

DAFTAR PUSTAKA

- [1] S. Pradani Informatika, “PENDEKATAN DEEP LEARNING UNTUK DETEKSI ANOMALI DALAM KEAMANAN SIBER,” *Teknologipintar.org*, vol. 4, no. 1, p. 1, 2024.
- [2] I. E. Maulani, D. R. S. Putra, and Komarudin, “SISTEM DETEKSI INTRUSI CERDAS: STUDI PERBANDINGAN ALGORITMA PEMBELAJARAN MESIN UNTUK KEAMANAN SIBER,” *Jurnal Sosial dan Teknologi*, vol. 3, no. 11, pp. 918–923, Nov. 2023.
- [3] J. T. Santoso, *TEKNOLOGI KEAMANAN SIBER (Cyber Security)*. Semarang: YAYASAN PRIMA AGUS TEKNIK, 2023.
- [4] A. Suryadi and I. Marzuki, “Pengembangan Intrusion Detection System (Ids) Berbasis Machine Learning,” *Jurnal Telekomunikasi dan Komputer*, vol. 13, no. 3, pp. 189–195, doi: 10.22441/incomtech.v13i3.15118.
- [5] B. Ananda, M. Sihombing, N. F. Saragih, and I. M. Sarkis, “Implementasi Long Short Term Memory dalam Deteksi Serangan DDoS pada Virtual Private Server,” 2024. [Online]. Available: <https://ejurnal.methodist.ac.id/index.php/methotika>
- [6] A. Prijuna Lubis, “INTRUSION DETECTION SYSTEM BERBASIS DEEP LEARNING UNTUK PENINGKATAN MITIGASI SQL INJECTION DAN SYN FLOOD ATTACK,” 2024. [Online]. Available: <http://jurnal.goretanpena.com/index.php/JSSR>
- [7] N. D. K. Salwa, “Tantangan & Hambatan Besar yang Dihadapi CSIRT-BSSN Indonesia,” Computer Security Incident Response Team Indonesia. Accessed: Jun. 23, 2025. [Online]. Available: <https://csirt.or.id/pengetahuan-dasar/tantangan-csirt-bssn>
- [8] R. H. Wicaksana, A. I. Munandar, and P. L. Samputra, “Studi Kebijakan Perlindungan Data Pribadi dengan Narrative Policy Framework: Kasus Serangan Siber Selama Pandemi Covid-19,” *Jurnal Ilmu Pengetahuan dan Teknologi Komunikasi*, vol. 22, no. 2, pp. 143–158, Nov. 2020, doi: 10.33164/iptekkom.22.2.2020.143-158.
- [9] T. Vimy, S. Wiranto, Rudiyanto, P. Widodo, and P. Suwarno, “ANCAMAN SERANGAN SIBER PADA KEAMANAN NASIONAL INDONESIA,” *Jurnal Kewarganegaraan*, vol. 6, no. 1, pp. 2319–2327, 2022.
- [10] L. I. Uzlal, R. A. Saputra, and Isnawaty, “DETEKSI SERANGAN SIBER PADA JARINGAN KOMPUTER MENGGUNAKAN METODE

- RANDOM FOREST,” *Jurnal Mahasiswa Teknik Informatika*, vol. 8, no. 3, pp. 2787–2793, 2024.
- [11] Telkomsel Enterprise, “Hadapi Serangan Siber: Peran Sistem Deteksi dan Respons dalam Mitigasi Risiko,” Telkomsel Enterprise. Accessed: Jun. 23, 2025. [Online]. Available: <https://www.telkomsel.com/enterprise/insight/blog/mengenal-sistem-deteksi-dan-respons>
- [12] A. A. Jihado and A. S. Girsang, “Hybrid Deep Learning Network Intrusion Detection System Based on Convolutional Neural Network and Bidirectional Long Short-Term Memory,” *Journal of Advances in Information Technology*, vol. 15, no. 2, pp. 219–232, 2024, doi: 10.12720/jait.15.2.219-232.
- [13] T. Tan, H. Sama, G. Wijaya, and O. E. Aboagye, “Studi Perbandingan Deteksi Intrusi Jaringan Menggunakan Machine Learning: (Metode SVM dan ANN),” *Jurnal Teknologi dan Informasi*, vol. 13, no. 2, pp. 152–164, Sep. 2023, doi: 10.34010/jati.v13i2.
- [14] M. Fluorida Fibrianda and A. Bhawiyuga, “Analisis Perbandingan Akurasi Deteksi Serangan Pada Jaringan Komputer Dengan Metode Naïve Bayes Dan Support Vector Machine (SVM),” 2018. [Online]. Available: <http://j-ptiik.ub.ac.id>
- [15] Graha Karya Informasi, “Apa Itu IDS (Intrusion Detection System): Jenis, Metode, dan Cara Kerja.” Accessed: Jun. 29, 2025. [Online]. Available: <https://grahakarya.com/blog/apa-itu-ids-intrusion-detection-system-jenis-metode-dan-cara-kerja>
- [16] Keylabs, “Neural Networks and Deep Learning for Classification,” Keylabs. Accessed: Jun. 23, 2025. [Online]. Available: <https://keylabs.ai/blog/neural-networks-and-deep-learning-for-classification/>
- [17] J. Hussain Kalwar and S. Bhatti, “Deep Learning Approaches for Network Traffic Classification in the Internet of Things (IoT): A Survey.”
- [18] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, “Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study,” *Journal of Information Security and Applications*, vol. 50, Feb. 2020, doi: 10.1016/j.jisa.2019.102419.