DAFTAR PUSTAKA

Ahsan, M. M., Mahmud, M. A. P., Saha, P. K., Gupta, K. D., & Siddique, Z. (2021). Effect of Data Scaling Methods on Machine Learning Algorithms and Model Performance. *Technologies*, *9*(3), 5–9. https://doi.org/10.3390/technologies9030052

Almahmoud, M., Alzu'bi, D., & Yaseen, Q. (2021). Redroiddet: Android malware detection based on recurrent neural network. *Procedia Computer Science*, *184*, 841–846. https://doi.org/10.1016/j.procs.2021.03.105

Almomani, I., Ahmed, M., & El-Shafai, W. (2022). Android malware analysis in a nutshell. *PLoS ONE*, *17*(7 July), 1–28. https://doi.org/10.1371/journal.pone.0270647

Alomari, H., Yaseen, Q. M., & Al-Betar, M. A. (2023). A Comparative Analysis of Machine Learning Algorithms for Android Malware Detection. *Procedia Computer Science*, *220*(2019), 763–768. https://doi.org/10.1016/j.procs.2023.03.101

Aung, W. T., Hay, K., & Saw, M. (2009). *Classification of Web Pages*. 372–376.

Batouche, A., & Jahankhani, H. (2021). A Comprehensive Approach to Android Malware Detection Using Machine Learning. In *Advanced Sciences and Technologies for Security Applications*. https://doi.org/10.1007/978-3-030-72120-6_7

Birba, D. E. (2020). A Comparative study of data splitting algorithms for machine learning model selection. *Degree Project in Computer Science and Engineering*, 1–23. https://www.diva-portal.org/smash/get/diva2:1506870/FULLTEXT01.pdf

Breiman. (2020). RFRSF: Employee Turnover Prediction Based on Random Forests and Survival Analysis. *Lecture Notes in Computer Science (Including*

Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), *12343 LNCS*, 503–515. https://doi.org/10.1007/978-3-030-62008-0_35

Chitayae, N., Muhammad, A. H., Komputer, T., Teknologi, I., & Ulama, N. (2023). *Identifikasi Malware pada Android menggunakan Algoritma K-Nearest Neighbor*. *3*(2).

Coccia, M. (2018). The Fishbone Diagram to Identify, Systematize and Analyze the Sources of General Purpose Technologies. *Journal of Social and Administrative Sciences*, *4*(4), 291–303. https://ssrn.com/abstract=3100011Electroniccopyavailableat:https://ssrn.com/abstract=3100011Electroniccopyavailableat:https://ssrn.com/abstract=3100011

Creswell, J. W., Hanson, W. E., Clark Plano, V. L., & Morales, A. (2007). Qualitative Research Designs: Selection and Implementation. *The Counseling Psychologist*, *35*(2), 236–264. https://doi.org/10.1177/0011000006287390

Diana, D., Indrajit, R. E., & Dazki, E. (2022). Komparasi Algoritma Naïve Bayes, Logistic Regression Dan Support Vector Machine pada Klasifikasi File Application Package Kit Android Malware. *Jutisi : Jurnal Ilmiah Teknik Informatika Dan Sistem Informasi*, *11*(1), 109. https://doi.org/10.35889/jutisi.v11i1.815

Efriyani, D., & Panjaitan, F. (2021). Klasifikasi Malware Menggunakan MetodeRecurrent Neural Network. *EAI/Springer Innovations in Communication and Computing*, *23*(3), 53–61.

García, S., Luengo, J., & Herrera, F. (2015). Preface. *Intelligent Systems Reference Library*, *72*. https://doi.org/10.1007/978-3-319-10247-4

Gholamy, A., Kreinovich, V., & Kosheleva, O. (2018). Why 70/30 Or 80/20 Relation Between Training And Testing Sets : A Pedagogical Explanation.

Departmental Technical Reports (CS), *1209*, 1–6.

