

DAFTAR PUSTAKA

- [1] A. Géron, *Hands-on machine learning with Scikit-Learn, Keras, and TensorFlow*. "O'Reilly Media, Inc.", 2022.
- [2] I. Sitorus, "Support vector machine (svm) and kernels trick," <https://medium.com/analytics-vidhya/introduction-to-svm-and-kernel-trick-part-1-theory-d990e2872ace>, August 2020.
- [3] S.-L. Developer, "scikit-learn machine learning in python," <https://scikit-learn.org/stable/index.html>, accessed on 12 June 2023.
- [4] C.-T. Cheng, z.-k. Feng, W.-J. Niu, and S. Liao, "Heuristic methods for reservoir monthly inflow forecasting: A case study of xinfengjiang reservoir in pearl river, china," *Water (Switzerland)*, vol. 7, pp. 4477–4495, 08 2015.
- [5] I. W. Saputro and B. W. Sari, "Uji performa algoritma naïve bayes untuk prediksi masa studi mahasiswa," *Creative Information Technology Journal*, vol. 6, no. 1, pp. 1–11, 2020.
- [6] A. Kumar, K. Kuppusamy, and G. Aghila, "A learning model to detect maliciousness of portable executable using integrated feature set," *Journal of King Saud University-Computer and Information Sciences*, vol. 31, no. 2, pp. 252–265, 2019.
- [7] N. Idika and A. P. Mathur, "A survey of malware detection techniques," *Purdue University*, vol. 48, no. 2, pp. 32–46, 2007.
- [8] S. Cook, "Malware statistics and facts," <https://www.comparitech.com/antivirus/malware-statistics-facts/#:~:text=In%202020%2C%2061%20percent%20of%20organizations%20experienced%20malware,infection%20since%20the%20SOES%20survey%20began%20in%202016.>, June 2023.
- [9] D. Karina, "Layanan bsi eror berhari-hari, pengamat: Aceh berpotensi rugi puluhan miliar rupiah," <https://www.kompas.tv/ekonomi/406137/layanan-bsi-eror-berhari-hari-pengamat-aceh-berpotensi-rugi-puluhan-miliar-rupiah>, 2023, accessed in June 2023.
- [10] F. A. Burhan, "Error bsi (bris) berdampak besar bagi warga aceh, kok bisa?" <https://finansial.bisnis.com/read/20230512/90/1655452/error-bsi-bris-berdampak-besar-bagi-warga-aceh-kok-bisa>, 2023, accessed on 12 May 2023.
- [11] M. K. Alfarizi, "Ada peluang bisnis yang hilang akibat gangguan layanan, bsi: Kami kembalikan ke kondisi normal," <https://bisnis.tempo.co/read/1730575/ada-peluang-bisnis-yang-hilang-akibat-gangguan-layanan-bsi-kami-kembalikan-ke-kondisi-normal>, 2023, accessed on 12 June 2023.
- [12] A. Nasrie, "Explained: The ransomware attack on bsi, indonesia's largest islamic bank," <https://coconuts.co/jakarta/news/explained-the-ransomware-attack-on-bsi-indonesias-largest-islamic-bank>, 2023, accessed on 12 June 2023.

