DAFTAR PUSTAKA

[1] H. S. Setiawan, "Pelatihan Guru dalam Penggunaan Internet of Things pada Madrasah Darussa'adah," *E-Dimas: Jurnal Pengabdian kepada Masyarakat*, vol. 9, no. 2, p. 167, 2018, doi: 10.26877/e-dimas.v9i2.1554.

[2] M. H. A. Sitanggang, "Memahami mekanisme crowdfunding dan motivasi berpartisipasi dalam platform Kitabisa.com," *E Journal UNDIP*, vol. 6, no. 3, pp. 1–11, 2018, [Online]. Available: https://ejournal3.undip.ac.id/index.php/interaksi-online/article/view/20859/19553

[3] S. Anwar and Hermanto, "Pemanfaatan Internet of Thing (IoT) Dalam Pengendalian Lampu Dan Kipas Berbasis Android," *Jurnal RESTIKOM : Riset Teknik Informatika dan Komputer*, vol. 2, no. 1, pp. 17–31, 2022, doi: 10.52005/restikom.v2i1.63.

[4] C. Baru, Institute of Electrical and Electronics Engineers, and IEEE Computer Society, *Detecting DoS Attack in Smart Home IoT Devices Using a Graph-Based Approach*.

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

[6] E. A. Winanto, K. Kurniabudi, S. Sharipuddin, I. S. Wijaya, and D. Sandra, "Deteksi Serangan pada Jaringan Kompleks IoT menggunakan Recurrent Neural Network," *JURIKOM (Jurnal Riset Komputer)*, vol. 9, no. 6, p. 1996, Dec. 2022, doi: 10.30865/jurikom.v9i6.5298.

[7] J. Fahana, R. Umar, and F. Ridho, "Pemanfaatan Telegram Sebagai Notifikasi Serangan untuk Keperluan Forensik Jaringan," *Jurnal Sistem Informasi*, vol. 5341, no. 6, p. 2, 2017.

[8] J. Pendidikan and D. Konseling, "Optimasi Metode Naïve Bayes dengan Particle Swarm Optimization untuk Sistem Deteksi Serangan D-Dos Universitas Pahlawan Tuanku Tambusai," vol. 4, 2022.

[9] R. Vishwakarma and A. K. Jain, “A survey of DDoS attacking techniques and defence mechanisms in the IoT network,” *Telecommun Syst*, vol. 73, no. 1, pp. 3–25, 2020, doi: 10.1007/s11235-019-00599-z.

[10] B. Arifwidodo, Y. Syuhada, and S. Ikhwan, “Analisis Kinerja Mikrotik Terhadap Serangan Brute Force Dan DDoS Analysis of Mikrotik Performance Against Brute Force and DDoS Attacks.”

[11] W. Syahputra, T. M. Diansyah, and R. Liza, “Pemanfaatan Mikrotik Router Board Sebagai Pengaman Serangan DDOS Menggunakan Metode IDS,” *Snastikom*, vol. 1, no. 1, pp. 492–499, 2020.

[12] I. Putu, A. E. Pratama, N. Kade, and M. Handayani, “IMPLEMENTASI IDS MENGGUNAKAN SNORT PADA SISTEM OPERASI UBUNTU,” *Jurnal Mantik Penusa*, vol. 3, no. 1, pp. 176–181, 2019, [Online]. Available: www.snort.org

[13] A. Elanda and D. Tjahjadi, “Analisis Manajemen Resiko Sistem Keamanan Ids (Intrusion Detection System) Dengan Framework Nist (National Institute of Standards and Technology) Sp 800-30 (Studi Kasus Disinfolahtaau Mabes Tni Au),” *Infoman’s*, vol. 12, no. 1, pp. 1–13, 2018, doi: 10.33481/infomans.v12i1.45.

[14] A. Q. Adhani, Y. Purwanto, and I. N. A. Ramatryana, “Mendeteksi Anomali Menggunakan Algoritma Holt-Winters berdasarkan Tingkat Keyakinan dari Teorema Bayes Anomaly Detection using Holt-Winters ’ s Algorithm based on the Level Probability from Bayes ’ s Theorem,” *eProceedings …*, vol. 4, no. 3, pp. 4036–4043, 2017, [Online]. Available: https://openlibrarypublications.telkomuniversity.ac.id/index.php/engineering/article/view/5193

[15] S. Ilahiyah and A. Nilogiri, “Implementasi Deep Learning Pada Identifikasi Jenis Tumbuhan Berdasarkan Citra Daun Menggunakan Convolutional Neural Network,” *JUSTINDO (Jurnal Sistem dan Teknologi Informasi Indonesia)*, vol. 3, no. 2, pp. 49–56, 2018.

