DAFTAR PUSTAKA

[1] K. Kurniabudi, A. Harris, and E. Rosanda, "Optimalisasi Seleksi Fitur Untuk Deteksi Serangan Pada IoT Menggunakan Classifier Subset Evaluator," *JURIKOM J. Ris. Komput.*, vol. 9, no. 4, p. 885, Aug. 2022, doi: 10.30865/jurikom.v9i4.4618.

[2] M. A. S. Arifin, A. A. T. Susilo, A. T. Martadinata, and B. Santoso, "Deteksi Aktifitas Malware pada *Internet of Things* menggunakan Algoritma Decision Tree dan Random Forest".

[3] R. Rahman and G. R. S. Odja, "Analisis dan Pencegahan Serangan DDoS Pada Jaringan Skala Besar," vol. 1, no. 2, 2024.

[4] M. N. Faiz, O. Somantri, A. R. Supriyono, and A. W. Muhammad, "Impact of Feature Selection Methods on Machine Learning-based for Detecting DDoS Attacks : Literature Review," *J. Inform. Telecommun. Eng.*, vol. 5, no. 2, pp. 305–314, Jan. 2022, doi: 10.31289/jite.v5i2.6112.

[5] Z. I. Sumayyah, S. D. S. Permana, M. Tsabit, and A. Setiawan, "Penerapan dan Mitigasi Teknik Slowloris dalam Serangan Distributed Denial-of-Service (DDos) terhadap Website Ilegal dengan Kali Linux," *J. Internet Softw. Eng.*, vol. 1, no. 2, p. 14, Jun. 2024, doi: 10.47134/pjise.v1i2.2694.

[6] M. Munir, I. Ardiansyah, J. D. Santoso, A. Mustopa, and S. Mulyatun, "DETECTION AND MITIGATION OF DISTRIBUTED DENIAL OF SERVICE ATTACKS ON NETWORK ARCHITECTURE SOFTWARE DEFINED NETWORKING USING THE *NAIVE BAYES* ALGORITHM," *J. Inf. Syst. Manag. JOISM*, vol. 3, no. 2, pp. 51–55, Jan. 2022, doi: 10.24076/joism.2022v3i2.656.

[7] R. Purba, W. S. Lestari, and M. Ulina, "Deteksi Serangan DDoS Mengunakan Deep Q-Network," vol. 9, no. 1, 2022.

[8] A. T. Zy, A. T. Sasongko, and A. Z. Kamalia, "Penerapan Naïve Bayes Classifier, Support Vector Machine, dan Decision Tree untuk Meningkatkan Deteksi Ancaman Keamanan Jaringan".

[9] M. Zidane, “Klasifikasi Serangan Distributed Denial-of-Service (DDoS) menggunakan Metode Data Mining Naïve Bayes”.

[10] D. Haryono and Y. Zulianda, “SISTEM PENDETEKSIAN SERANGAN JARINGAN LOCAL AREA NETWORK (LAN) MENGGUNAKAN ALGORITMA *NAIVE BAYES*”.

[11] A. D. Afifaturahman and F. Msn, “Perbandingan Algoritma K-Nearest Neighbour (KNN) dan *Naive Bayes* pada Intrusion Detection System (IDS),” *Innov. Res. Inform. Innov.*, vol. 3, no. 1, Mar. 2021, doi: 10.37058/innovatics.v3i1.2852.

[12] M. F. Fibrianda and A. Bhawiyuga, “Analisis Perbandingan Akurasi Deteksi Serangan Pada Jaringan Komputer Dengan Metode Naïve Bayes Dan Support Vector Machine (SVM)”.

[13] I. Maulana, “Optimalisasi Deteksi Serangan DDoS Menggunakan Algoritma Random Forest, SVM, KNN dan MLP pada Jaringan Komputer”.

[14] L. L. Pramita and A. P. Wibawa, “Perkembangan Teknologi Kesehatan di Era Society 5.0,” 2022.

