# DAFTAR PUSTAKA


[1] Y. Cahyaningrum, "Pengembangan *Web*site E-Commerce untuk Meningkatkan Efektivitas Media Promosi dan Penjualan Online," *Jurnal Inovasi dan Tren Pendidikan Teknologi Informasi*, vol. 2, no. 1, pp. 3026–3190, 2024, doi: 10.37630/inventor.v1i3.1421.

[2] A. Wahab Syakhrani STAI Rasyidiyah Khalidiyah Amuntai, M. Dongoran UIN Syekh Ali Hasan Ahmad Addary Padangsidimpuan, and A. Ruben Runtu Sekolah Tinggi Ilmu Kesehatan Bethesda Tomohon, "Strategi Pembelajaran dalam Pendidikan Jarak Jauh," vol. 11, no. 01, pp. 195–203, 2025.

[3] E. Nurnilawati, R. Jayanti Vijaya, S. Ngudi Wahyuni, V. Wulandari, P. Studi Komunikasi, and P. Studi Manajemen Informatika, "Pengembangan Sistem informasi Layanan Publik Berbasis *Web*site Menggunakan Framework CodeIgniter," Nov. 2022.

[4] M. Amirul Mu'min, N. Tristanti, G. Pramuja, and I. Fanani, "Analisis dan Pengujian Kerentanan *Web*site Menggunakan OWASP ZAP," *Jurnal Riset Sistem dan Teknologi Informasi (RESTIA*, vol. 3, no. 1, pp. 36–50, 2024.

[5] M. Soleh and Z. Tjenreng, "Strategi Pencegahan Kebocoran Data Pelayanan Publik Di Era Digital," *JKP) Journal of Government, Social and Politics*, vol. 11, 2024.

[6] D. Lo and M. Dodi Firmansyah, "Analisis Kerentanan Perlindungan Data Pribadi Pada Aplikasi Sistem Informasi Berbasis *Web*," Jan. 2025, doi: 10.38035/jemsi.v6i3.

[7] A. Januantoro, "Deteksi Serangan Jaringan Komputer Berbasis Snort Dengan Integrasi Notifikasi *Real-time* Melalui Telegram," 2025.

[8] I. Faisal, D. Handoko, and H. Putra, “Penerapan Metode Rule Based Dalam Mendeteksi Serangan Multi Attack Pada Network Attached Storage,” 2024.

[9] T. Tan, H. Sama, G. Wijaya, and O. E. Aboagye, “Studi Perbandingan Deteksi Intrusi Jaringan Menggunakan Machine Learning: (Metode SVM dan ANN),” vol. 13, 2023, doi: 10.34010/jati.v13i2.

[10] I. Faisal, D. Handoko, and H. Putra, “Penerapan Metode Rule Based Dalam Mendeteksi Serangan Multi Attack Pada Network Attached Storage,” 2024.

[11] Bashkara M, Hendra Suputra P dkk, “Klasifikasi Serangan Distributed Denial of *Service* (DDoS) Menggunakan *Random Forest* dengan CFS,” Nov. 2022, [Online]. Available: www.unb.ca.

[12] K. Inayah, K. Ramli, and P. Korespondensi, “Analisis Kinerja Intrusion Detection System Berbasis Algoritma *Random Forest* Menggunakan Dataset Unbalanced Honeynet BSSN,” Aug. 2024, doi: 10.25126/jtiik1148911.

[13] S. Rabbani and D. Diana, “Prediksi Kategori Serangan Siber dengan Algoritma Klasifikasi *Random Forest* Menggunakan Rapidminer,” *SMATIKA JURNAL*, vol. 13, no. 02, pp. 284–293, Dec. 2023, doi: 10.32664/smatika.v13i02.934.

[14] M. Mahendra Alvanof and R. Kesuma Dinata, “Penerapan Algoritma *Random Forest* dalam Deteksi dan Klasifikasi Ransomware,” 2024.

[15] N. Widiyasono, I. A. D. Giriantari, M. Sudarma, and L. Linawati, “Detection of Mirai Malware Attacks in IoT Environments Using *Random Forest* Algorithms,” *TEM Journal*, vol. 10, no. 3, pp. 1209–1219, Aug. 2023, doi: 10.18421/TEM103-27.

[16] mishra anupama, “Utilizing *Random Forest* for DDoS Attack Detection,” Jan. 2024. [Online]. Available: www.ijritcc.org

[17] A. Januantoro, “Deteksi Serangan Jaringan Computer Bebasis Snort Dengan Integrasi Notifikasi *Real-time* Melalui Telegram,” 2025.

