DAFTAR PUSTAKA

[1] Y. I. Mahendra and R. E. Putra, “Penerapan Algoritma Gradient Boosted Decision Tree (GBDT) untuk Klasifikasi Serangan DDoS,” *JINACS (Journal Informatics Comput. Sci. ISSN*, vol. 06, pp. 158–166, 2024.

[2] Y. Prihantono, M. T. Yusuf, A. Kurniawan, A. Ilarizky, I. Komputer, and U. Borobudur, “ANALISA PERBANDINGAN ALGORITMA MACHINE LEARNING DECISION TREES DAN EXTRA TREES TERHADAP KINERJA INTRUSION DETECTION SYSTEM DALAM MEMPREDIKSI,” vol. 10, no. 1, pp. 53–63, 2024.

[3] A. Nugraha and F. A. Rafrastara, “Botnet Detection Survey,” *Semin. Nas. Teknol. Inf. Komun. Terap. 2011*, vol. 1, no. Semantik, 2011.

[4] R. Firdaus, A. I. Hadiana, and F. Kasyidi, “Model Deteksi Botnet Menggunakan Algoritma Decision Tree Dengan Untuk Mengidentifikasi Serangan Click Fraud,” *J. Informatics Commun. Technol.*, vol. 4, no. 2, pp. 10–20, 2023, doi: 10.52661/j_ict.v4i2.122.

[5] G. Martha and G. Bororing, “Evaluasi Kinerja Algoritma Machine Learning Dalam Prediksi Serangan Malware,” *J. Rev. Pendidik. dan Pengajaran*, vol. 7, no. 1, pp. 3060–3066, 2024.

[6] S. Susanto, M. A. S. Arifin, and H. O. L. Wijaya, “IoT Botnet Detection Using Autoencoders and Decision Trees,” *J. Sisfokom (Sistem Inf. dan Komputer)*, vol. 12, no. 3, pp. 329–334, 2023, doi: 10.32736/sisfokom.v12i3.1693.

[7] M. Panda and M. R. Patra, “Detecting Network Intrusions : A Clustering Approach Detecting Network Intrusions - A Clustering Approach,” no. January 2009, 2014.

[8] M. Agus Syamsul Arifin, A. Anto Tri Susilo, A. Taqwa Martadinata, and B. Santoso, “KLIK: Kajian Ilmiah Informatika dan Komputer Deteksi Aktifitas Malware pada Internet of Things menggunakan Algoritma Decision Tree dan Random Forest,” *Media Online)*, vol. 4, no. 6, pp. 3073–3079, 2024, doi: 10.30865/klik.v4i6.1903.

[9] A. Rachmat, “Survei Penerapan Model Machine Learning Dalam Bidang Keamanan Informasi,” *J. Sist. Cerdas*, vol. 2, no. 1, pp. 47–60, 2019, doi: 10.37396/jsc.v2i1.20.

[10] N. Y. Abel Filemon Haganta Kaban, Indriati, “Analisis Sentimen Aplikasi E-Goverment berdasarkan Ulasan Pengguna menggunakan Metode Maximum Entropy dan Seleksi Fitur Mutual Information,” *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 5, no. 4, pp. 1452–1458, 2021.

[11] A. Selay *et al.*, “Karimah Tauhid, Volume 1 Nomor 6 (2022), e-ISSN 2963-590X,” *Karimah Tauhid*, vol. 1, no. 2963–590X, pp. 861–862, 2022.

[12] M. Zidane, “Klasifikasi Serangan Distributed Denial-of-Service (DDoS) menggunakan Metode Data Mining Naïve Bayes,” *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 6, no. 1, pp. 172–180, 2022, [Online]. Available: http://j-ptiik.ub.ac.id

[13] U. Maikudi, O. A. Abisoye, S. O. Ganiyu, and S. A. Bashir, “A Literature Survey on IoT Botnet Detection Techniques,” p. 110, 2021.

