DAFTAR PUSTAKA

[1] T. A. P. Santoso, "Smart Shirt untuk Mengukur Tingkat Kesehatan dengan Menggunakan Teknologi Sensor dan Fitur Digital," *J. Sist. Cerdas*, vol. 4, no. 2, pp. 104–113, Aug. 2021, doi: 10.37396/jsc.v4i2.94.

[2] A. F. K. Dewi and Y. Suryanto, "Desain Kerangka Kerja Manajemen Risiko Keamanan Informasi Berdasarkan Kajian Risk Profiling pada Sektor Kesehatan," vol. 8, no. 1, 2022.

[3] D. V. Dimitrov, "Medical Internet of Things and Big Data in Healthcare," *Healthc. Inform. Res.*, vol. 22, no. 3, p. 156, 2016, doi: 10.4258/hir.2016.22.3.156.

[4] Levina Lintang Pramita, Aji Prasetya Wibawa*, "Perkembangan Teknologi Kesehatan di Era Society 5.0," *J. Inov. Tek. Dan Edukasi Teknol. 27 2022 307-313*, vol. 2, no. 1, pp. 1–7, Jul. 2022, doi: 10.17977/um068v1i72022p307-313.

[5] S. Z. Effendi and U. Y. Oktiawati, "Implementasi dan Analisis Performa Sistem Monitoring Suhu dan Kelembaban Kondisi Ruang Server pada Jaringan Berbasis Lora," 2022.

[6] 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)".

[7] D. Oleh, "DESAIN KEAMANAN PADA KOMUNIKASI DATA SISTEM BANK AIR KAMI V2 MENGGUNAKAN TRIAS CIA".

[8] A. Khaliq and S. Novida Sari, "PEMANFAATAN KERANGKA KERJA INVESTIGASI FORENSIK JARINGAN UNTUK IDENTIFIKASI SERANGAN JARINGAN MENGGUNAKAN SISTEM DETEKSI INTRUSI (IDS)," *J. Nas. Teknol. Komput.*, vol. 2, no. 3, pp. 150–158, Aug. 2022, doi: 10.61306/jnastek.v2i3.52.

[9] T. Widodo and A. S. Aji, "Pemanfaatan Network Forensic Investigation Framework untuk Mengidentifikasi Serangan Jaringan Melalui Intrusion Detection System (IDS)," *JISKA J. Inform. Sunan Kalijaga*, vol. 7, no. 1, pp. 46–55, Jan. 2022, doi: 10.14421/jiska.2022.7.1.46-55.

[10] F. Mosaiyebzadeh, L. G. Araujo Rodriguez, D. Macedo Batista, and R. Hirata, "A Network Intrusion Detection System using Deep Learning against MQTT Attacks in IoT," in *2021 IEEE Latin-American Conference on Communications (LATINCOM)*, Santo Domingo, Dominican Republic: IEEE, Nov. 2021, pp. 1–6. doi: 10.1109/LATINCOM53176.2021.9647850.

[11] hector Alaiz Moreton Jorge Ondicol Garcia, 2, "prosedur klasifikasi multikelas untuk mendeteksi serangan pada prtokol MQTT-IoT," *2019*, vol. 2019, no. 1, pp. 1–11, 2019.

[12] A. Alzahrani and T. H. H. Aldhyani, "Artificial Intelligence Algorithms for Detecting and Classifying MQTT Protocol Internet of Things Attacks," *Electronics*, vol. 11, no. 22, p. 3837, Nov. 2022, doi: 10.3390/electronics11223837.

