

DAFTAR PUSTAKA

- Abood, R. A., & Al-Azawi, Dr. R. J. (2017). Design and Execute Media Website for the Sustainable Development Goals. *IARJSET*, 4(2), 6–9. <https://doi.org/10.17148/iarjset.2017.4202>
- Abutaha, M., Ababneh, M., Mahmoud, K., & Baddar, S. A. H. (2021). URL Phishing Detection using Machine Learning Techniques based on URLs Lexical Analysis. *2021 12th International Conference on Information and Communication Systems, ICICS 2021*, 147–152. <https://doi.org/10.1109/ICICS52457.2021.9464539>
- Adsul, S., Shah, P., Pathak, A., Pathak, Y., Patil, A., & Patil, K. (2024, Mei). IntelliMap: AI-Driven Terrain Exploration and Mapping. In *2024 5th International Conference for Emerging Technology (INCET)* (pp. 1-9). IEEE.
- Agrawal, S., & Fandi, N. (2023, Februari). Phishing detection browser. *International Journal of Ingenious Research, Invention and Development*, 1(2), 009–011. <https://doi.org/10.5281/zenodo.782101>
- Al-Ahmadi, S., Alotaibi, A., & Alsaleh, O. (2022). PDGAN: Phishing Detection With Generative Adversarial Networks. *IEEE Access*, 10, 42459–42468. <https://doi.org/10.1109/ACCESS.2022.3168235>
- Alanezi, M. (2021). *Phishing Detection Methods: A Review*. www.techniumscience.com
- Alani, A. A., & Al-Azzawia, A. (2025). Phishing Attacks Detection and Prevention Techniques: An Overview. *Journal of Al-Qadisiyah for Computer Science and Mathematics*, 17(1), 166–178. <https://doi.org/10.29304/jqcsms.2025.17.11972>
- Alfarizi, M. R. S., Al-farish, M. Z., Taufiqurrahman, M., Ardiansah, G., & Elgar, M. (2023). Penggunaan Python sebagai bahasa pemrograman untuk machine learning dan deep learning. *Karimah Tauhid*, 2(1), 1-6.

- Alshingiti, Z., Alaqel, R., Al-Muhtadi, J., Haq, Q. E. U., Saleem, K., & Faheem, M. H. (2023). A Deep Learning-Based Phishing Detection System Using CNN, LSTM, and LSTM-CNN. *Electronics (Switzerland)*, 12(1). <https://doi.org/10.3390/electronics12010232>
- APWG. (2024). *Phishing Activity Trends Reports*. <http://www.apwg.org>,
- Asiri, S., Xiao, Y., & Li, T. (2024). PhishTransformer: A Novel Approach to Detect Phishing Attacks Using URL Collection and Transformer. *Electronics (Switzerland)*, 13(1). <https://doi.org/10.3390/electronics13010030>
- Bu, S. J., & Cho, S. B. (2021). Deep character-level anomaly detection based on a convolutional autoencoder for zero-day phishing url detection. *Electronics (Switzerland)*, 10(12). <https://doi.org/10.3390/electronics10121492>
- Das Gupta, S., Shahriar, K. T., Alqahtani, H., Alsalman, D., & Sarker, I. H. (2024). Modeling Hybrid Feature-Based Phishing Websites Detection Using Machine Learning Techniques. *Annals of Data Science*, 11(1), 217–242. <https://doi.org/10.1007/s40745-022-00379-8>
- Do, N. Q., Selamat, A., Krejcar, O., Herrera-Viedma, E., & Fujita, H. (2022). Deep Learning for Phishing Detection: Taxonomy, Current Challenges and Future Directions. In *IEEE Access* (Vol. 10, pp. 36429–36463). Institute of Electrical and Electronics Engineers Inc. <https://doi.org/10.1109/ACCESS.2022.3151903>
- Dumoulin, V., & Visin, F. (2016). *A guide to convolution arithmetic for deep learning*. <http://arxiv.org/abs/1603.07285>
- Elmrabit, N., Zhou, F., Li, F., & Zhou, H. (2020, Juni). Evaluation of machine learning algorithms for anomaly detection. In 2020 international conference on cyber security and protection of digital services (cyber security) (pp. 1-8). IEEE.
- Handoyo, T. F., & Putra, M. P. K. (2025). Optimasi Bobot Kelas LSTM untuk Deteksi URL Phishing pada Dataset Tidak Berimbang. *Jurnal Informatika:*

Jurnal Pengembangan IT, 10(1), 20–36.
<https://doi.org/10.30591/jpit.v10i1.8128>

Haq, Q. E. U., Faheem, M. H., & Ahmad, I. (2024). Detecting Phishing URLs Based on a Deep Learning Approach to Prevent Cyber-Attacks. *Applied Sciences*, 14(22), 10086.

