DAFTAR PUSTAKA

[1] Z. Wang, Q. Liu, and Y. Chi, “Review of android malware detection based on deep learning,” *IEEE Access*, vol. 8, pp. 181102–181126, 2020, doi: 10.1109/ACCESS.2020.3028370.

[2] Y. D. Puji Rahayu and Nanang Trianto, “Analisis Malware Menggunakan Metode Analisis Statis dan Dinamis untuk Pembuatan IOC Berdasarkan STIX Versi 2.1,” *Info Kripto*, vol. 15, no. 3, pp. 105–111, 2021, doi: 10.56706/ik.v15i3.30.

[3] V. A. Manoppo, A. S. . Lumenta, and S. D. . Karouw, “Analisa Malware Menggunakan Metode Dynamic Analysis Pada Jaringan Universitas Sam Ratulangi,” *J. Tek. Elektro Dan Komput.*, vol. 9, no. 3, pp. 181–188, 2020.

[4] F. De Santonario and M. Moises, “Analisis Malware Android Menggunakan,” vol. 1, no. 2, pp. 41–53, 2023.

[5] E. V. Tjahjadi and B. Santoso, “Klasifikasi Malware Menggunakan Teknik Machine Learning,” *J. Ilm. Ilmu Komput.*, vol. 2, no. 1, pp. 60–70, 2023.

[6] M. A. Hama Saeed, “Malware in Computer Systems: Problems and Solutions,” *IJID (International J. Informatics Dev.*, vol. 9, no. 1, p. 1, 2020, doi: 10.14421/ijid.2020.09101.

[7] H. Kanaker, N. A. Karim, S. A. B. Awwad, N. H. A. Ismail, J. Zraqou, and A. M. F. Al ali, “Trojan Horse Infection Detection in Cloud Based Environment Using Machine Learning,” *Int. J. Interact. Mob. Technol.*, vol. 16, no. 24, pp. 81–106, 2022, doi: 10.3991/ijim.v16i24.35763.

[8] M. Rijal *et al.*, “Perbandingan Kinerja Metode Seleksi Fitur untuk Mendeteksi Aktivitas Trojan Performance Comparison of Feature Selection Methods for Detecting Trojan Activity,” *Jurnal_Pekommas_Vol._7_No*, vol. 2, no. april 2020, pp. 85–97, 2022.

[9] M. Ahmed and H. Saeed, “Malware dalam Sistem Komputer : Masalah dan Solusi,” no. 1, pp. 1–8, 2020.

[10] B. Vasu and N. Pari, “Combining Multimodal DNN and SigPid technique for detecting Malicious Android Apps,” *Proc. 11th Int. Conf. Adv. Comput. ICoAC 2019*, pp. 289–294, 2019, doi: 10.1109/ICoAC48765.2019.247134.

[11] L. Alzubaidi *et al.*, *Review of deep learning: concepts, CNN architectures, challenges, applications, future directions*, vol. 8, no. 1. Springer International Publishing, 2021. doi: 10.1186/s40537-021-00444-8.

[12] A. Peryanto, A. Yudhana, and R. Umar, “Rancang Bangun Klasifikasi Citra Dengan Teknologi Deep Learning BerbPeryanto, A., Yudhana, A., & Umar, R. (2020). Rancang Bangun Klasifikasi Citra Dengan Teknologi Deep Learning Berbasis Metode Convolutional Neural Network. Format : Jurnal Ilmiah Teknik I,” *Format J. Ilm. Tek. Inform.*, vol. 8, no. 2, p. 138, 2020.

[13] N. McLaughlin *et al.*, “Deep android malware detection,” *CODASPY 2017 - Proc. 7th ACM Conf. Data Appl. Secur. Priv.*, pp. 301–308, 2017, doi: 10.1145/3029806.3029823.

[14] A. Roihan, P. A. Sunarya, and A. S. Rafika, “Pemanfaatan Machine Learning dalam Berbagai Bidang: Review paper,” *IJCIT (Indonesian J. Comput. Inf. Technol.*, vol. 5, no. 1, pp. 75–82, 2020, doi: 10.31294/ijcit.v5i1.7951.