- [13] M. F. Fibrianda and A. Bhawiyuga, "Analisis perbandingan akurasi deteksi serangan pada jaringan komputer dengan metode naïve bayes dan support vector machine (svm)," *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer e-ISSN*, vol. 2548, p. 964X, 2018.
- [14] S. Treadwell and M. Zhou, "A heuristic approach for detection of obfuscated malware," in *2009 IEEE International Conference on Intelligence and Security Informatics*. IEEE, 2009, pp. 291–299.
- [15] I. Firdausi, A. Erwin, A. S. Nugroho *et al.*, "Analysis of machine learning techniques used in behavior-based malware detection," in *2010 second international conference on advances in computing, control, and telecommunication technologies*. IEEE, 2010, pp. 201–203.
- [16] J. Qin, H. Yan, Q. Si, and F. Yan, "A trojan horse detection technology based on behavior analysis," in *2010 6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM)*. IEEE, 2010, pp. 1–4.
- [17] M. G. Schultz, E. Eskin, F. Zadok, and S. J. Stolfo, "Data mining methods for detection of new malicious executables," in *Proceedings 2001 IEEE Symposium on Security and Privacy. S&P 2001*. IEEE, 2000, pp. 38–49.
- [18] K. Liu, S. Xu, G. Xu, M. Zhang, D. Sun, and H. Liu, "A review of android malware detection approaches based on machine learning," *IEEE Access*, vol. 8, pp. 124 579–124 607, 2020.
- [19] A. Cahyaningtyas, "Deteksi serangan denial of service (dos) menggunakan algoritma probabilistic neural network (pnn)," 2019.
- [20] F. A. Narudin, A. Feizollah, N. B. Anuar, and A. Gani, "Evaluation of machine learning classifiers for mobile malware detection," *Soft Computing*, vol. 20, pp. 343–357, 2016.
- [21] E. N. Hartiwati, "Keamanan jaringan dan keamanan sistem komputer yang mempengaruhi kualitas pelayanan warnet," *Jurnal Ilmiah Informatika Komputer*, vol. 19, no. 3, 2014.
- [22] N. Cristianini, J. Shawe-Taylor *et al.*, *An introduction to support vector machines and other kernel-based learning methods*. Cambridge university press, 2000.
- [23] M. N. Murty and R. Raghava, "Support vector machines and perceptrons: Learning, optimization, classification, and application to social networks," 2016.
- [24] G. Hackeling, *Mastering Machine Learning with scikit-learn*. Packt Publishing Ltd, 2017.
- [25] M. Yanto, S. Defit, and G. W. Nurcahyo, "Analisis jaringan syaraf tiruan untuk memprediksi jumlah reservasi kamar hotel dengan metode backpropagation (studi kasus hotel grand zuri padang)," *Jurnal KomTekInfo*, vol. 2, no. 1, 2016.
- [26] W. Budiharto and D. Suhartono, "Artificial intelligence konsep dan penerapannya," *Yogyakarta: Andi*, 2014.

- [27] A. Y. Prathama, “Pendekatan ann (artificial neural network) untuk penentuan prosentase bobot pekerjaan dan estimasi nilai pekerjaan struktur pada rumah sakit pertama,” *Jurnal Teknosains*, vol. 7, no. 1, pp. 14–25, 2018.
- [28] S. Rajan, “An introduction to artificial neural network,” <https://towardsdatascience.com/an-introduction-to-artificial-neural-networks-5d2e108ff2c3>, July 2020.
- [29] F. Amri, “Jaringan syaraf tiruan untuk memprediksi peringkat akreditasi program studi perguruan tinggi,” *Jurnal Sains dan Informatika*, vol. 1, no. 1, 2015.
- [30] B. Intelligence, “Data mining and optimization for decision making,” *Carlo Verce-llis*, 2009.
- [31] L. Qadrini, A. Seppewali, and A. Aina, “Decision tree dan adaboost pada klasifikasi penerima program bantuan sosial,” *Jurnal Inovasi Penelitian*, vol. 2, no. 7, pp. 1959–1966, 2021.
- [32] A. Kumar, “Clamp (classification of malware with pe headers),” Mendeley Data, 2020.
- [33] M. Z. Shafiq, S. M. Tabish, F. Mirza, and M. Farooq, “Pe-miner: Mining structural information to detect malicious executables in realtime,” in *Recent Advances in Intrusion Detection: 12th International Symposium, RAID 2009, Saint-Malo, France, September 23-25, 2009. Proceedings 12*. Springer, 2009, pp. 121–141.
- [34] K. Bridge, “Microsoft portable executable and common object file format specification,” <https://learn.microsoft.com/en-us/windows/win32/debug/pe-format?redirectedfrom=MSDN>, March 2023, accessed June 8, 2023.