[16] Z. C. Fanzhi Meng, Yunsheng Fu, Fang Lou, “An effective network attack detection method based on kernel PCA and LSTMRNN,” 2017.

[17] Institute of Electrical and Electronics Engineers, *SSH and FTP brute-force Attacks Detection in Computer Networks: L STM and Machine L earning Approaches Md*.

[18] S. K. Wanjau, G. M. Wambugu, and G. N. Kamau, “SSH-Brute Force Attack Detection Model based on Deep Learning,” *International Journal of Computer Applications Technology and Research*, vol. 10, no. 01, pp. 42–50, 2021, doi: 10.7753/ijcatr1001.1008.

[19] X. Song *et al.*, “Time-series well performance prediction based on Long Short-Term Memory (LSTM) neural network model,” *J Pet Sci Eng*, vol. 186, Mar. 2020, doi: 10.1016/j.petrol.2019.106682.

[20] A. Yadav, C. K. Jha, and A. Sharan, “Optimizing LSTM for time series prediction in Indian stock market,” in *Procedia Computer Science*, Elsevier B.V., 2020, pp. 2091–2100. doi: 10.1016/j.procs.2020.03.257.

[21] L. Wiranda and M. Sadikin, “PENERAPAN LONG SHORT TERM MEMORY PADA DATA TIME SERIES UNTUK MEMPREDIKSI PENJUALAN PRODUK PT. METISKA FARMA.”

[22] F. Nahdi and H. Dhika, “Analisis Dampak Internet of Things (IoT) Pada Perkembangan Teknologi di Masa Yang Akan Datang,” *INTEGER: Journal of Information Technology*, vol. 6, no. 1, pp. 33–40, 2021, doi: 10.31284/j.integer.2021.v6i1.1423.

[23] Y. Efendi, “Internet Of Things (Iot) Sistem Pengendalian Lampu Menggunakan Raspberry Pi Berbasis Mobile,” *Jurnal Ilmiah Ilmu Komputer*, vol. 4, no. 2, pp. 21–27, 2018, doi: 10.35329/jiik.v4i2.41.

[24] V. Rahmadhani and Widya Arum, “Literature Review Internet of Think (Iot): Sensor, Konektifitas Dan Qr Code,” *Jurnal Manajemen Pendidikan Dan Ilmu Sosial*, vol. 3, no. 2, pp. 573–582, 2022, doi: 10.38035/jmpis.v3i2.1120.

[25] E. D. Meutia, “Interet of Things – Keamanan dan Privasi,” *Semin. Nas. dan Expo Tek. Elektro*, no. June, pp. 85–89, 2015.

[26] W. Najib, S. Sulistyo, and Widyawan, “Tinjauan Ancaman dan Solusi Keamanan pada Teknologi Internet of Things,” *Jurnal Nasional Teknik Elektro dan Teknologi Informasi*, vol. 9, no. 4, pp. 375–384, 2020, doi: 10.22146/jnteti.v9i4.539.

[27] S. Aji, A. Fadlil, and I. Riadi, “Pengembangan Sistem Pengaman Jaringan Komputer Berdasarkan Analisis Forensik Jaringan,” *Jurnal Ilmiah Teknik Elektro Komputer dan Informatika*, vol. 3, no. 1, p. 11, 2017, doi: 10.26555/jiteki.v3i1.5665.

[28] M. K. Riskilah and F. A. Yulianto, “Studi Analisis Algoritma NaÏve Bayes Untuk Sistem Deteksi Intrusi Pada Internet Of Things,” *e-Proceeding of Engineering*, vol. 9, no. 3, pp. 2177–2189, 2022, [Online]. Available: https://openlibrarypublications.telkomuniversity.ac.id/index.php/engineering/article/view/18081

[29] R. Hermawan, “Analisis Konsep Dan Cara Kerja Serangan Komputer Distributed Denial of Service (Ddos),” *Analisis Konsep Dan Cara Kerja Serangan Komputer Distributed Denial of Service (Ddos)*, vol. 5, no. 1, pp. 1–14, 2013.

