DAFTAR PUSTAKA

[1] Zen Munawar and Novianti Indah Putri, "Keamanan IoT Dengan *Deep Learning* dan Teknologi *Big Data*," *Tematik*, vol. 7, no. 2, pp. 161–185, 2020, doi: 10.38204/tematik.v7i2.479.

[2] F. Ilhami, P. Sokibi, and A. Amroni, "Perancangan Dan Implementasi *Prototype* Kontrol Peralatan Elektronik Berbasis *Internet of Things* Menggunakan Nodemcu," *Jurnal Digit*, vol. 9, no. 2, p. 143, 2019, doi: 10.51920/jd.v9i2.115.

[3] R. Mehta, J. Sahni, and K. Khanna, *"Internet of Things: Vision, Applications and Challenges*," *Procedia Comput Sci*, vol. 132, no. 7, pp. 1263–1269, 2018, doi: 10.1016/j.procs.2018.05.042.

[4] E. Eko Prasetiyo, "APLIKASI *INTERNET OF THINGS* (IoT) UNTUK PEMANTAUAN DAN PENGENDALIAN BEBAN LISTRIK DI RUANGAN," *Jurnal Teknika STTKD*, vol. 4, no. 2, pp. 28–35, 2017.

[5] 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, 2022, doi: 10.30865/jurikom.v9i6.5298.

[6] L. Feronika Nainggolan, N. F. Saragih, F. G. N. Larosa, and H. Artikel, "Monitoring Keamanan Jaringan Pada Server Ubuntu Dari Serangan DDoS Menggunakan Snort IDS," *Jurnal Ilmiah Teknik Informatika*, vol. 2, no. 2, pp. 1–10, 2022, [Online]. Available: http://ojs.fikom-methodist.net/index.php/METHOTIKA

[7] M. Zidane, "Klasifikasi Serangan *Distributed Denial-Of-Service* (DDOS) Menggunakan Metode *Data Mining* Naïve Bayes Komputer :," *Universitas Brawijaya*, vol. 6, no. 1, p. 63, 2021.

[8] G. Ramadhan, Y. Kurniawan, and Chang-Soo Kim, "*Design of TCP SYN Flood DDoS attack detection using artificial immune systems,*" pp. 72–76, 2017, doi: 10.1109/icsengt.2016.7849626.

[9] H. Alamsyah, R. -, and A. Al Akbar, "Analisa Keamanan Jaringan Menggunakan *Network Intrusion Detection and Prevention System*," *JOINTECS (Journal of Information Technology and Computer Science)*, vol.5, no. 1, p. 17, 2020, doi: 10.31328/jointecs.v5i1.1240.

[10] Y. Li, R. Ma, and R. Jiao, "*A hybrid malicious code detection method based on deep learning*," *International Journal of Security and its Applications*, vol. 9, no. 5, pp. 205–216, 2015, doi: 10.14257/ijsia.2015.9.5.21.

[11] A. A. Kurniawan, "*Intrusion Detection System* Menggunakan *Deep Learning* Untuk Deteksi Serangan DoS," *Intrusion Detection System Menggunakan Deep Learning Untuk Deteksi Serangan DoS*, pp. 39–57, 2020.

[12] B. A. Pratomo, "Pendekatan *unsupervised* untuk Mendeteksi Serangan Tingkat Rendah pada Jaringan Komputer," *Briliant: Jurnal Riset dan Konseptual*, vol. 7, no. 2, p. 546, 2022, doi: 10.28926/briliant.v7i2.1004.

[13] A. R. Shaaban, E. Abd-Elwanis, and M. Hussein, "*DDoS attack detection and classification via Convolutional Neural Network (CNN)*," *Proceedings - 2019 IEEE 9th International Conference on Intelligent Computing and Information Systems, ICICIS 2019*, no. December 2019, pp. 233–238, 2019, doi: 10.1109/ICICIS46948.2019.9014826.

[14] D. Gunawan and H. Setiawan, "*Convolutional Neural Network* dalam Citra Medis," *KONSTELASI: Konvergensi Teknologi dan Sistem Informasi*, vol. 2, no. 2, pp. 376–390, 2022, doi: 10.24002/konstelasi.v2i2.5367.

[15] S. Issues, M. Kumar, A. Kumar, S. Verma, P. Bhattacharya, and D. Ghimire, "*Healthcare Internet of Things* (H-IoT): Current Trends , Future," 2023.

[16] E. Yoyon, "*INTERNET OF THINGS* (IOT) SISTEM PENGENDALIAN LAMPU," vol. 4, no. 1, pp. 19–26, 2018.

[17] G. H. Sandi, Y. Fatma, and F. I. Kompuer, "PEMANFAATAN TEKNOLOGI *INTERNET OF THINGS* (IOT) PADA BIDANG PERTANIAN," vol. 7, no. 1, pp. 1–5, 2023.

[18] K. M. Hosny, A. Magdi, A. Salah, O. El-Komy, and N. A. Lashin, "*Internet of things applications using Raspberry-Pi: a survey*," *International Journal of Electrical and Computer Engineering*, vol. 13, no. 1, pp. 902–910, 2023, doi: 10.11591/ijece.v13i1.pp902-910.

[19] M. Syani, "IMPLEMENTASI *INTRUSION DETECTION SYSTEM* (IDS) MENGGUNAKAN *SURICATA* PADA *LINUX DEBIAN* 9 BERBASIS*CLOUD VIRTUAL PRIVATE SERVERS* (VPS)," no. February, 2021, doi: 10.46846/jurnalinkofar.v1i1.155.

