on differences of traffic flow and position. *Applied Soft Computing Journal*, *75*, 712–727. https://doi.org/10.1016/j.asoc.2018.12.001

Linkedin. (2021). *About Us*. Linkedin. https://www.linkedin.com/company/virustotal

Liu, C. H., Zhang, Z. J., & Wang, S. De. (2017). An android malware detection approach using Bayesian inference. *Proceedings - 2016 16th IEEE International Conference on Computer and Information Technology, CIT 2016, 2016 6th International Symposium on Cloud and Service Computing, IEEE SC2 2016 and 2016 International Symposium on Security and Privacy in Social Netwo*, 476–483. https://doi.org/10.1109/CIT.2016.76

Ljubas, Z. (2020). *IT Specialists Warn of Malware Increase During COVID-19*. OCCRP. https://www.occrp.org/en/daily/12509-it-specialists-warn-of-malware-increase-during-covid-19

Lohrmann, D. (2020). *Ransomware During COVID-19*. Goverment Technology. The growing of mobile threat are getting harmful in recent years as much humans depend on phone everyday task.

Long, D. H., Nikolaevich, T. V., Tuan, D. M., Tuan, N. A., & Lam, N. T. (2020). Detecting malware using the mlp algorithm. *International Journal of Advanced Trends in Computer Science and Engineering*, *9*(4), 5640–5644. https://doi.org/10.30534/ijatcse/2020/214942020

Lopes, J., Serrão, C., Nunes, L., Almeida, A., & Oliveira, J. (2019). Overview of machine learning methods for Android malware identification. *7th International Symposium on Digital Forensics and Security, ISDFS 2019*, 1–6. https://doi.org/10.1109/ISDFS.2019.8757523

Love, J. (2018). *Malware Types and Classifications*. Lastline. https://www.lastline.com/blog/malware-types-and-classifications/

Mas'ud, M. Z., Sahib, S. S., Abdollah, M. F., Selamat, S. R., & Yusof, R. (2014). Android malware detection system classification. *Research Journal of Information Technology*, *6*(4), 325–341. https://doi.org/10.3923/rjit.2014.325.341

Mat, S. R. T., Ab Razak, M. F., 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 *Scientometrics* (Vol. 126, Issue 3). Springer International Publishing. https://doi.org/10.1007/s11192-020-03834-6

Microsoft. (2019). *https://docs.microsoft.com/en-us/legal/windows/agreements/app-developer-agreement*. https://docs.microsoft.com/en-us/legal/windows/agreements/app-developer-agreement

Mobiforge. (2019). *https://mobiforge.com/timeline/windows-phone-history*. https://mobiforge.com/timeline/windows-phone-history

Mohamad Arif, J., Ab Razak, M. F., 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*, *16*(9), e0257968. https://doi.org/10.1371/journal.pone.0257968

Moon, D., Pan, S. B., & Kim, I. (2016). Host-based intrusion detection system for secure human-centric computing. *Journal of Supercomputing*, *72*(7), 2520–2536. https://doi.org/10.1007/s11227-015-1506-9

Moran, D. (2020). *ANDROID MALWARE TAKES ADVANTAGE OF COVID-19*. Buguroo. https://www.buguroo.com/en/labs/android-malware-takes-advantage-of-covid-19

Mutlag, A. A., Abd Ghani, M. K., Arunkumar, N., Mohammed, M. A., & Mohd, O. (2019). Enabling technologies for fog computing in healthcare IoT systems. *Future Generation Computer Systems*, *90*, 62–78. https://doi.org/10.1016/j.future.2018.07.049

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

Nasri, N. N. M., Razak, M. F. A., Saedudin, R. D. R., Mohamad-Asmara, S., & Firdaus, A. (2020). Android malware detection system using machine learning. *International Journal of Advanced Trends in Computer Science and Engineering*, *9*(1 Special Issue 5), 327–333. https://doi.org/10.30534/ijatcse/2020/4691.52020

Niazi, R. A., & Faheem, Y. (2019). A Bayesian Game-Theoretic Intrusion Detection System for Hypervisor-Based Software Defined Networks in Smart Grids. *IEEE Access*, *7*, 88656–88672. https://doi.org/10.1109/ACCESS.2019.2924968

O'Dea, S. (2020). *Forecast number of mobile users worldwide from 2020 to 2024*. Statista. https://www.statista.com/statistics/218984/number-of-global-mobile-users-since-2010/

Or-Meir, O., Nissim, N., Elovici, Y., & Rokach, L. (2019). Dynamic malware analysis in the modern era—A state of the art survey. *ACM Computing Surveys*, *52*(5). https://doi.org/10.1145/3329786

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

Potteti, S., & Parati, N. (2015). Design of Intrusion Detection System for Internet of Things Based on Improved BP Neural Network. *International Journal of Engineering and Computer Science*, *4*(5), 12146–12151.