[30] F. Ridho, A. Yudhana, and I. Riadi, “Analisis Forensik Router Untuk Mendeteksi Serangan Distributed Danial of Service (DDoS) Secara Real Time,” vol. 2, no. 1, pp. 111–116, 2016, [Online]. Available: http://ars.ilkom.unsri.ac.id

[31] D. Santoso, A. Noertjahyana, and J. Andjarwirawan, “Implementasi dan Analisa Snort dan Suricata Sebagai IDS dan IPS Untuk Mencegah Serangan DOS dan DDOS,” *Jurnal Infra*, vol. 10, no. 1, pp. 1–6, 2022, [Online]. Available: https://publication.petra.ac.id/index.php/teknik-informatika/article/view/12033

[32] S. Geges and W. Wibisono, “Pengembangan Pencegahan Serangan Distributed Denial of Service (Ddos) Pada Sumber Daya Jaringan Dengan Integrasi Network Behavior Analysis Dan Client Puzzle,” *JUTI: Jurnal Ilmiah Teknologi Informasi*, vol. 13, no. 1, p. 53, 2015, doi: 10.12962/j24068535.v13i1.a388.

[33] Emir Risyad, Mahendra Data, and Eko Sakti Pramukantoro, “Perbandingan Performa Intrusion Detection System (IDS) Snort Dan Suricata Dalam Mendeteksi Serangan TCP SYN Flood | Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer,” *Jptik*, vol. 2, no. 9, pp. 2615–2624, 2018, [Online]. Available: https://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/2373

[34] R. Aulianita, N. Musyaffa, and R. Martiwi, “PENGGUNAAN METODE IDS DALAM IMPLEMENTASI FIREWALL PADA JARINGAN UNTUK DETEKSI SERANGAN Distributed Denial Of Service (DDoS),” *Jusikom: Jurnal Sistem Komputer Musirawas*, vol. 6, no. 2, pp. 94–104, 2021, [Online]. Available: http://jurnal.univbinainsan.ac.id/index.php/jusikom/article/download/1411/760

[35] J. Chris, 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),” *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, vol. 3, no. 10, pp. 9608–9613, 2019, [Online]. Available: http://j-ptiik.ub.ac.id

[36] K. Terapan, I. Sreeram, V. Praveen, and K. Vuppala, “Machine Translated by Google Artikel asli Deteksi serangan banjir HTTP di lapisan aplikasi menggunakan metrik pembelajaran mesin dan algoritma kelelawar yang terinspirasi oleh bio Machine Translated by Google,” vol. 15, pp. 59–66, 2019.

[37] K. Singh, P. Singh, and K. Kumar, “Application layer HTTP-GET flood DDoS attacks: Research landscape and challenges,” *Comput Secur*, vol. 65, pp. 344–372, 2017, doi: 10.1016/j.cose.2016.10.005.

[38] I. Meiditra, “Analisis Dan Perancangan Private Cloud Storage Menggunakan Metode Pengamanan Ids (Intrusion Detection System) Dan Ips(Intrusion Prevention System) (Studi Kasus: Diskominfo Kota Padang Panjang),” *Riau Journal of Computer Science*, vol. 9, no. 2, pp. 124–133, 2023.

[39] I. Ramadhan, “Monitoring Keamanan Jaringan Dengan Snort Ids Menggunakan Metode Forensic Jaringan (Studi Kasus: Cv.Triem Gunung Mas Sejahtera),” *Jurnal Ilmiah MIKA AMIK Al Muslim*, vol. 3, no. 1, pp. 13–18, 2019.

[40] Jupriyadi, “IMPLEMENTASI SELEKSI FITUR MENGGUNAKAN ALGORITMA FVBRM UNTUK KLASIFIKASI SERANGAN PADA INTRUSION DETECTION SYSTEM (IDS),” pp. 1–6, 2018.

[41] S. Z. Harahap, “IMPLEMENTASI SNORT INTRUSION DETECTION SYSTEM (IDS) PADA SISTEM JARINGAN KOMPUTER,” vol. 6, no. 3, pp. 24–27, 2018.