[15] R. M. Surya Fadli, “SISTEM PENDETEKSIAN SERANGAN JARINGAN LOCAL AREA NETWORK (LAN) MENGGUNAKAN ALGORITMA *NAIVE BAYES*,” vol. 1, pp. 24–35, Jun. 2024.

[16] S. Vishnu, S. R. J. Ramson, and R. Jegan, “Internet of Medical Things (IoMT) - An overview,” in 2020 5th International Conference on Devices, Circuits and Systems (ICDCS), Coimbatore, India: IEEE, Mar. 2020, pp. 101–104. doi: 10.1109/ICDCS48716.2020.243558.

[17] T. G. Laksana, “Perlindungan Hukum Konsumen E-Commerce pada Produk Kesehatan: Pembelajaran pada Kejahatan Siber,” green, vol. 2, no. 1, Jan. 2024, doi: 10.31004/green.v2i1.45.

[18] M. A. Syaiful Bachri M, “Transparansi dan Auditabilitas Data Pribadi dalam Layanan Berbasis Cloud Pada Proyek PACE: Studi Literatur,” vol. 1, pp. 1–8, 2024.

[19] B. Arifwidodo, Y. Syuhada, and S. Ikhwan, “Analisis Kinerja Mikrotik Terhadap Serangan Brute Force Dan DDoS,” tc, vol. 20, no. 3, pp. 392–399, Aug. 2021, doi: 10.33633/tc.v20i3.4615.

[20] Smith, J. A. (2010). *Introduction to cybersecurity*. New York, NY: McGraw-Hill.

[21] Jones, D. B., & Lee, K. H. (2015). *A study on IoT security* (Laporan Teknis No. TR-2015-01). Seoul, Korea: Korea Advanced Institute of Science and Technology.

[22] Pratama, A. D., & Rahmawati, D. (2023). Deteksi dini serangan zero-day pada jaringan perusahaan menggunakan teknik machine learning berbasis anomali. *Jurnal Teknologi Informasi dan Komunikasi*, 15(2), 55-68.

[23] Putri, A. N. (2021). *Implementasi Sistem Deteksi Intrusi Berbasis Machine Learning untuk Mengamankan Jaringan IoT di Rumah Pintar* (Tesis S1). Bandung: Institut Teknologi Bandung.

[24] Raharjo, A. S., & Susanto, B. (2023). Deteksi anomali lalu lintas jaringan untuk mengidentifikasi serangan *cyber* berbasis anomali. *Jurnal Sistem Informasi*, 12(2), 45-58.

[25] Setiawan, D., Hidayat, R., & Lestari, S. (2021). Analisis serangan berbasis anomali pada sistem kontrol industri: Studi kasus pada pembangkit listrik tenaga air. *Jurnal Teknik Elektro*, 8(3), 110-125.

[26] Setiawan, D., Hidayat, R., & Lestari, S. (2021). Deteksi serangan targeted attack yang mengeksploitasi kelemahan IDS. *Jurnal Sistem Informasi*, 8(3), 110-125.

[27] Putri, A. N., & Pratama, M. (2022). Mitigasi serangan DDoS pada IoT dengan penerapan sistem deteksi intrusi berbasis deep learning. *Jurnal Keamanan Siber Indonesia*, 9(1), 20-32.

[28] Lee, J. H., Kim, S. W., & Park, C. H. (2020). Pengembangan sistem pencegahan serangan DDoS pada IoT berbasis blockchain. Dalam *Prosiding Seminar Nasional Teknologi Informasi dan Komunikasi* (hal. 123-130). Bandung: Universitas Padjadjaran.

[29] Chen, X., Zhang, Y., & Liu, S. (2019). Analisis karakteristik serangan DDoS IoT dan evolusi botnet. Dalam *Prosiding Konferensi Nasional Teknologi Informasi* (hal. 250-257). Yogyakarta: Universitas Gadjah Mada.

