

DAFTAR PUSTAKA

- [1] L. Suharlim, “7 Fakta Virus Trojan Horse, Merusak Komputer dari Dalam,” *IDN Times*, Sep. 2021, Accessed: Jun. 23, 2025. [Online]. Available: <https://www.idntimes.com/tech/trend/lukita-surhalim/fakta-virus-trojan-horse/2>
- [2] R. Adenansi, L. A. Novarina, J. Pendidikan, and T. Informasi, “Malware dynamic,” *JoEICT (Journal of Education And ICT)*, vol. 1, no. 1, pp. 37–43, Mar. 2017, doi: 10.29100/V1I1.91.
- [3] A. Subasi, “Machine learning techniques,” *Practical Machine Learning for Data Analysis Using Python*, pp. 91–202, 2020, doi: 10.1016/B978-0-12-821379-7.00003-5.
- [4] “Apa itu Jaringan Neural? | IBM.” Accessed: Jul. 10, 2025. [Online]. Available: <https://www.ibm.com/id-id/think/topics/neural-networks>
- [5] “Mengenal Artificial Neural Network – School of Information Systems.” Accessed: Jul. 10, 2025. [Online]. Available: <https://sis.binus.ac.id/2022/02/14/mengenal-artificial-neural-network/>
- [6] H. M. Deylami, R. C. Muniyandi, I. T. Ardekani, and A. Sarrafzadeh, “Taxonomy of malware detection techniques: A systematic literature review,” *2016 14th Annual Conference on Privacy, Security and Trust, PST 2016*, pp. 629–636, 2016, doi: 10.1109/PST.2016.7906998.
- [7] D. Smith, S. Khorsandroo, and K. Roy, “Supervised and Unsupervised Learning Techniques Utilizing Malware Datasets,” in *2023 IEEE 2nd International Conference on AI in Cybersecurity, ICAIC 2023*, 2023. doi: 10.1109/ICAIC57335.2023.10044169.
- [8] D. Cevallos-Salas, F. Grijalva, J. Estrada-Jimenez, D. Benitez, and R. Andrade, “Obfuscated Privacy Malware Classifiers Based on Memory Dumping Analysis,” *IEEE Access*, vol. 12, 2024, doi: 10.1109/ACCESS.2024.3358840.
- [9] M. A. Talukder *et al.*, “A dependable hybrid machine learning model for network intrusion detection,” *Journal of Information Security and Applications*, vol. 72, 2023, doi: 10.1016/j.jisa.2022.103405.
- [10] L. Tuggener, J. Schmidhuber, and T. Stadelmann, “Is it enough to optimize CNN architectures on ImageNet?,” *Front Comput Sci*, vol. 4, 2022, doi: 10.3389/fcomp.2022.1041703.
- [11] A. W. Salehi *et al.*, “A Study of CNN and Transfer Learning in Medical Imaging: Advantages, Challenges, Future Scope,” 2023. doi: 10.3390/su15075930.
- [12] X. Lei, H. Pan, and X. Huang, “A dilated cnn model for image classification,” *IEEE Access*, vol. 7, 2019, doi: 10.1109/ACCESS.2019.2927169.
- [13] X. Xu *et al.*, “Crack Detection and Comparison Study Based on Faster R-CNN and Mask R-CNN,” *Sensors*, vol. 22, no. 3, 2022, doi: 10.3390/s22031215.
- [14] D. Bhatt *et al.*, “Cnn variants for computer vision: History, architecture, application, challenges and future scope,” 2021. doi: 10.3390/electronics10202470.
- [15] K. Viikki, M. Juhola, I. Pyykkö, and P. Honkavaara, “Evaluating training data suitability for decision tree induction,” *J Med Syst*, vol. 25, no. 2, 2001, doi: 10.1023/A:1005624715089.
- [16] T. M. Alam, M. M. A. Khan, M. A. Iqbal, A. Wahab, and M. Mushtaq, “Cervical cancer prediction through different screening methods using data mining,” *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 2, 2019, doi: 10.14569/ijacsa.2019.0100251.