[15] I. Nurhaida, V. Ayumi, D. Fitrianah, R. A. M. Zen, H. Noprisson, and H. Wei, “Implementation of deep neural networks (DNN) with batch normalization for batik pattern recognition,” *Int. J. Electr. Comput. Eng.*, vol. 10, no. 2, pp. 2045–2053, 2020, doi: 10.11591/ijece.v10i2.pp2045-2053.

[16] H. Haidros Rahima Manzil and S. Manohar Naik, “DynaMalDroid: Dynamic Analysis-Based Detection Framework for Android Malware Using Machine Learning Techniques,” *IEEE Int. Conf. Knowl. Eng. Commun. Syst. ICKES 2022*, pp. 1–6, 2022, doi: 10.1109/ICKECS56523.2022.10060106.

[17] Dieta Wahyu Asry, Eko Siswanto, Dendy Kurniawan, and Haris Ihsanil Huda, “Deteksi Malware Statis Menggunakan Deep Neural Networks Pada Portable Executable,” *Tek. J. Ilmu Tek. dan Inform.*, vol. 3, no. 1, pp. 19–34, 2023, doi: 10.51903/teknik.v3i1.325.

[18] M. Tokmak, E. U. Küçüksille, and U. Köse, “Deep Learning Based Malware Detection Tool Development for Android Operating System,” *BRAIN. Broad Res. Artif. Intell. Neurosci.*, vol. 12, no. 4, pp. 28–56, 2021, doi: 10.18662/brain/12.4/237.

[19] E. Rasywir, R. Sinaga, and Y. Pratama, “Evaluasi Pembangunan Sistem Pakar Penyakit Tanaman Sawit dengan Metode Deep Neural Network (DNN),” *J. Media ...*, vol. 4, no. 5, pp. 1206–1215, 2020, doi: 10.30865/mib.v4i4.2518.

[20] A. Faisal and A. Subekti, “Deep Neural Network untuk Prediksi Stroke,” vol. 7, no. 3, pp. 443–449, 2021.

[21] E. C. Bayazit, O. K. Sahingoz, and B. Dogan, “Deep Learning based Malware Detection for Android Systems: A Comparative Analysis,” *Teh. Vjesn.*, vol. 30, no. 3, pp. 787–796, 2023, doi: 10.17559/TV-20220907113227.

[22] M. S. Akhtar and T. Feng, “Malware Analysis and Detection Using Machine Learning Algorithms,” *Symmetry (Basel).*, vol. 14, no. 11, 2022, doi: 10.3390/sym14112304.

[23] Y. Ilhamdi, Y. N. Kunang, F. I. Komputer, U. B. Darma, D. Analysis, and C. Crime, “ANALISIS MALWARE PADA SISTEM OPERASI WINDOWS,” pp. 256–264.

[24] U. Divakarla, K. H. K. Reddy, and K. Chandrasekaran, “A Novel Approach towards Windows Malware Detection System Using Deep Neural Networks,” *Procedia Comput. Sci.*, vol. 215, no. 2022, pp. 148–157, 2022, doi: 10.1016/j.procs.2022.12.017.

[25] A. Siddiq, H. Yudiastuti, and F. Panjaitan, “Analisis Perilaku Malware Dengan Metode Surface Analysis Dan Runtime Analysis,” *J. Softw. Eng. Ampera*, vol. 1, no. 3, pp. 160–174, 2020, doi: 10.51519/journalsea.v1i3.53.

[26] M. N. Alenezi, H. Alabdulrazzaq, A. A. Alshaher, and M. M. Alkharang, “Evolution of Malware Threats and Techniques: A Review,” *Int. J. Commun. Networks Inf. Secur.*, vol. 12, no. 3, pp. 326–337, 2020, doi: 10.17762/ijcnis.v12i3.4723.

[27] S. Sinambela, A. R. Pangestu, and R. Feriyanto, “Analisis Aplikasi Malware pada Android dengan Metode Statik,” *J. Ilm. Ilk. - Ilmu Komput. Inform.*, vol. 3, no. 2, pp. 88–94, 2020, doi: 10.47324/ilkominfo.v3i2.101.

[28] M. M. Alani and A. I. Awad, “AdStop: Efficient flow-based mobile adware detection using machine learning,” *Comput. Secur.*, vol. 117, p. 102718, 2022, doi: 10.1016/j.cose.2022.102718.

