BIBLIOGRAPHY

[1] Kaspersky Lab, "Kaspersky reports 6.4 million shopping phishing attempts and over 20 million gaming attacks detected in 2025." Accessed: Nov. 11, 2025. [Online]. Available: https://www.kaspersky.com/about/press-releases/kaspersky-reports-64-million-shopping-phishing-attempts-and-over-20-million-gaming-attacks-detected-in-2025

[2] S. Lesmana, "10 Modus Penipuan dengan Kerugian Tertinggi di Indonesia Menurut OJK." Accessed: Dec. 04, 2025. [Online]. Available: https://www.bicaranetwork.com/ekonomi/29515976856/10-modus-penipuan-dengan-kerugian-tertinggi-di-indonesia-menurut-ojk

[3] S. Sheng, B. Wardman, G. Warner, L. F. Cranor, J. Hong, and C. Zhang, "An Empirical Analysis of Phishing Blacklists," in *roceedings of the Sixth Conference on Email and Anti-Spam (CEAS)*., 2009.

[4] F. Ji *et al.*, "Evaluating the Effectiveness and Robustness of Visual Similarity-based Phishing Detection Models," *ArXiv*, Jan. 2025, [Online]. Available: http://arxiv.org/abs/2405.19598

[5] S. Alnemari and M. Alshammari, "Detecting Phishing Domains Using Machine Learning," *Applied Sciences (Switzerland)*, vol. 13, Apr. 2023, doi: 10.3390/app13084649.

[6] P. Maturure, A. Ali, and A. Gegov, "'Hybrid Machine Learning Model for Phishing Detection,'" in *International IEEE Conference proceedings, IS*, Institute of Electrical and Electronics Engineers Inc., 2024. doi: 10.1109/IS61756.2024.10705257.

[7] Y. Taşer and P. Taşer, "Multimodal Machine Learning in Cybersecurity," *Innovative Artificial Intelligence (INNAI)*, vol. 1, no. 1, pp. 47–55, 2025.

[8] S. Karmakar, D. Santra, and A. Tewary, "AI/ML Dual Approach for Phishing Domain Detection: URL and Image Analysis," in *Optimization and Artificial Intelligent Strategies for Engineering and Management*, BS Publications, Oct. 2024. doi: 10.37285/bsp.oaisem2025.39.

[9] M. W. Shaukat, R. Amin, M. M. A. Muslam, A. H. Alshehri, and J. Xie, "A Hybrid Approach for Alluring Ads Phishing Attack Detection Using Machine Learning," *Sensors*, vol. 23, Oct. 2023, doi: 10.3390/s23198070.

[10] S. Aslam, H. Aslam, A. Manzoor, C. Hui, and A. Rasool, "AntiPhishStack: LSTM-based Stacked Generalization Model for Optimized Phishing URL Detection," *MDPI*, vol. 10, 2022, doi: 10.3390/xxxxx.

[11] S. Gan, S. Shao, L. Chen, L. Yu, and L. Jiang, "Adapting hidden naive bayes for text classification," *Mathematics*, vol. 9, no. 19, Oct. 2021, doi: 10.3390/math9192378.

[12] H. B. Swaminathan, A. Sommer, U. Iurgel, A. Becker, and M. Atzmueller, "Comparative Analysis of Deep Learning-Based Feature Extractors for Change Detection in Automotive Radar Maps," *IEEE Access*, 2024, doi: 10.1109/ACCESS.2024.0429000.

[13] Lukito and W. Bambang Triadi Handaya, "Deteksi Website Phishing Menggunakan Teknik Machine Learning," *Jurnal Informatika Atma Jogja*, 2025.

[14] S. Marchal, G. Armano, T. Grondahl, K. Saari, N. Singh, and N. Asokan, "Off-the-hook: An efficient and usable client-side phishing prevention application," *IEEE Transactions on Computers*, vol. 66, no. 10, pp. 1717–1733, Oct. 2017, doi: 10.1109/TC.2017.2703808.

[15] R. M. Mohammad, F. Thabtah, and L. McCluskey, "Intelligent rule-based phishing websites classification," *IET Inf. Secur.*, vol. 8, no. 3, pp. 153–160, 2014, doi: 10.1049/iet-ifs.2013.0202.

[16] H. Le, Q. Pham, D. Sahoo, and S. C. H. Hoi, "URLNet: Learning a URL Representation with Deep Learning for Malicious URL Detection," *ArXiv*, Mar. 2018, [Online]. Available: http://arxiv.org/abs/1802.03162

[17] H. Zhang, G. Liu, T. W. S. Chow, and W. Liu, "Textual and visual content-based anti-phishing: A Bayesian approach," *IEEE Trans. Neural Netw.*, vol. 22, no. 10, pp. 1532–1546, Oct. 2011, doi: 10.1109/TNN.2011.2161999.

[18] T. Chung *et al.*, "A Longitudinal, End-to-End View of the DNSSEC Ecosystem," USENIX Association, 2005, p. 72.