- [17] Q. Xin, S. Hu, S. Liu, L. Zhao, and Y. D. Zhang, “An Attention-Based Wavelet Convolution Neural Network for Epilepsy EEG Classification,” *IEEE Transactions on Neural Systems and Rehabilitation Engineering*, vol. 30, 2022, doi: 10.1109/TNSRE.2022.3166181.
- [18] A. D. Kulkarni, “Convolution Neural Networks for Phishing Detection,” *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 4, 2023, doi: 10.14569/IJACSA.2023.0140403.

- [19] C. Cheng and K. K. Parhi, "Fast 2D Convolution Algorithms for Convolutional Neural Networks," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 67, no. 5, 2020, doi: 10.1109/TCSI.2020.2964748.
- [20] P. K. Mall *et al.*, "A comprehensive review of deep neural networks for medical image processing: Recent developments and future opportunities," *Healthcare Analytics*, vol. 4, 2023, doi: 10.1016/j.health.2023.100216.
- [21] V. Borisov, T. Leemann, K. Sebler, J. Haug, M. Pawelczyk, and G. Kasneci, "Deep Neural Networks and Tabular Data: A Survey," *IEEE Trans Neural Netw Learn Syst*, vol. 35, no. 6, 2024, doi: 10.1109/TNNLS.2022.3229161.
- [22] Y. Chen, Y. Xie, L. Song, F. Chen, and T. Tang, "A Survey of Accelerator Architectures for Deep Neural Networks," 2020. doi: 10.1016/j.eng.2020.01.007.
- [23] J. Gawlikowski *et al.*, "A survey of uncertainty in deep neural networks," *Artif Intell Rev*, vol. 56, 2023, doi: 10.1007/s10462-023-10562-9.
- [24] V. Buhrmester, D. Münch, and M. Arens, "Analysis of Explainers of Black Box Deep Neural Networks for Computer Vision: A Survey," *Mach Learn Knowl Extr*, vol. 3, no. 4, 2021, doi: 10.3390/make3040048.
- [25] S. Lyu and J. Liu, "Convolutional recurrent neural networks for text classification," *Journal of Database Management*, vol. 32, no. 4, 2021, doi: 10.4018/JDM.2021100105.
- [26] F. García and B. Lev, *Introduction to Internet of Things in Management Science and Operations Research*, vol. 311. 2021.
- [27] R. Borghi and G. De Rossi, "Machine Learning for Asset Management: New Developments and Financial Applications," in *Machine Learning for Asset Management*, 2020.
- [28] C. F. Rodríguez-Hernández, M. Musso, E. Kyndt, and E. Cascallar, "Artificial neural networks in academic performance prediction: Systematic implementation and predictor evaluation," *Computers and Education: Artificial Intelligence*, vol. 2, 2021, doi: 10.1016/j.caeai.2021.100018.
- [29] A. Kurani, P. Doshi, A. Vakharia, and M. Shah, "A Comprehensive Comparative Study of Artificial Neural Network (ANN) and Support Vector Machines (SVM) on Stock Forecasting," 2023. doi: 10.1007/s40745-021-00344-x.
- [30] R. Rahmadewi, E. Purwanti, and V. Efelina, "IDENTIFIKASI JENIS TUMBUHAN MENGGUNAKAN CITRA DAUN BERBASIS JARINGAN SARAF TIRUAN (ARTIFICIAL NEURAL NETWORKS)," *Jurnal Media Elektro*, 2018, doi: 10.35508/jme.v0i0.427.
- [31] M. Rizki and H. Dhika, "ANALISIS PENGAPLIKASIAN JARINGAN SARAF TIRUAN DALAM KEAMANAN JARINGAN KOMPUTER," *MULTITEK INDONESIA*, vol. 14, no. 2, 2021, doi: 10.24269/mtkind.v14i2.2056.
