DAFTAR PUSTAKA

Abdurrasyid, A., Susanti, M. N. I., & Indrianto, I. (2024). Web Vulnerability Scanner pada Jenis Serangan SQL Injection dan Cross-Site Scripting. *SNEKTI*, *5*(1).

Abdurrasyid, Sitohang, B., Asnar, Y. D. W., & Saptawati, G. A. P. (2024). Securing Cross-Site Request Forgery Vulnerabilities in Web Applications Using Mutation Analysis. *2024 2nd International Conference on Software Engineering and Information Technology (ICoSEIT)*, 227–232. https://doi.org/10.1109/ICoSEIT60086.2024.10497499

Ahmed, H. A., Muhammad Ali, P. J., Faeq, A. K., & Abdullah, S. M. (2022). An Investigation on Disparity Responds of Machine Learning Algorithms to Data Normalization Method. *ARO-The Scientific Journal of Koya University*, *10*(2), 29–37. https://doi.org/10.14500/aro.10970

Alhassan, S., Abdul-Salaam, G., Asante, M., Missah, Y., & Ganaa, E. (2023). Analyzing Autoencoder-Based Intrusion Detection System Performance. *Journal of Information Security and Cybercrimes Research*, *6*(2), 105–115. https://doi.org/10.26735/ylxb6430

Ali, M. L., Thakur, K., Schmeelk, S., Debello, J., & Dragos, D. (2025). Deep Learning vs. Machine Learning for Intrusion Detection in Computer Networks: A Comparative Study. *Applied Sciences*, *15*(4), 1903. https://doi.org/10.3390/app15041903

Altalhan, M., Algarni, A., & Turki-Hadj Alouane, M. (2025). Imbalanced Data Problem in Machine Learning: A Review. *IEEE Access*, *13*, 13686–13699. https://doi.org/10.1109/ACCESS.2025.3531662

Antony, B., Fitriani, Y., & Sudirman, M. (2024). *PENERAPAN FOOTPRINTING DAN VULNERABILITY SCANNING DALAM MENGIDENTIFIKASI KERENTANAN KEAMANAN WEBSITE STUDI KASUS: PT INTERCLOUD DIGITAL INOVASI*. ITPLN.

Cabello-Solorzano, K., Peña Marco, Correia, L., J Tallón-Ballesteros, A., & Ortigosa de Araujo, I. (2023). The Impact of Data Normalization on the Accuracy of Machine Learning Algorithms: A Comparative Analysis. In H. and M. de P. F. J. and M. Á. F. and T. L. A. and H. Á. and C. R. J. L. and Q. H. and C. E. García Bringas Pablo and Pérez García (Ed.), *18th International Conference on Soft Computing Models in Industrial and Environmental Applications (SOCO 2023)* (pp. 344–353). Springer Nature Switzerland.

Chee, K. O., Ge, M., Bai, G., & Kim, D. D. (2025). Unveiling the evolution of IoT threats: Trends, tactics, and simulation analysis. *Computers and Security*, *157*. https://doi.org/10.1016/j.cose.2025.104537

Chindove, H., & Brown, D. (2021). *Adaptive Machine Learning Based Network Intrusion Detection*. 1–6. https://doi.org/10.1145/3487923.3487938

Cisco. (2020). *Cisco Annual Internet Report (2018–2023)*.

De Bettignies, J. (2021). *LSTM Autoencoders for Botnet Detection*. https://doi.org/https://doi.org/10.34726/hss.2021.87961

Díaz-Verdejo, J., Muñoz-Calle, J., Estepa Alonso, A., Estepa Alonso, R., & Madinabeitia, G. (2022). On the Detection Capabilities of Signature-Based Intrusion Detection Systems in the Context of Web Attacks. *Applied Sciences*, *12*(2), 852. https://doi.org/10.3390/app12020852

Dini, P., Elhanashi, A., Begni, A., Saponara, S., Zheng, Q., & Gasmi, K. (2023). Overview on Intrusion Detection Systems Design Exploiting Machine Learning for Networking Cybersecurity. In *Applied Sciences (Switzerland)* (Vol. 13, Number 13). Multidisciplinary Digital Publishing Institute (MDPI). https://doi.org/10.3390/app13137507

Duan, L., Zhou, J., Wu, Y., & Xu, W. (2022). A novel and highly efficient botnet detection algorithm based on network traffic analysis of smart systems. *International Journal of Distributed Sensor Networks*, *18*(3), 155014772110499. https://doi.org/10.1177/15501477211049910

Fadhlurrohman, M. D., Sudirman, M., & Putra, R. I. (2024). *REKOMENDASI KEAMANAN CONTENT MANAGEMENT SYSTEM DENGAN UJI PENETRASI MENGGUNAKAN METODOLOGI OWASP WEB SECURITY TEST GUIDE*. ITPLN.

Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications*, *50*, 102419. https://doi.org/10.1016/j.jisa.2019.102419

Geetha, K., & Brahmananda, S. H. (2025). Botnet Detection Through Flow-Based Deep Feature Extraction and Ensemble Classification. *Journal of The Institution of Engineers (India): Series B*. https://doi.org/10.1007/s40031-025-01221-4

Georgoulias, D. ;, Pedersen, J. M., Hutchings, A. ;, Falch, M. ;, & Vasilomanolakis, E. (2023). *In the market for a Botnet? An in-depth analysis of botnet-related listings on Darkweb marketplaces*. APA.

Ghosh, K., Bellinger, C., Corizzo, R., Branco, P., Krawczyk, B., & Japkowicz, N. (2024). The class imbalance problem in deep learning. *Machine Learning*, *113*(7), 4845–4901. https://doi.org/10.1007/s10994-022-06268-8

Goodfellow, Ian., Bengio, Yoshua., & Courville, Aaron. (2017). *Deep learning*. The MIT Press.

Hinton, G. E., & Salakhutdinov, R. R. (2006). Reducing the Dimensionality of Data with Neural Networks. *Science*, *313*(5786), 504–507. https://doi.org/10.1126/science.1127647

Hossain, Md. A., & Islam, Md. S. (2023). A novel hybrid feature selection and ensemble-based machine learning approach for botnet detection. *Scientific Reports*, *13*(1), 21207. https://doi.org/10.1038/s41598-023-48230-1

Iwanowski, M., Olszewski, D., Graniszewski, W., Krupski, J., & Pelc, F. (2025). The Choice of Training Data and the Generalizability of Machine Learning Models for

Network Intrusion Detection Systems. *Applied Sciences*, *15*(15), 8466. https://doi.org/10.3390/app15158466

Kanimozhi, V., & Jacob, T. P. (2021). Artificial Intelligence outflanks all other machine learning classifiers in Network Intrusion Detection System on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing. *ICT Express*, *7*(3), 366–370. https://doi.org/10.1016/j.icte.2020.12.004

Khan, F. A., Shah, A. A., Alshammry, N., Saif, S., Khan, W., Malik, M. O., & Ullah, Z. (2024). Balanced Multi-Class Network Intrusion Detection Using Machine Learning. *IEEE Access*, *12*, 178222–178236. https://doi.org/10.1109/ACCESS.2024.3503497

Maseno, E. M., Wang, Z., & Xing, H. (2022). A Systematic Review on Hybrid Intrusion Detection System. *Security and Communication Networks*, *2022*, 1–23. https://doi.org/10.1155/2022/9663052

Mirsky, Y., Doitshman, T., Elovici, Y., & Shabtai, A. (2018). Kitsune: An Ensemble of Autoencoders for Online Network Intrusion Detection. *Proceedings 2018 Network and Distributed System Security Symposium*. https://doi.org/10.14722/ndss.2018.23204

Moriano, P., Hespeler, S. C., Li, M., & Mahbub, M. (2025). Adaptive anomaly detection for identifying attacks in cyber-physical systems: A systematic literature review. *Artificial Intelligence Review*, *58*(9). https://doi.org/10.1007/s10462-025-11292-w

Mudassir, M., Unal, D., Hammoudeh, M., & Azzedin, F. (2022). Detection of Botnet Attacks against Industrial IoT Systems by Multilayer Deep Learning Approaches. *Wireless Communications and Mobile Computing*, *2022*(1). https://doi.org/10.1155/2022/2845446

Mujahid, M., Kına, E. R. O. L., Rustam, F., Villar, M. G., Alvarado, E. S., De La Torre Diez, I., & Ashraf, I. (2024). Data oversampling and imbalanced datasets: an investigation of performance for machine learning and feature engineering. *Journal of Big Data*, *11*(1). https://doi.org/10.1186/s40537-024-00943-4

Nadeem, M. W., Goh, H. G., Aun, Y., & Ponnusamy, V. (2023). Detecting and Mitigating Botnet Attacks in Software-Defined Networks Using Deep Learning Techniques. *IEEE Access*, *11*, 49153–49171. https://doi.org/10.1109/ACCESS.2023.3277397

Najmul, I., Sundara, R., Abdurrasyid, A., & Saptawati, G. A. P. (2025). Uji Mutasi pada Penerapan Token Mitigasi Kerentanan Cross Site Request Forgery. *PETIR*, *17*(2), 143–153. https://doi.org/10.33322/petir.v17i2.2493

Nasdaq. (2020). *Cybercrime to cost the world $10.5 trillion annually by 2025*. https://www.nasdaq.com/press-release/cybercrime-to-cost-the-world-$10.5-trillion-annually-by-2025-2020-11-18

Nicholas Sibarani, J., Ronaldo Sirait, D., & Salma Safira Ramadhanti, dan. (2023). *Intrusion Detection Systems pada Bot-IoT Dataset Menggunakan Algoritma Machine Learning* (Vol. 14, Number 1).