[29] H. Owen, J. Zarrin, and S. M. Pour, “A Survey on Botnets, Issues, Threats, Methods, Detection and Prevention,” *J. Cybersecurity Priv.*, vol. 2, no. 1, pp. 74–88, 2022, doi: 10.3390/jcp2010006.

[30] S. Liang and Y. Hartanto, “Implementasi Bug Tracking System dengan Metodologi Scrum dan Algoritma Cosine Similarity,” *JURIKOM (Jurnal Ris. Komputer)*, vol. 9, no. 1, p. 24, 2022, doi: 10.30865/jurikom.v9i1.3861.

[31] A. Alraizza and A. Algarni, “Ransomware Detection Using Machine Learning: A Survey,” *Big Data Cogn. Comput.*, vol. 7, no. 3, p. 143, 2023, doi: 10.3390/bdcc7030143.

[32] R. Nagy, K. Németh, D. Papp, and L. Buttyán, *Rootkit Detection on Embedded IoT Devices*, vol. 25, no. 2. 2021. doi: 10.14232/ACTACYB.288834.

[33] M. Naser and Q. Abu Al-Haija, “Spyware Identification for Android Systems Using Fine Trees,” *Inf.*, vol. 14, no. 2, 2023, doi: 10.3390/info14020102.

[34] N. Ochieng, W. Mwangi, and I. Ateya, “Optimizing Computer Worm Detection Using Ensembles,” *Secur. Commun. Networks*, vol. 2019, 2019, doi: 10.1155/2019/4656480.

[35] S. Murdowo, “Mengenal Lebih Dalam Tentang Virus-Virus Komputer dan Perilakunya,” *J. Ilm. Infokam*, vol. 19, no. 1, pp. 74–84, 2023, doi: 10.53845/infokam.v19i1.344.

[36] V. S. Pavlíčková, J. Škubník, T. Ruml, and S. Rimpelová, “A Trojan horse approach for efficient drug delivery in photodynamic therapy: focus on taxanes,” *J. Mater. Chem. B*, pp. 8622–8638, 2023, doi: 10.1039/d2tb02147a.

[37] J. Kan, Y. Shen, J. Xu, E. Chen, J. Zhu, and V. Chen, “RF Analog Hardware Trojan Detection Through Electromagnetic Side-Channel,” *IEEE Open J. Circuits Syst.*, vol. 3, no. June, pp. 237–251, 2022, doi: 10.1109/ojcas.2022.3210163.

[38] G. Li, “Research on Smartphone Trojan Detection Based on the Wireless Sensor Network,” *Secur. Commun. Networks*, vol. 2022, 2022, doi: 10.1155/2022/2455102.

[39] Y. Özkan, “Malware Detection in Forensic Memory Dumps: The Use of Deep Meta-Learning Models,” *Acta Infologica,* vol. 7, no. 1, pp. 165–172, 2023, doi: 10.26650/acin.1282824.

[40] M. F. Ab Razak, M. I. Jaya, Z. Ismail, and A. Firdaus, “Trojan Detection System Using Machine Learning Approach,” *Indones. J. Inf. Syst.*, vol. 5, no. 1, pp. 38–47, 2022, doi: 10.24002/ijis.v5i1.5673.

[41] B. Wijaya and A. Pratama, “Deteksi Penyusupan Pada Server Menggunakan Metode Intrusion Detection System (IDS) Berbasis Snort,” vol. 09, pp. 97–101, 2020.

[42] N. L. Putri, R. A. Nugroho, and R. Herteno, “INTRUSION DETECTION SYSTEM BERBASIS SELEKSI FITUR DENGAN KOMBINASI FILTER INFORMATION GAIN RATIO DAN CORRELATION INTRUSION DETECTION SYSTEM BASED ON FEATURE SELECTION WITH,” vol. 8, no. 3, pp. 457–464, 2021, doi: 10.25126/jtiik.202183154.

[43] W. Muftihaturrahmah, T. Sau, and S. Siswantyo, “Analisis Penggunaan Hasil Deteksi IDS Snort pada Tools RITA dalam Mendeteksi Aktivitas Beacon,” no. 1.

[44] F. A. Aboaoja, A. Zainal, F. A. Ghaleb, B. A. S. Al-rimy, T. A. E. Eisa, and A. A. H. Elnour, “Malware Detection Issues, Challenges, and Future Directions: A Survey,” *Appl. Sci.*, vol. 12, no. 17, 2022, doi: 10.3390/app12178482.

