

DAFTAR PUSTAKA

- [1] E. Susanto, Lady Antira, K. Kevin, E. Stanzah, and A. A. Majid, "Manajemen Keamanan Cyber di Era Digital," *Journal of Business and Entrepreneurship*, vol. 11, no. 1, pp. 23–33, 2023, doi: 10.46273/job&e.v11i1.365.
- [2] N. Anwar, D. Rosian Adhy, N. Widiyasono, R. Hermawan, M. A. Hadi, and M. Tarigan, "Internet of Things ; Model Moda Layanan Sistem Transportasi Internet of Vehicle," *QoS*, 2022.
- [3] H. P. Hanifah, "Survey of Future Internet of Thing," *ITEJ*, vol. 5, no. 1, 2020.
- [4] F. A. Rafrastara, W. Khozi, and A. Wardoyo, "Deteksi Serangan berbasis Machine Learning pada Internet of Vehicle," *Seminar Nasional Informatika-FTI UPGRIS*, vol. 2, 2024.
- [5] R. A. Khairulah and R. Herdianto, "Klasifikasi Serangan Pada Jaringan Internet of Thing (IoT): Tinjauan Literatur Komparatif," *Jurnal Inovasi Teknologi dan Edukasi*, vol. 3, no. 2, pp. 47–53, 2023.
- [6] R. U. and F. R. J. Fahana, "Pemanfaatan Telegram Sebagai Notifikasi Serangan untuk Keperluan Forensik Jaringan," *jurnal Sistem Informasi*, vol. 5341, no. 6, 2017.
- [7] R. Hermawan, "ANALISIS KONSEP DAN CARA KERJA SERANGAN KOMPUTER DISTRIBUTED DENIAL OF SERVICE (DDOS)," 2015.
- [8] M. Zidane, "Klasifikasi Serangan Distributed Denial-of-Service (DDoS) menggunakan Metode Data Mining Naïve Bayes," 2022. [Online]. Available: <http://j-ptiik.ub.ac.id>
- [9] H. Alamsyah and A. Al Akbar, "Analisa Keamanan Jaringan Menggunakan Network Intrusion Detection and Prevention System," 2018.
- [10] S. Ilahiyah and A. Nilogiri, "Implementasi Deep Learning Pada Identifikasi Jenis Tumbuhan Berdasarkan Citra Daun Menggunakan Convolutional Neural Network," *JUSTINDO (Jurnal Sistem dan Teknologi Informasi Indonesia)*, vol. 3, no. 2, pp. 49–56, 2018.
- [11] "Institute of Electrical and Electronics Engineers, SSH and FTP brute-force Attacks Detection in Computer Networks: L STM and Machine Learning Approaches Md."
- [12] G. M. W. and G. N. K. S. K. Wanjau, "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.
- [13] A. A. Kurniawan, "Intrusion Detection System Menggunakan Deep Learning Untuk Deteksi Serangan DoS," pp. 39–57, 2020.
- [14] M. Zidane, "Klasifikasi Serangan Distributed Denial-of-Service (DDoS) menggunakan Metode Data Mining Naïve Bayes," 2022. [Online]. Available: <http://j-ptiik.ub.ac.id>
- [15] R. U. and F. R. M. Aziz, "Implemetasi Jaringan Saraf Tiruan untuk Mendeteksi Serangan DDoS pada Forensik Jaringan," *QUERY J. Sist. Inf.*, vol. 3, no. 1, pp. 46–52, 2019.
- [16] J. Elektronik and I. Komputer Udayana, "Klasifikasi Serangan Distributed Denial of Service (DDoS) Menggunakan Random Forest dengan CFS", [Online]. Available: www.unb.ca.

