

DAFTAR PUSTAKA

- [1] F. Tchakounté, R. C. N. Ngassi, V. C. Kamla, and K. P. Udagepola, “LimonDroid: a system coupling three signature-based schemes for profiling Android malware,” *Iran Journal of Computer Science*, vol. 4, no. 2, pp. 95–114, Jun. 2021, doi: 10.1007/s42044-020-00068-w.
- [2] A. Muzaffar, H. Ragab Hassen, M. A. Lones, and H. Zantout, “An in-depth review of machine learning based Android malware detection,” *Comput Secur*, vol. 121, p. 102833, Oct. 2022, doi: 10.1016/j.cose.2022.102833.
- [3] “Desktop Operating System Market Share Worldwide | Statcounter Global Stats.” Accessed: Oct. 22, 2025. [Online]. Available: <https://gs.statcounter.com/os-market-share/desktop/worldwide>
- [4] “Android Usage Statistics (2025) - Global Market Share.” Accessed: Oct. 22, 2025. [Online]. Available: <https://www.demandsage.com/android-statistics/>
- [5] A. Pathak, Th. S. Kumar, and U. Barman, “Static analysis framework for permission-based dataset generation and android malware detection using machine learning,” *EURASIP J Inf Secur*, vol. 2024, no. 1, p. 33, Oct. 2024, doi: 10.1186/s13635-024-00182-3.
- [6] J. Mohamad Arif, M. F. Ab Razak, S. Awang, S. R. Tuan Mat, N. S. N. Ismail, and A. Firdaus, “A static analysis approach for Android permission-based malware detection systems,” *PLoS One*, vol. 16, no. 9, p. e0257968, Sep. 2021, doi: 10.1371/journal.pone.0257968.
- [7] O. E. Saied and K. H. Thanoon, “Static Analysis-based Detection of Android Malware using Machine Learning Algorithms,” *SISTEMASI*, vol. 14, no. 5, p. 2540, Sep. 2025, doi: 10.32520/stmsi.v14i5.5498.
- [8] A. Mathur, L. M. Podila, K. Kulkarni, Q. Niyaz, and A. Y. Javaid, “NATICUSdroid: A malware detection framework for Android using native

- and custom permissions,” *Journal of Information Security and Applications*, vol. 58, p. 102696, May 2021, doi: 10.1016/j.jisa.2020.102696.
- [9] F. Akbar, M. Hussain, R. Mumtaz, Q. Riaz, A. W. A. Wahab, and K.-H. Jung, “Permissions-Based Detection of Android Malware Using Machine Learning,” *Symmetry (Basel)*, vol. 14, no. 4, p. 718, Apr. 2022, doi: 10.3390/sym14040718.
- [10] “Apa Itu Cloud Server? - Indonesian Cloud | Cloud Computing.” Accessed: Oct. 22, 2025. [Online]. Available: <https://indonesiancloud.com/apa-itu-cloud-server/>
- [11] AWS, “Apa itu Server Cloud?” Accessed: Sep. 01, 2025. [Online]. Available: <https://aws.amazon.com/id/what-is/cloud-server/>
- [12] S. S. and I. Smalley, “What is Docker?,” IBM. Accessed: Sep. 03, 2025. [Online]. Available: <https://www.ibm.com/think/topics/docker>
- [13] C. R. Prabowo, E. Rohadi, and D. Irmanto, “Study and Analysis of Docker Internal System Security From Docker Daemon Attack and DDOS on The Open Journal System,” *JPUA: Jurnal Perpustakaan Universitas Airlangga: Media Informasi dan Komunikasi Kepustakawanan*, vol. 14, no. 1, pp. 61–68, Jun. 2024, doi: 10.20473/jpua.v14i1.2024.61-68.
- [14] “Docker Explained: How To Create Docker Containers Running Memcached | DigitalOcean.” Accessed: Oct. 22, 2025. [Online]. Available: <https://www.digitalocean.com/community/tutorials/docker-explained-how-to-create-docker-containers-running-memcached>
- [15] W. S. Shameem Ahamed, P. Zavorsky, and B. Swar, “Security Audit of Docker Container Images in Cloud Architecture,” in *2021 2nd International Conference on Secure Cyber Computing and Communications (ICSCCC)*, IEEE, May 2021, pp. 202–207. doi: 10.1109/ICSCCC51823.2021.9478100.