[45] R. B. Auliar and G. Bekaroo, “Security in IoT-based smart homes: A taxonomy study of detection methods of mirai malware and countermeasures,” *Int. Conf. Electr. Comput. Commun. Mechatronics Eng. ICECCME 2021*, no. May, 2021, doi: 10.1109/ICECCME52200.2021.9590841.

[46] D. Prayitno, N. Adhi, and R. Dwi, “Systematic Literature Review : Implementasi Metode Statis Dan Dinamis Pada Analisa Malware,” vol. 16, no. 2, pp. 53–57, 2022.

[47] 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, 2021, doi: 10.1371/journal.pone.0257968.

[48] A. Nugraha and D. A. Gustian, “Deteksi Malware Dridex Menggunakan Signature-based Snort,” *Indones. J. Comput. Sci.*, vol. 10, no. 1, pp. 54–64, 2022, doi: 10.33022/ijcs.v10i1.3068.

[49] N. Li, Z. Zhang, X. Che, Z. Guo, and J. Cai, “A Survey on Feature Extraction Methods of Heuristic Malware Detection,” *J. Phys. Conf. Ser.*, vol. 1757, no. 1, 2021, doi: 10.1088/1742-6596/1757/1/012071.

[50] Z. Hao, “Deep learning review and discussion of its future development,” *MATEC Web Conf.*, vol. 277, p. 02035, 2019, doi: 10.1051/matecconf/201927702035.

[51] A. Raup, W. Ridwan, Y. Khoeriyah, S. Supiana, and Q. Y. Zaqiah, “Deep Learning dan Penerapannya dalam Pembelajaran,” *JIIP - J. Ilm. Ilmu Pendidik.*, vol. 5, no. 9, pp. 3258–3267, 2022, doi: 10.54371/jiip.v5i9.805.

[52] I. H. Sarker, “Deep Learning: A Comprehensive Overview on Techniques, Taxonomy, Applications and Research Directions,” *SN Comput. Sci.*, vol. 2, no. 6, pp. 1–20, 2021, doi: 10.1007/s42979-021-00815-1.

[53] Muhammad Haris Diponegoro, Sri Suning Kusumawardani, and Indriana Hidayah, “Tinjauan Pustaka Sistematis: Implementasi Metode Deep Learning pada Prediksi Kinerja Murid,” *J. Nas. Tek. Elektro dan Teknol. Inf.*, vol. 10, no. 2, pp. 131–138, 2021, doi: 10.22146/jnteti.v10i2.1417.

[54] M. Gopinath and S. C. Sethuraman, “A comprehensive survey on deep learning based malware detection techniques,” *Comput. Sci. Rev.*, vol. 47, p. 100529, 2023, doi: 10.1016/j.cosrev.2022.100529.

[55] H. Abdel-Jaber, D. Devassy, A. Al Salam, L. Hidaytallah, and M. El-Amir, “A Review of Deep Learning Algorithms and Their Applications in Healthcare,” *Algorithms*, vol. 15, no. 2, 2022, doi: 10.3390/a15020071.

[56] R. K. Mishra, G. Y. S. Reddy, and H. Pathak, “The Understanding of Deep Learning: A Comprehensive Review,” *Math. Probl. Eng.*, vol. 2021, 2021, doi: 10.1155/2021/5548884.

[57] S. Jabeen, X. Li, M. S. Amin, O. Bourahla, S. Li, and A. Jabbar, “A Review on Methods and Applications in Multimodal Deep Learning,” *ACM Trans. Multimed. Comput. Commun. Appl.*, vol. 19, no. 2s, pp. 1–41, 2023, doi: 10.1145/3545572.

[58] P. R. Sihombing, “Perbandingan Metode Artificial Neural Network (ANN) dan Support Vector Machine (SVM) untuk Klasifikasi Kinerja Perusahaan Daerah Air Minum (PDAM) di Indonesia,” *J. Ilmu Komput.*, vol. 13, no. 1, p. 9, 2020, doi: 10.24843/jik.2020.v13.i01.p02.

[59] S. Schmidgall *et al.*, “Brain-inspired learning in artificial neural networks: a review,” pp. 1–13, 2023.

