DAFTAR PUSTAKA

Abu-Aisheh, Z., Raveaux, R., & Ramel, J.-Y. (2020). Efficient k-nearest neighbors search in graph space. *Pattern Recognition Letters*, *134*, 77–86. https://doi.org/10.1016/j.patrec.2018.05.001

Akman, G., Yorur, B., Boyaci, A. I., & Chiu, M.-C. (2023). Assessing innovation capabilities of manufacturing companies by combination of unsupervised and supervised machine learning approaches. *Applied Soft Computing*, *147*, 110735. https://doi.org/10.1016/j.asoc.2023.110735

Assy, A. T., Mostafa, Y., El-khaleq, A. A., & Mashaly, M. (2023). Anomaly-Based Intrusion Detection System using One-Dimensional Convolutional Neural Network. *Procedia Computer Science*, *220*, 78–85. https://doi.org/10.1016/j.procs.2023.03.013

Behnia, P., Harris, J., Liu, H., Jørgensen, T. R. C., Naghizadeh, M., & Roots, E. A. (2023). Random forest classification for volcanogenic massive sulfide mineralization in the Rouyn-Noranda Area, Quebec. *Ore Geology Reviews*, *161*, 105612. https://doi.org/10.1016/j.oregeorev.2023.105612

Berger, E. (2024). *scalene: Scalene: A high-resolution, low-overhead CPU and memory profiler for Python* (Version 1.5.44.1) [Python; MacOS :: MacOS X, POSIX :: Linux]. https://pypi.org/project/scalene/1.5.44.1/

Chapman, C. (2016). Chapter 7—Using Wireshark and TCP dump to visualize traffic. In C. Chapman (Ed.), *Network Performance and Security* (pp. 195–225). Syngress. https://doi.org/10.1016/B978-0-12-803584-9.00007-X

Farrukh, Y. A., Wali, S., Khan, I., & Bastian, N. D. (2024). AIS-NIDS: An intelligent and self-sustaining network intrusion detection system. *Computers & Security*, *144*, 103982. https://doi.org/10.1016/j.cose.2024.103982

Fatima, M., Rehman, O., Ali, S., & Niazi, M. F. (2024). ELIDS: Ensemble Feature Selection for Lightweight IDS against DDoS Attacks in Resource-Constrained IoT Environment. *Future Generation Computer Systems*, *159*, 172–187. https://doi.org/10.1016/j.future.2024.05.013

Ferriyan, A. (2022). Graduate School of Media and Governance Keio University 5322 Endo Fujisawa, Kanagawa, Japan 252-0882.

Harikrishnakumar, R., Dand, A., Nannapaneni, S., & Krishnan, K. (2019). Supervised Machine Learning Approach for Effective Supplier Classification. *2019 18th IEEE International Conference On Machine Learning And Applications (ICMLA)*, 240–245. https://doi.org/10.1109/ICMLA.2019.00045

Hasan, Md. A. M., Nasser, M., Ahmad, S., & Molla, K. I. (2016). Feature Selection for Intrusion Detection Using Random Forest. *Journal of Information Security*, *07*(03), 129–140. https://doi.org/10.4236/jis.2016.73009

Hua, T. K. (2022). *A Short Review on Machine Learning*. https://www.authorea.com/users/510271/articles/587406-a-short-review-on-machine-learning?commit=adb3126655cb1e97c77fee92fa68b5461b720f85

Jia, W., Sun, M., Lian, J., & Hou, S. (2022). Feature dimensionality reduction: A review. *Complex & Intelligent Systems*, *8*(3), 2663–2693. https://doi.org/10.1007/s40747-021-00637-x

Kshirsagar, D., & Kumar, S. (2021). An efficient feature reduction method for the detection of DoS attack. *ICT Express*, *7*(3), 371–375. https://doi.org/10.1016/j.icte.2020.12.006

Kumar, P. (2021, June 26). Time Complexity of ML Models. *Analytics Vidhya*. https://medium.com/analytics-vidhya/time-complexity-of-ml-models-4ec39fad2770. (Akses terakhir pada 20 Februari 2025)

Layeghy, S., Gallagher, M., & Portmann, M. (2024). Benchmarking the benchmark—Comparing synthetic and real-world Network IDS datasets. *Journal of Information Security and Applications*, *80*, 103689. https://doi.org/10.1016/j.jisa.2023.103689

Mobarak, M. H., Mimona, M. A., Islam, Md. A., Hossain, N., Zohura, F. T., Imtiaz, I., & Rimon, M. I. H. (2023). Scope of machine learning in materials research—A review. *Applied Surface Science Advances*, *18*, 100523. https://doi.org/10.1016/j.apsadv.2023.100523

