DAFTAR PUSTAKA

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

[2] A. K. S. M. N. A. and B. S. U. Javaid, "Mitigating loT Device based Mirai Attacks using Blockchain," *Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems - CryBlock'18*, p. pp.71-76, 2018.

[3] Mohammad Sani Rafsanjani, Vera Suryani, and Rizka Reza Pahlevi, "Deteksi Serangan Botnet Pada Jaringan Internet of Things Menggunakan Algoritma Random Forest (RF)," bandung, Jun. 2022.

[4] M. , A. T. , B. M. , B. M. , B. E. , C. J. , . . . & Z. Y. (2017). U. the mirai botnet. I. 26th U. security symposium (USENIX S. 17) (pp. 1093-1110). Antonakakis, "Understanding the Mirai Botnet," *USENIX security symposium*, pp. 1093–1110, 2017.

[5] A. Affinito, S. Zinno, G. Stanco, A. Botta, and G. Ventre, "The evolution of Mirai botnet scans over a six-year period," *Journal of Information Security and Applications*, vol. 79, Dec. 2023, doi: 10.1016/j.jisa.2023.103629.

[6] A. Wijoyo, M. Aziz, R. Diphan, and Priyatna, "CHIPSET : Jurnal Ilmu Komputer, Teknik, dan Multimedia "Analisis Keamanan Komputer Di Era Internet Of Things Studi Kasus Mirai Malware Dan Serangan Botnets," *CHIPSET : Jurnal Ilmu Komputer*, vol. 1, no. no.2, pp. 92–96, 2023,

[7] Niko Suwaryo, Ismasari Nawangsih, and Sri Rejeki, "Deteksi Serangan Pada Intrusion Detection System (Ids) Untuk Klasifikasi Serangan Dengan Algoritma Naïve Bayes, C.45 Dan K-Nn Dalam Meminimalisasi Resiko Terhadap Pengguna," Jakarta Raya, *JSI (Jurnal sistem Informasi) Universitas Suryadarma*, *8*(2), 171-180.

[8] Didin Nizarul Fuadin, "Deteksi Botnet Menggunakan Naïve Bayes Classifier Dengan Smote Dan Metode Bfs," Program Magister Bidang Keahlian Teknik Telematika - Cio, Institut Teknologi Sepuluh Nopember, Surabaya, 2017.

[9] 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.

[10] J. Chandra, H. Hermanto, and A. Rahman, "Deteksi Serangan Port Scanning Menggunakan Algoritma Naive Bayes," *core.ac.uk*, pp. 1–12, 2021.

[11] E. Martantoh and N. Yanih, “Implementasi Metode Naïve Bayes Untuk Klasifikasi Karakteristik Kepribadiaan Siswa Di Sekolah MTS Darussa’adah Menggunakan PHP MySQL Implementation of Naive Bayes Method for Classification of Student’s Personality Characteristics at MTS Darussa’adah School Using PHP Mysql,” 2022.

[12] M. Fluorida Fibrianda and A. Bhawiyuga, “Analisis Perbandingan Akurasi Deteksi Serangan Pada Jaringan Komputer Dengan Metode Naïve Bayes Dan Support Vector Machine (SVM),” 2018.

[13] Y. N. K. dan F. Inda Anggraini, “Penerapan Naive Bayes Pada Detection Malware dengan Diskritisasi Variabel,” *Telematika*, vol. 13, no. 1, pp. 11–21, Feb. 2020, doi: 10.35671/telematika.v13i1.886.

[14] R. A. Khairulah, R. Herdianto, and M. A. Setiawan, “Klasifikasi Serangan Pada Jaringan Internet of Thing (IoT): Tinjauan Literatur Komparatif,” *Jurnal Inovasi Teknik dan Edukasi Teknologi*, vol. 3, no. 1, pp. 47–53, 2023, doi: 10.17977/um068v3i12023p47-53.

[15] W. Najib, T. Ancaman dan Solusi Keamanan, S. Sulistyo, and K. Kunci, “Tinjauan Ancaman dan Solusi Keamanan pada Teknologi Internet of Things (Review on Security Threat and Solution of Internet of Things Technology),” 2020.

[16] G. D. A. M. A. A. M. I. B. W. M. N. F. M. K. M. E. Arief Selay, “Internet Of Things,” *Karimah Tauhid*, vol. 1, no. no 6, 2022.

[17] D. Suryono and D. W. Chandra, “Analisis Keamanan Jaringan Hardware Trojan Pada IoT,” *Jurnal Teknik Informatika dan Sistem Informasi*, vol. 9, no. 4, 2022.

[18] M. Zekeriya Gündüz and R. Da, “Analysis of cyber-attacks in IoT-based critical infrastructures,” 2019.

[19] T. , & K. S. Rachmadi, *Mengenal apa itu internet of things*, Tiga Ebook., vol. 1. 2020.

[20] Z. Masyhur, D. Hermawan, K. Kunci, and J. S. Informasi, “Internet of Things (IoT): Security, Threats and Countermeasures,” *Journal Shift Vol*, vol. 2, no. 2, pp. 15–19, Jun. 2022.

[21] Z. Munawar and N. I. Putri, “Keamanan Iot Dengan Deep Learning Dan Teknologi Big Data,” 2020.

[22] Anggika Rahmadiani Kurnia, Lia Wulandari, Treviliana Eka Putri, and Ristyanadya Laksmi Gupita, “Kelemahan Keamanan Siber :Mirai Malware dan Serangan Botnets,” *cfds.fisipol.ugm*, pp. 1–10.

[23] Warstek Media, “Mengungkap Cerita di Balik Serangan Pertama Virus Malware IoT: Botnet Mirai,” *Warung Sains Teknologi*, Yogyakarta, Oct. 23, 2023.