[19] W. Cavnar and J. M. Trenkle, "N-Gram-Based Text Categorization," 2001. [Online]. Available: https://www.researchgate.net/publication/2375544

[20] C. D. Manning, P. Raghavan, and H. Schütze, *An Introduction to Information Retrieval*. Cambridge: Cambridge University Press, 2009.

[21] R. Fauzan, A. V. Vitianingsih, D. Cahyono, A. L. Maukar, and Y. A. B. Suprio, "Penerapan Algoritma Klasifikasi pada Machine Learning untuk Deteksi Phishing," *MALCOM: Indonesian Journal of Machine Learning and Computer Science*, vol. 5, no. 2, pp. 531–540, Mar. 2025, doi: 10.57152/malcom.v5i2.1968.

[22] A. Niculescu-Mizil and R. Caruana, "Predicting Good Probabilities With Supervised Learning," in *Proceedings of the 22nd International Conference on Machine Learning,* 2005.

[23] Ian Goodfellow, Yoshua Bengio, Aaron Courville, and Francis Bach, *Deep Learning (Adaptive Computation and Machine Learning Series)*. The MIT Press, 2017.

[24] S. K. Birthriya, P. Ahlawat, and A. K. Jain, "Enhanced Phishing Website Detection Using Dual-Layer CNN and GRU with Attention Mechanism and Lexical NLP Features," *SN Comput. Sci.*, vol. 5, no. 7, Oct. 2024, doi: 10.1007/s42979-024-03282-6.

[25] R. Yang, K. Zheng, B. Wu, C. Wu, and X. Wang, "Phishing website detection based on deep convolutional neural network and random forest ensemble learning," *Sensors*, vol. 21, no. 24, Dec. 2021, doi: 10.3390/s21248281.

[26] C. Sivasankar, A. Tamilarasan, S. Christy, and S. Parthiban, "Towards Practical Phishing Detection: Addressing Challenges with Hybrid Machine Learning Architectures," IEEE, 2025. doi: 10.1109/ICCRTEE64519.2025.11053024.

[27] A. Mirugwe, M. ; Lillian Tamale, and J. Nyirenda, "Improving Tuberculosis Detection in Chest X-Ray Images Through Transfer Learning and Deep Learning: Comparative Study of Convolutional Neural Network Architectures," *JMIRx Med*, vol. 6, 2025, doi: 10.1101/2024.08.02.24311396v1.

[28] H. Ghuge, D. Ghuge, A. Rangneniwar, P. Samudra, and A. V Markad, "Real-Time Detection of Malicious URLs Using Feature-Based Machine Learning Approaches," *IJIRMPS*, vol. 13, no. 2, pp. 2349–7300, 2025, [Online]. Available: www.ijirmps.org

[29] L. Zhang, "Features extraction based on Naive Bayes algorithm and TF-IDF for news classification," *PLoS One*, vol. 20, no. 7 July, Jul. 2025, doi: 10.1371/journal.pone.0327347.

[30] W. Hussain *et al.*, "Ensemble genetic and CNN model-based image classification by enhancing hyperparameter tuning," *Sci. Rep.*, vol. 15, no. 1, Dec. 2025, doi: 10.1038/s41598-024-76178-3.

[31] D. Masters and C. Luschi, "Revisiting Small Batch Training for Deep Neural Networks," *ArXiv*, Apr. 2018, [Online]. Available: http://arxiv.org/abs/1804.07612

[32] Q. T. Bui *et al.*, "Gradient boosting machine and object-based cnn for land cover classification," *Remote Sens. (Basel).*, vol. 13, no. 14, Jul. 2021, doi: 10.3390/rs13142709.

[33] M. M. Opentext, A. Narayanan, O. Canada, S. Jou, M. Arlitt, and M. Pospelova, "Is F 1 Score Suboptimal for Cybersecurity Models? Introducing C score , a Cost-Aware Alternative for Model Assessment."

[34] M. A. Razzaq *et al.*, "A Hybrid Multimodal Emotion Recognition Framework for UX Evaluation Using Generalized Mixture Functions," *Sensors*, vol. 23, no. 9, May 2023, doi: 10.3390/s23094373.

[35] A. Aljofey *et al.*, "An effective detection approach for phishing websites using URL and HTML features," *Sci. Rep.*, vol. 12, no. 1, Dec. 2022, doi: 10.1038/s41598-022-10841-5.

[36] S. Handayani and D. Toresa, "Naïve Bayes Alpha Parameter Optimization with Ant Colony for Clinical Text Classification," *Jurnal Teknologi Informasi & Komunikasi*, vol. 16, no. 1, pp. 48–57, 2025, doi: 10.31849/digitalzone.v16i1.

[37] M. Korkmaz, E. Kocyigit, O. K. Sahingoz, and B. Diri, "Phishing Web Page Detection Using N-gram Features Extracted from URLs," in *HORA 2021 - 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications, Proceedings*, Institute of Electrical and Electronics Engineers Inc., Jun. 2021. doi: 10.1109/HORA52670.2021.9461378.

[38] E. H. Yulianti, O. Soesanto, and Y. Sukmawaty, "Penerapan Metode Extreme Gradient Boosting (XGBOOST) pada Klasifikasi Nasabah Kartu Kredit," *JOMTA Journal of Mathematics: Theory and Applications*, vol. 4, no. 1, 2022.