Hidayatullah, T. (2022). Implementasi Algoritma Base-64 Dalam Mengamankan Url (Uniform Resource Locator) Website Layanan Pengaduan Masyarakat Desa Bojongraharja. *Jurnal Media Infotama*, 18(2).

Hossain, S., Sarma, D., & Chakma, R. J. (2020). Machine Learning-Based Phishing Attack Detection. In *IJACSA) International Journal of Advanced Computer Science and Applications* (Vol. 11, Issue 9). www.ijacsa.thesai.org

IDADX. (2024). LAPORAN AKTIVITAS ABUSE DOMAIN .ID Indonesia Domain Abuse Data Exchange. www.pandi.id

Inaya, A. N., Rahma, A. U., Jannah, M., Arafah, L. R. K., Ishak, L. L., & Edy, M. R. (2024). Klasifikasi Citra Dengan Pendekatan Transfer Learning Pada Gambar Fauna Terbang. *Jurnal MediaTIK*, 85-89.

Irsan, M., & Husain, A. (2024). Implementasi Aplikasi Pandas (Python) Dalam Mengelola Data Excel Sebagai Media Persiapan Pelaporan Nilai Raport Siswa. *Jurnal Pengabdian Masyarakat Bangsa*, 2(4), 1243-1249.

Karim, A., Shahroz, M., Mustofa, K., Belhaouari, S. B., & Joga, S. R. K. (2023). Phishing Detection System Through Hybrid Machine Learning Based on URL. *IEEE Access*, 11, 36805–36822.
<https://doi.org/10.1109/ACCESS.2023.3252366>

Kingma, D. P., & Welling, M. (2019). *An Introduction to Variational Autoencoders*. <https://doi.org/10.1561/22000000056>

Komadina, A., Martinić, M., Groš, S., & Mihajlović, Ž. (2024). Comparing Threshold Selection Methods for Network Anomaly Detection. *IEEE access*.

- Lecun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. In *Nature* (Vol. 521, Issue 7553, pp. 436–444). Nature Publishing Group. <https://doi.org/10.1038/nature14539>
- Liu, Y., Zhang, H., Huang, Y., Zhu, F., Liang, Y., & Gao, D. (2023, Desember). An Anomaly Detection Model Based on CNN-VAE for IoT Devices. In *Proceedings of the 2023 7th International Conference on Computer Science and Artificial Intelligence* (pp. 301-305)
- Maesaroh, S., Lukman, A., Yunita, H., Sari, S., Yusuf, M., Budi, E., Wiranti, P., Utami, S., Tri, N., Saptadi, S., Mutmainah, S., Eka, K., Harahap, P., Alamin, Z., Sabily, I., Saputra, K. A., & Mubarak, R. (2024). *BAHASA PEMROGRAMAN PYTHON*. Sada Kurnia Pustaka.
- Mianah, A. N., & Fiolana, F. A. (2023). Klasifikasi Helm Keselamatan Menggunakan Metode Convolutional Neural Network (CNN). *JOURNAL ZETROEM*, 5(2), 94-102.
- Nagarajan, S. (2024). An Investigation of AI-Enabled Comprehensive Survey of Phishing Attacks detection techniques. *International Journal of Innovative Research in Engineering*, 5(1), 55–59. <https://doi.org/10.59256/ijire.20240501001>
- Nelli, F. (2023). Machine Learning with scikit-learn. In *Python data analytics: with pandas, numPy, and matplotlib* (pp. 259-287). Berkeley, CA: Apress.
- Pandian, A. P. D. (2024). Variational Autoencoders using Convolutional neural network for highly advanced cyber threats. *2024 IEEE Integrated STEM Education Conference, ISEC 2024*. <https://doi.org/10.1109/ISEC61299.2024.10664944>
- Pang, G., Shen, C., Cao, L., & Hengel, A. Van Den. (2021). Deep Learning for Anomaly Detection: A Review. In *ACM Computing Surveys* (Vol. 54, Issue 2). Association for Computing Machinery. <https://doi.org/10.1145/3439950>

