# DAFTAR PUSTAKA


Ammara, D. A., Ding, J., & Tutschku, K. (2024). *Synthetic Network Traffic Data Generation: A Comparative Study*. http://arxiv.org/abs/2410.16326

Anande, T. J., Al-Saadi, S., & Leeson, M. S. (2023). Generative adversarial networks for network traffic feature generation. In *International Journal of Computers and Applications* (Vol. 45, Issue 4, pp. 297–305). https://doi.org/10.1080/1206212X.2023.2191072

Arjovsky, M., Chintala, S., & Bottou, L. (2017). *Wasserstein GAN*. Cornell University. https://arxiv.org/abs/1701.07875

Bakır, R. (2025). UniEmbed: A Novel Approach to Detect XSS and SQL Injection Attacks Leveraging Multiple Feature Fusion with Machine Learning Techniques. *Arabian Journal for Science and Engineering*, *50*(19), 15591–15604. https://doi.org/10.1007/s13369-024-09916-4

Bangun, C. S. (2012). *Uji Perbandingan Sistem Deteksi Intrusi Berdasarkan Sumber Data Header dan Payload*. https://repository.uksw.edu/bitstream/123456789/6489/7/T1_672008233_Judul.pdf

Dasari, N. S., Badii, A., Moin, A., & Ashlam, A. (2025). *Enhancing SQL Injection Detection and Prevention Using Generative Models*. *January*, 1–13. http://arxiv.org/abs/2502.04786

Fathoni, W. (2015). *DETEKSI PENYUSUPAN PADA JARINGAN KOMPUTER MENGGUNAKAN IDS SNORT*. https://openlibrary.telkomuniversity.ac.id/pustaka/files/114823/persembahan/deteksi-penyusupan-pada-jaringan-komputer-menggunana-ids-snort.pdf

Goodfellow, I., Pouget-Abadie, J., & Mirza, M. (2020). *Generative adversarial networks*. Communications of the ACM. https://dl.acm.org/doi/10.1145/3422622

IBM. (2025). *IBM X-Force 2025 Threat Intelligence Index*. 30.

Ignacio, C., & Campazas, A. (2022). *SQL Injection Attack Netflow*. Zenodo Home. https://zenodo.org/records/6907252

Leni, D., Ade, Berli, U., Dytchia, Kesuma, S., Haris, & Ruzita. (2023). Evaluasi Pemodelan Augmentasi Data Sifat Mekanik Aluminium Menggunakan Generative Adversarial Networks. *Jurnal Engine*, *8*, 09–21.

LI, Y.-H., ASLAM, M. S., HARFIYA, L. N., & CHANG, C.-C. (2021). *Conditional Wasserstein Generative Adversarial Networks for Rebalancing Iris Image Datasets*. IEICE Transactions on Information and Systems. https://www.jstage.jst.go.jp/article/transinf/E104.D/9/E104.D_2021EDP7079/_article/-char/en

Lie, I. (2018). *Analisis Dan Pencegahan SQL Injection dengan Honeypot.* UPB Repository Administration. http://repository.upbatam.ac.id/4614/1/cover s.d bab III.pdf

Lin, Z., Shi, Y., & Xue, Z. (2022). *IDSGAN: Generative Adversarial Networks for Attack Generation Against Intrusion Detection*. ACM Digital Library. https://dl.acm.org/doi/10.1007/978-3-031-05981-0_7

Manocchio, L. D., Layeghy, S., & Portmann, M. (2021). FlowGAN - Synthetic Network Flow Generation using Generative Adversarial Networks. In *Proceedings - 2021 IEEE 24th International Conference on Computational Science and Engineering, CSE 2021* (pp. 168–176). https://doi.org/10.1109/CSE53436.2021.00033

Nielsen, F. (2019). On the Jensen-Shannon symmetrization of distances relying on abstract means. *Entropy*, *21*(5), 1–23. https://doi.org/10.3390/e21050485

Unikom, E. (2021). *Analisis dan Perancangan Sistem Deteksi Serangan SQL Injection.* https://elib.unikom.ac.id/files/disk1/696/jbptunikompp-gdl-toniprabow-34771-12-13.unik-i.pdf

Xu, L., Skoularidou, M., Cuesta-Infante, A., & Veeramachaneni, K. (2019). Modeling tabular data using conditional GAN. *Advances in Neural Information Processing Systems*, *32*(NeurIPS).

Zeng, Q., & Farid Nait-Abdesselam. (2025). *Enhancing UAV Network Security: A Human-in-the-Loop and GAN-Based Approach to Intrusion Detection*. IEEE INTERNET OF THINGS JOURNAL. https://www.researchgate.net/publication/389295141_Enhancing_UAV_Network_Security_A_Human-in-the-Loop_and_GAN-Based_Approach_to_Intrusion_Detection