[14] M. Lefoane, I. Ghafir, S. Kabir, and I. U. Awan, “Machine Learning for Botnet Detection: An Optimized Feature Selection Approach,” *ACM Int. Conf. Proceeding Ser.*, pp. 195–200, 2021, doi: 10.1145/3508072.3508102.

[15] R. F. A. Bintoro, P. H. Trisnawan, and M. Data, “Deteksi Bot Network (BOTNET) menggunakan Metode Decision Tree dari Dataset CTU,” *... Teknol. Inf. dan Ilmu ...*, vol. 7, no. 6, pp. 2921–2930, 2023, [Online]. Available: https://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/12857

[16] S. Saifullah, M. Zarlis, Z. Zakaria, and R. W. Sembiring, “Analisa Terhadap Perbandingan Algoritma Decision Tree Dengan Algoritma Random Tree Untuk Pre-Processing Data,” *J-SAKTI (Jurnal Sains Komput. dan Inform.*, vol. 1, no. 2, p. 180, 2017, doi: 10.30645/j-sakti.v1i2.41.

[17] S. Haryati, A. Sudarsono, and E. Suryana, “Implementasi Data Mining Untuk Memprediksi Masa Studi Mahasiswa Menggunakan Algoritma C4.5 (Studi Kasus: Universitas Dehasen Bengkulu),” *J. Media Infotama*, vol. 11, no. 2, pp. 130–138, 2015.

[18] D. Irawan, E. B. Perkasa, Y. Yurindra, D. Wahyuningsih, and E. Helmud, “Perbandingan Klassifikasi SMS Berbasis Support Vector Machine, Naive Bayes Classifier, Random Forest dan Bagging Classifier,” *J. Sisfokom (Sistem Inf. dan Komputer)*, vol. 10, no. 3, pp. 432–437, 2021, doi: 10.32736/sisfokom.v10i3.1302.

[19] H. Apriyani and K. Kurniati, “Perbandingan Metode Naïve Bayes Dan Support Vector Machine Dalam Klasifikasi Penyakit Diabetes Melitus,” *J. Inf. Technol. Ampera*, vol. 1, no. 3, pp. 133–143, 2020, doi:

10.51519/journalita.volume1.isssue3.year2020.page133-143.

[20] A. Wibowo, “Uji Chi-Square pada Statistika dan SPSS,” *J. Ilm. SINUS*, vol. 4, no. 2, p. 38, 2017.

[21] A. Hidayat, Y. Samudra, and L. P. Andriyanto, “Sosialisasi Pengenalan Pentingnya Cyber SecurityBagi Siswa Untuk Membangun Keamanan Informasi Dalam Era Digital,” *J. Pengabdi. Masy.*, vol. 2, no. 5, pp. 450–457, 2023.

[22] M. K. Harto and A. Basuki, “Deteksi Serangan DDoS Pada Jaringan Berbasis SDN Dengan Klasifikasi Random Forest,” *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 5, no. 4, pp. 1329–1333, 2021, [Online]. Available: http://j-ptiik.ub.ac.id

[23] Arqi Muhammad Fauzi, “Klasifikasi Serangan Malware Android Berdasarkan Analisis Fitur Dinamis Menggunakan Algoritma Random Forest,” vol. 4, no. 1, pp. 1–23, 2024.

[24] A. Guerra-Manzanares, J. Medina-Galindo, H. Bahsi, and S. Nomm, “MedBIoT: Generation of an IoT Botnet Dataset in a Medium-sized IoT Network,” *Int. Conf. Inf. Syst. Secur. Priv.*, no. Icissp 2020, pp. 207–218, 2020, doi: 10.5220/0009187802070218.

[25] S. Nurul, Shynta Anggrainy, and Siska Aprelyani, “Faktor-Faktor Yang Mempengaruhi Keamanan Sistem Informasi: Keamanan Informasi, Teknologi Informasi Dan Network (Literature Review Sim),” *J. Ekon. Manaj. Sist. Inf.*, vol. 3, no. 5, pp. 564–573, 2022, doi: 10.31933/jemsi.v3i5.992.

