

DAFTAR PUSTAKA

- [1] M. Anif, S. Hws, and M. D. Huri, “Penerapan Intrusion Detection System (IDS) dengan metode Deteksi Port Scanning pada Jaringan Komputer di Politeknik Negeri Semarang,” vol. 13, pp. 25–30, 2016.
- [2] N. A. Amalia Rizqi Utami, Yudha Purwanto, “Pengelompokan Trafik Berdasarkan Waktu Dengan Algoritma Clustream Untuk Deteksi Anomali Pada Aliran Trafik,” vol. 4, no. 1, pp. 848–854, 2017.
- [3] R. Bahtiar, M. D. Sakti, A. Setiawan, and P. Rosyani, “Analisis Perbandingan Detection Traffic Anomaly dengan Metode Naive Bayes dan DBSCAN,” *J. Kreat. Mhs. Inform.*, vol. 1, no. 2, pp. 99–103, 2020.
- [4] M. K. Harto and A. Basuki, “Deteksi Serangan DDoS Pada Jaringan Berbasis SDN Dengan Klasifikasi Random Forest,” vol. 5, no. 4, pp. 1329–1333, 2021.
- [5] M. Fadhlurrohman, A. Muliawati, and B. Hananto, “Analisis Kinerja Intrusion Detection System pada Deteksi Anomali dengan Metode Decision Tree Terhadap Serangan Siber Analysis of Intrusion Detection System Performance on Anomaly Detection with Decision Tree Method Against Cyber Attacks,” vol. 8, no. Pratomo 2016, pp. 90–94.
- [6] S. K. AM Siregar, S Kom, MKDANA Puspabhuana, *DATA MINING : Pengolahan Data Menjadi Informasi dengan RapidMiner*. 2017.
- [7] M. Pramana, Endang Setyati, and F.X. Ferdinandus, “Identifikasi Serangan Denial Of Service (Dos) Di Jaringan Dengan Algoritma Decision Tree C4.5,” *Wahana*, vol. 73, no. 2, pp. 13–29, 2021, doi: 10.36456/wahana.v73i2.4071.
- [8] M. S. Rafsanjani, F. Informatika, U. Telkom, and R. Forest, “Deteksi Serangan Botnet Pada Jaringan Internet of Things Menggunakan Algoritma Random Forest (RF),” vol. 9, no. 3, pp. 1862–1871, 2022.
- [9] K. Kurniabudi, A. Harris, and V. Veronica, “Komparasi Performa Tree-Based Classifier Untuk Deteksi Anomali Pada Data Berdimensi Tinggi dan Tidak Seimbang,” *J. Media Inform. Budidarma*, vol. 6, no. 1, p. 370, 2022, doi: 10.30865/mib.v6i1.3473.
- [10] Y. Mulyanto, H. Herfandi, and R. Candra Kirana, “Analisis Keamanan Wireless Local Area Network (Wlan) Terhadap Serangan Brute Force Dengan Metode Penetration Testing (Studi kasus:RS H.LMANAMBAI ABDULKADIR),” *J. Inform. Teknol. dan Sains*, vol. 4, no. 1, pp. 26–35, 2022, doi: 10.51401/jinteks.v4i1.1528.
- [11] E. Gunadhi and A. P. Nugraha, “Penerapan Kriptografi Base64 Untuk

- Keamanan URL (Uniform Resource Locator) Website Dari Serangan SQL Injection,” *J. Algoritm.*, vol. 13, no. 2, pp. 391–398, 2017, doi: 10.33364/algoritma/v.13-2.391.
- [12] Bangkit Wiguna, W. Adi Prabowo, and R. Ananda, “Implementasi Web Application Firewall Dalam Mencegah Serangan SQL Injection Pada Website,” *Digit. Zo. J. Teknol. Inf. dan Komun.*, vol. 11, no. 2, pp. 245–256, 2020, doi: 10.31849/digitalzone.v11i2.4867.
- [13] S. Suroto and A. Asman, “Ancaman Terhadap Keamanan Informasi Oleh Serangan Cross-Site Scripting (Xss) Dan Metode Pencegahannya,” *Zo. Komput.*, vol. 11, no. 1, pp. 11–19, 2021, [Online]. Available: <http://www.hackers.com?yid=>.
- [14] S. Anwar, F. Septian, and R. D. Septiana, “Klasifikasi Anomali Intrusion Detection System (IDS) Menggunakan Algoritma Naïve Bayes Classifier dan Correlation-Based Feature Selection,” *J. Teknol. Sist. Inf. dan Apl.*, vol. 2, no. 4, p. 135, 2019, doi: 10.32493/jtsi.v2i4.3453.
- [15] S. R. Niko Suwaryo¹, Ismasari Nawangsih², “Deteksi Serangan pada Intrusion Detection System (IDS) untuk Klasifikasi Serangan dengan Algoritma Naïve Bayes, C.45 dan K-NN dalam Meminimalisasi Resiko Terhadap Pengguna,” *Angew. Chemie Int. Ed. 6(11)*, 951–952., pp. 2013–2015, 2021.
- [16] G. Meena, “2017 International Conference on Computer, Communications and Electronics, COMPTELIX 2017,” *2017 Int. Conf. Comput. Commun. Electron. COMPTELIX 2017*, pp. 553–558, 2017.
- [17] Jupriyadi, “Implementasi Seleksi Fitur Menggunakan Algoritma FVBRM Untuk Klasifikasi Serangan Pada Intrusion Detection System (Ids),” *Semin. Nas. Teknol. Inf.*, vol. 17, no. January 2018, pp. 1–6, 2018, [Online]. Available: <https://jurnal.umj.ac.id/index.php/semnastek/article/view/3452/2601>.
- [18] Z. K. Maseer, R. Yusof, N. Bahaman, S. A. Mostafa, and C. F. M. Foozy, “Benchmarking of Machine Learning for Anomaly Based Intrusion Detection Systems in the CICIDS2017 Dataset,” *IEEE Access*, vol. 9, pp. 22351–22370, 2021, doi: 10.1109/ACCESS.2021.3056614.
- [19] I. Sharafaldin, “Intrusion Detection Evaluation Dataset (CIC-IDS2017),” *www.unb.ca*, 2018. <https://www.unb.ca/cic/datasets/ids-2017.html> (accessed May 20, 2022).
- [20] Kurniabudi, D. Stiawan, Darmawijoyo, M. Y. Bin Bin Idris, A. M. Bamhdi, and R. Budiarto, “CICIDS-2017 Dataset Feature Analysis with Information Gain for Anomaly Detection,” *IEEE Access*, vol. 8, pp. 132911–132921, 2020, doi: 10.1109/ACCESS.2020.3009843.
- [21] F. Elfaladonna and A. Rahmadani, “Analisa Metode Classification-