[42] S. P. Allwine, M. Kom, and ..., “Keamanan Jaringan Terpusat Mengunakan Intrusion Detection System (Ids) Di Stmik Methodist Binjai,” *Jurnal Armada …*, pp. 1–11, 2020, [Online]. Available: http://download.garuda.kemdikbud.go.id/article.php?article=2813181&val=25059&title=KEAMANAN JARINGAN TERPUSAT MENGUNAKAN INTRUSION DETECTION SYSTEM IDS DI STMIK METHODIST BINJAI KEAMANAN JARINGAN TERPUSAT MENGUNAKAN INTRUSION DETECTION SYSTEM IDS DI STMI

[43] P. A. Nugroho, I. Fenriana, and R. Arijanto, “Implementasi Deep Learning Menggunakan Convolutional Neural Network (CNN) Pada Ekspresi Manusia,” *Algor*, vol. 2, no. 1, pp. 12–21, 2020.

[44] S. Wahyuni and M. Sulaeman, “Penerapan Algoritma Deep Learning Untuk Sistem Absensi Kehadiran Deteksi Wajah Di PT Karya Komponen Presisi,” *Jurnal Informatika SIMANTIK*, vol. 7, no. 1, pp. 5–6, 2022, [Online]. Available: https://simantik.panca-sakti.ac.id/index.php/simantik/article/view/127

[45] Muhammad Haris Diponegoro, Sri Suning Kusumawardani, and Indriana Hidayah, “Tinjauan Pustaka Sistematis: Implementasi Metode Deep Learning pada Prediksi Kinerja Murid,” *Jurnal Nasional Teknik Elektro dan Teknologi Informasi*, vol. 10, no. 2, pp. 131–138, 2021, doi: 10.22146/jnteti.v10i2.1417.

[46] S. Al-Emadi, A. Al-Mohannadi, and F. Al-Senaid, “Using Deep Learning Techniques for Network Intrusion Detection,” *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies, ICIoT 2020*, pp. 171–176, 2020, doi: 10.1109/ICIoT48696.2020.9089524.

[47] I. M. W. Bhaskara, I. P. G. H. Suputra, I. M. Widiartha, I. G. A. G. A. Kadyanan, I. G. N. A. C. Putra, and I. B. G. Dwidasmara, “Klasifikasi Serangan Distributed Denial of Service (DDoS) Menggunakan Random Forest Dengan CFS,” *JELIKU (Jurnal Elektronik Ilmu Komputer Udayana)*, vol. 11, no. 2, p. 215, 2022, doi: 10.24843/jlk.2022.v11.i02.p01.

[48] S. H. Park, H. J. Park, and Y. J. Choi, “RNN-based Prediction for Network Intrusion Detection,” *2020 International Conference on Artificial Intelligence in Information and Communication, ICAIIC 2020*, pp. 572–574, 2020, doi: 10.1109/ICAIIC48513.2020.9065249.

[49] M. Zidane, “Klasifikasi Serangan Distributed Denial-Of-Service (DDOS) Menggunakan Metode Data Mining Naïve Bayes memperoleh gelar Sarjana Komputer Disusun oleh :,” *Universitas Brawijaya*, vol. 6, no. 1, p. 63, 2021.

[50] D. B. Satmoko, P. Sukarno, and E. M. Jadied, “Peningkatan Akurasi Pendeteksian Serangan DDoS Menggunakan Multiclassifier Ensemble Learning dan Chi-Square,” *e-Proceeding of Engineering*, vol. 5, no. 3, pp. 7877–7985, 2018.

[51] K. Kurniabudi, A. Harris, and A. Rahim, “Seleksi Fitur Dengan Information Gain Untuk Meningkatkan Deteksi Serangan DDoS menggunakan Random Forest,” *Techno.Com*, vol. 19, no. 1, pp. 56–66, 2020, doi: 10.33633/tc.v19i1.2860.

[52] Constantin Menteng, Arief Setyanto, and Hanif Al Fatta, “Model Deteksi Serangan Ssh-Brute Force Berdasarkan Deep Belief Network,” *Jurnal Teknologi Informasi: Jurnal Keilmuan dan Aplikasi Bidang Teknik Informatika*, vol. 7, no. 2, pp. 101–110, 2023, doi: 10.47111/jti.v7i2.8151.