[30] Setiawan, D., Hidayat, R., & Lestari, S. (2021). Analisis dampak serangan DDoS Mirai terhadap perangkat IoT di rumah pintar. *Jurnal Teknik Elektro*, 8(3), 110-125.

[31] M. D. Firmansyah, "Analisa Keamanan Web Server terhadap Serangan Distributed Denial of Service menggunakan Modevasive," no. 1, 2021.

[32] F. Ridho, A. Yudhana, I. Riadi, and U. A. Dahlan, "Implementasi Log Dalam Forensik Router Terhadap Serangan Distributed Denial of Service(DDoS)," no. 2, 2017.

[33] A. F. K. Dewi and Y. Suryanto, "Desain Kerangka Kerja Manajemen Risiko Keamanan Informasi Berdasarkan Kajian Risk Profiling pada Sektor Kesehatan," vol. 8, no. 1, 2022.

[34] Boyd, S. (2024). Apa itu Serangan DDoS dan Cara Mencegahnya di 2024. Diakses pada 18 Desember 2024, https://id.safetydetectives.com/blog/apa-itu-serangan-ddos-dan-bagaimana-mencegahnya/

[35] M. Syani, "IMPLEMENTASI INTRUSION DETECTION SYSTEM (IDS) MENGGUNAKAN SURICATA PADA LINUX DEBIAN 9 BERBASIS CLOUD VIRTUAL PRIVATE SERVERS (VPS)," JurnalInkofar, vol. 1, no. 1, Aug. 2020, doi: 10.46846/jurnalinkofar.v1i1.155.

[36] E. Stephani, Fitri Nova, and Ervan Asri, "Implementasi dan Analisa Keamanan Jaringan IDS (Intrusion Detection System) Menggunakan Suricata Pada Web Server," jitsi, vol. 1, no. 2, pp. 67–74, Dec. 2020, doi: 10.30630/jitsi.1.2.10

[37] D. N. Awangga, H. Sajati, and Y. Astuti, "PEMANFAATAN INTRUSION DETECTION SYSTEM (IDS) SEBAGAI OTOMATISASI KONFIGURASI FIREWALL BERBASIS WEB SERVICE MENGGUNAKAN ARSITEKTUR REPRESENTATIONAL STATE TRANSFER (REST)," Compiler, vol. 2, no. 2, Nov. 2013, doi: 10.28989/compiler.v2i2.49.

[38] N. Furqan and I. Suandi, “IMPLEMENTASI INTRUSION DETECTION SYSTEM (IDS) PADA SISTEM KEAMANAN JARINGAN MENGGUNAKAN TELEGRAM SEBAGAI MEDIA NOTIFIKASI,” 2023.

[39] Y. P. Atmojo, “Bot Alert Snort dengan Telegram Bot API pada Intrusion Detection System: Studi Kasus IDS pada Server Web,” 2018.

[40] V. Arinal, F. A. Nuari, W. Sanip, M. Taufik, and D. Sarikah, “IMPLEMENTASI ALAT DETEKSI PLAT NOMOR KENDARAAN UNTUK OTOMATISASI PALANG PINTU PADA LINGKUNGAN PERUMAHAN RT 05/05 GONDRONG DENGAN MACHINE LEARNING,” vol. 2, no. 10, 2024.

[41] Y. A. Hasma and W. Silfianti, “IMPLEMENTASI DEEP LEARNING MENGGUNAKAN FRAMEWORK TENSORFLOW DENGAN METODE FASTER REGIONAL CONVOLUTIONAL NEURAL NETWORK UNTUK PENDETEKSIAN JERAWAT,” tekno, vol. 23, no. 2, pp. 89–102, 2018, doi: 10.35760/tr.2018.v23i2.2459.

[42] A. Roihan, P. A. Sunarya, and A. S. Rafika, “Pemanfaatan Machine Learning dalam Berbagai Bidang: Review paper,” IJCIT, vol. 5, no. 1, May 2020, doi: 10.31294/ijcit.v5i1.7951.

