BIBLIOGRAPHY

[1] Petroc Taylor, "Number of Internet of Things (IoT) connections worldwide from 2022 to 2023, with forecasts from 2024 to 2034," statista. Accessed: Dec. 01, 2025. [Online]. Available: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

[2] A. A. Alahmadi *et al.*, "DDoS Attack Detection in IoT-Based Networks Using Machine Learning Models: A Survey and Research Directions," Jul. 01, 2023, *Multidisciplinary Digital Publishing Institute (MDPI)*. doi: 10.3390/electronics12143103.

[3] M. S. Ranjana *et al.*, "Challenges of Securing IOT Devices: A Big Data Approach to Cyber Risk Reduction," Jun. 2025. [Online]. Available: www.ijert.org

[4] M. Aziz Al Kabir, W. Elmedany, and M. S. Sharif, "Securing IoT Devices Against Emerging Security Threats: Challenges and Mitigation Techniques," 2023, *Taylor and Francis Ltd.* doi: 10.1080/23742917.2023.2228053.

[5] J. P. Omer Yoachimik, "4.2 Tbps of bad packets and a whole lot more: Cloudflare's Q3 DDoS report," cloudflare. Accessed: Dec. 01, 2025. [Online]. Available: https://blog.cloudflare.com/ddos-threat-report-for-2024-q3/

[6] awanpintar.id, "Laporan Semester 1 Tahun 2025," Aug. 2025. Accessed: Nov. 30, 2025. [Online]. Available: https://www.awanpintar.id/publikasi/

[7] C. Singh and A. K. Jain, "A comprehensive survey on DDoS attacks detection & mitigation in SDN-IoT network," *e-Prime - Advances in Electrical Engineering, Electronics and Energy*, vol. 8, Jun. 2024, doi: 10.1016/j.prime.2024.100543.

[8] K. Al-Begain, M. Khan, B. Alothman, C. Joumaa, and E. Alrashed, "A DDoS Detection and Prevention System for IoT Devices and Its Application to Smart Home Environment," *Applied Sciences (Switzerland)*, vol. 12, no. 22, Nov. 2022, doi: 10.3390/app122211853.

[9] S. H. Lee, Y. L. Shiue, C. H. Cheng, Y. H. Li, and Y. F. Huang, "Detection and Prevention of DDoS Attacks on the IoT," *Applied Sciences (Switzerland)*, vol. 12, no. 23, Dec. 2022, doi: 10.3390/app122312407.

[10] Y. Meidan, D. Avraham, H. Libhaber, and A. Shabtai, "CADeSH: Collaborative Anomaly Detection for Smart Homes," Mar. 2023, doi: 10.1109/JIOT.2022.3194813.

[11] S. Shakya and R. Abbas, "A Comparative Analysis of Machine Learning Models for DDoS Detection in IoT Networks," Nov. 2024, [Online]. Available: http://arxiv.org/abs/2411.05890

[12] N. Tekin, A. Acar, A. Aris, A. S. Uluagac, and V. C. Gungor, "Energy consumption of on-device machine learning models for IoT intrusion detection," *Internet of Things (Netherlands)*, vol. 21, Apr. 2023, doi: 10.1016/j.iot.2022.100670.

[13] H. A. Sakr, M. M. Fouda, A. F. Ashour, A. Abdelhafeez, M. I. El-Afifi, and M. Refaat Abdellah, "Machine learning-based detection of DDoS attacks on IoT devices in multi-energy systems," *Egyptian Informatics Journal*, vol. 28, Dec. 2024, doi: 10.1016/j.eij.2024.100540.

[14] A. Hussain, E. Marin Tordera, X. Masip-Bruin, and H. C. Leligou, "Rule-Based With Machine Learning IDS for DDoS Attack Detection in Cyber-Physical Production Systems (CPPS)," *IEEE Access*, vol. 12, pp. 114894–114911, 2024, doi: 10.1109/ACCESS.2024.3445261.