[18] D. P. Sari, Z. Halim, I. Irlon, B. Waseso, and S. Saromah, “Implementasi *Machine learning* untuk Deteksi Intrusi pada Jaringan Komputer,” *Jurnal Minfo Polgan*, vol. 13, no. 2, pp. 1389–1394, Sep. 2024, doi: 10.33395/jmp.v13i2.14074.

[19] R. P. Simanjuntak, R. Parlindungan Simanjuntak, R. Rikson, M. Sijabat, and E. P. Korespondensi, “Meningkatkan Keamanan Siber dalam Lingkungan Internet of Things (IoT) dengan Menggunakan Sistem Deteksi Intrusi Berbasis Pembelajaran Mesin,” 2024.

[20] M. K. Harto and A. Basuki, “Deteksi Serangan DDoS Pada Jaringan Berbasis SDN Dengan Klasifikasi Random Forest,” 2021. [Online]. Available: http://j-ptiik.ub.ac.id

[21] N. A. Prasetiyo, R. B. Huwae, and A. H. Jatmika, “Audit Dan Analisis *Web*site Pemerintah Menggunakan Pengujian Penetrasi *SQL Injection* and Cross-Site *Script*ing (XSS),” Sep. 2024. [Online]. Available: http://jtika.if.unram.ac.id/index.php/JTIKA/

[22] M. Zidane, “Klasifikasi Serangan Distributed Denial-of-*Service* (DDoS) menggunakan Metode Data Mining Naïve Bayes,” 2022. [Online]. Available: http://j-ptiik.ub.ac.id

[23] Istiani Aulia, “Implementasi Metode *Random Forest* Untuk Klasifikasi Kategori Berita Online,” Malang, Jun. 2024.

[24] N. Tou, P. M. Endraswari, and C. Responden, “Implementasi Data Mining Dalam Klasifikasi Hasil Diagnosa Pasien Bpjs Menggunakan Algoritma Cart,” 2022.

[25] C. E. Brita, J. G. M. Van Der Linden, and D. Demirovi´c, “Optimal Classification Trees for Continuous Feature Data Using Dynamic Programming with Branch-and-Bound,” 2025. [Online]. Available: www.aaai.org

[26] A. D. Harahap, D. Juardi, and A. S. Y. Irawan, “Rancang Bangun Sistem Pendeteksi Link Phishing Menggunakan Algoritma *Random Forest* Berbasis *Web*,” *Jurnal Informatika dan Teknik Elektro Terapan*, vol. 12, no. 3, Aug. 2024, doi: 10.23960/jitet.v12i3.4858.

[27] M. Zidane, “Klasifikasi Serangan Distributed Denial-of-*Service* (DDoS) menggunakan Metode Data Mining Naïve Bayes,” Jan. 2022. [Online]. Available: http://j-ptiik.ub.ac.id

[28] M. M. C. P. Ir. Munawar, “Analisis Perancangan Berorientasi Objek dengan Unified Model Language (UML),” 2005.

[29] A. Majumdar, S. Raj, and T. Subbulakshmi, “ARP Poisoning Detection and Prevention using *Scapy*,” in *Journal of Physics: Conference Series*, IOP Publishing Ltd, Jun. 2021. doi: 10.1088/1742-6596/1911/1/012022.

[30] D. D. Sahara, A. ; Sapri, and S. Akbar, “The Design And Implementation Of Computer Network Monitoring And Security System Using Linux *Ubuntu Server*,” ARTICLE HISTORY, 2024.

[31] I. Penggunaan Jaringan Intranet Menggunakan Linux *Ubuntu Server*, A. Adhi Dharma, and F. Hari Utami, “Implementasi Penggunaan Jaringan Intranet Menggunakan Linux *Ubuntu Server*,” *Jurnal Media Infotama*, vol. 20, no. 2, p. 341139, Oct. 2024.

[32] G. Pradita and A. Pramono, “Implementasi Monitoring Keamanan Jaringan Pada *Server Ubuntu* Menggunakan Snort Intrusion Detection Prevention System (IDPS) Dan Telegram Bot Sebagai Media Notifikasi di PT SS UTAMA,” Aug. 2024.

[33] M. Zidane, “Klasifikasi Serangan Distributed Denial-of-*Service* (DDoS) menggunakan Metode Data Mining Naïve Bayes,” 2022. [Online]. Available: http://j-ptiik.ub.ac.id

[34] J. Elektronik and I. Komputer Udayana, “Klasifikasi Serangan Distributed Denial of *Service* (DDoS) Menggunakan *Random Forest* dengan CFS,” Nov. 2022, [Online]. Available: www.unb.ca.

[35] Y. C. Wang, Y. C. Houng, H. X. Chen, and S. M. Tseng, “Network Anomaly Intrusion Detection Based on Deep Learning Approach,” *Sensors*, vol. 23, no. 4, Feb. 2023, doi: 10.3390/s23042171.