[13] GALUH MUHAMMAD IMAN AKBAR, "DETEKSI SERANGAN PADA PROTOKOL MQTT IOT MENGGUNAKAN RANDOM FOREST," *2023*, vol. 1, no. 1, pp. 1–77, 2023.
[14] A. I. N. Iman, F. D. Sumadi, and Z. Sari, "Low Rate DDOS Attack Detection Using KNN On SD-IOT," vol. 5, no. 1.
[15] E. Lapian, A. B. Osmond, and R. E. Saputra, "RECURRENT NEURAL NETWORK UNTUK PENGENALAN UCAPAN PADA DIALEK MANADO".
[16] D. E. B. Jabat, L. Y. Sipayung, K. Raih, and S. Dakhi, "Penerapan Algoritma Recurrent Neural Networks (RNN) Untuk Klasifikasi Ulos Batak Toba," vol. 1, no. 2, 2024.
[17] Andre Arta Kurniawan, "INTRUSION DETECTION SYSTEM MENGGUNAKAN DEEP LEARNING UNTUK DETEKSI SERANGAN DoS," *2020*, vol. 1, no. 1, pp. 1–60, 2020.
[18] "Man in the Middle Attack Detection for MQTT based IoT devices using different Machine Learning Algorithms," *Proc. 2022 2nd Int. Conf. Artif. Intell. ICAI IEEE Xplore*, vol. 1, no. 1, pp. 1–5, Mar. 2021.
[19] Surya Fadli1, Romi Mulyadi2, "PROTOTIPE PENDETEKSI TINGKAT DIABETES DAN ALKOHOL PADA PH URIN MENGGUNAKAN RASPBERRY PI 3 YANG TERINTEGRASI IoMT," *Interdiscip. J. MedTech EcoEngineering IJME*, vol. 1, pp. 1–12, Jun. 2024.
[20] R. Arisandi and A. L. Dewi, "ANALISIS FAKTOR RISIKO GAGAL JANTUNG DENGAN REGRESI LOGISTIK BERBASIS IoMT," *J. Gaussian*, vol. 12, no. 4, pp. 549–559, Jun. 2024, doi: 10.14710/j.gauss.12.4.549-559.
[21] S. Dadkhah, E. C. P. Neto, R. Ferreira, R. C. Molokwu, S. Sadeghi, and A. A. Ghorbani, "CICIoMT2024: A benchmark dataset for multi-protocol security assessment in IoMT," *Internet Things*, vol. 28, p. 101351, Dec. 2024, doi: 10.1016/j.iot.2024.101351.
[22] D. Oleh, "Cloud Computing Data Mining dan Data Warehouse Kecerdasan Buatan Komputasi Komunikasi Data dan Jaringan Komputer Mobile Computing Multimedia dan Grafika Pemodelan dan Aplikasi Sistem Informasi Pengolahan Citra Pengolahan Sinyal Teknologi Basis Data Simulasi dan Permainan Komputer Sistem Kendali dan Robotika," 2016.
[23] S. O. Tarigan, H. I. Sitepu, and M. Hutagalung, "Pengukuran Kinerja Sistem Publish/ Subscribe Menggunakan Protokol MQTT (Message Queuing Telemetry Transport)," *J. Telematika*, vol. 9, no. 1, p. 20, Aug. 2014, doi: 10.61769/telematika.v9i1.85.
[24] R. P. Pratama, "PENGENDALI LAMPU RUMAH BERBASIS ESP8266 DENGAN PROTOKOL MQTT," *TESLA J. Tek. Elektro*, vol. 22, no. 1, p. 56, Mar. 2020, doi: 10.24912/tesla.v22i1.7862.
[25] S. Mulyono, M. Qomaruddin, and M. S. Anwar, "Penggunaan Node-RED pada Sistem Monitoring dan Kontrol Green House berbasis Protokol MQTT," vol. 3, no. 1, 2018.
[26] G. Y. Saputra, A. D. Afrizal, F. K. R. Mahfud, F. A. Pribadi, and F. J. Pamungkas, "PENERAPAN PROTOKOL MQTT PADA TEKNOLOGI WAN (STUDI KASUS SISTEM PARKIR UNIVERISTAS BRAWIJAYA)".

