DAFTAR PUSTAKA

[1] S. Razdan and S. Sharma, “Internet of Medical Things (IoMT): Overview, Emerging Technologies, and Case Studies,” 2022, *Taylor and Francis Ltd.* doi: 10.1080/02564602.2021.1927863.

[2] D. Koutras, G. Stergiopoulos, T. Dasaklis, P. Kotzanikolaou, D. Glynos, and C. Douligeris, “Security in iomt communications: A survey,” Sep. 01, 2020, *MDPI AG*. doi: 10.3390/s20174828.

[3] A. E. Khaled, “Internet of Medical Things (IoMT): Overview, Taxonomies, and Classifications,” *Journal of Computer and Communications*, vol. 10, no. 08, pp. 64–89, 2022, doi: 10.4236/jcc.2022.108005.

[4] M. Wazid, A. K. Das, J. J. P. C. Rodrigues, S. Shetty, and Y. Park, “IoMT Malware Detection Approaches: Analysis and Research Challenges,” *IEEE Access*, vol. 7, pp. 182459–182476, 2019, doi: 10.1109/ACCESS.2019.2960412.

[5] W. Toghuj and N. Turab, “A SURVEY ON SECURITY THREATS IN THE INTERNET OF MEDICAL THINGS (IoMT),” *J Theor Appl Inf Technol*, vol. 100, no. 10, 2022, [Online]. Available: www.jatit.org

[6] G. J. Joyia, R. M. Liaqat, A. Farooq, and S. Rehman, “Internet of medical things (IOMT): Applications, benefits and future challenges in healthcare domain,” *Journal of Communications*, vol. 12, no. 4, pp. 240–247, Apr. 2017, doi: 10.12720/jcm.12.4.240-247.

[7] A. Reji, B. Pranggono, J. Marchang, and A. Shenfield, “Anomaly Detection for the Internet of Medical Things,” 2023.

[8] H. Tauqeer, M. M. Iqbal, A. Ali, S. Zaman, and M. U. Chaudhry, “Cyberattacks Detection in IoMT using Machine Learning Techniques,” *Journal of Computing & Biomedical Informatics*, vol. 4, no. 01, pp. 13–20, Dec. 2022, doi: 10.56979/401/2022/80.

[9] 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.

[10] A. Khan, M. Rizwan, O. Bagdasar, A. Alabdulatif, S. Alamro, and A. Alnajim, “Deep Learning-Driven Anomaly Detection for IoMT-Based Smart Healthcare Systems,” *CMES - Computer Modeling in Engineering and Sciences*, vol. 141, no. 3, pp. 2121–2141, 2024, doi: 10.32604/cmes.2024.054380.

[11] Pritika, B. Shanmugam, and S. Azam, “Risk Evaluation and Attack Detection in Heterogeneous IoMT Devices Using Hybrid Fuzzy Logic Analytical Approach,” *Sensors*, vol. 24, no. 10, May 2024, doi: 10.3390/s24103223.

[12] A. Ghubaish, T. Salman, M. Zolanvari, D. Unal, A. Al-Ali, and R. Jain, “Recent Advances in the Internet-of-Medical-Things (IoMT) Systems Security,” *IEEE Internet Things J*, vol. 8, no. 11, pp. 8707–8718, Jun. 2021, doi: 10.1109/JIOT.2020.3045653.

[13] D. Koutras, G. Stergiopoulos, T. Dasaklis, P. Kotzanikolaou, D. Glynos, and C. Douligeris, “Security in iomt communications: A survey,” Sep. 01, 2020, *MDPI AG*. doi: 10.3390/s20174828.

[14] D. J. Brown, B. Suckow, and T. Wang, “A Survey of Intrusion Detection Systems.”

[15] A. Shenfield, D. Day, and A. Ayesh, “Intelligent intrusion detection systems using artificial neural networks,” *ICT Express*, vol. 4, no. 2, pp. 95–99, Jun. 2018, doi: 10.1016/j.icte.2018.04.003.

[16] H. J. Liao, C. H. Richard Lin, Y. C. Lin, and K. Y. Tung, “Intrusion detection system: A comprehensive review,” Jan. 2013. doi: 10.1016/j.jnca.2012.09.004.