[24] B. Lampung, “Jurnal Simada Jurnal Simada Sistem Informasi & Manajemen Basis Data,” 2019.

[25] H. Alamsyah, Riska, and A. Al Akbar, “Analisa Keamanan Jaringan Menggunakan Network Intrusion Detection and Prevention System,” *JOINTECS (Journal of Information Technology and Computer Science)*, vol. 3, no. 1, pp. 17–24, 2018.

[26] R. Kurniawan and F. Prakoso, “Implementasi Metode IPS (Intrusion Prevention System) dan IDS (Intrusion Detection System) untuk Meningkatkan Keamanan Jaringan,” *SENTINEL*, vol. 2, no. 02, Jan. 2020.

[27] Agusa Navirgo and Ahmad Habibbullaah, “Implementasi Data Mining Dengan Algoritma Berbasis Tree Untuk Klasifikasi Serangan Pada Intrusion Detection System (Ids),” *Jurnal Sistem Informasi & Manajemen Basis Data (SIMADA)*, vol. 2, pp. 91–181, Oct. 2019.

[28] L. Saroha, R. Octavianto, and E. S. S. Malays, “Pencegahan Dan Konsep IDS (Intrusion Detection System) Dalam Mendeteksi Serangan Siber Pada Sistem Keamanana Di Universitas Persada Indonesia Y.A.i,” *Jurnal Ilmiah Teknik Informatika (TEKINFO)*, vol. 25, no. 1, pp. 168–176, 2024, doi: 10.37817/tekinfo.v25i1.

[29] M. Riziq sirfatullah Alfarizi, M. Zidan Al-farish, M. Taufiqurrahman, G. Ardiansah, and M. Elgar, “Penggunaan Python Sebagai Bahasa Pemrograman Untuk Machine Learning Dan Deep Learning,” 2023.

[30] HADI PRASETYO, “10 Algoritma Machine Learning Teratas Untuk Pemula.” Accessed: Aug. 01, 2024.

[31] “Penerapan Naive Bayes Pada Detection Malware dengan Diskritisasi Variabel,” *Telematika*, vol. 13, no. 1, pp. 11–21, Feb. 2020, doi: 10.35671/telematika.v13i1.886.

[32] D. Putra Tarigan, P. Sari Ramadhan, S. Yakub, S. Informasi, and S. Triguna Dharma, “Penerapan Teorema Bayes Untuk Mendeteksi Kerusakan Mesin Sepeda Motor,” *jurnal sistem informasi tgd*, vol. 1, pp. 73–79, Mar. 2022.

[33] Angelina M. T. I. Sambi Ua *et al.*, “Penggunaan Bahasa Pemrograman Python Dalam Analisis Faktor Penyebab Kanker Paru-Paru,” *Jurnal Publikasi Teknik Informatika*, vol. 2, no. 2, pp. 88–99, Jul. 2023, doi: 10.55606/jupti.v2i2.1742.

[34] M. Fluorida Fibrianda and A. Bhawiyuga, “Analisis Perbandingan Akurasi Deteksi Serangan Pada Jaringan Komputer Dengan Metode Naïve Bayes Dan Support Vector Machine (SVM),” *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, vol. 2, no. 9, pp. 3112–3123, Sep. 2018.

[35] A. Sandriana, Rianto, and F. Maulana, “Klasifikasi serangan Malware terhadap Lalu Lintas Jaringan Internet of Things menggunakan Algoritma K-Nearest

Neighbour (K-NN)," *E- JOINT (Electronica and Electrical Journal of Innovation Technology)*, vol. 03, no. 1, pp. 12–22, Jun. 2022.

[36] M. Habeeb Abdulhasan, "Detection of Mirai attack on IoT environment using Machine Learning Techniques," *ishraqat tanmawia*, 2024.

[37] A. Sharma, V. Mansotra, and K. Singh, "Detection of Mirai Botnet Attacks on IoT devices Using Deep Learning," *JOURNAL OF SCIENTIFIC RESEARCH AND TECHNOLOGY(JSRT)*, vol. 1, no. 6, pp. 174–187, Sep. 2023.

[38] 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. 2021, doi: 10.18421/TEM103-27.

[39] I. Masud, K. Kusrini, and A. B. Prasetio, "Distributed Denial Of Service (DDOS) Attack Detection On Zigbee Protocol Using Naive Bayes Algoritm," *International Journal of Artificial Intelligence Research*, vol. 5, no. 2, Jun. 2021, doi: 10.29099/ijair.v5i2.214.

[40] Inda Anggraini, Yesi Novaria Kunang, and Firdaus, "Penerapan Naive Bayes Pada Detection Malware dengan Diskritisasi Variabel," *Telematika*, vol. 13, no. 1, pp. 11–21, Feb. 2020, doi: 10.35671/telematika.v13i1.886.

[41] N. Suwaryo, I. Nawangsih, S. Rejeki, and J. Raya, "Deteksi Serangan Pada Intrusion Detection System (Ids) Untuk Klasifikasi Serangan Dengan Algoritma Naïve Bayes, C.45 Dan K-Nn Dalam Meminimalisasi Resiko Terhadap Pengguna," *JSI (Jurnal sistem Informasi) Universitas Suryadarma*, pp. 171–180, 2021.

[42] A. Rahmatulloh, G. M. Ramadhan, I. Darmawan, N. Widiyasono, and D. Pramesti, "Identification of Mirai Botnet in IoT Environment through Denial-of- Service Attacks for Early Warning System," *JOIV : Int. J. Inform. Visualization*, vol. 6 no 3, pp. 623–628, Sep. 2022.