DAFTAR PUSTAKA

[1] S. Razdan and S. Sharma, "Internet of Medical Things (IoMT): Overview, Emerging Technologies, and Case Studies," *IETE Tech. Rev.*, vol. 39, no. 4, pp. 775–788, Jul. 2022, doi: 10.1080/02564602.2021.1927863.

[2] P. Wal, A. Wal, N. Verma, R. Karunakakaran, and A. Kapoor, "Internet of Medical Things – The Future of Healthcare," *Open Public Health J.*, vol. 15, no. 1, p. e187494452212150, Dec. 2022, doi: 10.2174/18749445-v15-e221215-2022-142.

[3] National University of Sciences and Technology, Islamabad, Pakistan, G. J. Joyia, R. M. Liaqat, A. Farooq, and S. Rehman, "Internet of Medical Things (IOMT): Applications, Benefits and Future Challenges in Healthcare Domain," *J. Commun.*, 2017, doi: 10.12720/jcm.12.4.240-247.

[4] M. K. Hasan *et al.*, "A review on security threats, vulnerabilities, and counter measures of 5G enabled Internet-of-Medical-Things," *IET Commun.*, vol. 16, no. 5, pp. 421–432, Mar. 2022, doi: 10.1049/cmu2.12301.

[5] ANDRE ARTA KURNIAWAN, "INTRUSION DETECTION SYSTEM MENGGUNAKAN DEEP LEARNING UNTUK DETEKSI SERANGAN DoS," *2020*, vol. 1, pp. 1–60, 2020.

[6] S. Nurwenda and B. Irawan, "Analisis Kelakuan Denial-of-Service attack (DoS attack) pada Jaringan Komputer dengan Pendekatan pada Level Sekuritas".

[7] A. I. Haris, B. Riyanto, F. Surachman, and A. A. Ramadhan, "Analisis Pengamanan Jaringan Menggunakan Router Mikrotik dari Serangan DoS dan Pengaruhnya Terhadap Performansi," *Komputika J. Sist. Komput.*, vol. 11, no. 1, pp. 67–76, Jan. 2022, doi: 10.34010/komputika.v11i1.5227.

[8] M. M. Abualhaj, A. A. Abu-Shareha, M. O. Hiari, Y. Alrabanah, M. Al-Zyoud, and M. A. Alsharaiah, "A Paradigm for DoS Attack Disclosure using Machine Learning Techniques," *Int. J. Adv. Comput. Sci. Appl.*, vol. 13, no. 3, 2022, doi: 10.14569/IJACSA.2022.0130325.

[9] M. Pramana, Endang Setyati, and F.X. Ferdinandus, "Identifikasi Serangan Denial Of Service (Dos) Di Jaringan Dengan Algoritma Decision Tree C4.5," *Wahana*, vol. 73, no. 2, pp. 13–29, Dec. 2021, doi: 10.36456/wahana.v73i2.4071.

[10] M. Abushwereb and M. Mustafa, "Attack based DoS attack detection using multiple classifier".

[11] 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," vol. 23, 2023.

[12] S. K. Gebresilassie, J. Rafferty, L. Chen, Z. Cui, and M. Abu-Tair, "Transfer and CNN-Based De-Authentication (Disassociation) DoS Attack Detection in IoT Wi-Fi Networks," *Electronics*, vol. 12, no. 17, p. 3731, Sep. 2023, doi: 10.3390/electronics12173731.

[13] F. Paraijun, R. N. Aziza, and D. Kuswardani, "Implementasi Algoritma Convolutional Neural Network Dalam Mengklasifikasi Kesegaran Buah Berdasarkan Citra Buah," *KILAT*, vol. 11, no. 1, pp. 1–9, Apr. 2022, doi: 10.33322/kilat.v10i2.1458.

