BIBLIOGRAPHY

[1] S. O'Dea, "Forecast number of mobile users worldwide 2020-2025 — statista," 2021. [Online]. Available: https://www.statista.com/statistics/218984/number-of-global-mobile-users-since-2010/

[2] "World population clock: 7.9 billion people (2022) - worldometer," 2022. [Online]. Available: https://www.worldometers.info/world-population/

[3] "Mobile operating system market share worldwide — statcounter global stats," 2022. [Online]. Available: https://gs.statcounter.com/os-market-share/mobile/worldwide

[4] F. Tong and Z. Yan, "A hybrid approach of mobile malware detection in android," *Journal of Parallel and Distributed Computing*, vol. 103, pp. 22–31, 5 2017.

[5] N. S. Kumar, P. V. Vardhan, P. A. Chandra, S. V. S. Kumar, and T. N. P. Madhuri, "Analysis of malware in android features using machine learning," *Journal of Engineering Sciences*, vol. 13, 2022. [Online]. Available: www.jespublication.com

[6] A. Fatima, R. Maurya, M. K. Dutta, R. Burget, and J. Masek, "Android malware detection using genetic algorithm based optimized feature selection and machine learning," *2019 42nd International Conference on Telecommunications and Signal Processing, TSP 2019*, pp. 220–223, 7 2019.

[7] U. S. Jannat, S. M. Hasnayeen, M. K. B. Shuhan, and M. S. Ferdous, "Analysis and detection of malware in android applications using machine learning," *2nd International Conference on Electrical, Computer and Communication Engineering, ECCE 2019*, 4 2019.

[8] B. Baskaran and A. L. Ralescu, "A study of android malware detection techniques and machine learning," in *MAICS*, 2016.

[9] Y. Zhauniarovich and O. Gadyatskaya, "Small changes, big changes: An updated view on the android permission system," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 9854 LNCS, pp. 346–367, 2016.

[10] S. Holla and M. M. Katti, "Android based mobile application development and its security," *International Journal of Computer Trends and Technology*, vol. 3, pp. 486–490, 2012. [Online]. Available: http://www.internationaljournalssrg.org

[11] A. Nayak, Y. Kang, and A. Pons, "Fuzzy logic based android malware classification approach," *International Journal of Computer Networks and*

Security, vol. 24, pp. 2051–6878, 2014. [Online]. Available: http://cgi.cs.indiana.edu/~nhusted/dokuwiki/doku.php?id=

[12] K. Tam, A. Feizollah, N. B. Anuar, R. Salleh, and L. Cavallaro, "The evolution of android malware and android analysis techniques," *ACM Computing Surveys*, vol. 49, 1 2017.

[13] M. Rho, S. Sezer, and E. G. Im, "A multimodal deep learning method for android malware detection using various features," *IEEE Transactions on Information Forensics and Security*, vol. 14, p. 773, 2018.

[14] D. Arp, M. Spreitzenbarth, M. Hübner, H. Gascon, and K. Rieck, "Drebin: Effective and explainable detection of android malware in your pocket," *Network and Distributed System Security Symposium (NDSS)*, 5 2014.

[15] D. J. Wu, C. H. Mao, T. E. Wei, H. M. Lee, and K. P. Wu, "Droidmat: Android malware detection through manifest and api calls tracing," *Proceedings of the 2012 7th Asia Joint Conference on Information Security, AsiaJCIS 2012*, pp. 62–69, 2012.

[16] F. Idrees and M. Rajarajan, "Investigating the android intents and permissions for malware detection," *International Conference on Wireless and Mobile Computing, Networking and Communications*, pp. 354–358, 11 2014.

[17] B. Sanz, I. Santos, C. Laorden, X. Ugarte-Pedrero, P. G. Bringas, and G. Álvarez, "Puma: Permission usage to detect malware in android," *Advances in Intelligent Systems and Computing*, vol. 189 AISC, pp. 289–298, 2013. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-642-33018-6_30

[18] A. Kapratwar, "Static and dynamic analysis for android malware detection," *Master's Projects*, 6 2016. [Online]. Available: https://scholarworks.sjsu.edu/etd_projects/488

[19] X. Liu and J. Liu, "A two-layered permission-based android malware detection scheme," *Proceedings - 2nd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering, MobileCloud 2014*, pp. 142–148, 2014.

[20] M. Ashawa and S. Morris, "Analysis of android malware detection techniques: A systematic review," *International Journal of Cyber-Security and Digital Forensics*, vol. 8, pp. 177–187, 2019.

[21] A. Kapratwar, F. D. Troia, and M. Stamp, "Static and dynamic analysis of android malware," 2017, pp. 653–662.