[39] E. Fazzari, D. Romano, F. Falchi, and C. Stefanini, "ARTEMIS: animal recognition through enhanced multimodal integration system," *International Journal of Machine Learning and Cybernetics*, vol. 16, no. 9, pp. 5877–5892, Sep. 2025, doi: 10.1007/s13042-025-02602-3.

[40] K. R. Sheth and V. S. Vora, "Preserving authenticity: transfer learning methods for detecting and verifying facial image manipulation," *Vietnam J. Sci. Technol.*, vol. 62, no. 3, pp. 562–576, Jun. 2024, doi: 10.15625/2525-2518/18626.

[41] A. Arini, M. Azhari, I. I. A. Fitri, and F. Fahrianto, "Performance Analysis of Transfer Learning Models for Identifying AI-Generated and Real Images," *JURNAL TEKNIK INFORMATIKA*, vol. 17, no. 2, pp. 139–152, Oct. 2024, doi: 10.15408/jti.v17i2.40453.

[42] H. Xu, Y. Yu, J. Chang, X. Hu, Z. Tian, and O. Li, "Precision lung cancer screening from CT scans using a VGG16-based convolutional neural network," *Front. Oncol.*, vol. 14, 2024, doi: 10.3389/fonc.2024.1424546.

[43] J. Yang, Z. Li, Z. Gu, and W. Li, "Research on floating object classification algorithm based on convolutional neural network," *Sci. Rep.*, vol. 14, no. 1, Dec. 2024, doi: 10.1038/s41598-024-83543-9.

[44] N. V Chawla, N. Japkowicz, and A. Ko, "Editorial: Special Issue on Learning from Imbalanced Data Sets," *ACM SIGKDD Explorations Newsletter*, 2004, [Online]. Available: http://purl.org/peter.turney/bibliographies/cost-

[45] 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.

[46] M. K. Hasan, M. A. Alam, D. Das, E. Hossain, and M. Hasan, "Diabetes prediction using ensembling of different machine learning classifiers," *IEEE Access*, vol. 8, pp. 76516–76531, 2020, doi: 10.1109/ACCESS.2020.2989857.

[47] L. R. Kalabarige, R. S. Rao, A. Abraham, and L. A. Gabralla, "Multilayer Stacked Ensemble Learning Model to Detect Phishing Websites," *IEEE Access*, vol. 10, pp. 79543–79552, 2022, doi: 10.1109/ACCESS.2022.3194672.

[48] N. Innab *et al.*, "Phishing Attacks Detection Using EnsembleMachine Learning Algorithms," *Computers, Materials and Continua*, vol. 80, no. 1, pp. 1325–1345, 2024, doi: 10.32604/cmc.2024.051778.

[49] Enas Mohammed Hussien Saeed, "An Ensemble Voting Classifier based on Machine Learning Models for Phishing Detection," *Int. J. Sci. Res. Sci. Eng. Technol.*, vol. 12, no. 1, pp. 15–27, Jan. 2025, doi: 10.32628/ijsrset251211.

[50] A. A. Albishri and M. M. Dessouky, "A Comparative Analysis of Machine Learning Techniques for URL Phishing Detection," *Engineering, Technology and Applied Science Research*, vol. 14, no. 6, pp. 18495–18501, Dec. 2024, doi: 10.48084/etasr.8920.

[51] P. K. Atrey, M. A. Hossain, A. El Saddik, and M. S. Kankanhalli, "Multimodal fusion for multimedia analysis: A survey," *Multimed. Syst.*, vol. 16, no. 6, pp. 345–379, Nov. 2010, doi: 10.1007/s00530-010-0182-0.

[52] S. J. I. Ismail, Hendrawan, B. Rahardjo, T. Juhana, and Y. Musashi, "MIDALF—multimodal image and audio late fusion for malware detection," *EURASIP J. Inf. Secur.*, vol. 2025, no. 1, Dec. 2025, doi: 10.1186/s13635-025-00188-5.

[53] H. Lee and H. Kwon, "DBF: Dynamic Belief Fusion for Combining Multiple Object Detectors," *ArXiv*, Apr. 2022, doi: 10.1109/TPAMI.2019.2952847.

[54] S. Al-Ahmadi and Y. Alharbi, "A Deep Learning Technique For Web Phishing Detection Combined Url Features And Visual Similarity," *International Journal of Computer Networks and Communications*, vol. 12, no. 5, pp. 41–54, Sep. 2020, doi: 10.5121/ijcnc.2020.12503.

[55] N. Abdelhamid, A. Ayesh, and F. Thabtah, “Phishing detection based Associative Classification data mining,” *Expert Syst. Appl.*, vol. 41, pp. 5948–5959, Oct. 2014, doi: 10.1016/j.eswa.2014.03.019.

[56] S. Marchal, J. Francois, R. State, and T. Engel, “Phish storm: Detecting phishing with streaming analytics,” *IEEE Transactions on Network and Service Management*, vol. 11, no. 4, pp. 458–471, Dec. 2014, doi: 10.1109/TNSM.2014.2377295.