DAFTAR PUSTAKA

Abidoye, A. P., & Kabaso, B. (2021). Hybrid Machine Learning: A Tool to Detect Phishing Attacks in Communication Networks. *ECTI Transactions on Computer and Information Technology (ECTI-CIT)*, *15*(3), 374–389. https://doi.org/10.37936/ecti-cit.2021153.240565

Akrout, M., Feriani, A., Bellili, F., Mezghani, A., & Hossain, E. (2023). *Domain Generalization in Machine Learning Models for Wireless Communications: Concepts, State-of-the-Art, and Open Issues*. http://arxiv.org/abs/2303.08106

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. In *Frontiers in Computer Science* (Vol. 3). Frontiers Media S.A. https://doi.org/10.3389/fcomp.2021.563060

Altan, I., Bachir, A., Parbhulkar, Y., Rizvi, A. M., & Farazi, M. (2025). *Dual-Path Phishing Detection: Integrating Transformer-Based NLP with Structural URL Analysis*. http://arxiv.org/abs/2509.20972

Ari Kustiawan, Y., & Ghauth, K. I. (2025). PhishOFE: A Novel Machine Learning Framework for Real-Time Phishing URL Detection With Optimized Feature Engineering. *IEEE Access*, *13*, 169606–169627. https://doi.org/10.1109/ACCESS.2025.3614126

Breiman, L. (2001). *Random Forests* (Vol. 45).

Castaño, F., Fidalgo, E., Alegre, E., Chaves, D., & Sanchez-Paniagua, M. (2021). *State of the Art: Content-based and Hybrid Phishing Detection*. http://arxiv.org/abs/2101.12723

Chen, T., & Guestrin, C. (2016). XGBoost: A scalable tree boosting system. *Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, *13-17-August-2016*, 785–794. https://doi.org/10.1145/2939672.2939785

Fisher, A., Rudin, C., & Dominici, F. (2019). All Models are Wrong, but Many are Useful: Learning a Variable's Importance by Studying an Entire Class of Prediction Models Simultaneously. In *Journal of Machine Learning Research* (Vol. 20). http://jmlr.org/papers/v20/18-760.html.

Hassija, V., Chamola, V., Mahapatra, A., Singal, A., Goel, D., Huang, K., Scardapane, S., Spinelli, I., Mahmud, M., & Hussain, A. (2024). Interpreting Black-Box Models: A Review on Explainable Artificial Intelligence. In *Cognitive Computation* (Vol. 16, Number 1, pp. 45–74). Springer. https://doi.org/10.1007/s12559-023-10179-8

Jayaprakash, S. M., Moody, E. W., Lauría, E. J. M., Regan, J. R., & Baron, J. D. (2014). Early Alert of Academically At-Risk Students: An Open Source Analytics Initiative. In *Journal of Learning Analytics* (Vol. 1, Number 1). https://confluence.sakaiproject.org/pages/viewpage.action?pageId=75671025

Joshi, A., Lloyd, L., & Westin, P. (2019). *Using Lexical Features for Malicious URL Detection-A Machine Learning Approach*.

Kalla, D., Samaah, F., Kuraku, S., & Smith, N. (2023). Phishing Detection Implementation using Databricks and Artificial Intelligence. In *International Journal of Computer Applications* (Vol. 185, Number 11).

Kehkashan, T., Abdelhaq, M., Al-Shamayleh, A. S., Huda, N., Yaseen, I. A., Ahmed, A. I. A., & Akhunzada, A. (2025). Explainable phishing website detection for secure and sustainable cyber infrastructure. *Scientific Reports*, *15*(1). https://doi.org/10.1038/s41598-025-27984-w

Khairunnisya, A., Lindawati, L., & Zefi, S. (2025). Phishing URL Detection System Using Random Forest and Gradient Boosting for Cybercrime Prevention. *CSRID (Computer Science Research and Its Development Journal)*, *17*(3), 296–310. https://doi.org/10.22303/csrid-.17.3.2025.296-310