[27] R. Dismantoro, A. Kusyanti, and M. Data, “Implementasi Algoritme Lizard untuk Pengamanan Protokol MQTT pada Perangkat NodeMCU”.
[28] A. S. Fadhlillah, “ANALISIS PERFORMANSI IDS MENGGUNAKAN METODE DETEKSI ANOMALY- BASED TERHADAP SERANGAN DOS”.
[29] C. A. Putra and M. S. Munir, “DETEKSI SERANGAN TROJAN HORSE DENGAN MEMANFAATKAN IDS SNORT,” 2019.
[30] Z. A. Tyas, A. Firdonsyah, and W. Ramdhani, “Analisis Keamanan Jaringan dari Serangan DoS pada Sistem Inventaris Sanggar Tari Natya Lakshita menggunakan IDS,” *INFORMAL Inform. J.*, vol. 7, no. 3, p. 258, Dec. 2022, doi: 10.19184/isj.v7i3.34943.
[31] We Muftihaturrahmah Tenri Sau and Sepha Siswantyo, “Analisis Penggunaan Hasil Deteksi IDS Snort pada Tools RITA dalam Mendeteksi Aktivitas Beacon,” *Info Kripto*, vol. 15, no. 2, pp. 97–104, Aug. 2021, doi: 10.56706/ik.v15i2.21.
[32] M. A. Aydın, A. H. Zaim, and K. G. Ceylan, “A hybrid intrusion detection system design for computer network security,” *Comput. Electr. Eng.*, vol. 35, no. 3, pp. 517–526, May 2009, doi: 10.1016/j.compeleceng.2008.12.005.
[33] 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.
[34] N. Furqan and I. Suandi, “IMPLEMENTASI INTRUSION DETECTION SYSTEM (IDS) PADA SISTEM KEAMANAN JARINGAN MENGGUNAKAN TELEGRAM SEBAGAI MEDIA NOTIFIKASI,” 2023.
[35] Y. P. Atmojo, “Bot Alert Snort dengan Telegram Bot API pada Intrusion Detection System: Studi Kasus IDS pada Server Web,” 2018.
[36] Ricky Gunawan, “MPLEMENTASI INTRUSION DETECTION SYSTEM SNORT MENGGUNAKAN LINUX UBUNTU 16.04 PADA JARINGAN PT SUMBER INOVASI SEJATI,” *Univ. Putera Batam UPB Repro*, vol. 1, pp. 1–57, agustus 2019.
[37] 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.
[38] D. Oleh, “ANALISIS PERFORMA TEKNIK RESAMPLING UNTUK MENGATASI KETIDAKSEIMBANGAN DATA LATIH PADA MODEL DETEKSI INTRUSI JARINGAN”.
[39] Y. Yang, K. McLaughlin, S. Sezer, Y. B. Yuan, and W. Huang, “Stateful intrusion detection for IEC 60870-5-104 SCADA security,” in *2014 IEEE PES General Meeting | Conference & Exposition*, National Harbor, MD, USA: IEEE, Jul. 2014, pp. 1–5. doi: 10.1109/PESGM.2014.6939218.
[40] A. Irvannanda, “FAKULTAS SAINS DAN TEKNOLOGI UNIVERSITAS ISLAM NEGERI SULTAN SYARIF KASIM RIAU PEKANBARU 202”.
[41] H. S. Mare and W. Syafitri, “SISTEM PENDETEKSIAN PENYUSUPAN JARINGAN KOMPUTER DENGAN ACTIVE RESPONSE

MENGGUNAKAN METODE HYBRID INTRUSION DETECTION, SIGNATURES DAN ANOMALY DETECTION," 2011.
[42] F. Firdausillah, M. Hafidz, E. D. Udayanti, and E. Kartikadarma, "Sistem Deteksi Surel SPAM Dengan DNSBL Dan Support Vector Machine Pada Penyedia Layanan Mail Marketing," *J. Inf. Syst. Res. JOSH*, vol. 3, no. 4, pp. 618–625, Jul. 2022, doi: 10.47065/josh.v3i4.1795.
[43] J. Pujoseno, "Diajukan Sebagai Salah Satu Syarat Untuk Memperoleh Gelar Sarjana Program Studi Statistika".
[44] D. Oleh, "DEEP LEARNING UNTUK DETEKSI WAJAH YANG BERHIJAB MENGGUNAKAN ALGORITMA CONVOLUTIONAL NEURAL NETWORK (CNN) DENGAN TENSORFLOW".
[45] M. Z. Ersyad, K. N. Ramadhani, and A. Arifianto, "Pengenalan Bentuk Tangan dengan Convolutional Neural Network (CNN)".
[46] M. Rizki, S. Basuki, and Y. Azhar, "Implementasi Deep Learning Menggunakan Arsitektur Long Short Term Memory Untuk Prediksi Curah Hujan Kota Malang," vol. 2, no. 3.
[47] N. Lubis, Mhd. Z. Siambaton, and R. Aulia, "Implementasi Algoritma Deep Learning pada Aplikasi Speech to Text Online dengan Metode Recurrent Neural Network (RNN)," *Sudo J. Tek. Inform.*, vol. 3, no. 3, pp. 113–126, Sep. 2024, doi: 10.56211/sudo.v3i3.583.
[48] A. Yunizar, T. Rismawan, and D. M. Midyanti, "PENERAPAN METODE RECURRENT NEURAL NETWORK MODEL GATED RECURRENT UNIT UNTUK PREDIKSI HARGA CRYPTOCURRENCY," *Coding J. Komput. Dan Apl.*, vol. 11, no. 1, p. 32, May 2023, doi: 10.26418/coding.v11i1.58073.
[49] H. Salehinejad, S. Sankar, J. Barfett, E. Colak, and S. Valaee, "Recent Advances in Recurrent Neural Networks," Feb. 22, 2018, *arXiv*: arXiv:1801.01078. Accessed: Nov. 05, 2024. [Online]. Available: http://arxiv.org/abs/1801.01078
[50] D. A. H. Panggabean, F. M. Sihombing, and N. M. Aruan, "PREDIKSI TINGGI CURAH HUJAN DAN KECEPATAN ANGIN BERDASARKAN DATA CUACA DENGAN PENERAPAN ALGORITMA ARTIFICIAL NEURAL NETWORK (ANN)," *SEMINASTIKA*, vol. 3, no. 1, pp. 1–7, Nov. 2021, doi: 10.47002/seminastika.v3i1.237.
[51] Moch Farryz Rizkilloh and Sri Widiyanesti, "Prediksi Harga Cryptocurrency Menggunakan Algoritma Long Short Term Memory (LSTM)," *J. RESTI Rekayasa Sist. Dan Teknol. Inf.*, vol. 6, no. 1, pp. 25–31, Feb. 2022, doi: 10.29207/resti.v6i1.3630.
[52] P. P. O. Mahawardana, G. A. Sasmita, and I. P. A. E. Pratama, "Analisis Sentimen Berdasarkan Opini dari Media Sosial Twitter terhadap 'Figure Pemimpin' Menggunakan Python," *JITTER J. Ilm. Teknol. Dan Komput.*, vol. 3, no. 1, p. 810, Jan. 2022, doi: 10.24843/JTRTI.2022.v03.i01.p17.
[53] M. Romzi and B. Kurniawan, "PEMBELAJARAN PEMROGRAMAN PYTHON DENGAN PENDEKATAN LOGIKA ALGORITMA," vol. 3, no. 2, 2020.
[54] I. W. Sukerta Wijaya, I. G. Harjumawan Wiratmaja Ks., I. D. M. A. Pramana Setya Bintara, and I. K. G. Ryan Aditya Permana, "Program Menghitung

