

DAFTAR PUSTAKA

- [1] M. Murhej and G. Nallasivan, “Multimodal framework for phishing attack detection and mitigation through behavior analysis using EM-BERT and SPCA-BASED EAI-SC-LSTM,” *Frontiers in Communications and Networks*, vol. 6, 2025, doi: 10.3389/frcmn.2025.1587654.
- [2] F. Tamimi and S. Munawaroh, “Teknologi Sebagai Kegiatan Manusia Dalam Era Modern Kehidupan Masyarakat,” *Saturnus : Jurnal Teknologi dan Sistem Informasi*, vol. 2, no. 3, pp. 66–74, 2024, doi: 10.61132/saturnus.v2i3.157
- [3] S. Agustin, “Dampak Kemajuan Teknologi Informasi Era Digital Terhadap Keamanan Data Pribadi Tantangan Dan Penanggulangan Terhadap Kejahatan Cyber,” vol. 1, no. 6, pp. 500–504, 2024, [Online]. Available: <https://ejournal.amirulbangunbangsapublishing.com/index.php/jpnmb/index>
- [4] Ionescu, A., & Ionica, D, “ENISA Threat Landscape 2024 Report: Cyber threat landscape in the financial sector”, 2025, [Online]. Available: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025>
- [5] Anti-Phishing Working Group, “Phishing Activity Trends Report – 4th Quarter 2024”, 2024, [Online]. Available: <https://apwg.org/trendsreports>
- [6] Federal Bureau of Investigation, “FBI Releases Annual Internet Crime Report”, 2025, [Online]. Available: <https://www.fbi.gov/news/press-releases/fbi-releases-annual-internet-crime-report>
- [7] Anti-Phishing Working Group, “Phishing Activity Trends Report – 1st Quarter 2025”, 2025, [Online]. Available: https://docs.apwg.org/reports/apwg_trends_report_q1_2025.pdf

- [8] BSSN, "Lanskap Keamanan Siber Indonesia 2024", Badan Siber dan Sandi Negara, 2024
- [9] S. Bahdra, "Phisher - A Multimodal Approach for Phishing Detection," Research Archive of Rising Scholars, 2025, [Online]. Available: <https://doi.org/10.58445/rars.3223>
- [10] Trend Micro, "Email Threat Landscape Report: Evolving Threats in Email-Based Attacks", 2025, [Online]. Available: <https://www.trendmicro.com/vinfo/us/security/news/threat-landscape/email-threat-landscape-report-evolving-threats-in-email-based-attacks>
- [11] Microsoft Security, "Cyber Signals Issue 9: AI-powered deception – Emerging fraud threats and countermeasures", 2025, [Online]. Available: <https://www.microsoft.com/en-us/security/blog/2025/04/16/cyber-signals-issue-9-ai-powered-deception-emerging-fraud-threats-and-countermeasures/>
- [12] V. Adeyemi Onih, "Phishing Detection Using Machine Learning: A Model Development and Integration," International Journal of Scientific and Management Research, vol. 07, no. 04, pp. 27–63, 2024, doi: 10.37502/ijsmr.2024.7403
- [13] H. Fares et al., "Machine Learning Approach for Email Phishing Detection," in Procedia Computer Science, Elsevier B.V., 2024, pp. 746–751. doi: 10.1016/j.procs.2024.11.179.
- [14] Y. S. Murti and P. Naveen, "Machine Learning Algorithms for Phishing Email Detection," Journal of Logistics, Informatics and Service Science, vol. 10, no. 2, pp. 249–261, 2023, doi: 10.33168/JLISS.2023.0217.