Hadiprakoso, R. B., Aditya, W. R., & Pramitha, F. N. (2022). Analisis Statis Deteksi Malware Android Menggunakan Algoritma Supervised Machine Learning. *Cyber Security Dan Forensik Digital*, *5*(1), 1–5. https://doi.org/10.14421/csecurity.2022.5.1.3116

Hastjarjo, D. T. (2011). Validitas Eksperimen. *Buletin Psikologi*, *19*(2), 70–80.

Islam, R., Sayed, M. I., Saha, S., Hossain, M. J., & Masud, M. A. (2023). Android malware classification using optimum feature selection and ensemble machine learning. *Internet of Things and Cyber-Physical Systems*, *3*(January), 100–111. https://doi.org/10.1016/j.iotcps.2023.03.001

Junaedi, H., Budianto, H., Maryati, I., & Melani, Y. (2011). Data Transformation pada Data Mining. *Prosiding Konferensi Nasional Inovasi Dalam Desain Dan Teknologi*, *7*, 93–99. https://ideatech.stts.edu/proceeding2011/12-000113_INF Hartarto p93-99.pdf

Kamiran, F., & Calders, T. (2012). Data preprocessing techniques for classification without discrimination. In *Knowledge and Information Systems* (Vol. 33, Issue 1). https://doi.org/10.1007/s10115-011-0463-8

Lu, T., Du, Y., Ouyang, L., Chen, Q., & Wang, X. (2020). Android malware detection based on a hybrid deep learning model. *Security and Communication Networks*, *2020*(ii). https://doi.org/10.1155/2020/8863617

Ma, Z., Ge, H., Liu, Y., Zhao, M., & Ma, J. (2019). A Combination Method for Android Malware Detection Based on Control Flow Graphs and Machine Learning Algorithms. *IEEE Access*, *7*, 21235–21245. https://doi.org/10.1109/ACCESS.2019.2896003

Muzaffar, A., Ragab Hassen, H., Lones, M. A., & Zantout, H. (2022). An in-depth review of machine learning based Android malware detection. *Computers and Security*, *121*, 102833. https://doi.org/10.1016/j.cose.2022.102833

Neeraj, Kumar, N., & Maurya, V. K. (2020). a Review on Machine Learning (Feature Selection, Classification and Clustering) Approaches of Big Data Mining in Different Area of Research. *Article in Journal of Critical Reviews*, *7*(August), 2020. https://doi.org/10.31838/jcr.07.19.322

Nguyen, Q. H., Ly, H. B., Ho, L. S., Al-Ansari, N., Van Le, H., Tran, V. Q., Prakash, I., & Pham, B. T. (2021). Influence of data splitting on performance of machine learning models in prediction of shear strength of soil. *Mathematical Problems in Engineering*, *2021*. https://doi.org/10.1155/2021/4832864

Parmar, A., Katariya, R., & Patel, V. (2019). A Review on Random Forest: An Ensemble Classifier. *Lecture Notes on Data Engineering and Communications Technologies*, *26*, 758–763. https://doi.org/10.1007/978-3-030-03146-6_86

Permana, I., & Salisah, F. N. (2022). The Effect of Data Normalization on the Performance of the Classification Results of the Backpropagation Algorithm. *IJIRSE: Indonesian Journal of Informatic Research and Software Engineering*, *2*(1), 67–72.

Rafrastara, F. A., Supriyanto, C., Paramita, C., & Astuti, Y. P. (2023). Deteksi Malware menggunakan Metode Stacking berbasis Ensemble. *Jurnal Informatika: Jurnal Pengembangan IT*, *8*(1), 11–16. https://doi.org/10.30591/jpit.v8i1.4606

Rahali, A., Lashkari, A. H., Kaur, G., Taheri, L., Gagnon, F., & Massicotte, F. (2020). DIDroid: Android malware classification and characterization using deep image learning. *ACM International Conference Proceeding Series*, 70–82. https://doi.org/10.1145/3442520.3442522

Ramadhan, A., Lindawati, L., & Rose, M. M. (2023). Komparasi Algoritma Neural Network dan K-Nearest Neighbor Dalam Mendeteksi Malware Android. *Building of Informatics, Technology and Science (BITS)*, *5*(1), 191–199. https://doi.org/10.47065/bits.v5i1.3538

