DAFTAR PUSTAKA

[1] S. Soliman, W. Oudah, and A. Aljuhani, “Deep learning-based intrusion detection approach for securing industrial Internet of Things,” *Alexandria Engineering Journal*, vol. 81, pp. 371–383, Oct. 2023, doi: 10.1016/j.aej.2023.09.023.

[2] 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.

[3] K. B. Virupakshar, M. Asundi, K. Channal, P. Shettar, S. Patil, and D. G. Narayan, “Distributed Denial of Service (DDoS) Attacks Detection System for OpenStack-based Private Cloud,” *Procedia Comput Sci*, vol. 167, pp. 2297–2307, 2020, doi: 10.1016/j.procs.2020.03.282.

[4] M. Aljanabi, R. Hayder, S. Talib, A. H. Ali, M. A. Mohammed, and T. Sutikno, “Distributed denial of service attack defense system-based auto machine learning algorithm,” *Bulletin of Electrical Engineering and Informatics*, vol. 12, no. 1, pp. 544–551, Feb. 2023, doi: 10.11591/eei.v12i1.4537.

[5] Lukman and M. Suci, “Analisis Perbandingan Kinerja Snort Dan Suricata Sebagai Intrusion Detection System Dalam Mendeteksi Serangan Syn Flood Pada Web Server Apache,” *Jurnal Teknologi Informasi*, vol. 15, no. 2, pp. 6–15, Jul. 2020, doi: 10.35842/jtir.v15i2.343.

[6] Y. Ariyanto, H. A. V. Firdaus, and H. Pramana, “Klasifikasi Jenis serangan DOS dan Probing pada IDS menggunakan metode K-Nearest Neighbor,” *Seminar Informatika Aplikatif Polinema (SIAP)*, pp. 472–476, 2020.

[7] V. K. Rahul, R. Vinayakumar, K. Soman, and P. Poornachandran, “Evaluating Shallow and Deep Neural Networks for Network Intrusion Detection Systems in Cyber Security,” *2018 9th International Conference on Computing, Communication and Networking Technologies, ICCCNT 2018*, Oct. 2018, doi: 10.1109/ICCCNT.2018.8494096.

[8] A. E. Cil, K. Yildiz, and A. Buldu, “Detection of DDoS attacks with feed forward based deep neural network model,” *Expert Syst Appl*, vol. 169, May 2021, doi: 10.1016/j.eswa.2020.114520.

[9] N. Rezaee, S. M. Zanjirchi, N. Jalilian, and S. M. H. Bamakan, “Internet of things empowering operations management; A systematic review based on bibliometric and content analysis,” *Telematics and Informatics Reports*, vol. 11, Sep. 2023, doi: 10.1016/j.teler.2023.100096.

[10] Ferdiansyah Zulkifli and Handy N, *INTERNET OF THINGS (IOT) MEDIA PEMBELAJARAN PRAKTIKUM ERA 4.0*. CV. Eureka Media Aksara, 2022.

[11] F. Behmann and Kwok wu., *Collaborative Internet Of Things (C-IoT): for future smart connected life and business*. Texas: John Wiley & Sons, 2015.

[12] Mambang, *BUKU AJAR TEKNOLOGI KOMUNIKASI INTERNET (Internet of Things)*. Purwokerto: CV. Pena Persada, 2022.

[13] R. Vivin, N. Riza, A. Erna, D. Astuti, M. Pramudia, and D. Rahmawati, *FUNDAMENTAL INTERNET OF THINGS (IOT) TEORI DAN APLIKASI PENERBIT CV.EUREKA MEDIA AKSARA*. Jawa Tengah: CV. Eureka Media Aksara, 2023.

[14] K. Lone and S. A. Sofi, "A review on offloading in fog-based Internet of Things: Architecture, machine learning approaches, and open issues," *High-Confidence Computing*, vol. 3, no. 2, Jun. 2023, doi: 10.1016/j.hcc.2023.100124.

[15] Sharipuddin *et al.*, "Enhanced Deep Learning Intrusion Detection in IoT Heterogeneous Network with Feature Extraction," *Indonesian Journal of Electrical and Engineering and Informatics (IJEEI)*, vol. 9, no. 3, pp. 747–755, 2021, doi: 10.52549/ijeei.v9i3.3134.

[16] E. A. Winanto, Kurniabudi, 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.

[17] M. Zidane, "Klasifikasi Serangan Distributed Denial-of-Service (DDoS) menggunakan Metode Data Mining Naïve Bayes," vol. 6, no. 1, pp. 172–180, 2022.