- [17] 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.
- [18] R. Hermawan, "ANALISIS KONSEP DAN CARA KERJA SERANGAN KOMPUTER DISTRIBUTED DENIAL OF SERVICE (DDOS)," vol. 5, no. 1, pp. 1–14, 1979.
- [19] Y. S. and S. I. B. Arifwidodo, "Analisis Kinerja Mikrotik Terhadap Serangan Brute Force Dan DDoS," *Techno.Com*, vol. 20, no. 3, pp. 392–399, 2021.
- [20] M. A. N. Anargya, W. Khozi, and F. A. Rafrastara, "Random Under Sampling for Performance Improvement in Attack Detection on Internet of Vehicles Using Machine Learning," *Jurnal Informatika: Jurnal Pengembangan IT*, vol. 10, no. 1, pp. 11–19, Jan. 2025, doi: 10.30591/jpit.v10i1.8034.
- [21] H. , et al Guo, "Cybersecurity Challenges in Internet of Vehicles: A Review",," *Vehicular Communications*, vol. 37, p. 100481, 2023.
- [22] Y. , & L. J. Li, "A Survey of Internet of Vehicles: Architectures, Enabling Technologies, Security and Privacy, and Applications," *IEEE Internet Things J*, vol. 8, no. 6, pp. 4250–4291, 2021.
- [23] I. Meiditra, "Analisis Dan Perancangan Private Cloud Storage Menggunakan Metode Pengamanan Ids (Intrusion Detection System) Dan Ips(Intrusion Prevention System) (Studi Kasus: Diskominfo Kota Padang Panjang)," *Riau Journal of Computer Science*, vol. 9, no. 2, pp. 124–133, 2023.
- [24] M. K. Riskilah and F. A. Yulianto, "Studi Analisis Algoritma Naïve Bayes Untuk Sistem Deteksi Intrusi Pada Internet Of Things," *e-Proceeding of Engineering*, vol. 9, no. 3, pp. 2177–2189, 2022.
- [25] I. F. and R. A. P. A. Nugroho, "Implementasi Deep Learning Menggunakan Convolutional Neural Network (CNN) Pada Ekspresi Manusia," *Algor*, vol. 2, no. 1, pp. 12–21, 2020.
- [26] "J. Nurhakiki et al., 'Studi Kepustakaan: Pengenalan 4 Algoritma Pada Pembelajaran Deep Learning Beserta Implikasinya,' Jurnal Pendidikan Berkarakter, no. 1, pp. 270–281, 2024, doi: 10.51903/pendekar.v2i1.598."
- [27] "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."
- [28] "Muhammad Haris Diponegoro, Sri Suning Kusumawardani, and Indriana Hidayah, 'Tinjauan Pustaka Sistematis: Implementasi Metode Deep Learning pada Prediksi Kinerja Murid,' Jurnal Nasional Teknik Elektro dan Teknologi Informasi, vol. 10, no. 2, pp. 131–138, 2021, doi: 10.22146/jnteti.v10i2.1417."
- [29] "R. A. Tilasefana and R. E. Putra, 'Penerapan Metode Deep Learning Menggunakan Algoritma CNN Dengan Arsitektur VGG NET Untuk Pengenalan Cuaca,' JINACS (Journal of Informatics and Computer Science), vol. 05, no. 1, pp. 48–57, Jun. 2023."
- [30] M. S. N. Agustina Purwitasari, "Implementasi Algoritma Artificial Neural . Network Dalam Pembuatan Chatbot Menggunakan Pendekatan Natural Language Processing," *IPTEK (Jurnal Ilmu Pengetahuan dan Teknologi*, vol. 6, no. 1, pp. 14–21, Mar. 2022.