[14] S. Salmi and L. Oughdir, “Performance evaluation of deep learning techniques for DoS attacks detection in wireless sensor network,” *J. Big Data*, vol. 10, no. 1, p. 17, Feb. 2023, doi: 10.1186/s40537-023-00692-w.
[15] S. A. Panchbudhe, “Internet of medical things (IoMT) – A review article.”.
[16] E. R. Fauzi, A. Maharesi, and N. A. Setiyadi, “MONOGRAF : IMPLEMENTASI TEKNOLOGI IOT DI INFANT WARMER”.
[17] R. M. Surya Fadli, “PROTOTIPE PENDETEKSI TINGKAT DIABETES DAN ALKOHOL PADA PH URIN MENGGUNAKAN RASPBERRY PI 3 YANG TERINTEGRASI IoMT,” vol. 1, pp. 24–35, Jun. 2024.
[18] L. L. Pramita and A. P. Wibawa, “Perkembangan Teknologi Kesehatan di Era Society 5.0,” 2022.
[19] 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 J. Ilm. Teknol. Inf.*, vol. 13, no. 1, p. 53, Jan. 2015, doi: 10.12962/j24068535.v13i1.a388.
[20] E. Ginting, P. Sahara, and S. N. Tambunan, “ANCAMAN DENIAL OF SERVICE ATTACK DALAM EKSPLOITASI KEAMANAN SISTEM INFORMASI”.
[21] S. M. S and D. Sukma, “PENERAPAN METODE NIJ UNTUK ANALISIS SERANGAN DOS PADA PERANGKAT IOT,” *Power Elektron. J. Orang Elektro*, vol. 12, no. 2, p. 93, Apr. 2023, doi: 10.30591/polektro.v12i2.5093.
[22] W. Haniyah, M. C. Hidayat, Z. F. I. Putra, V. A. Pertama, and A. Setiawan, “Simulasi Serangan Denial of Service (DoS) menggunakan Hping3 melalui Kali Linux,” *J. Internet Softw. Eng.*, vol. 1, no. 2, p. 8, Jun. 2024, doi: 10.47134/pjise.v1i2.2654.
[23] E. Ginting, P. Sahara, and S. N. Tambunan, “ANCAMAN DENIAL OF SERVICE ATTACK DALAM EKSPLOITASI KEAMANAN SISTEM INFORMASI”.
[24] M. H. Dar and S. Z. Harahap, “IMPLEMENTASI SNORT INTRUSION DETECTION SYSTEM (IDS) PADA SISTEM JARINGAN KOMPUTER,” *J. Inform.*, vol. 6, no. 3, pp. 14–23, Sep. 2017, doi: 10.36987/informatika.v6i3.1619.
[25] L. Saroha and R. Octavianto, “Pencegahan Dan Konsep IDS (Intrusion Detection System) Dalam Mendeteksi Serangan Siber Pada Sistem Keamanana Di Universitas Persada Indonesia Y.A.i”.
[26] R. Aulianita, N. Musyaffa, and R. Martiwi, “PENGGUNAAN METODE IDS DALAM IMPLEMENTASI FIREWALL PADA JARINGAN UNTUK DETEKSI SERANGAN Distributed Denial Of Service,” vol. 6, no. 2, 2021.
[27] D. N. Awangga, H. Sajati, and Y. Astuti, “PEMANFAATAN INTRUSION DETECTION SYSTEM (IDS) SEBAGAI OTOMATISASI KONFIGURASI FIREWALL BERBASIS WEB SERVICE MENGGUNAKAN ARSITEKTUR REPRESENTATIONAL STATE TRANSFER (REST),” *Compiler*, vol. 2, no. 2, Nov. 2013, doi: 10.28989/compiler.v2i2.49.
[28] “DETEKSI SERANGAN PADA INTRUSION DETECTION SYSTEM (IDS) UNTUK KLASIFIKASI SERANGAN DENGAN ALGORITMA

NAÏVE BAYES, C.45 DAN K-NN DALAM MEMINIMALISASI RESIKO TERHADAP PENGGUNA," *J. Sist. Inf. Univ. SURYADARMA*, vol. 8, no. 2, Jun. 2014, doi: 10.35968/jsi.v8i2.732.