[60] M. Madhiarasan and M. Louzazni, “Analysis of Artificial Neural Network: Architecture, Types, and Forecasting Applications,” *J. Electr. Comput. Eng.*, vol. 2022, no. i, 2022, doi: 10.1155/2022/5416722.

[61] W. Li, H. Chen, J. Guo, Z. Zhang, and Y. Wang, “Brain-inspired Multilayer Perceptron with Spiking Neurons,” *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit.*, vol. 2022-June, pp. 773–783, 2022, doi: 10.1109/CVPR52688.2022.00086.

[62] A. Ajit, K. Acharya, and A. Samanta, “A Review of Convolutional Neural Networks,” *Int. Conf. Emerg. Trends Inf. Technol. Eng. ic-ETITE 2020*, pp. 1–5, 2020, doi: 10.1109/ic-ETITE47903.2020.049.

[63] A. D. Tarkus, S. R. U. A. Sompie, and A. Jacobus, “Implementasi Metode Recurrent Neural Network pada Pengklasifikasian Kualitas Telur Puyuh,” *J. Tek. Inform.*, vol. 15, no. 2, pp. 137–144, 2020.

[64] K. Y. Chan *et al.*, “Deep neural networks in the cloud: Review, applications, challenges and research directions,” *Neurocomputing*, vol. 545, p. 126327, 2023, doi: 10.1016/j.neucom.2023.126327.

[65] M. Khodayar and J. Regan, “Deep Neural Networks in Power Systems: A Review,” *Energies*, vol. 16, no. 12, 2023, doi: 10.3390/en16124773.

[66] C. Lin, Z. Chen, Y. Huang, H. Jiang, W. Du, and Q. Chen, “A Deep Neural Network Based on Circular Representation for Target Detection,” *J. Sensors*, vol. 2022, 2022, doi: 10.1155/2022/4437446.

[67] M. Hibat-Allah, M. Ganahl, L. E. Hayward, R. G. Melko, and J. Carrasquilla, “Recurrent neural network wave functions,” *Phys. Rev. Res.*, vol. 2, no. 2, pp. 1–17, 2020, doi: 10.1103/PhysRevResearch.2.023358.

[68] H. I. Fawaz, G. Forestier, J. Weber, L. Idoumghar, and P. A. Muller, “Deep Neural Network Ensembles for Time Series Classification,” *Proc. Int. Jt. Conf. Neural Networks*, vol. 2019-July, 2019, doi: 10.1109/IJCNN.2019.8852316.

[69] D. Elbrachter, D. Perekrestenko, P. Grohs, and H. Bolcskei, “Deep Neural Network Approximation Theory,” *IEEE Trans. Inf. Theory*, vol. 67, no. 5, pp. 2581–2623, 2021, doi: 10.1109/TIT.2021.3062161.

[70] R. B. Hadiprakoso, N. Qomariasih, and R. N. Yasa, “Identifikasi Malware Android Menggunakan Pendekatan Analisis Hibrid Dengan Deep Learning,” *J. Teknol. Inf. Univ. Lambung Mangkurat*, vol. 6, no. 2, pp. 77–84, 2021, doi: 10.20527/jtiulm.v6i2.82.

[71] T. Informatics and E. Vol, “ADVANCED MALICIOUS SOFTWARE DETECTION USING DNN Sulartopo 1 , Dani Sasmoko 2 , Zaenal Mustofa 3 , Arsito Ari Kuncoro 4 Universita Sains dan Teknologi Komputer,” vol. 1, no. 1, pp. 80–107, 2022.

[72] O. N. Elayan and A. M. Mustafa, “Android malware detection using deep learning,” *Procedia Comput. Sci.*, vol. 184, no. 2019, pp. 847–852, 2021, doi: 10.1016/j.procs.2021.03.106.

[73] Didih Rizki Chandranegara, Jafar Shodiq Djawas, Faiq Azmi Nurfaizi, and Zamah Sari, “Malware Image Classification Using Deep Learning InceptionResNet-V2 and VGG-16 Method,” *J. Online Inform.*, vol. 8, no. 1, pp. 61–71, 2023, doi: 10.15575/join.v8i1.1051.

[74] S. Lu, Q. Li, and X. Zhu, “Stealthy Malware Detection Based on Deep Neural Network,” *J. Phys. Conf. Ser.*, vol. 1437, no. 1, 2020, doi: 10.1088/1742-6596/1437/1/012123.