- [15] P. C. R. Chinta, C. S. Moore, L. M. Karaka, M. Sakuru, V. Bodepudi, and S. R. Maka, “Building an Intelligent Phishing Email Detection System Using Machine Learning and Feature Engineering,” *European Journal of Applied Science, Engineering and Technology*, vol. 3, no. 2, pp. 41–54, Mar. 2025, doi: 10.59324/ejaset.2025.3(2).04.
- [16] N. Altwaijry, I. Al-Turaiki, R. Alotaibi, and F. Alakeel, “Advancing Phishing Email Detection: A Comparative Study of Deep Learning Models,” *Sensors*, vol. 24, no. 7, Apr. 2024, doi: 10.3390/s24072077.
- [17] A. Raihan, M. Fadhli, and L. Lindawati, “Implementation of Deep Learning for Detecting Phishing Attack on Websites With Combination of CNN and LSTM,” *Jurnal Teknik Informatika (Jutif)*, vol. 5, no. 5, pp. 1451–1459, Oct. 2024, doi: 10.52436/1.jutif.2024.5.5.2446.
- [18] A. F. Mahmud and S. Wirawan, “Deteksi Phishing Website menggunakan Machine Learning Metode Klasifikasi,” *Sistemasi: Jurnal Sistem Informasi*, vol. 13, no. 4, pp. 2540–9719, 2024, [Online]. Available: <http://sistemasi.ftik.unisi.ac.id>
- [19] H. Brioua, H. Siyambas, and D. O. Sahin, “Phishing E-mail Detection with Machine Learning and Deep Learning: Improving Classification Performance with Proposed New Features,” *Balkan Journal of Electrical & Computer Engineering*, vol. 13, pp. 183–193, 2025.
- [20] M. Hosseinzadeh et al., “Improving phishing email detection performance through deep learning with adaptive optimization,” *Sci Rep*, vol. 15, no. 1, Dec. 2025, doi: 10.1038/s41598-025-20668-5.
- [21] A. Al Tawil, L. Almazaydeh, D. Qawasmeh, B. Qawasmeh, M. Alshinwan, and K. Elleithy, “Comparative Analysis of Machine Learning Algorithms for Email Phishing Detection Using TF-IDF, Word2Vec, and BERT,” *Computers, Materials and Continua*, vol. 81, no. 2, pp. 3395–3412, 2024, doi: 10.32604/cmc.2024.057279.

- [22] R. Meléndez, M. Ptaszynski, and F. Masui, “Comparative Investigation of Traditional Machine-Learning Models and Transformer Models for Phishing Email Detection,” *Electronics (Switzerland)*, vol. 13, no. 24, Dec. 2024, doi: 10.3390/electronics13244877.
- [23] I. Goodfellow, Y. Bengio, and A. Courville, “Deep Learning.”
- [24] Vanita. (2024). An Extant of Natural Language Processing. *International Journal for Multidisciplinary Research*, 6(2), 1–6. www.ijfmr.com
- [25] H. Wang, C. Pan, X. Guo, C. Ji, and K. Deng, “From object detection to text detection and recognition: A brief evolution history of optical character recognition,” *Wiley Interdiscip Rev Comput Stat*, 2021, doi: 10.1002/wics.1547
- [26] M. Rahayu Ningsih and Jumanto, “Sentiment Analysis on SocialMedia Using TF-IDF Vectorization and H2O Gradient Boosting for Student Anxiety Detection,” *Scientific Journal of Informatics*, vol. 11, no. 4, pp. 1137–1144, 2024, doi: 10.15294/sji.v11i4.20582
- [27] A. Vaswani et al., “Attention Is All You Need,” Jun. 2017, [Online]. Available: <http://arxiv.org/abs/1706.03762>
- [28] V. Sanh, L. Debut, J. Chaumond, and T. Wolf, “DistilBERT, a distilled version of BERT: smaller, faster, cheaper and lighter,” Oct. 2019, [Online]. Available: <http://arxiv.org/abs/1910.01108>
- [29] I. Sparta Adi Wayan and E. P. Parianthana, “Support Vector Machine Performance In Diabetes Data Classification With GridsearchCV Optimization,” *Jurnal Multidisiplin Sahombu*, vol. 5, no. 1, pp. 179–186, 2025, doi: 10.58471/jms.v5i01.

- [30] N. W. Wardani, A. A. S. Pradhana, and I. N. D. Kotama, “Binary Classification of Exchange Rate Trends Using Logistic Regression,” JSIKTI: Jurnal Sistem Informasi dan Komputer Terapan Indonesia, vol. 7, no. 4, pp. 137–144, 2025, [Online]. Available: www.infoteks.orgJournalPageisavailableto<https://infoteks.org/journals/index.php/jsikti>
- [31] D. Ahgil Misman, F. Ramadhan Verdiansyah, F. Dika Permana, and R. Ramadhan, “Literatur Review: Klasifikasi Penyakit Hati Menggunakan Metode Deep Neural Networks,” JRIIN : Jurnal Riset Informatika dan Inovasi, vol. 2, no. 8, pp. 1322–1327, 2025, [Online]. Available: <https://jurnalmahasiswa.com/index.php/jriin>
- [32] L. Hakim, A. Sobri, L. Sunardi, and D. Nurdiansyah, “Prediksi penyakit jantung berbasis mesin learning dengan menggunakan metode k-nn,” Jurnal Digital Teknologi Informasi, vol. 7, pp. 14–20, 2025, doi: 10.32502/digital.v7i2.9429
- [33] X. Song, A. Salcianu, Y. Song, D. Dopson, and D. Zhou, “Fast WordPiece Tokenization,” Oct. 2021, [Online]. Available: <https://arxiv.org/abs/2012.15524>