Rana, M. S., Gudla, C., & Sung, A. H. (2018). Evaluating machine learning models for android malware detection - A comparison study. *ACM International Conference Proceeding Series*, *December*, 17–21. https://doi.org/10.1145/3301326.3301390

Refhaldo, M., Budiarto, E., Anggun Sari, P., Monica, S., Studi Teknik Informatika, P., Teknik, F., & Pelita Bangsa, U. (2022). *Klasifikasi Aplikasi Malware Android Menggunakan Algoritma C5.0*. *1*(1), 854.

Roihan, A., Sunarya, P. A., & Rafika, A. S. (2020). Pemanfaatan Machine Learning dalam Berbagai Bidang: Review paper. *IJCIT (Indonesian Journal on Computer and Information Technology)*, *5*(1), 75–82. https://doi.org/10.31294/ijcit.v5i1.7951

Shatnawi, A. S., Yassen, Q., & Yateem, A. (2022). An Android Malware Detection Approach Based on Static Feature Analysis Using Machine Learning Algorithms. *Procedia Computer Science*, *201*(C), 653–658. https://doi.org/10.1016/j.procs.2022.03.086

Sinambela, S., Pangestu, A. R., & Feriyanto, R. (2020). Analisis Aplikasi Malware pada Android dengan Metode Statik. *Jurnal Ilmiah ILKOMINFO - Ilmu Komputer & Informatika*, *3*(2), 88–94. https://doi.org/10.47324/ilkominfo.v3i2.101

Sitorus, Y. W., Sukarno, P., Mandala, S., Informatika, F., & Telkom, U. (2021). Analisis Deteksi Malware Android menggunakan metode Support Vector Machine & Random Forest. *E-Proceeding of Engineering*, *8*(6), 12500.

Soofi, A. A., & Awan, A. (2017). Classification Techniques in Machine Learning: Applications and Issues. *Journal of Basic & Applied Sciences*, *13*, 459–465.

Subaeki, B. (2014). Perancangan Arsitektur Sistem Informasi Menggunakan Metode Enterprise Arsitektur Planning (Studi Kasus : Universitas Purwakarta - Purwakarta). *Jurnal Informatika*, *1*(1), 1–18.

Tharwat, A. (2018). Classification assessment methods. *Applied Computing and*

Informatics, *17*(1), 168–192. https://doi.org/10.1016/j.aci.2018.08.003

Tjahjadi, E. V., & Santoso, B. (2023). Klasifikasi Malware Menggunakan Teknik Machine Learning. *Jurnal Ilmiah Ilmu Komputer*, *2*(1), 60–70.

Turnip, T. N. T., Chatrine Febryanti Manurung, Yogi Septian Lubis, & Gultom, R. (2023). Klasifikasi Malware Android Aplikasi Menggunakan Random Forest Berdasarkan Fitur Statik. *Teknik Informatika Dan Sistem Informasi*, *10*(1), 926–936. blob:https://jurnal.mdp.ac.id/b5c3fbd3-cbb1-4677-a16b-2c5300377815

Wongvorachan, T., He, S., & Bulut, O. (2023). A Comparison of Undersampling, Oversampling, and SMOTE Methods for Dealing with Imbalanced Classification in Educational Data Mining. *Information (Switzerland)*, *14*(1). https://doi.org/10.3390/info14010054

Yogaswara, A. R. (2021). Klasifikasi Malware Family menggunakan Metode k-Nearest Neighbor (k-NN). *Jurnal Repositor*, *3*(3), 305–314. https://doi.org/10.22219/repositor.v2i3.1313

Zakariya, R. A. I., & Ramli, K. (2023). Desain Penilaian Risiko Privasi pada Aplikasi Seluler Melalui Model Machine Learning Berbasis Ensemble Learning dan Multiple Application Attributes. *Jurnal Teknologi Informasi Dan Ilmu Komputer*, *10*(4), 831–842. https://doi.org/10.25126/jtiik.20241047029