[43] “Karimah Tauhid, Volume 2 Nomor 1 (2023), e-ISSN 2963-590X,” vol. 2, 2023.pinter

[44] I. Abdurrohim and A. Saputri, “Aplikasi Koreksi Kata Berbahasa Indonesia Dengan Metode k-Nearest Neighbor Berbasis Web,” vol. 10, 2019.

[45] A. Syarifah, “PEMANFAATAN NAÏVE BAYES UNTUK MERESPON EMOSI DARI KALIMAT BERBAHASA INDONESIA,” 2015.

[46] A. M. Hidayat and M. Syafrullah, “ALGORITMA NAÏVE BAYES DALAM ANALISIS SENTIMEN UNTUK KLASIFIKASI PADA LAYANAN INTERNET PT.XYZ,” 2017.

[47] “Karimah Tauhid, Volume 2 Nomor 1 (2023), e-ISSN 2963-590X,” vol. 2, 2023.

[48] A. Sumoko, A. B. P. Negara, and H. S. Pratiwi, “Perbandingan Tipe Metode PoS Tagger Terhadap Nilai Akurasi Untuk Bahasa Melayu Pontianak,” justin, vol. 9, no. 3, p. 342, Aug. 2021, doi: 10.26418/justin.v9i3.44116.

[49] I. N. T. Battoa, M. Basri, and A. Selao, “Aplikasi Karaoke Berbasis Raspberry Pi”.

[50] F. Febriansyah, Z. A. Dwiyanti, and D. Firdaus, “Deteksi Serangan Low Rate DDoS pada Jaringan Tradisional menggunakan Algoritma Decision Tree”.

[51] M. K. Harto and A. Basuki, “Deteksi Serangan Ddos Pada Jaringan Berbasis Sdn Dengan Klasifikasi Random Forest”.

[52] A. Ekawijana, A. Bakhrun, and M. T. Kurniawan, “Deteksi Serangan DDOS Pada Jaringan SDN dengan Metode Random Forest,” vol. 8, 2024.

[53] D. Y. D. Pratiwi and R. Adrian, “Deteksi Dan Mitigasi Serangan Distributed Denial of Service Pada Software Defined Network,” JuTISI, vol. 10, no. 1, May 2024, doi: 10.28932/jutisi.v10i1.6995.

[54] N. Sugianti, Y. Galuh, S. Fatia, and K. F. H. Holle, “Deteksi Serangan Distributed Denial of Services (DDOS) Berbasis HTTP Menggunakan Metode Fuzzy Sugeno,” vol. 4, no. 3, 2020.

[55] R. Rizal, N. Widiyasono, and S. Yuliyanti, “Kecerdasan Buatan untuk Klasifikasi Serangan Siber pada *Internet of Things* Network Traffic”.

[56] M. Hawarizmi Hafiz, M. Kurniawan Teguh, and M. Fathinuddin, “Sistem Deteksi Serangan Ddos Pada Software Defined Network Menggunakan Metode Entropy,” smartcomp, vol. 11, no. 4, Oct. 2022, doi: 10.30591/smartcomp.v11i4.4246.

[57] J. C. J. Sihombing, D. P. Kartikasari, and A. Bhawiyuga, “Implementasi Sistem Deteksi dan Mitigasi Serangan Distributed Denial of Service (DDoS) menggunakan SVM Classifier pada Arsitektur Software-Defined Network (SDN)”.

[58] A. W. Muhammad, I. Riadi, and S. Sunardi, “Deteksi Serangan DDoS Menggunakan Neural Network dengan Fungsi Fixed Moving Average

Window," JISKa, vol. 1, no. 3, pp. 115–122, Mar. 2017, doi: 10.14421/jiska.2017.13-03.

[59] D. B. Satmoko, P. Sukarno, and E. M. Jadied, "Peningkatan Akurasi Pendeteksian Serangan DDoS Menggunakan Multiclassifier Ensemble Learning dan Chi-Square".