Linh, D. M., & Hung, T. C. (2025). Mendeley Data. *Data in Brief*, *63*. https://doi.org/10.1016/j.dib.2025.112162

Lundberg, S. M., Allen, P. G., & Lee, S.-I. (n.d.). *A Unified Approach to Interpreting Model Predictions*. Retrieved https://github.com/slundberg/shap

Lundberg, S. M., Erion, G., Chen, H., DeGrave, A., Prutkin, J. M., Nair, B., Katz, R., Himmelfarb, J., Bansal, N., & Lee, S. I. (2020). From local explanations to global understanding with explainable AI for trees. *Nature Machine Intelligence*, *2*(1), 56–67. https://doi.org/10.1038/s42256-019-0138-9

Nayak, G. S., Muniyal, B., & Belavagi, M. C. (2025). Enhancing Phishing Detection: A Machine Learning Approach With Feature Selection and Deep Learning Models. *IEEE Access*, *13*, 33308–33320. https://doi.org/10.1109/ACCESS.2025.3543738

Raj, M. M., & Arul Jothi, J. A. (2022). Hybrid Approach for Phishing Website Detection Using Classification Algorithms. *ParadigmPlus*, *3*(3), 16–29. https://doi.org/10.55969/paradigmplus.v3n3a2

Ramchand, S., Ploszajski, M., Virdi, A., Cole, D., & Xie, X. (2024). *Explainable Machine Learning to Uncover Distinct Phenotypic Signatures of Hypertrophic Cardiomyopathy and Fabry Disease*. https://doi.org/10.21203/rs.3.rs-3864850/v1

Saha Roy, S., & Nilizadeh, S. (2024). *Utilizing Large Language Models to Optimize the Detection and Explainability of Phishing Websites* (Vol. 1). Retrieved https://freephish.org

Sahingoz, O. K., Buber, E., Demir, O., & Diri, B. (2019). Machine learning based phishing detection from URLs. *Expert Systems with Applications*, *117*, 345–357. https://doi.org/10.1016/j.eswa.2018.09.029

Sankaranarayanan, S., Sivachandran, A. T., Mohd Khairuddin, A. S., Hasikin, K., & Wahab Sait, A. R. (2024). An ensemble classification method based on machine learning models for malicious Uniform Resource Locators (URL). *PLoS ONE*, *19*(5). https://doi.org/10.1371/journal.pone.0302196

Uddin, K. M. M., Biswas, N., Rikta, S. T., Nur -A-Alam, Md., & Mostafiz, R. (2025). Explainable Machine Learning for Phishing Site Detection: A High-Efficiency Approach Using Boosting Models and SHAP. *The Journal of Engineering*, *2025*(1). https://doi.org/10.1049/tje2.70110

Vadhil, F. A., Salihi, M. L., & Nanne, M. F. (2024). Machine learning-based intrusion detection system for detecting web attacks. *IAES International Journal of Artificial Intelligence*, *13*(1), 711–721. https://doi.org/10.11591/ijai.v13.i1.pp711-721

Vivas, D. E. D., Pena, W. Y. G., Botero, S. P. C., & Rojas, A. E. (2024). A Controlled Phishing Attack in a University Community: A Case Study. *Journal of Internet Services and Information Security*, *14*(2), 98–110. https://doi.org/10.58346/JISIS.2024.I2.007

Wang, H., Liang, Q., Hancock, J. T., & Khoshgoftaar, T. M. (2024). Feature selection strategies: a comparative analysis of SHAP-value and importance-based methods. *Journal of Big Data*, *11*(1). https://doi.org/10.1186/s40537-024-00905-w

Wang, J., Lan, C., Liu, C., Ouyang, Y., Qin, T., Lu, W., Chen, Y., Zeng, W., & Yu, P. S. (2022). *Generalizing to Unseen Domains: A Survey on Domain Generalization*. http://arxiv.org/abs/2103.03097