Nursiaga, R., Mulyana, N., & Sanjaya, H. (2025). Model Jaringan Neural Untuk Deteksi Anomali Pada Sistem Keamanan (SIBER): Rancangan, Implementasi, dan Analisis. *JAREKOM: Jurnal Jaringan Dan Rekayasa Komputer*, *1*, 1–9. https://doi.org/https://doi.org/10.9020/jarekom.v1i1.905

Park, C., Lee, J., Kim, Y., Park, J. G., Kim, H., & Hong, D. (2023). An Enhanced AI-Based Network Intrusion Detection System Using Generative Adversarial Networks. *IEEE Internet of Things Journal*, *10*(3), 2330–2345. https://doi.org/10.1109/JIOT.2022.3211346

Pinto, A., Herrera, L. C., Donoso, Y., & Gutierrez, J. A. (2023). Survey on Intrusion Detection Systems Based on Machine Learning Techniques for the Protection of Critical Infrastructure. In *Sensors* (Vol. 23, Number 5). MDPI. https://doi.org/10.3390/s23052415

Sakurada, M., & Yairi, T. (2014). Anomaly Detection Using Autoencoders with Nonlinear Dimensionality Reduction. *Proceedings of the MLSDA 2014 2nd Workshop on Machine Learning for Sensory Data Analysis*, 4–11. https://doi.org/10.1145/2689746.2689747

Saltz, J. S. (2021). CRISP-DM for Data Science: Strengths, Weaknesses and Potential Next Steps. *2021 IEEE International Conference on Big Data (Big Data)*, 2337–2344. https://doi.org/10.1109/BigData52589.2021.9671634

Saputra, D. R. K., Via, Y. V., & Sihananto, A. N. (2024). DETEKSI ANOMALI MENGGUNAKAN ENSEMBLE LEARNING DAN RANDOM OVERSAMPLING PADA PENIPUAN TRANSAKSI KEUANGAN. *Jurnal Informatika Dan Teknik Elektro Terapan*, *12*(3). https://doi.org/10.23960/jitet.v12i3.4910

Sathyanarayanan, S. (2024). Confusion Matrix-Based Performance Evaluation Metrics. *African Journal of Biomedical Research*, 4023–4031. https://doi.org/10.53555/ajbr.v27i4s.4345

Schröer, C., Kruse, F., & Gómez, J. M. (2021). A systematic literature review on applying CRISP-DM process model. *Procedia Computer Science*, *181*, 526–534. https://doi.org/10.1016/j.procs.2021.01.199

Shanmugam, V., Razavi-Far, R., & Hallaji, E. (2024). Addressing Class Imbalance in Intrusion Detection: A Comprehensive Evaluation of Machine Learning Approaches. *Electronics*, *14*(1), 69. https://doi.org/10.3390/electronics14010069

Sharafaldin, I., Habibi Lashkari, A., & Ghorbani, A. A. (2018). Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization. *Proceedings of the 4th International Conference on Information Systems Security and Privacy*, 108–116. https://doi.org/10.5220/0006639801080116

Shimaoka, A. M., Ferreira, R. C., & Goldman, A. (2024). The evolution of CRISP-DM for Data Science: Methods, Processes and Frameworks. *SBC Reviews on Computer Science*, *4*(1), 28–43. https://doi.org/10.5753/reviews.2024.3757

Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A Deep Learning Approach to Network Intrusion Detection. *IEEE Transactions on Emerging Topics in Computational Intelligence*, *2*(1), 41–50. https://doi.org/10.1109/TETCI.2017.2772792

Silva, S. S. C., Silva, R. M. P., Pinto, R. C. G., & Salles, R. M. (2013). Botnets: A survey. *Computer Networks*, *57*(2), 378–403. https://doi.org/10.1016/j.comnet.2012.07.021

Sudirman, M. Y. D. (2024). Penerapan Open Worldwide Application Security Project untuk Analisis Keamanan pada Open-Source Content Management System. *SNEKTI*, *5*(1).

Talukder, M. A., Islam, M. M., Uddin, M. A., Hasan, K. F., Sharmin, S., Alyami, S. A., & Moni, M. A. (2024). Machine learning-based network intrusion detection for big and imbalanced data using oversampling, stacking feature embedding and feature extraction. *Journal of Big Data*, *11*(1). https://doi.org/10.1186/s40537-024-00886-w

Tatarnikova, T. M., Sikarev, I. A., Bogdanov, P. Yu., & Timochkina, T. V. (2022). Botnet Attack Detection Approach in IoT Networks. *Automatic Control and Computer Sciences*, *56*(8), 838–846. https://doi.org/10.3103/S0146411622080259

Vergara Cobos, E., Cakir, S., Straub, S., Qiang, C. Z., & Torgusson, C. (n.d.). *A Review of the Economic Costs of Cyber Incidents*.

Wongvorachan, T., He, S., & Bulut, O. (2023). A Comparison of Undersampling, Oversampling, and SMOTE Methods for Dealing with Imbalanced Classification in Educational Data Mining. *Information (Switzerland)*, *14*(1). https://doi.org/10.3390/info14010054