[29] N. Furqan and I. Suandi, "IMPLEMENTASI INTRUSION DETECTION SYSTEM (IDS) PADA SISTEM KEAMANAN JARINGAN MENGGUNAKAN TELEGRAM SEBAGAI MEDIA NOTIFIKASI".

[30] I. M. Amir, Y. Mardiana, S. Kom, and M. Kom, "SIMULASI INTRUSION DETECTION SYSTEM (IDS) DALAM KEAMANAN WEB SERVER PADA JARINGAN," 2023.

[31] S. Alviana and I. D. Sumitra, "ANALISIS PENGUKURAN PENGGUNAAN SUMBER DAYA KOMPUTER PADA INTRUSION DETECTION SYSTEM DALAM MEMINIMALKAN SERANGAN JARINGAN," *Komputa J. Ilm. Komput. Dan Inform.*, vol. 7, no. 1, pp. 27–34, Mar. 2018, doi: 10.34010/komputa.v7i1.2533.

[32] F. Ramadhani, A. Satria, and S. Salamah, "Implementasi Algoritma Convolutional Neural Network dalam Mengidentifikasi Dini Penyakit pada Mata Katarak," *Sudo J. Tek. Inform.*, vol. 2, no. 4, pp. 167–175, Dec. 2023, doi: 10.56211/sudo.v2i4.408.

[33] N. Wakhidah, P. T. Pungkasanti, and A. P. R. Pinem, "Deteksi Objek menggunakan Deep Learning untuk Mengetahui Tingkat Kerumunan Mahasiswa," *J. Edukasi Dan Penelit. Inform. JEPIN*, vol. 9, no. 3, p. 465, Dec. 2023, doi: 10.26418/jp.v9i3.70132.

[34] P. A. Nugroho, I. Fenriana, R. Arijanto, and M. Kom, "IMPLEMENTASI DEEP LEARNING MENGGUNAKAN CONVOLUTIONAL NEURAL NETWORK (CNN) PADA EKSPRESI MANUSIA," vol. 2, no. 1, 2020.

[35] S. R. Dewi, "Diajukan Sebagai Salah Satu Syarat untuk Memperoleh Gelar Sarjana Program Studi Statistika".

[36] A. S. Wardhani, F. T. Anggraeny, and A. M. Rizki, "PENERAPAN MODEL HIBRIDA CNN-KNN UNTUK KLASIFIKASI PENYAKIT MATA," *JATI J. Mhs. Tek. Inform.*, vol. 8, no. 3, pp. 3662–3667, Jun. 2024, doi: 10.36040/jati.v8i3.9774.

[37] K. Azmi, S. Defit, and S. Sumijan, "Implementasi Convolutional Neural Network (CNN) Untuk Klasifikasi Batik Tanah Liat Sumatera Barat," *J. UNITEK*, vol. 16, no. 1, pp. 28–40, Jun. 2023, doi: 10.52072/unitek.v16i1.504.

[38] A. Kholik, "KLASIFIKASI MENGGUNAKAN CONVOLUTIONAL NEURAL NETWORK (CNN) PADA TANGKAPAN LAYAR HALAMAN INSTAGRAM," *J. Data Min. Dan Sist. Inf.*, vol. 2, no. 2, p. 10, Aug. 2021, doi: 10.33365/jdmsi.v2i2.1345.

[39] G. W. Intyanto, "Klasifikasi Citra Bunga dengan Menggunakan Deep Learning: CNN (Convolution Neural Network)," *J. Arus Elektro Indones.*, vol. 7, no. 3, p. 80, Dec. 2021, doi: 10.19184/jaei.v7i3.28141.

[40] I. Wulandari, H. Yasin, and T. Widiharih, "KLASIFIKASI CITRA DIGITAL BUMBU DAN REMPAH DENGAN ALGORITMA CONVOLUTIONAL NEURAL NETWORK (CNN)".