- [31] H. F. Fadli and A. F. Hidayatullah, "Identifikasi Cyberbullying pada Media Sosial Twitter Menggunakan Metode LSTM dan BILSTM," *AUTOMATA (Ajang Untuk Tugas Akhir oleh Mahasiswa Informatika)*, vol. 2, no. 1, 2020.
- [32] D. S. and A. R. S. Sen, "Komparasi Metode Multilayer Perceptron (MLP) dan Long Short Term Memory (LSTM) dalam Peramalan Harga Beras," *ULTIMATICS (Jurnal Teknik Informatika)*, vol. 12, no. 1, pp. 34–41, Jun. 2020.
- [33] H. Zakaria Yahya and Y. Ramdhani, "Klasifikasi Bumbu Dapur Pasar Menggunakan Metode Deep Neural Network Berbasis Android," *JNKTII (Jurnal Nasional Komputasi dan Teknologi Informasi)*, vol. 6, no. 1, pp. 19–23, Feb. 2023.
- [34] "S. Adiningsi and R. A. Saputra, 'IDENTIFIKASI JENIS DAUN TANAMAN OBAT MENGGUNAKAN METODE CONVOLUTIONAL NEURAL NETWORK (CNN) DENGAN MODEL VGG16,' pp. 451–460, 2020."
- [35] M. T. A. Syech Ahmad and B. Sugiarto, "Implementasi Convolutional Neural Network (CNN) untuk Klasifikasi Ikan Cupang Berbasis Mobile," *Digital Transformation Technology*, vol. 3, no. 2, pp. 712–723, Dec. 2023, doi: 10.47709/digitech.v3i2.3245.
- [36] M. Zahir and R. Adi Saputra, "DETEKSI PENYAKIT RETINOPATI DIABETES MENGGUNAKAN CITRA MATA DENGAN IMPLEMENTASI DEEP LEARNING CNN," 2024. [Online]. Available: <https://www.kaggle.com/datasets/gunavenkatdoddi/eye-diseases-classification>
- [37] N. Q. Do, A. Selamat, O. Krejcar, T. Yokoi, and H. Fujita, "Phishing webpage classification via deep learning-based algorithms: An empirical study," *Applied Sciences (Switzerland)*, vol. 11, no. 19, Oct. 2021, doi: 10.3390/app11199210.
- [38] M. F. Ansari, P. Kasproski, and M. Obetkal, "Gaze tracking using an unmodified web camera and convolutional neural network," *Applied Sciences (Switzerland)*, vol. 11, no. 19, Oct. 2021, doi: 10.3390/app11199068.
- [39] D. Gunawan and H. Setiawan, "Convolutional Neural Network dalam Analisis Citra Medis," 2022.
- [40] Ridwan Nazar, "IMPLEMENTASI PEMROGRAMAN PYTHON MENGGUNAKAN GOOGLE COLAB," vol. 15, 2024.
- [41] R. Andarsyah and A. Yanuar, "SENTIMEN ANALISIS APLIKASI POSAJA PADA GOOGLE PLAYSTORE UNTUK PENINGKATAN POSPAY SUPERAPP MENGGUNAKAN SUPPORT VECTOR MEACHINE," 2024.
- [42] R. Gelar Guntara, "Pemanfaatan Google Colab Untuk Aplikasi Pendeteksian Masker Wajah Menggunakan Algoritma Deep Learning YOLOv7," *Jurnal Teknologi Dan Sistem Informasi Bisnis*, vol. 5, no. 1, pp. 55–60, Feb. 2023, doi: 10.47233/jteksis.v5i1.750.
- [43] "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."
- [44] "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."

- [45] “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.”.
- [46] “S. H. Park, H. J. Park, and Y. J. Choi, ‘RNN-based Prediction for Network Intrusion Detection,’ 2020 International Conference on Artificial Intelligence in Information and Communication, ICAIIC 2020, pp. 572–574, 2020, doi: 10.1109/ICAIIIC48513.2020.9065249.”.
- [47] “M. Q. Syahputra, D. R. Akbi, and D. Risqiwati, ‘Deteksi Dan Mitigasi Serangan DDoS Pada Software Defined Network Menggunakan Algoritma Decision Tree,’ *Jurnal Repositor*, vol. 2, no. 11, p. 1491, 2020, doi: 10.22219/repositor.v2i11.795.”.
- [48] “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, 2020, doi: 10.33633/tc.v19i1.2860.”.
- [49] “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.”.
- [50] “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.”.
- [51] L. Ikhwanul Uzlah and R. Adi Saputra, “DETEKSI SERANGAN SIBER PADA JARINGAN KOMPUTER MENGGUNAKAN METODE RANDOM FOREST,” 2024. [Online]. Available: <https://bit.ly/CyberSecurityAttacks>.
- [52] E. O. Nasution and A. Basuki, “Implementasi Algoritme C5.0 Untuk Klasifikasi Serangan DDoS,” 2021. [Online]. Available: <http://j-ptiik.ub.ac.id>