[20] N. Fidyatun and S. Ramadona, "Sistem Pencegahan Serangan *Distributed Denial Of Service* Pada Jaringan SDN," vol. 5, no. 3, pp. 1–8, 2023, doi: 10.60083/jsisfotek.v5i3.269.

[21] I. Y. Arulampalam Kunaraj, P.Chelvanathan, Ahmad AA Bakar, "DETEKSI SERANGAN *DISTRIBUTED DENIAL OF SERVICE* (DDOS)

MENGGUNAKAN *CATBOOST CLASSIFIER*)," *Journal of Engineering Research*, 2023.

[22] 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

[23] 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

[24] 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

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

[26] R. Hermawan, "ANALISIS KONSEP DAN CARA KERJA SERANGAN KOMPUTER *DISTRIBUTED DENIAL OF SERVICE* (DDOS)," vol. 5, no.1, pp. 1–14, 1979.

[27] B. N. Ramkumar and T. Subbulakshmi, "*Tcp Syn Flood Attack Detection and Prevention System using Adaptive Thresholding Method*," *ITM Web of Conferences*, vol. 37, p. 01016, 2021, doi: 10.1051/itmconf/20213701016.

[28] F. Riza, "Jurnal Sistim Informasi dan Teknologi Sistem Deteksi Intrusi pada Server secara Realtime Menggunakan Seleksi Fitur dan *Firebase Cloud Messaging*," vol. 5, pp. 7–9, 2023, doi: 10.37034/jsisfotek.v5i1.161.

[29] M. Halmi Dar, "IMPLEMENTASI *SNORT INTRUSION DETECTION SYSTEM* (IDS) PADA SISTEM JARINGAN KOMPUTER," vol. 6, no. 3, 2018.

[30] Jupriyadi, "Implementasi Seleksi Fitur Menggunakan Algoritma FVBRM Untuk Klasifikasi Serangan Pada *Intrusion Detection System* (Ids),"

Seminar Nasional Teknologi Informasi (SEMNASTEK), vol. 17, pp. 1–6, 2018, [Online]. Available: https://jurnal.umj.ac.id/index.php/semnastek/article/view/3452/2601

[31] L. Wahyuni, B. Triandi, M. Zarlis, and Z. Nasution, "Pendekatan Filsafat Ilmu Terhadap Perkembangan *Deep Learning* dalam Perspektif Aksiologi," vol. 15, no. 1, pp. 62–72, 2023.

[32] L. Faizal, "Identifikasi Sampah Plastik Menggunakan Algoritma *Deep Learning*," vol. 6, pp. 162–171, 2023.

[33] U. Bina, S. Informaika, R. Forest, and D. Learning, "Komparasi Akurasi Metode *Random Forest* Dan *Deep Learning* pada Reservasi Hotel," vol. 5, no. 2, pp. 124–128, 2023.

[34] M. H. Diponegoro, S. S. Kusumawardani, and I. Hidayah, "Implementasi Metode *Deep Learning* pada Prediksi Kinerja Murid *(Implementation of Deep Learning Methods in Predicting Student Performance : A Systematic Literature Review*)," vol. 10, no. 2, pp. 131–138, 2021.

[35] 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.

[36] 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.

[37] 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.

[38] 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.

[39] 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.

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

[41] S. Adiningsi and R. A. Saputra, “IDENTIFIKASI JENIS DAUN TANAMAN OBAT MENGGUNAKAN METODE *CONVOLUTIONAL NEURAL NETWORK* (CNN) DENGAN MODEL VGG16,” pp. 451–460, 2020.

[42] A. M. Tama, R. Candra, N. Santi, and U. Semarang, “KLASIFIKASI JENISTANAMAN HIAS MENGGUNAKAN METODE *CONVOLUTIONAL NEURAL NETWORK* (CNN),” *journal of InfomationTechnology and Computer Science (INTECOMS)*, vol. 6 No 2, pp. 764– 770,2023.

[43] F. Hafifah, S. Rahman, and S. Asih, “Klasifikasi Jenis Kendaraan Pada Jalan Raya Menggunakan Metode *Convolutional Neural Networks* (CNN),” *TIN: Terapan Informatika Nusantara*, vol. 2, no. 5, pp. 292–301, 2021, [Online].
Available: https://ejurnal.seminar-id.com/index.php/tin

[44] I. Nihayatul Husna, M. Ulum, A. Kurniawan Saputro, D. Tri Laksono, and
D. Neipa Purnamasari, “Rancang Bangun Sistem Deteksi Dan Perhitungan Jumlah Orang Menggunakan Metode *Convolutional Neural Network* (CNN),” *Seminar Nasional Fortei Regional*, vol. 7, p. 2, 2022.

[45] I. Wulandari, H. Yasin, and T. Widiharih, “Klasifikasi Citra Digital Bumbu Dan Rempah Dengan Algoritma *Convolutional Neural Network* (Cnn),” *Jurnal Gaussian*, vol. 9, no. 3, pp. 273–282, 2020, doi: 10.14710/j.gauss.v9i3.27416.

[46] 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.

[47] A. K. Gárate-Escamila, A. Hajjam El Hassani, and E. Andrès, “*Classificationmodels for heart disease prediction using feature selection and PCA*,” *Inform Med Unlocked*, vol. 19, 2020, doi:

10.1016/j.imu.2020.100330.

[48] 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.