DAFTAR PUSTAKA

Ahmed, M., Naser Mahmood, A., & Hu, J. (2016). A survey of network anomaly detection techniques. *Journal of Network and Computer Applications*, *60*, 19–31. https://doi.org/10.1016/j.jnca.2015.11.016

Al-mhiqani, M. N., Ahmad, R., Abidin, Z. Z., & Yassin, W. (n.d.). *A-review-of-insider-threat-detection-Classification-machine-learning-techniques-datasets-open-challenges-and-recommendations2020Applied-Sciences-SwitzerlandOpen-Access.pdf*.

Artioli, P., Maci, A., & Magrì, A. (2024). A comprehensive investigation of clustering algorithms for User and Entity Behavior Analytics. *Frontiers in Big Data*, *7*(May). https://doi.org/10.3389/fdata.2024.1375818

Blei, D. M. (2012). Probabilistic topic models. *Communications of the ACM*, *55*(4), 77–84. https://doi.org/10.1145/2133806.2133826

Boettiger, C. (2015). An introduction to Docker for reproducible research (atau sering diterbitkan dengan judul penuh: An introduction to Docker for reproducible research, with examples from the R environment). *ACM SIGOPS Operating Systems Review, Volume 49, Edisi 1, Halaman 71–79.* https://gist.github.com/samth/9641364

Campbell, J. C., Hindle, A., & Stroulia, E. (2015). Latent Dirichlet Allocation: Extracting Topics from Software Engineering Data. *The Art and Science of Analyzing Software Data*, *3*, 139–159. https://doi.org/10.1016/B978-0-12-411519-4.00006-9

Cutting, V., & Stephen, N. (2021). Comparative Review of JAVA and Python. *International Journal of Research and Development in Applied Science and Engineering (IJRDASE)*. www.ijrdase.com

Desetty, A. G. (2024). Unveiling Hidden Threats with ML-Powered User and Entity Behavior Analytics (UEBA). *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *15*(1), 44–50. https://doi.org/10.61841/turcomat.v15i1.14394

Elastic N.V. (2024). *Elasticsearch Guide*. https://www.elastic.co/docs/reference/elasticsearch

Fawcett, T. (2006). An introduction to ROC analysis. *Pattern Recognition Letters*, *27*(8), 861–874. https://doi.org/10.1016/j.patrec.2005.10.010

Fragkoulis, M., Carbone, P., Kalavri, V., & Katsifodimos, A. (2024). A survey on the evolution of stream processing systems. *VLDB Journal*, *33*(2), 507–541. https://doi.org/10.1007/s00778-023-00819-8

Galtsev, A. A., & Sukhov, A. M. (2011). Network attack detection at flow level. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *6869 LNCS*, 326–334. https://doi.org/10.1007/978-3-642-22875-9_30

García, S., Grill, M., Stiborek, J., & Zunino, A. (2014). An empirical comparison of botnet detection methods. *Computers & Security*, *45*, 100–123. https://doi.org/10.1016/J.COSE.2014.05.011

GÖRMEZ, Y., ARSLAN, H., IŞIK, Y. E., & DADAŞ, İ. E. (2023). A User and Entity Behavior Analysis for SIEM Systems: Preprocessing of The Computer Emergency and Response Team Dataset. *Journal of Soft Computing and Artificial Intelligence*, *4*(1), 1–6. https://doi.org/10.55195/jscai.1213782

Haldorai, A., Kandaswamy, U., & Ramu, A. (2018). Survey on Big Data Analytic and Challenges to Cyber Security. *Information Technology Journal*, *18*(1), 8–16. https://doi.org/10.3923/itj.2019.8.16

Han, J., Kamber, M., & Pei, J. (2011). *Data Mining. Concepts and Techniques, 3rd Edition (The Morgan Kaufmann Series in Data Management Systems)*.

Kaur, P., & Vashisht, S. (2013). Mingle Intrusion Detection System Using Fuzzy Logic. In *International Journal of Engineering and Advanced Technology (IJEAT)*. www.ijeat.org

Komisarek, M., Pawlicki, M., Kozik, R., & Choraś, M. (2021). Machine learning based approach to anomaly and cyberattack detection in streamed network traffic data. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, *12*(1), 3–19. https://doi.org/10.22667/JOWUA.2021.03.31.003

Koumar, J., Hynek, K., Čejka, T., & Šiška, P. (2025). CESNET-TimeSeries24: Time Series Dataset for Network Traffic Anomaly Detection and Forecasting. *Scientific Data*, *12*(1). https://doi.org/10.1038/s41597-025-04603-x

Liu, F. T., Ting, K. M., & Zhou, Z.-H. (2012). *Isolation-based Anomaly Detection*.

Rahmawati, T., Karna, N., Shin, S. Y., & Putra, M. A. P. (2024). Enhancing Network Security Through Real-Time Threat Detection with Intrusion Prevention System (Case Study on Web Attack). *Jurnal Ilmiah Teknik Elektro Komputer Dan Informatika (JITEKI)*, *10*(4), 1004–1020. https://doi.org/10.26555/jiteki.v10i4.30380

Shiravi, A., Shiravi, H., Tavallaee, M., & Ghorbani, A. A. (2012). Toward developing a systematic approach to generate benchmark datasets for intrusion detection. *Computers & Security*, *31*(3), 357–374. https://doi.org/10.1016/J.COSE.2011.12.012

Shvachko, K., Kuang, H., Radia, S., & Chansler, R. (2010). The Hadoop distributed file system. *2010 IEEE 26th Symposium on Mass Storage Systems and*

Technologies, MSST2010, 1–10. https://doi.org/10.1109/MSST.2010.5496972

Streamlit Inc. (2024). *Streamlit Documentation*. Https://Docs.Streamlit.Io/.

Subhadra, A. (2020). An Analysis of Data Security and Privacy for Cloud Computing. *Asian Journal of Computer Science and Technology*, *9*(1), 27–39. https://doi.org/10.51983/ajcst-2020.9.1.2153

Towle, J. (n.d.). *Apache Spot : A More Effective Approach to Cyber Security*. 1–5.

Tuyishime, E., Balan, T. C., Cotfas, P. A., Cotfas, D. T., & Rekeraho, A. (2023). Enhancing Cloud Security—Proactive Threat Monitoring and Detection Using a SIEM-Based Approach. *Applied Sciences (Switzerland)*, *13*(22). https://doi.org/10.3390/app132212359

Zadeh, L. A. (1965). Fuzzy S e t s *. In *INFOR~ATIO~ AND CONTROL* (Vol. 8).

Zaharia, M., Chowdhury, M., Franklin, J. M., Shenker, S., & Stoica, I. (2010). Spark: Cluster Computing with Working Sets Matei. *Spark: Cluster Computing with Working Sets Matei*.

Zaharia, M., Xin, R. S., Wendell, P., Das, T., Armbrust, M., Dave, A., Meng, X., Rosen, J., Venkataraman, S., Franklin, M. J., Ghodsi, A., Gonzalez, J., Shenker, S., & Stoica, I. (2016). Apache spark: A unified engine for big data processing. *Communications of the ACM*, *59*(11), 56–65. https://doi.org/10.1145/2934664

Zhang, Y., Jin, R., & Zhou, Z.-H. (n.d.). *Understanding Bag-of-Words Model: A Statistical Framework*.