Decision Tree Dan Algoritma C.45 Untuk Memprediksi Penyakit Diabetes Dengan Menggunakan Aplikasi Rapid Miner,” *SINTECH (Science Inf. Technol. J.*, vol. 2, no. 1, pp. 10–17, 2019, doi: 10.31598/sintechjournal.v2i1.293.

- [22] M. S. Indah Werdiningsih, S.Si., M.Kom., Barry Nuqoba, S.Si., M.Kom., Muhammadun, S.Si., *Data Mining Menggunakan Android, Weka, dan SPSS*. Jawa Timur: Airlangga University Press, 2020.
- [23] Y. D. Atma and A. Setyanto, “Perbandingan algoritma c4.5 dan k-nn dalam identifikasi mahasiswa berpotensi drop out,” *Metik J. ISSN 2580-1503*, vol. 2, no. 2, pp. 31–37, 2018.
- [24] D. P. Utomo and M. Mesran, “Analisis Komparasi Metode Klasifikasi Data Mining dan Reduksi Atribut Pada Data Set Penyakit Jantung,” *J. Media Inform. Budidarma*, vol. 4, no. 2, p. 437, 2020, doi: 10.30865/mib.v4i2.2080.
- [25] M. Faid, “Perbandingan Kinerja Tool Data Mining Weka dan Rapidminer Dalam Algoritma Klasifikasi,” vol. 8, 2019, doi: 10.34148/teknika.v8i1.95.
- [26] R. Annisa, “Analisis Komparasi Algoritma Klasifikasi Data Mining Untuk Prediksi Penderita Penyakit Jantung,” *J. Tek. Inform. Kaputama*, vol. 3, no. 1, pp. 22–28, 2019, [Online]. Available: <https://jurnal.kaputama.ac.id/index.php/JTIK/article/view/141/156>.
- [27] Ainurrohmah, “Akurasi Algoritma Klasifikasi pada Software Rapidminer dan Weka,” *Prisma*, vol. 4, pp. 493–499, 2021, [Online]. Available: <https://journal.unnes.ac.id/sju/index.php/prisma/>.
- [28] M. D. Muafa, “Pengembangan Aplikasi Berbasis Web dengan Rshiny untuk Data Klasifikasi Menggunakan Metode Naive Bayes,” 2018.
- [29] D. K. Nurilahi, R. Munadi, S. Syahrial, And A. Bahri, “Penerapan Metode Naïve Bayes Pada Honeypot Dionaea Dalam Mendeteksi Serangan Port Scanning,” *Elkomika J. Tek. Energi Elektr. Tek. Telekomun. Tek. Elektron.*, Vol. 10, No. 2, P. 309, 2022, Doi: 10.26760/Elkomika.V10i2.309.
- [30] K. Kurniabudi, A. Harris, and A. E. Mintaria, “Komparasi Information Gain, Gain Ratio, CFs-Bestfirst dan CFs-PSO Search Terhadap Performa Deteksi Anomali,” *J. Media Inform. Budidarma*, vol. 5, no. 1, p. 332, 2021, doi: 10.30865/mib.v5i1.2258.
- [31] V. W. Saputra, Y. A. Sari, and A. W. Widodo, “Klasifikasi Jenis Makanan menggunakan Neighbor Weighted K-Nearest Neighbor dengan Seleksi Fitur Information Gain,” *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 3, no. Mei 2019, pp. 4749–4758, 2019.
- [32] A. Harris and A. Rahim, “Seleksi Fitur dengan Information Gain untuk Meningkatkan Deteksi Serangan DDoS Menggunakan Random Forest An Information Gain Feature Selection to Improve DDoS Detection using

Random Forest,” *Februari*, vol. 19, no. 1, pp. 56–66, 2020.

- [33] V. Junita and F. A. Bachtiar, “Klasifikasi Aktivitas Manusia menggunakan Algoritme Decision Tree C4.5 dan Information Gain untuk Seleksi Fitur,” *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 3, no. 10, pp. 9426–9433, 2020, [Online]. Available: <http://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/6446>.