Ngo, V.-D., Vuong, T.-C., Van Luong, T., & Tran, H. (2023). *Machine Learning-Based Intrusion Detection: Feature Selection versus Feature Extraction* (No. arXiv:2307.01570). arXiv. http://arxiv.org/abs/2307.01570

Petrosyan, A. (2023, September 21). *Number of internet users worldwide 2023*. Statista. https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/

Rbah, Y., Mahfoudi, M., Balboul, Y., Fattah, M., Mazer, S., Elbekkali, M., & Bernoussi, B. (2022). *Machine Learning and Deep Learning Methods for Intrusion Detection Systems in IoMT: A survey*. 1–9. https://doi.org/10.1109/IRASET52964.2022.9738218

Rojas, C., Ballabio, D., Consonni, V., Suárez-Estrella, D., & Todeschini, R. (2023). Classification-based machine learning approaches to predict the taste of molecules: A review. *Food Research International*, *171*, 113036. https://doi.org/10.1016/j.foodres.2023.113036

Sahoo, T. R., Patra, S., & Vipsita, S. (2023). Decision tree classifier based on topological characteristics of subgraph for the mining of protein complexes from large scale PPI networks. *Computational Biology and Chemistry*, *106*, 107935. https://doi.org/10.1016/j.compbiolchem.2023.107935

Sawyer, S. F. (2009). Analysis of Variance: The Fundamental Concepts. *Journal of Manual & Manipulative Therapy*, *17*(2), 27E-38E. https://doi.org/10.1179/jmt.2009.17.2.27E

Seth, S., Singh, G., & Kaur Chahal, K. (2021). A novel time efficient learning-based approach for smart intrusion detection system. *Journal of Big Data*, *8*(1), 111. https://doi.org/10.1186/s40537-021-00498-8

Sheikhan, M., Bejani, M., & Gharavian, D. (2013). Modular neural-SVM scheme for speech emotion recognition using ANOVA feature selection method. *Neural Computing and Applications*, *23*(1), 215–227. https://doi.org/10.1007/s00521-012-0814-8

Siddiqi, M. A., & Pak, W. (2021). An Agile Approach to Identify Single and Hybrid Normalization for Enhancing Machine Learning-Based Network Intrusion Detection. *IEEE Access*, *9*, 137494–137513. https://doi.org/10.1109/ACCESS.2021.3118361

Siraj, M., Ahmad, T., & Ijtihadie, R. (2022). Analyzing ANOVA F-test and Sequential Feature Selection for Intrusion Detection Systems. *International Journal of Advances in Soft Computing and Its Applications*, *14*(2), 186–194. https://doi.org/10.15849/IJASCA.220720.13

Su, M.-Y. (2011). Using clustering to improve the KNN-based classifiers for online anomaly network traffic identification. *Journal of Network and Computer Applications*, *34*(2), 722–730. https://doi.org/10.1016/j.jnca.2010.10.009

Vergara, J. R., & Estévez, P. A. (2014). A review of feature selection methods based on mutual information. *Neural Computing and Applications*, *24*(1), 175–186. https://doi.org/10.1007/s00521-013-1368-0

Verma, J., Bhandari, A., & Singh, G. (2022). iNIDS: SWOT Analysis and TOWS Inferences of State-of-the-Art NIDS solutions for the development of Intelligent

Network Intrusion Detection System. *Computer Communications*, *195*, 227–247. https://doi.org/10.1016/j.comcom.2022.08.022

Waleed, A., Jamali, A. F., & Masood, A. (2022). Which open-source IDS? Snort, Suricata or Zeek. *Computer Networks*, *213*, 109116. https://doi.org/10.1016/j.comnet.2022.109116

Wang, A. X., Chukova, S. S., & Nguyen, B. P. (2023). Ensemble *k*-nearest neighbors based on centroid displacement. *Information Sciences*, *629*, 313–323. https://doi.org/10.1016/j.ins.2023.02.004

Wang, X., Wang, Y., Javaheri, Z., Almutairi, L., Moghadamnejad, N., & Younes, O. S. (2023). Federated deep learning for anomaly detection in the internet of things. *Computers and Electrical Engineering*, *108*, 108651. https://doi.org/10.1016/j.compeleceng.2023.108651

Zhou, Y., & Skidmore, S. (2018). A Reassessment of ANOVA Reporting Practices: A Review of Three APA Journals. *Journal of Methods and Measurement in the Social Sciences*, *8*(1). https://doi.org/10.2458/v8i1.22019