DAFTAR PUSTAKA

[1] Ericsson, "Ericsson mobility report," 2022, last accessed 8 February 2023. [Online]. Available: https://www.ericsson.com/4ae28d/assets/local/reports-papers/mobility-report/documents/2022/ericsson-mobility-report-november-2022.pdf

[2] Statista, "Global mobile os market share 2022," 2022, last accessed 11 May 2023. [Online]. Available: https://www.statista.com/statistics/272698/global-market-share-held-by-mobile-operating-systems-since-2009

[3] Dicoding, "Apa itu machine learning? beserta pengertian dan cara kerjanya," 2020, last accessed 16 May 2023. [Online]. Available: https://www.dicoding.com/blog/machine-learning-adalah

[4] B. C. Ross, "Mutual information between discrete and continuous data sets," *PLOS ONE*, vol. 9, no. 2, pp. 1–5, 02 2014. [Online]. Available: https://doi.org/10.1371/journal.pone.0087357

[5] M. Schubach, M. Re, P. Robinson, and G. Valentini, "Imbalance-aware machine learning for predicting rare and common disease-associated non-coding variants," *Scientific Reports*, vol. 7, 06 2017.

[6] A. H. Lashkari, A. F. A. Kadir, H. Gonzalez, K. F. Mbah, and A. A. Ghorbani, "Towards a network-based framework for android malware detection and characterization," in *2017 15th Annual Conference on Privacy, Security and Trust (PST)*. IEEE, 2017, pp. 233–242.

[7] Kaspersky, "Types of malware," 2023, last accessed 11 May 2023. [Online]. Available: https://www.kaspersky.com/resource-center/threats/malware-classifications

[8] A. Kapratwar, F. Di Troia, and M. Stamp, "Static and dynamic analysis of android malware." 1st International Workshop on FORmal methods for Security Engineering, 01 2017, pp. 653–662.

[9] A. R. Yogaswara, "Klasifikasi malware family menggunakan metode k-nearest neighbor (k-nn)." Seminar Nasional Teknologi dan Rekayasa (SENTRA) 2020, 2021, pp. 319–323.

[10] T. N. Turnip, C. F. Manurung, Y. S. Lubis, and R. Gultom, "Klasifikasi malware android aplikasi menggunakan random forest berdasarkan fitur statik," *Jurnal Teknik Informatika dan Sistem Informasi*, vol. 10, no. 1, pp. 926–936, 2023.

[11] M. K. Abuthawabeh and K. Mahmoud, "Android malware detection and categorization based on conversation-level network traffic features." 2019 International Arab Conference on Information Technology (ACIT), 12 2019, pp. 42–47.

[12] A. Rahali, A. H. Lashkari, G. Kaur, L. Taheri, F. GAGNON, and F. Massicotte, "Didroid: Android malware classification and characterization using deep image learning," in *2020 the 10th International Conference on Communication and*

Network Security, ser. ICCNS 2020. New York, NY, USA: Association for Computing Machinery, 2021, p. 70–82. [Online]. Available: https://doi.org/10.1145/3442520.3442522

[13] I. W. Canada, "Understanding android malware families (uamf) – the foundations (article 1)," 2021, last accessed 16 May 2023. [Online]. Available: https://www.itworldcanada.com/blog/understanding-android-malware-families-uamf-the-foundations-article-1/441562

[14] N. V. Chawla, K. W. Bowyer, L. O. Hall, and W. P. Kegelmeyer, "SMOTE: Synthetic minority over-sampling technique," *Journal of Artificial Intelligence Research*, vol. 16, pp. 321–357, jun 2002. [Online]. Available: https://doi.org/10.1613%2Fjair.953

[15] J. D. Kelleher, B. M. Namee, and A. D'Arcy, *Fundamentals of Machine Learning for Predictive Data Analytics: Algorithms, Worked Examples, and Case Studies*. The MIT Press, 2015.

[16] R. Kohavi, "A study of cross-validation and bootstrap for accuracy estimation and model selection," in *Proceedings of the 14th International Joint Conference on Artificial Intelligence - Volume 2*, ser. IJCAI'95. San Francisco, CA, USA: Morgan Kaufmann Publishers Inc., 1995, p. 1137–1143.