[26] R. Purba, W. S. Lestari, and M. Ulina, “Deteksi Serangan DDoS Mengunakan Deep Q-Network,” *J. Tek. Inform. dan Sist. Inf.*, vol. 9, no. 1, pp. 648–658, 2022, [Online]. Available: http://jurnal.mdp.ac.id

[27] G. A. Sandag, “Prediksi Rating Aplikasi App Store Menggunakan Algoritma Random Forest,” *CogITo Smart J.*, vol. 6, no. 2, pp. 167–178, 2020, doi: 10.31154/cogito.v6i2.270.167-178.

[28] V. S. Ginting, K. Kusrini, and E. Taufiq, “Implementasi Algoritma C4.5 untuk Memprediksi Keterlambatan Pembayaran Sumbangan Pembangunan Pendidikan Sekolah Menggunakan Python,” *Inspir. J. Teknol. Inf. dan Komun.*, vol. 10, no. 1, pp. 36–44, 2020, doi: 10.35585/inspir.v10i1.2535.

[29] T. P. Botnet, S. Khattak, N. R. Ramay, K. R. Khan, A. A. Syed, and A. Khayam, “Taksonomi Perilaku Botnet, Deteksi, dan Pertahanan,” pp. 1–40.

[30] B. A. B. Ii and A. K. Pustaka, “Ii, B A B Pustaka, A Kajian,” *“Penerapan Pendekatan Reciprocal Teach. Berbas. Media Pembelajaran*, p. 5, 2010.

[31] B. Triandi, “Keamanan Informasi secara Aksiologi Dalam Menghadapi Era Revolusi Industri 4.0,” *JURIKOM (Jurnal Ris. Komputer)*, vol. 6, no. 5, pp. 477–483, 2019, [Online]. Available: http://ejurnal.stmik-budidarma.ac.id/index.php/jurikom/article/view/1556

[32] T. Wahyono, “Fundamental of Python for Machine Learning Dasar-Dasar Pemrograman Python untuk Machine Learning dan Kecerdasan Buatan Edisi Revisi,” no. September 2018, 2021.

[33] M. Alshamkhany, W. Alshamkhany, M. Mansour, M. Khan, S. Dhou, and F. Aloul, “Botnet Attack Detection using Machine Learning,” *Proc. 2020*

14th Int. Conf. Innov. Inf. Technol. IIT 2020, no. November, pp. 203–208, 2020, doi: 10.1109/IIT50501.2020.9299061.

[34] E. O. Nasution and A. Basuki, "Implementasi Algoritme C5.0 Untuk Klasifikasi Serangan DDoS," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 5, no. 1, pp. 389–395, 2021.

[35] I. B. Gagananta Amartya *et al.*, "Implementasi Algoritma Naive Bayes Classifier (NBC) Dan Information Gain Untuk Mendeteksi DDoS," *JELIKU (Jurnal Elektron. Ilmu Komput. Udayana)*, vol. 11, no. 2, p. 273, 2022, doi: 10.24843/jlk.2022.v11.i02.p06.

[36] D. Suprihadi and I. Magfira, "Forensik Pada Jaringan Komputer Lokal Dengan Klasifikasi Svm Berbasis Framework Taara Universitas Kebangsaan Republik Indonesia," *J. Rev. Pendidik. dan Pengajaran*, vol. 7, no. 1, pp. 666–673, 2023, [Online]. Available: http://journal.universitaspahlawan.ac.id/index.php/jrpp/article/view/23541

[37] B. N. Kasmara, E. T. E. Handayani, and N. D. Nathasia, "Perbandingan Kinerja Algoritma K-Nearest Neighbors (K-NN) Dan Decision Tree dalam Deteksi Paket Malis pada Jaringan," *STRING (Satuan Tulisan Ris. dan Inov. Teknol.*, vol. 8, no. 3, p. 320, 2024, doi: 10.30998/string.v8i3.22362.

[38] T. R. Abdillah, "Analisis Komparasi Cycles X Render Dan Cycles Render Menggunakan Google Colab," *J. TIKA*, vol. 8, no. 1, pp. 90–94, 2023, doi: 10.51179/tika.v8i1.1937.