- [16] “Cloudflare Tunnel · Cloudflare Zero Trust docs.” Accessed: Oct. 22, 2025. [Online]. Available: <https://developers.cloudflare.com/cloudflare-one/networks/connectors/cloudflare-tunnel/>
- [17] “Mobile App Static Analysis Menggunakan MobSF | by Fauzan | Medium.” Accessed: Oct. 22, 2025. [Online]. Available: <https://fauzanf.medium.com/mobile-app-static-analysis-menggunakan-mobsf-a3f828d0bf49>
- [18] “Run your security static analysis tests on the cloud with MobSF, AWS, and Bitrise - Bitrise Blog.” Accessed: Oct. 22, 2025. [Online]. Available: <https://bitrise.io/blog/post/run-your-security-static-analysis-tests-on-the-cloud-with-mobsf-aws-and-bitrise>
- [19] N. Sarangpure, V. Dhamde, A. Roge, J. Doye, S. Patle, and S. Tamboli, “Automating the Machine Learning Process using PyCaret and Streamlit,” in *2023 2nd International Conference for Innovation in Technology (INOCON)*, IEEE, Mar. 2023, pp. 1–5. doi: 10.1109/INOCON57975.2023.10101357.
- [20] V. Sundaram, S. Abhi, and R. Agarwal, “Building a Multi-class Prediction App for Malicious URLs,” 2023, pp. 455–475. doi: 10.1007/978-3-031-28183-9_32.
- [21] M. Tanha and S. Kafaie, “A Review of Explainable AI for Android Malware Detection and Analysis,” *IEEE Access*, vol. 13, pp. 141958–141974, 2025, doi: 10.1109/ACCESS.2025.3597575.
- [22] S. Roy, S. Bhanja, and A. Das, “AndyWar: an intelligent android malware detection using machine learning,” *Innov Syst Softw Eng*, vol. 21, no. 1, pp. 303–311, Mar. 2025, doi: 10.1007/s11334-023-00530-5.
- [23] R. S. Kumar, A. R. Singh, P. L. Narayana, V. S. Chandrika, M. Bajaj, and I. Zaitsev, “Hybrid machine learning framework for predictive maintenance and anomaly detection in lithium-ion batteries using enhanced random

- forest,” *Sci Rep*, vol. 15, no. 1, p. 6243, Feb. 2025, doi: 10.1038/s41598-025-90810-w.
- [24] “Random forest - Wikipedia.” Accessed: Oct. 22, 2025. [Online]. Available: https://en.wikipedia.org/wiki/Random_forest
- [25] R. Kanniappan and V. Jamuna, “Leveraging Fine-Tuned LightGBM for Advanced AI-Driven Android Malware Detection,” in *2025 3rd International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA)*, IEEE, Apr. 2025, pp. 1–6. doi: 10.1109/ICAECA63854.2025.11012253.
- [26] M. Gan, S. Pan, Y. Chen, C. Cheng, H. Pan, and X. Zhu, “Application of the Machine Learning LightGBM Model to the Prediction of the Water Levels of the Lower Columbia River,” *J Mar Sci Eng*, vol. 9, no. 5, p. 496, May 2021, doi: 10.3390/jmse9050496.
- [27] “Extra Trees | Medium.” Accessed: Oct. 22, 2025. [Online]. Available: <https://medium.com/@samybaladram/extra-trees-explained-a-visual-guide-with-code-examples-4c2967cedc75>
- [28] “What? When? How?: ExtraTrees Classifier | Towards Data Science.” Accessed: Oct. 22, 2025. [Online]. Available: <https://towardsdatascience.com/what-when-how-extratrees-classifier-c939f905851c/>
- [29] N. Hussein and S. R. M. Zeebaree, “Performance Evaluation of Extra Trees Classifier by using CPU Parallel and Non-Parallel Processing,” *Indonesian Journal of Computer Science*, vol. 13, no. 2, Apr. 2024, doi: 10.33022/ijcs.v13i2.3802.
- [30] L. Cao *et al.*, “Interpretable Soft Sensors using Extremely Randomized Trees and SHAP,” *IFAC-PapersOnLine*, vol. 56, no. 2, pp. 8000–8005, 2023, doi: 10.1016/j.ifacol.2023.10.922.