- [32] M. F. Naufal and S. F. Kusuma, "Analisis Perbandingan Algoritma Machine Learning dan Deep Learning untuk Klasifikasi Citra Sistem Isyarat Bahasa Indonesia (SIBI)," *Jurnal Teknologi Informasi dan Ilmu Komputer*, vol. 10, no. 4, 2023, doi: 10.25126/jtiik.20241046823.
- [33] A. A. Ningrum, I. Syarif, A. I. Gunawan, E. Satriyanto, and R. Muchtar, "Algoritma Deep Learning-LSTM untuk Memprediksi Umur Transformator," *Jurnal Teknologi Informasi dan Ilmu Komputer*, vol. 8, no. 3, 2021, doi: 10.25126/jtiik.2021834587.
- [34] R. A. de Oliveira and M. H. J. Bollen, "Deep learning for power quality," 2023. doi: 10.1016/j.eprsr.2022.108887.
- [35] A. Santoso and G. Ariyanto, "Implementasi Deep Learning berbasis Keras untuk Pengenalan Wajah," *Emitor: Jurnal Teknik Elektro*, vol. 18, no. 1, 2018, doi: 10.23917/emitor.v18i01.6235.
- [36] A. A. Tulbure, A. A. Tulbure, and E. H. Dulf, "A review on modern defect detection models using DCNNs – Deep convolutional neural networks," 2022. doi: 10.1016/j.jare.2021.03.015.
- [37] C. Janiesch, P. Zschech, and K. Heinrich, "Machine learning and deep learning," *Electronic Markets*, vol. 31, no. 3, pp. 685–695, Sep. 2021, doi: 10.1007/S12525-021-00475-2.

- [38] C. Janiesch, P. Zschech, and K. Heinrich, "Machine learning and deep learning," *Electronic Markets*, vol. 31, no. 3, 2021, doi: 10.1007/s12525-021-00475-2.
- [39] T. A. Cahyanto, V. Wahanggara, and D. Ramadana, "Analisis dan Deteksi Malware Menggunakan Metode Malware Analisis Dinamis dan Malware Analisis Statis," *Jurnal Sistem & Teknologi Informasi Indonesia*, vol. 2, no. 1, 2017.
- [40] J. Cruz, C. Posada, N. V. R. Masna, P. Chakraborty, P. Gaikwad, and S. Bhunia, "A Framework for Automated Exploration of Trojan Attack Space in FPGA Netlists," *IEEE Transactions on Computers*, vol. 72, no. 10, 2023, doi: 10.1109/TC.2023.3266592.
- [41] K. I. Gubbi *et al.*, "Hardware Trojan Detection Using Machine Learning: A Tutorial," *ACM Transactions on Embedded Computing Systems*, vol. 22, no. 3, 2023, doi: 10.1145/3579823.
- [42] "Jenis Malware dan Contoh Malware." Accessed: Jun. 24, 2025. [Online]. Available: <https://www.kaspersky.com/resource-center/threats/types-of-malware>
- [43] "Perkuat Sektor Keamanan Siber, Indonesia dan Australia Jalin Kerja Sama Pengembangan SDM - Kementerian Koordinator Bidang Perekonomian Republik Indonesia." Accessed: Jun. 24, 2025. [Online]. Available: <https://www.ekon.go.id/publikasi/detail/6186/perkuat-sektor-keamanan-siber-indonesia-dan-australia-jalin-kerja-sama-pengembangan-sdm>
- [44] O. Yildiz and I. A. Doğru, "Permission-based Android Malware Detection System Using Feature Selection with Genetic Algorithm," *International Journal of Software Engineering and Knowledge Engineering*, vol. 29, no. 2, pp. 245–262, Feb. 2019, doi: 10.1142/S0218194019500116.
- [45] Togu Novriansyah Turnip, Chatrine Febryanti Manurung, Yogi Septian Lubis, and Rachel Gultom, "Klasifikasi Malware Android Aplikasi Menggunakan Random Forest Berdasarkan Fitur Statik," *Teknik Informatika dan Sistem Informasi*, vol. 10, no. 1, pp. 926–936, 2023.