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

Qasim, O., & Al-Saedi, K. (2017). Malware Detection using Data Mining Naïve Bayesian Classification Technique with Worm Dataset. *International Journal of Advanced Research in Computer and Communication Engineering*, *6*(11), 211–213. https://doi.org/10.17148/IJARCCE.2017.61131

Rafter, D. (2021). *Android vs. iOS: Which is more secure?* Norton. https://us.norton.com/internetsecurity-mobile-android-vs-ios-which-is-more-secure.html

Razak, M. F. A. (2018). *A malware risk analysis and detection system for mobile devices using permission- based features faculty of computer science and information technology*.

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

Rehman, Z. U., Khan, S. N., Muhammad, K., Lee, J. W., Lv, Z., Baik, S. W., Shah, P. A., Awan, K., & Mehmood, I. (2018). Machine learning-assisted signature and heuristic-based detection of malwares in Android devices. *Computers and Electrical Engineering*, *69*, 828–841. https://doi.org/10.1016/j.compeleceng.2017.11.028

Salah, Y., Hamed, I., Nabil, S., Abdulkader, A., & Mostafa, M. M. (2019). *Mobile Malware Detection : A Survey*. *17*(1).

Saxena, V., Shrivastava, S., & Mourya, S. (2016). Behavior Analysis of Android malware detection for Smart phone. *International Journal of Engineering Research & Science*, *2*(12), 55–60.

Sean O'dea. (2020). *Number of smartphones sold to end users worldwide from 2007 to 2021*. Statista. https://www.statista.com/statistics/263437/global-smartphone-sales-to-end-users-since-2007/

Sean O'Dea. (2020a). *Forecast number of mobile devices worldwide from 2020 to 2024*. Statista. https://www.statista.com/statistics/245501/multiple-mobile-device-ownership-worldwide/

Sean O'Dea. (2020b). *Mobile operating systems' market share worldwide from January 2012 to October 2020*. Statista. https://www.statista.com/statistics/272698/global-market-share-held-by-mobile-operating-systems-since-2009/

Security, R. (2020). *WHY YOU SHOULD BE FOCUSING ON YOUR MOBILE SECURITY*. RSI. https://blog.rsisecurity.com/importance-of-mobile-security/

Security, S. (2020). *COVID-19 Pandemic Sparks 72% Ransomware Growth, Mobile Vulnerabilities Grow 50%*. Cision. https://www.prnewswire.com/in/news-releases/covid-19-pandemic-sparks-72-ransomware-growth-mobile-vulnerabilities-grow-50--817268901.html

Seo, S. H., Gupta, A., Sallam, A. M., Bertino, E., & Yim, K. (2014). Detecting mobile malware threats to homeland security through static analysis. *Journal of Network and Computer Applications*, *38*(1), 43–53. https://doi.org/10.1016/j.jnca.2013.05.008

Sharma, K., & Gupta, B. B. (2019). Towards privacy risk analysis in android applications using machine learning approaches. *International Journal of E-Services and Mobile Applications*, *11*(2), 1–21. https://doi.org/10.4018/IJESMA.2019040101

Sheen, S., Anitha, R., & Natarajan, V. (2015). Android based malware detection using a multifeature collaborative decision fusion approach. *Neurocomputing*, *151*(P2), 905–912. https://doi.org/10.1016/j.neucom.2014.10.004

Shetu, S. F., Saifuzzaman, M., Moon, N. N., Sultana, S., & Yousuf, R. (2021). Student's performance prediction using data mining technique depending on overall academic status and environmental attributes. In *Advances in Intelligent Systems and Computing* (Vol. 1166). https://doi.org/10.1007/978-981-15-5148-2_66

Shrivastava, G., & Kumar, P. (2019). Intent and permission modeling for privacy leakage detection in android. *Energy Systems*. https://doi.org/10.1007/s12667-019-00359-7

Singhal, S., Maheshwari, S., & Meena, M. (2019). *Recent Findings in Intelligent Computing Techniques*. *707*, 229–238. https://doi.org/10.1007/978-981-10-8639-7

Skybox, S. (2020). *COVID-19 pandemic sparks 72% ransomware growth, mobile vulnerabilities grow 50%*. Security. https://www.securitymagazine.com/articles/92886-covid-19-pandemic-sparks-72-ransomware-growth-mobile-vulnerabilities-grow-50

Srivastava. (2019). Cyber Security in Parallel and Distributed Computing. In *Cyber Security in Parallel and Distributed Computing*. https://doi.org/10.1002/9781119488330

Statcounter. (2020). *Mobile Operating System Market Share Worldwide*. Globalstat. https://gs.statcounter.com/os-market-share/mobile/worldwide