- [31] “How to Split Machine Learning Datasets: Training, Validation, & Test Sets.” Accessed: Oct. 22, 2025. [Online]. Available: <https://encord.com/blog/train-val-test-split/>
- [32] “Memahami Confusion Matrix: Accuracy, Precision, Recall, Specificity, dan F1-Score untuk Evaluasi Model Klasifikasi | by Rina | Medium.” Accessed: Oct. 22, 2025. [Online]. Available: <https://esairina.medium.com/memahami-confusion-matrix-accuracy-precision-recall-specificity-dan-f1-score-610d4f0db7cf>
- [33] “Evaluation Metrics in Machine Learning - GeeksforGeeks.” Accessed: Oct. 22, 2025. [Online]. Available: <https://www.geeksforgeeks.org/machine-learning/metrics-for-machine-learning-model/>
- [34] “Understanding Precision, Recall, and F1 Score Metrics | by Piyush Kashyap | Medium.” Accessed: Oct. 22, 2025. [Online]. Available: <https://medium.com/@piyushkashyap045/understanding-precision-recall-and-f1-score-metrics-ea219b908093>
- [35] “Importance of Datasets in Machine Learning and AI Research.” Accessed: Oct. 22, 2025. [Online]. Available: <https://www.datatobiz.com/blog/datasets-in-machine-learning/>
- [36] “What Is Data Labeling? | IBM.” Accessed: Oct. 22, 2025. [Online]. Available: <https://www.ibm.com/think/topics/data-labeling>
- [37] “What is the difference between labeled and unlabeled data? - GeeksforGeeks.” Accessed: Oct. 22, 2025. [Online]. Available: <https://www.geeksforgeeks.org/machine-learning/what-is-the-difference-between-labeled-and-unlabeled-data/>
- [38] “Machine Learning Datasets: A Complete 2025 Guide | Label Your Data.” Accessed: Oct. 22, 2025. [Online]. Available: <https://labeleyourdata.com/articles/machine-learning/datasets>

- [39] J. Misquitta and A. Kannan, “A Comparative Study of Malicious URL Detection: Regular Expression Analysis, Machine Learning, and VirusTotal API,” 2024, pp. 219–232. doi: 10.1007/978-3-031-52760-9_16.
- [40] N. Okazaki *et al.*, “Optimal Weighted Voting-Based Collaborated Malware Detection for Zero-Day Malware: A Case Study on VirusTotal and MalwareBazaar,” *Future Internet*, vol. 16, no. 8, p. 259, Jul. 2024, doi: 10.3390/fi16080259.
- [41] F. Nettersheim, S. Arlt, and M. Rademacher, “Utilizing DNS and VirusTotal for Automated Ad-Malware Detection,” 2024, pp. 393–396. doi: 10.1007/978-3-031-62362-2_31.
- [42] M. Gouasmia, A. E. Kiouche, and H. Seba, “Advanced Malware Detection in Code Repositories Using Graph Neural Networks,” 2025, pp. 13–23. doi: 10.1007/978-3-031-94139-9_2.
- [43] Y. Chen, Q. Wang, Y. Yang, Y. Chen, Y. Li, and S. Ji, “Unveiling Security Vulnerabilities in Git Large File Storage Protocol,” in *2025 IEEE Symposium on Security and Privacy (SP)*, IEEE, May 2025, pp. 468–485. doi: 10.1109/SP61157.2025.00123.
- [44] Muhammad Shumail Naveed, “Correlation Between GitHub Stars and Code Vulnerabilities,” *Journal of Computing & Biomedical Informatics*, vol. 4, no. 01, pp. 141–151, Dec. 2022, doi: 10.56979/401/2022/111.
- [45] “NATICUSdroid (Android Permissions) - UCI Machine Learning Repository.” Accessed: Oct. 22, 2025. [Online]. Available: <https://archive.ics.uci.edu/dataset/722/naticusdroid+android+permissions+dataset>