[18] F. Nisa and S. Ramadona, "Jurnal Sistim Informasi dan Teknologi https://jsisfotek.org/index.php Sistem Pencegahan Serangan Distributed Denial Of Service Pada Jaringan SDN," vol. 5, no. 3, 2023, doi: 10.60083/jsisfotek.v5i3.269.

[19] X. Yu, D. Han, Z. Du, Q. Tian, and G. Yin, "Design of DDoS attack detection system based on intelligent bee colony algorithm," *International Journal of Computational Science and Engineering*, vol. 19, no. 2, pp. 223–232, 2019, doi: 10.1504/IJCSE.2019.100243.

[20] S. Iswandi Walad, M. Zarlis, and M. I. T. Syahril Efendi, "Analysis of denial of service attack on web security systems," *J Phys Conf Ser*, 2021, doi: 10.1088/1742-6596/1811/1/012127.

[21] V. Nagaraju, A. Raaza, V. Rajendran, and D. Ravikumar, "Deep learning binary fruit fly algorithm for identifying SYN flood attack from TCP/IP," *Mater Today Proc*, vol. 80, pp. 3086–3091, Jan. 2023, doi: 10.1016/j.matpr.2021.07.171

.

[22] G. Mendonca, G. H. A. Santos, E. De Souza E Silva, R. M. M. Leao, D. S. Menasche, and D. Towsley, “An Extremely Lightweight Approach for DDoS Detection at Home Gateways,” *Proceedings - 2019 IEEE International Conference on Big Data*, pp. 5012–5021, Dec. 2019, doi: 10.1109/BigData47090.2019.9006548.

[23] D. Nashat and F. A. Hussain, “Multifractal Detrended Fluctuation Analysis Based Detection For SYN Flooding Attack,” *Comput Secur*, vol. 107, Aug. 2021, doi: 10.1016/j.cose.2021.102315.

[24] M. Dody Firmansyah, “Analisa Keamanan Web Server terhadap Serangan Distributed Denial of Service menggunakan Modevasive,” *TELCOMATICS*, vol. 6, no. 1, pp. 2541–5867, 2021, doi: 10.37253/telcomatics.v6i1.4990.

[25] S. M. Othman, N. T. Alsohybe, F. Mutaher Ba-Alwi, and A. T. Zahary, “Survey on Intrusion Detection System Types,” *International Journal of Cyber-Security and Digital Forensics*, vol. 7, no. 4, pp. 444–462, 2018.

[26] A. Rodiah Machdi, Waryani, and Sugeng, “Analisa dan Implementasi Sistem Kemananan Jaringan Intrusion Detection System (IDS) Berbasis Mikrotik,” *JET Jurnal Elektro Teknik*, vol. 1, no. 1, pp. 16–21, 2021.

[27] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, “A survey of intrusion detection in Internet of Things,” *Journal of Network and Computer Applications*, vol. 84, pp. 25–37, Apr. 2017, doi: 10.1016/j.jnca.2017.02.009.

[28] P. Kamboj, T. M. Chandra, Y. V. Kumar, and S. V. Kumar, “Detection Techhniques of DDoS Attacks: A Survey,” *2017 4th IEEE Uttar Pradesh Section International Conference on Electrical, Computer and Electronics (UPCON)*, pp. 26–28, 2017, doi: 10.1109/UPCON.2017.8251130.

[29] P. Kaur, M. Kumar, and A. Bhandari, “A review of detection approaches for distributed denial of service attacks,” *Systems Science and Control Engineering*, vol. 5, no. 1, pp. 301–320, Jan. 2017, doi: 10.1080/21642583.2017.1331768.

[30] I. Cholissodin, Sutrisno, A. A. Soebroto, U. Hasanah, and Y. I. Febiola, *AI, Machine Learning & Deep Learning (Teori & Implementasi)*. 2019.

[31] R. Mayer and H.-A. Jacobsen, “Scalable Deep Learning on Distributed Infrastructures: Challenges, Techniques and Tools,” *ACM Comput. Surv*, vol. 1, no. 1, p. 35, 2019, doi: 10.1145/3363554.

[32] C. Huang, J. Wang, S. Wang, and Y. Zhang, “A review of deep learning in dentistry,” *Neurocomputing*, vol. 554, Oct. 2023, doi: 10.1016/j.neucom.2023.126629.