Stevanovic, I. (2020). *The One OS to Rule Them All – 33 Android vs iOS Market Share Stats*. KommandoTech. https://kommandotech.com/statistics/android-vs-ios-market-share/

Stock, J. (2020). *INTERPOL report shows alarming rate of cyberattacks during COVID-19*. Interpol. https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

Subba, B., Biswas, S., & Karmakar, S. (2017). Host based intrusion detection system using frequency analysis of n-gram terms. *IEEE Region 10 Annual International Conference, Proceedings/TENCON*, *2017-Decem*, 2006–2011. https://doi.org/10.1109/TENCON.2017.8228190

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

Tahir, M., Li, M., Zheng, X., Carie, A., Jin, X., Azhar, M., Ayoub, N., Wagan, A., Aamir, M., Jamali, L. A., Imran, M. A., & Hulio, Z. H. (2019). A novel network user behaviors and profile testing based on anomaly detection techniques. *International Journal of Advanced Computer Science and Applications*, *10*(6), 305–324. https://doi.org/10.14569/ijacsa.2019.0100641

Tchakounté, F., & Dayang, P. (2013). System Calls Analysis of Malwares on Android. *International Journal of Science and …*, *2*(9), 669–674. http://ieeexplore.ieee.org/document/6298136/

Technologies, P. (2019). *Vulnerabilities and threats in mobile applications, 2019*. Positive Technologies. https://www.ptsecurity.com/ww-en/analytics/mobile-application-security-threats-and-vulnerabilities-2019/

Tong, F., & Yan, Z. (2017). A hybrid approach of mobile malware detection in Android. *Journal of Parallel and Distributed Computing*, *103*, 22–31. https://doi.org/10.1016/j.jpdc.2016.10.012

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. *Proceedings - 2021 International Conference on Software Engineering and Computer Systems and 4th International Conference on Computational Science and Information Management, ICSECS-ICOCSIM 2021*, 574–579. https://doi.org/10.1109/ICSECS52883.2021.00111

Turner, A. (2020). *How Many Smartphones are in the World*. Bankmycell. https://www.bankmycell.com/blog/how-many-phones-are-in-the-world#:~:text=According to GSMA real-time,mobile device in the world.&text=Statista predicts that by 2023,will increase to 7.33 billion.

Venkatraman, S., Alazab, M., & Vinayakumar, R. (2019). A hybrid deep learning image-based analysis for effective malware detection. *Journal of Information Security and Applications*, *47*, 377–389. https://doi.org/10.1016/j.jisa.2019.06.006

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

Wazid, M., Zeadally, S., & Das, A. K. (2019). Mobile Banking: Evolution and Threats: Malware Threats and Security Solutions. *IEEE Consumer Electronics Magazine*, *8*(2), 56–60. https://doi.org/10.1109/MCE.2018.2881291

Wu, F., Xiao, L., & Zhu, J. (2019). Bayesian model updating method based android malware detection for IoT services. *2019 15th International Wireless Communications and Mobile Computing Conference, IWCMC 2019*, 61–66. https://doi.org/10.1109/IWCMC.2019.8766754

Wu, Y. H., & Li, D. P. (2014). Research on smartphone application malicious behavior evaluation using fuzzy analytical hierarchy process. *Applied Mechanics and Materials*, *644–650*, 5733–5736. https://doi.org/10.4028/www.scientific.net/AMM.644-650.5733

Yang, A., Zhuansun, Y., Liu, C., Li, J., & Zhang, C. (2019). Design of Intrusion Detection System for Internet of Things Based on Improved BP Neural Network. *IEEE Access*, *7*, 106043–106052. https://doi.org/10.1109/ACCESS.2019.2929919

Yerima, S. Y., Sezer, S., & McWilliams, G. (2014). Analysis of Bayesian classification-based approaches for Android malware detection. *IET Information Security*, *8*(1), 25–36. https://doi.org/10.1049/iet-ifs.2013.0095

Yildiz, O., & Doğru, I. A. (2019). Permission-based Android Malware Detection System Using Feature Selection with Genetic Algorithm. *International Journal of Software Engineering and Knowledge Engineering*, *29*(2), 245–262. https://doi.org/10.1142/S0218194019500116

Yu, L., Pan, Z., Liu, J., & Shen, Y. (2013). Android malware detection technology based on improved Bayesian classification. *Proceedings - 3rd International Conference on Instrumentation and Measurement, Computer, Communication and Control, IMCCC 2013*, 1338–1341. https://doi.org/10.1109/IMCCC.2013.297

Zhu, H. J., You, Z. H., Zhu, Z. X., Shi, W. L., Chen, X., & Cheng, L. (2018). DroidDet: Effective and robust detection of android malware using static analysis along with rotation forest model. *Neurocomputing*, *272*, 638–646. https://doi.org/10.1016/j.neucom.2017.07.030