[22] H. J. Zhu, T. H. Jiang, B. Ma, Z. H. You, W. L. Shi, and L. Cheng, "Hemd: a highly efficient random forest-based malware

detection framework for android," *Neural Computing and Applications 2017 30:11*, vol. 30, pp. 3353–3361, 3 2017. [Online]. Available: https://link.springer.com/article/10.1007/s00521-017-2914-y

[23] G. Meng, Y. Xue, Z. Xu, Y. Liu, J. Zhang, and A. Narayanan, "Semantic modelling of android malware for effective malware comprehension, detection, and classification," *ISSTA 2016 - Proceedings of the 25th International Symposium on Software Testing and Analysis*, pp. 306–317, 7 2016.

[24] H. Sayadi, N. Patel, P. D. S. Manoj, A. Sasan, S. Rafatirad, and H. Homayoun, "Ensemble learning for effective run-time hardware-based malware detection: A comprehensive analysis and classification," *Proceedings - Design Automation Conference*, vol. Part F137710, 6 2018.

[25] G. Wang, J. Sun, J. Ma, K. Xu, and J. Gu, "Sentiment classification: The contribution of ensemble learning," *Decision Support Systems*, vol. 57, pp. 77–93, 1 2014.

[26] S. Y. Yerima, S. Sezer, and I. Muttik, "High accuracy android malware detection using ensemble learning," *IET Information Security*, vol. 9, pp. 313–320, 11 2015.

[27] A. Mahindru, "Android permissions dataset," vol. 2, 2020.

[28] Z.-H. Zhou, "Ensemble learning," *Machine Learning*, pp. 181–210, 2021. [Online]. Available: https://link.springer.com/chapter/10.1007/978-981-15-1967-3_8

[29] N. T. Rincy and R. Gupta, "Ensemble learning techniques and its efficiency in machine learning: A survey," *2nd International Conference on Data, Engineering and Applications, IDEA 2020*, 2 2020.

[30] T. G. Dietterichl, "Ensemble learning," in *The Handbook of Brain Theory and Neural Networks*, M. Arbib, Ed. MIT Press, 2002, pp. 405–408.

[31] R. Polikar, "Ensemble learning," *Ensemble Machine Learning*, pp. 1–34, 2012.

[32] H. M. Gomes, J. P. Barddal, I. Enembreck, A. Bifet, and F. Enembreck, "A survey on ensemble learning for data stream classification," *ACM Comput. Surv*, vol. 50, 2017. [Online]. Available: http://dx.doi.org/10.1145/3054925

[33] V. Svetnik, T. Wang, C. Tong, A. Liaw, R. P. Sheridan, and Q. Song, "Boosting: An ensemble learning tool for compound classification and qsar modeling," *Journal of Chemical Information and Modeling*, vol. 45, pp. 786–799, 5 2005.

[34] B. de Ville, "Decision trees," *Wiley Interdisciplinary Reviews: Computational Statistics*, vol. 5, pp. 448–455, 11 2013.

[35] N. Wilim and R. Oetama, "Sentiment analysis about indonesian lawyers club television program using k-nearest neighbor, naïve bayes classifier, and decision tree," *IJNMT (International Journal of New Media Technology)*, vol. 8, no. 1, pp. 50–56, Jun. 2021. [Online]. Available: https://ejournals.umn.ac.id/index.php/IJNMT/article/view/1965

[36] I. Rish, "An empirical study of the naïve bayes classifier," *IJCAI 2001 Work Empir Methods Artif Intell*, vol. 3, 01 2001.

[37] A. B. Musa, "Comparative study on classification performance between support vector machine and logistic regression," *International Journal of Machine Learning and Cybernetics*, vol. 4, pp. 13–24, 2 2013.

[38] S. Y. Yerima, S. Sezer, and I. Muttik, "High accuracy android malware detection using ensemble learning," *IET Information Security*, vol. 9, pp. 313–320, 11 2015.

[39] A. Luque, A. Carrasco, A. Martín, and A. de las Heras, "The impact of class imbalance in classification performance metrics based on the binary confusion matrix," *Pattern Recognition*, vol. 91, pp. 216–231, 7 2019.

[40] Željko . Vujović, "Classification model evaluation metrics," *(IJACSA)International Journal of Advanced Computer Science and Applications*, vol. 12, 2021. [Online]. Available: https://www.researchgate.net/publication/352902406

[41] A. Mishra, "Metrics to evaluate your machine learning algorithm — by aditya mishra — towards data science," 2018. [Online]. Available: https://towardsdatascience.com/metrics-to-evaluate-your-machine-learning-algorithm-f10ba6e38234

[42] S. Lessmann, B. Baesens, C. Mues, and S. Pietsch, "Benchmarking classification models for software defect prediction: A proposed framework and novel findings," *IEEE Transactions on Software Engineering*, vol. 34, pp. 485–496, 2008.