- Prabakaran, M. K., Meenakshi Sundaram, P., & Chandrasekar, A. D. (2023). An enhanced deep learning-based phishing detection mechanism to effectively identify malicious URLs using variational autoencoders. *IET Information Security*, 17(3), 423–440. <https://doi.org/10.1049/ise2.12106>
- Raihan, A., Fadhli, M., & Lindawati. (2024). Implementation Of Deep Learning For Detecting Phishing Attacks On Websites With Combination Of Cnn And Lstm. *Jurnal Teknik Informatika (JUTIF)*, 5(5), 1451–1459. <https://doi.org/10.52436/1.jutif.2024.5.5.2446>
- Rismawan, S. A. (2023). Implementasi website berita online menggunakan metode crawling data dengan bahasa pemrograman Python. *JATISI (Jurnal Teknik Informatika dan Sistem Informasi)*, 10(3), 167-178.
- Safi, A., & Singh, S. (2023). A systematic literature review on phishing website detection techniques. *Journal of King Saud University-Computer and Information Sciences*, 35(2), 590–611.
- Samat, N. A., Salleh, M. N. M., & Ali, H. (2020). The comparison of pooling functions in convolutional neural network for sentiment analysis task. In *Recent Advances on Soft Computing and Data Mining: Proceedings of the Fourth International Conference on Soft Computing and Data Mining (SCDM 2020), Melaka, Malaysia, January 22– 23, 2020* (pp. 202-210). Springer International Publishing.
- Sasi, J. K., & Balakrishnan, A. (2024). Generative adversarial network-based phishing URL detection with variational autoencoder and transformer. *IAES International Journal of Artificial Intelligence*, 13(2), 2163–2170. <https://doi.org/10.11591/ijai.v13.i2.pp2165-2172>
- Satria, H. (2024, 11 April). *helimisatria/tweet-harvest* [Repositori GitHub]. <https://github.com/helimisatria/tweet-harvest>
- Soebroto, A. A. (2019). *Buku Ajar AI, Machine Learning & Deep Learning*. <https://www.researchgate.net/publication/348003841>

- Subray, S., Tschimben, S., & Gifford, K. (2021). Towards enhancing spectrum sensing: Signal classification using autoencoders. *IEEE Access*, 9, 82288-82299.
- Sutisna, I. (2020). Statistika penelitian. *Universitas Negeri Gorontalo*, 1(1), 1–15.
- Tanti, R. (2024, Oktober). Study of Phishing Attack and their Prevention Techniques. *International Journal for Multidisciplinary Research*, 08(10). <https://doi.org/10.55041/IJSREM38042>
- Thivaharan, S., Srivatsun, G., & Sarathambekai, S. (2020, September). A survey on python libraries used for social media content scraping. In *2020 International Conference on Smart Electronics and Communication (ICOSEC)* (pp. 361-366). IEEE.
- Wang, R., Nie, K., Wang, T., Yang, Y., & Long, B. (2020). Deep Learning for Anomaly Detection. *Proceedings of the 13th International Conference on Web Search and Data Mining*, 894–896. <https://doi.org/10.1145/3336191.3371876>
- Windarni, V. A., Ferdita Nugraha, A., Tri Atmaja Ramadhani, S., Anisa Istiqomah, D., Mahananing Puri, F., & Setiawan, A. (2023). Deteksi Website Phishing Menggunakan Teknik Filter Pada Model Machine Learning. In *Information System Journal (INFOS)*, 6(01), 39-43.
- Yerima, S. Y. , & Alzaylaee, M. K. (2020). High Accuracy Phishing Detection Based on Convolutional Neural Networks. *2020 3rd International Conference on Computer Applications & Information Security (ICCAIS)*, 1–6. <https://doi.org/10.1109/iccais48893.2020.9096869>