[41] M. Z. Andrekha and Y. Huda, "Deteksi Warna Manggis Menggunakan Pengolahan Citra dengan Opencv Python," *Voteteknika Vocat. Tek. Elektron.*

Dan Inform., vol. 9, no. 4, p. 27, Dec. 2021, doi: 10.24036/voteteknika.v9i4.114251.

[42] "Karimah Tauhid, Volume 2 Nomor 1 (2023), e-ISSN 2963-590X," vol. 2, 2023.

[43] Kalyani Jeslyn Lim *et al.*, "Penggunaan Bahasa Pemrograman Python Untuk Memvisualisasikan Data Peluang Selamat Dari Kecelakaan Titanic," *J. Publ. Tek. Inform.*, vol. 2, no. 2, pp. 66–79, May 2023, doi: 10.55606/jupti.v2i2.1735.

[44] S. Junaidi, M. Devegi, and H. Kurniawan, "Pelatihan Pengolahan dan Visualisasi Data Penduduk menggunakan Python," *ADMA J. Pengabdi. Dan Pemberdaya. Masy.*, vol. 4, no. 1, pp. 151–162, Jul. 2023, doi: 10.30812/adma.v4i1.2963.

[45] Y. Yuliana, D. H. Supriyadi, M. R. Fahlevi, and M. R. Arisagas, "Analysis of NSL-KDD for the Implementation of Machine Learning in Network Intrusion Detection System," *J. Inform. Inf. Syst. Softw. Eng. Appl. INISTA*, vol. 6, no. 2, pp. 80–89, Feb. 2024, doi: 10.20895/inista.v6i2.1389.

[46] F. Muhammad, I. Wahidah, and A. I. Irawan, "ANALISIS PENDETEKSIAN SERANGAN DENIAL OF SERVICE (DOS) MENGGUNAKAN LOGIKA FUZZY METODE MAMDANI PADA JARINGAN INTERNET OF THINGS (IOT)".

[47] M. Pramana, Endang Setyati, and F.X. Ferdinandus, "Identifikasi Serangan Denial Of Service (Dos) Di Jaringan Dengan Algoritma Decision Tree C4.5," *Wahana*, vol. 73, no. 2, pp. 13–29, Dec. 2021, doi: 10.36456/wahana.v73i2.4071.

[48] F. A. Rafrastara, W. Ghozi, and A. Wardoyo, "Deteksi Serangan berbasis Machine Learning pada Internet of Vehicle," vol. 2024, 2024.

[49] R. N. Wibowo, P. Sukarno, and E. M. Jadied, "Pendeteksian Serangan DoS Menggunakan Multiclassfier Pada NSL-KDD Dataset".

[50] M. M. Abualhaj, A. A. Abu-Shareha, M. O. Hiari, Y. Alrabanah, M. Al-Zyoud, and M. A. Alsharaiah, "A Paradigm for DoS Attack Disclosure using Machine Learning Techniques," *Int. J. Adv. Comput. Sci. Appl.*, vol. 13, no. 3, 2022, doi: 10.14569/IJACSA.2022.0130325.

[51] N. D. Primadya, A. Nugraha, A. Luthfiarta, and S. Y. Fahrezi, "Optimasi Logistic Regression untuk Deteksi Serangan DoS pada Keamanan IoT," *J. Eksplora Inform.*, vol. 13, no. 2, pp. 245–252, Mar. 2024, doi: 10.30864/eksplora.v13i2.1065.

[52] F. F. Setiadi, M. W. A. Kesiman, and K. Y. E. Aryanto, "Detection of dos attacks using naive bayes method based on internet of things (iot)," *J. Phys. Conf. Ser.*, vol. 1810, no. 1, p. 012013, Mar. 2021, doi: 10.1088/1742-6596/1810/1/012013.

[53] Y. Ariyanto and H. Pramana, "Klasifikasi Jenis serangan DOS dan Probing pada IDS menggunakan metode K- Nearest Neighbor," 2020.

[54] M. A. Fauzi, "SISTEM DETEKSI INTRUSI MENGGUNAKAN ALGORITMA GENETIK PADA SERANGAN DOS DI PROTOKOL TCP DAN UDP".