Banyak Bata pada Ruangan Menggunakan Bahasa Python," *TIERS Inf. Technol. J.*, vol. 2, no. 1, Dec. 2021, doi: 10.38043/tiers.v2i1.2840.

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

[56] A. Al Hanif and M. Ilyas, "Effective Feature Engineering Framework for Securing MQTT Protocol in IoT Environments," *Sensors*, vol. 24, no. 6, p. 1782, Mar. 2024, doi: 10.3390/s24061782.

[57] A. I. Gide and A. A. Mu'azu, "A Real-Time Intrusion Detection System for DoS/DDoS Attack Classification in IoT Networks Using KNN-Neural Network Hybrid Technique," *Babylon. J. Internet Things*, vol. 2024, pp. 60–69, Jul. 2024, doi: 10.58496/BJIoT/2024/008.

[58] T. T. Tanggal, "Farhan 17201109 Mueth Ul Ihsan Ananno".

[59] Jose Aveleira Mata ,Jorge Ondicol Garcia, "Prosedur Klasifikasi Multikelas untuk Mendeteksi Serangan pada Protokol MQTT-IoT," *Hindawi Complex.*, vol. 2019, no. 1, pp. 1–11, Apr. 2019.

[60] H. Zeghida, M. Boulaiche, and R. Chikh, "Securing MQTT protocol for IoT environment using IDS based on ensemble learning," *Int. J. Inf. Secur.*, vol. 22, no. 4, pp. 1075–1086, Aug. 2023, doi: 10.1007/s10207-023-00681-3.

[61] Imran, M. F. A. Zuhairi, S. M. Ali, Z. Shahid, M. M. Alam, and M. M. Su'ud, "Improving Reliability for Detecting Anomalies in the MQTT Network by Applying Correlation Analysis for Feature Selection Using Machine Learning Techniques," *Appl. Sci.*, vol. 13, no. 11, p. 6753, Jun. 2023, doi: 10.3390/app13116753.

[62] Department of Electrical and Electronic Engineering, Faculty of Engineering, University of Peradeniya, Sri Lanka and M. B. Dissanayake, "Feature Engineering for Cyber-attack detection in Internet of Things," *Int. J. Wirel. Microw. Technol.*, vol. 11, no. 6, pp. 46–54, Dec. 2021, doi: 10.5815/ijwmt.2021.06.05.

[63] A. Alatram, L. F. Sikos, M. Johnstone, P. Szewczyk, and J. J. Kang, "DoS/DDoS-MQTT-IoT: A dataset for evaluating intrusions in IoT networks using the MQTT protocol," *Comput. Netw.*, vol. 231, p. 109809, Jul. 2023, doi: 10.1016/j.comnet.2023.109809.

[64] Ali Ghannadrad, "Machine leaning-based DoS attacks detection for MQTT sensor networks," *Sch. Ind. Inf. Eng.*, pp. 1–74, 2021 2020.

[65] N. F. Syed, Z. Baig, A. Ibrahim, and C. Valli, "Denial of service attack detection through machine learning for the IoT," *J. Inf. Telecommun.*, vol. 4, no. 4, pp. 482–503, Oct. 2020, doi: 10.1080/24751839.2020.1767484.