[17] G. Karatas, O. Demir, and O. K. Sahingoz, “Deep Learning in Intrusion Detection Systems,” in *International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism, IBIGDELFT 2018 - Proceedings*, Institute of Electrical and Electronics Engineers Inc., Jan. 2019, pp. 113–116. doi: 10.1109/IBIGDELFT.2018.8625278.

[18] “Importance of Intrusion Detection System (IDS),” 2010, [Online]. Available: http://www.ijser.org

[19] “A Review of Anomaly based Intrusion Detection Systems.”

[20] H. T. Le, P. Loh, and C. T. Lau, “Performance evaluation of cyber reconnaissance tools,” 2016.

[21] H. P. Sanghvi, M. S. Dahiya, and C. Security, “Cyber Reconnaissance: An Alarm before Cyber Attack General Terms,” 2013. [Online]. Available: www.whois.com

[22] P. Kashyap and V. Selvarajah, “Analysis of Different Methods of Reconnaissance,” 2021.

[23] W. Adi Prabowo, R. Adhitama, A. Burhanuddin, K. Fauziah, and A. Salsabila Nahrowi, “Peningkatan Kesadaran Keamanan Informasi Siswa

SMK Telkom Purwokerto Melalui Pelatihan Footprinting dan Reconnaissance," *Online) Indonesian Journal of Community Service and Innovation (IJCOSIN)*, vol. 4, no. 1, pp. 2807–6370, 2024, doi: 10.20895/ijcosin.v4i1.1346.

[24] R. White *et al.*, "Network Reconnaissance and Vulnerability Excavation of Secure DDS Systems," Aug. 2019, [Online]. Available: http://arxiv.org/abs/1908.05310

[25] F. Lau and S. H. Rubin, "Distributed Denial of Service Attacks."

[26] S. kumarasamy, "Distributed Denial of Service (DDOS) Attacks Detection Mechanism," *International Journal of Computer Science, Engineering and Information Technology*, vol. 1, no. 5, pp. 39–49, Dec. 2011, doi: 10.5121/ijcseit.2011.1504.

[27] S. Yu, "Distributed Denial of Service Attack and Defence-Monograph," 2013.

[28] M. H. Bhuyan, H. J. Kashyap, D. K. Bhattacharyya, and J. K. Kalita, "Detecting Distributed Denial of Service Attacks: Methods, Tools and Future Directions." [Online]. Available: http://www.garykessler.net/library/ddos.html

[29] M. H. Ali *et al.*, "Threat Analysis and Distributed Denial of Service (DDoS) Attack Recognition in the Internet of Things (IoT)," *Electronics (Switzerland)*, vol. 11, no. 3, Feb. 2022, doi: 10.3390/electronics11030494.

[30] Y. Bengio, I. Goodfellow, and A. Courville, "Deep Learning," 2015.

[31] C. C. Aggarwal, "Neural Networks and Deep Learning." [Online]. Available: www.dbooks.org

[32] Francois. Chollet, *Deep Learning with Python by Francois Chollet*. Manning Publications : [distributed by] Skillsoft Books, 2019.

[33] C. M. Bishop, "Deep Learning." [Online]. Available: https://www.bishopbook.com

[34] "Introduction to Deep Learning." [Online]. Available: https://chat.openai.com/chat

[35] N. Shlezinger and Y. C. Eldar, "Model-Based Deep Learning," *Foundations and Trends in Signal Processing*, vol. 17, no. 4, pp. 291–416, Aug. 2023, doi: 10.1561/2000000113.

[36] A. Mosavi, S. Faizollahzadeh ardabili, and A. R. Várkonyi-Kóczy, "List of Deep Learning Models," Aug. 13, 2019. doi: 10.20944/preprints201908.0152.v1.

[37] M. Vakalopoulou, S. Christodoulidis, N. Burgos, O. Colliot, and V. Lepetit, “Deep learning: basics and convolutional neural networks (CNN)”, doi: 10.1007/978-1-0716-3195-9_3ï.

[38] C. Janiesch, P. Zschech, and K. Heinrich, “Machine learning and deep learning”, doi: 10.1007/s12525-021-00475-2/Published.

[39] F. Monti, D. Boscaini, J. Masci, E. Rodoì, J. Svoboda, and M. M. Bronstein, “Geometric deep learning on graphs and manifolds using mixture model CNNs.”