[33] F. Handayani *et al.*, "Komparasi Support Vector Machine, Logistic Regression Dan Artificial Neural Network dalam Prediksi Penyakit Jantung," *Jurnal Edukasi dan Penelitian Innformatika*, vol. 7, no. 3, pp. 329–334, 2021, doi: 10.26418/jp.v7i3.48053.

[34] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho, "Deep learning approach for Network Intrusion Detection in Software Defined Networking," *International Conference on Wireless Networks and Mobile Communications, WINCOM 2016: Green Communications and Networking*, pp. 258–263, Dec. 2016, doi: 10.1109/WINCOM.2016.7777224.

[35] X. Yuan, C. Li, and X. Li, "DeepDefense: Identifying DDoS Attack via Deep Learning," *IEEE International Conference on Smart Computing (SMARTCOMP)*, pp. 1–8, 2017, doi: 10.1109/SMARTCOMP.2017.7946998.

[36] B. Vasu and N. Pari, "Combining Multimodal DNN and SigPid technique for detecting Malicious Android Apps," *Proceedings of the 11th International Conference on Advanced Computing, ICoAC* , pp. 289–294, Dec. 2019, doi: 10.1109/ICoAC48765.2019.247134.

[37] S. Choudhary and N. Kesswani, "Analysis of KDD-Cup'99, NSL-KDD and UNSW-NB15 Datasets using Deep Learning in IoT," *Procedia Comput Sci*, vol. 167, pp. 1561–1573, 2020, doi: 10.1016/j.procs.2020.03.367.

[38] M. Vishwakarma and N. Kesswani, "DIDS: A Deep Neural Network based real-time Intrusion detection system for IoT," *Decision Analytics Journal*, vol. 5, Dec. 2022, doi: 10.1016/j.dajour.2022.100142.

[39] R. Anushiya and V. S. Lavanya, "A new deep-learning with swarm based feature selection for intelligent intrusion detection for the Internet of things," *Measurement: Sensors*, vol. 26, Apr. 2023, doi: 10.1016/j.measen.2023.100700.

[40] V. Sze, Y.-H. Chen, T.-J. Yang, and J. Emer, "Efficient Processing of Deep Neural Networks: A Tutorial and Survey," Mar. 2017, doi: 10.1109/JPROC.2017.2761740.

[41] G. Montavon, W. Samek, and K. R. Müller, "Methods for interpreting and understanding deep neural networks," *Digital Signal Processing: A Review Journal*, vol. 73, pp. 1–15, Feb. 2018, doi: 10.1016/j.dsp.2017.10.011.

[42] P. M. Addo, D. Guegan, and B. Hassani, "Credit risk analysis using machine and deep learning models," *Risks*, vol. 6, no. 2, pp. 1–20, Jun. 2018, doi: 10.3390/risks6020038.

[43] K. Y. Chan *et al.*, "Deep neural networks in the cloud: Review, applications, challenges and research directions," *Neurocomputing*, vol. 545. Elsevier B.V., Aug. 07, 2023. doi: 10.1016/j.neucom.2023.126327.

[44] 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, Jul. 2023, doi: 10.3390/s23135941.

[45] J. Xu, Y. Zhang, and D. Miao, "Three-way confusion matrix for classification: A measure driven view," *Inf Sci (N Y)*, vol. 507, pp. 772–794, Jan. 2020, doi: 10.1016/j.ins.2019.06.064.

[46] M. K. Suryadewiansyah, T. Endra, and E. Tju, "Jurnal Nasional Teknologi dan Sistem Informasi Naïve Bayes dan Confusion Matrix untuk Efisiensi Analisa Intrusion Detection System Alert," *Jurnal Nasional Teknologi dan Sistem Informasi*, vol. 8, no. 2, pp. 81–88, 2022, doi: 10.25077/TEKNOSI.v8i2.2022.081-088.

[47] S. Das, A. M. Mahfouz, D. Venugopal, and S. Shiva, "DDoS Intrusion Detection Through Machine Learning Ensemble," *Proceedings - Companion of the 19th IEEE International Conference on Software Quality, Reliability and Security, QRS-C* , pp. 471–477, Jul. 2019, doi: 10.1109/QRS-C.2019.00090.

[48] C. Tang, N. Luktarhan, and Y. Zhao, "SAAE-DNN: Deep Learning Method on Intrusion Detection," *Symmetry (Basel)*, vol. 12, no. 10, pp. 1–20, Oct. 2020, doi: 10.3390/sym12101695.