[75] N. Afifah and D. Stiawan, “The Implementation of Deep Neural Networks Algorithm for Malware Classification,” *Comput. Eng. Appl. J.*, vol. 8, no. 3, pp. 189–202, 2019, doi: 10.18495/comengapp.v8i3.294.

[76] T. Carrier, P. Victor, A. Tekeoglu, and A. Lashkari, “Detecting Obfuscated Malware using Memory Feature Engineering,” no. Icissp, pp. 177–188, 2022, doi: 10.5220/0010908200003120.

[77] S. S. Shafin, G. Karmakar, and I. Mareels, “Obfuscated Memory Malware Detection in Resource-Constrained IoT Devices for Smart City Applications,” *Sensors*, vol. 23, no. 11, pp. 1–18, 2023, doi: 10.3390/s23115348.

[78] E. A. Winanto, K. Kurniabudi, S. Sharipuddin, I. S. Wijaya, and D. Sandra, “Deteksi Serangan pada Jaringan Kompleks IoT menggunakan Recurrent Neural Network,” *JURIKOM (Jurnal Ris. Komputer)*, vol. 9, no. 6, p. 1996, 2022, doi: 10.30865/jurikom.v9i6.5298.

[79] Kurniabudi, D. Stiawan, Darmawijoyo, M. Y. Bin Bin Idris, A. M. Bamhdi, and R. Budiarto, "CICIDS-2017 Dataset Feature Analysis with Information Gain for Anomaly Detection," *IEEE Access*, vol. 8, pp. 132911–132921, 2020, doi: 10.1109/ACCESS.2020.3009843.

[80] K. Kurniabudi, A. Harris, and A. Rahim, "Seleksi Fitur Dengan Information Gain Untuk Meningkatkan Deteksi Serangan DDoS menggunakan Random Forest," *Techno.Com*, vol. 19, no. 1, pp. 56–66, 2020, doi: 10.33633/tc.v19i1.2860.

[81] R. Galih, "Deteksi Malware Android Menggunakan Pengklasifikasi Pembelajaran Mesin Paralel," vol. 10, no. 5, pp. 4887–4895, 2023.

[82] I. Muhamad Malik Matin, "Hyperparameter Tuning Menggunakan GridsearchCV pada Random Forest untuk Deteksi Malware," *Multinetics*, vol. 9, no. 1, pp. 43–50, 2023, doi: 10.32722/multinetics.v9i1.5578.

[83] Togu Novriansyah Turnip, Chatrine Febryanti Manurung, Yogi Septian Lubis, and Rachel Gultom, "Klasifikasi Malware Android Aplikasi Menggunakan Random Forest Berdasarkan Fitur Statik," *Tek. Inform. dan Sist. Inf.*, vol. 10, no. 1, pp. 926–936, 2023.

[84] Baiq Nurul Azmi, Arief Hermawan, and Donny Avianto, "Analisis Pengaruh Komposisi Data Training dan Data Testing pada Penggunaan PCA dan Algoritma Decision Tree untuk Klasifikasi Penderita Penyakit Liver," *JTIM J. Teknol. Inf. dan Multimed.*, vol. 4, no. 4, pp. 281–290, 2023, doi: 10.35746/jtim.v4i4.298.

[85] A. Nurhopipah and U. Hasanah, "Dataset Splitting Techniques Comparison For Face Classification on CCTV Images," *IJCCS (Indonesian J. Comput. Cybern. Syst.*, vol. 14, no. 4, p. 341, 2020, doi: 10.22146/ijccs.58092.

[86] D. S. Suparno, “Pengenalan Pola Untuk Mengetahui Jumlah Target Pengunjung Mall Berdasarkan Usia, Gender, Pendapatan Pertahun, Pengeluaran, Tujuannya Untuk Mempermudah Mengetahui Target Pasar Menggunakan Metode EDA, K-Means, Hierarchial Clustering, Confusion Matrix,” *Sains, Apl. Komputasi, dan Teknol. Inf.*, vol. 3, no. 2, pp. 61–69, 2021.

[87] F. Bourebaa and M. Benmohamed, “A Deep Neural Network Model for Android Malware Detection,” *Int. J. Informatics Appl. Math.*, vol. 4, no. 1, pp. 1–14, 2020.