[53] M. Q. Syahputra, D. R. Akbi, and D. Risqiwati, “Deteksi Dan Mitigasi Serangan DDoS Pada Software Defined Network Menggunakan Algoritma Decision

Tree," *Jurnal Repositor*, vol. 2, no. 11, p. 1491, 2020, doi: 10.22219/repositor.v2i11.795.

[54] N. Afifah and D. Stiawan, "The Implementation of Deep Neural Networks Algorithm for Malware Classification," *Computer Engineering and Applications Journal*, vol. 8, no. 3, pp. 189–202, 2019, doi: 10.18495/comengapp.v8i3.294.

[55] G. R. Kanagachidambaresan, A. Ruwali, D. Banerjee, and K. B. Prakash, "Klasifikasi Malware Menggunakan MetodeRecurrent Neural Network," *EAI/Springer Innovations in Communication and Computing*, vol. 23, no. 3, pp. 53–61, 2021.

[56] P. Sugiartawan, A. A. Jiwa Permana, and P. I. Prakoso, "Forecasting Kunjungan Wisatawan Dengan Long Short Term Memory (LSTM)," *Jurnal Sistem Informasi dan Komputer Terapan Indonesia (JSIKTI)*, vol. 1, no. 1, pp. 43–52, 2018, doi: 10.33173/jsikti.5.

[57] M. Q. Andiyantama, I. Zahira, and A. Irawan, "Prediksi Energi Listrik Kincir Angin Berdasarkan Data Kecepatan Angin Menggunakan LSTM," *JITCE (Journal of Information Technology and Computer Engineering)*, vol. 5, no. 01, pp. 1–7, 2021, doi: 10.25077/jitce.5.01.1-7.2021.

[58] V. Nourani and N. Behfar, "Multi-station runoff-sediment modeling using seasonal LSTM models," *J Hydrol (Amst)*, vol. 601, no. April, p. 126672, 2021, doi: 10.1016/j.jhydrol.2021.126672.

[59] S. Ameur, A. Ben Khalifa, and M. S. Bouhlel, "A novel hybrid bidirectional unidirectional LSTM network for dynamic hand gesture recognition with Leap Motion," *Entertain Comput*, vol. 35, no. August 2019, p. 100373, 2020, doi: 10.1016/j.entcom.2020.100373.

[60] E. C. P. Neto, S. Dadkhah, R. Ferreira, A. Zohourian, R. Lu, and A. A. Ghorbani, "CICIoT2023: A Real-Time Dataset and Benchmark for Large-Scale Attacks in IoT Environment," *Sensors*, vol. 23, no. 13, 2023, doi: 10.3390/s23135941.

[61] A. Z. Amrullah, A. Sofyan Anas, and M. A. J. Hidayat, "Analisis Sentimen Movie Review Menggunakan Naive Bayes Classifier Dengan Seleksi Fitur Chi Square," *Jurnal*, vol. 2, no. 1, pp. 40–44, 2020, doi: 10.30812/bite.v2i1.804.

[62] E. N. Fitri, S. Winarno, F. Budiman, A. Rohmani, J. Zeniarja, and E. Sugiarto, "Decision Tree Simplification Through Feature Selection Approach in Selecting Fish Feed Sellers," *Jurnal Teknik Informatika (Jutif)*, vol. 4, no. 2, pp. 301–309, 2023, doi: 10.52436/1.jutif.2023.4.2.747.

[63] T. Desyani, A. Saifudin, and Y. Yulianti, "Feature Selection Based on Naive Bayes for Caesarean Section Prediction," *IOP Conf Ser Mater Sci Eng*, vol. 879, no. 1, 2020, doi: 10.1088/1757-899X/879/1/012091.

[64] D. Normawati and S. A. Prayogi, "Implementasi Naïve Bayes Classifier Dan Confusion Matrix Pada Analisis Sentimen Berbasis Teks Pada Twitter," *Jurnal Sains Komputer & Informatika (J-SAKTI*, vol. 5, no. 2, pp. 697–711, 2021.

[65] R. R. Adhitya, Wina Witanti, and Rezki Yuniarti, "Perbandingan Metode Cart Dan Naïve Bayes Untuk Klasifikasi Customer Churn," *INFOTECH journal*, vol. 9, no. 2, pp. 307–318, 2023, doi: 10.31949/infotech.v9i2.5641.