[40] J. Teuwen and N. Moriakov, “Convolutional neural networks,” in *Handbook of Medical Image Computing and Computer Assisted Intervention*, Elsevier, 2019, pp. 481–501. doi: 10.1016/B978-0-12-816176-0.00025-9.

[41] Canadian Institute for Cybersecurity, “CIC IoMT dataset 2024,” https://www.unb.ca/cic/datasets/iomt-dataset-2024.html.

[42] S. Megawan, W. S. Lestari, and A. Halim, “Deteksi Non-Spoofing Wajah pada Video secara Real Time Menggunakan Faster R-CNN,” *Journal of Information System Research (JOSH)*, vol. 3, no. 3, pp. 291–299, Apr. 2022, doi: 10.47065/josh.v3i3.1519.

[43] M. Iqbal Yoshanda, “Penerapan Model Hibrida CNN-GRU-BiLSTM-PCA Untuk Meningkatkan Akurasi Deteksi Serangan Jaringan Pada Intrusion Detection System,” 2023. [Online]. Available: http://journal.unnes.ac.id/nju/index.php/JM

[44] 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, Feb. 2020, doi: 10.33633/tc.v19i1.2860.

[45] R. Budiarto Hadiprakoso and I. K. S. Buana, “Deteksi Serangan Spoofing Wajah Menggunakan Convolutional Neural Network,” *Jurnal Teknik Informatika dan Sistem Informasi*, vol. 7, no. 3, Dec. 2021, doi: 10.28932/jutisi.v7i3.4001.

[46] C. L. Mindara, A. Zulianto, H. P. Utomo, T. Hatati, and G. P. Mindara, “Deteksi Intrusi Untuk Klasifikasi Serangan Jaringan Dengan Penerapan Algoritma Convolutional Neural Network,” *Jurnal ICT : Information Communication & Technology*, vol. 23, pp. 517–522, 2023.

[47] P. Simarmata, N. F. Saragih, I. K. Jaya, and H. Artikel, “Deteksi Serangan DDOS Pada VPS Menggunakan Metode Deep Neural Network,” 2023. [Online]. Available: http://ojs.fikom-methodist.net/index.php/methotika

[48] S. Munawarah, Kurniabudi, and E. Arip Winanto, “Jurnal Informatika Dan Rekayasa Komputer (JAKAKOM) Deteksi Serangan DDoS SYN Flood Pada Jaringan Internet of Things (IoT) Menggunakan Metode Deep Neural Network (DNN),” vol. 4, no. 1, 2024, doi: 10.33998/jakakom.v4i1.

[49] M. I. C. Rachmatullah, A. Wicaksono, and V. Putratama, “Perbandingan Metoda K-NN, Random Forest dan 1D CNN untuk Mengklasifikasi Data EEG Eye State,” *Journal of Information System Research (JOSH)*, vol. 4, no. 2, pp. 669–675, Jan. 2023, doi: 10.47065/josh.v4i2.2998.

[50] R. Dhanya, I. R. Paul, S. S. Akula, M. Sivakumar, and J. J. Nair, “F-test feature selection in Stacking ensemble model for breast cancer prediction,” in *Procedia Computer Science*, Elsevier B.V., 2020, pp. 1561–1570. doi: 10.1016/j.procs.2020.04.167.

[51] MUHAMMAD HILMI HAFID, “INVESTIGASI LOG JARINGAN UNTUK DETEKSI SERANGAN DISTRIBUTED DENIAL OF SERVICE (DDOS) DENGAN MENGGUNAKAN METODE GENERAL REGRESSIONNEURAL NETWORK,” 2019.

[52] J. H. J. C. Ortega, “Analysis of Performance of Classification Algorithms in Mushroom Poisonous Detection using Confusion Matrix Analysis,” *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 9, no. 1.3, pp. 451–456, Jun. 2020, doi: 10.30534/ijatcse/2020/7191.32020.

[53] D. Krstinić, M. Braović, L. Šerić, and D. Božić-Štulić, “Multi-label Classifier Performance Evaluation with Confusion Matrix,” Academy and Industry Research Collaboration Center (AIRCC), Jun. 2020, pp. 01–14. doi: 10.5121/csit.2020.100801.