[15] N. Gavric, G. Prasad Bhandari, and A. Shalaginov, “Towards Resource-Efficient DDoS Detection in IoT: Leveraging Feature Engineering of System and Network Usage Metrics,” *Journal of Network and Systems Management*, vol. 32, no. 4, Oct. 2024, doi: 10.1007/s10922-024-09848-2.
[16] M. Nawaz, S. Tahira, D. Shah, S. Ali, and M. Tahir, “Lightweight machine learning framework for efficient DDoS attack detection in IoT networks,” *Sci. Rep.*, vol. 15, no. 1, Dec. 2025, doi: 10.1038/s41598-025-10092-0.
[17] “Raspberry Pi 4 Model B Specifications.,” Raspberry Pi Foundation. Accessed: Dec. 01, 2025. [Online]. Available: https://www.raspberrypi.com/products/raspberry-pi-4-model-b/specifications/
[18] O. Mitchell and C. Osazuwa, “Confidentiality, Integrity, and Availability in Network Systems: A Review of Related Literature,” 2023.
[19] A. Thakkar and R. Lohiya, “A Review on Machine Learning and Deep Learning Perspectives of IDS for IoT: Recent Updates, Security Issues, and Challenges,” *Archives of Computational Methods in Engineering*, vol. 28, no. 4, pp. 3211–3243, Jun. 2021, doi: 10.1007/s11831-020-09496-0.
[20] E. Džaferović, A. Sokol, A. A. Almisreb, and S. M. Norzeli, “DoS and DDoS vulnerability of IoT: A review,” 2020.
[21] U. Persada Indonesia, L. Saroha, R. Octavianto, E. Malays, and S. Sakti, “Pencegahan Dan Konsep IDS (Intrusion Detection System) Dalam Mendeteksi Serangan Siber Pada Sistem Keamanana Di”, doi: 10.37817/tekinfo.v25i1.
[22] M. Ulfa *et al.*, “Implementasi Intrusion Detection System (Ids) Di Jaringan Universitas Bina Darma,” 2013.
[23] A. Visioli, “Editorial: Insights in control and automation systems,” *FronTiers in Control Engineering*, vol. 4, Jun. 2023, doi: 10.3389/fcteg.2023.1228462.
[24] S. Latif, Z. Zou, Z. Idrees, and J. Ahmad, “A Novel Attack Detection Scheme for the Industrial Internet of Things Using a Lightweight Random Neural Network,” *IEEE Access*, vol. 8, pp. 89337–89350, 2020, doi: 10.1109/ACCESS.2020.2994079.
[25] R. Widodo and I. Riadi, “Intruder Detection Systems on Computer Networks Using Host Based Intrusion Detection System Techniques,” *Buletin Ilmiah Sarjana Teknik Elektro*, vol. 3, no. 1, pp. 21–30, Apr. 2021, doi: 10.12928/biste.v3i1.1752.
[26] S. Kasus dan Implementasi Menggunakan Python Edisi, “MACHINE LEARNING Ibnu Daqiqil ID.”
[27] L. Muflikhah, W. Mahmudy, and D. Kurnianingtyas, *Machine Learning*. Universitas Brawijaya Press, 2023. [Online]. Available: https://books.google.co.id/books?id=tu_uEAAAQBAJ
[28] A. Agung, A. Daniswara, I. Kadek, and D. Nuryana, “Data Preprocessing Pola Pada Penilaian Mahasiswa Program Profesi Guru,” *Journal of Informatics and Computer Science*, vol. 05, 2023.
[29] W. Sudrajat and I. Cholid, “K-NEAREST NEIGHBOR (K-NN) UNTUK PENANGANAN MISSING VALUE PADA DATA UMKM,” 2023.
[30] A. F. Hidayatullah, A. Dwi Prasetyo, D. P. Sari, and I. Pratiwi, “Analisis Kualitas Data dan Klasifikasi Data Pasien Kanker,” 2014. [Online]. Available: https://archive.ics.uci.edu.
[31] M. R. Kusnaidi, T. Gulo, and S. Aripin, “Penerapan Normalisasi Data Dalam Mengelompokkan Data Mahasiswa Dengan Menggunakan Metode K-Means Untuk Menentukan Prioritas Bantuan Uang Kuliah Tunggal,” *Journal of*

Computer System and Informatics (JoSYC), vol. 3, no. 4, pp. 330–338, Sep. 2022, doi: 10.47065/josyc.v3i4.2112.

[32] P. Palinggik Allorerung, A. Erna, M. Bagussahrir, and S. Alam, "Analisis Performa Normalisasi Data untuk Klasifikasi K-Nearest Neighbor pada Dataset Penyakit," 2024.

[33] M. Guntara and F. D. Astuti, "Komparasi Kinerja Label-Encoding dengan One-Hot-Encoding pada Algoritma K-Nearest Neighbor menggunakan Himpunan Data Campuran," *JIKO (Jurnal Informatika dan Komputer)*, vol. 9, no. 2, p. 352, Jun. 2025, doi: 10.26798/jiko.v9i2.1605.

[34] D. Azzahra Nasution, H. H. Khotimah, and N. Chamidah, "PERBANDINGAN NORMALISASI DATA UNTUK KLASIFIKASI WINE MENGGUNAKAN ALGORITMA K-NN," 2019.

[35] M. Mahendra Alvanof and R. Kesuma Dinata, "Penerapan Algoritma Random Forest dalam Deteksi dan Klasifikasi Ransomware," 2024.

[36] A. Maulana, Inayah Khasnaputri Afifah, Asghafi Mubarrak, Kiagus Rachmat Fauzan, Ardhan Dwintara, and B. P. Zen, "COMPARISON OF LOGISTIC REGRESSION, MULTINOMIALNB, SVM, AND K-NN METHODS ON SENTIMENT ANALYSIS OF GOJEK APP REVIEWS ON THE GOOGLE PLAY STORE," *Jurnal Teknik Informatika (Jutif)*, vol. 4, no. 6, pp. 1487–1494, Dec. 2023, doi: 10.52436/1.jutif.2023.4.6.863.

[37] M. F. Rahman, M. Ilham Darmawidjadja, and D. Alamsah, "KLASIFIKASI UNTUK DIAGNOSA DIABETES MENGGUNAKAN METODE BAYESIAN REGULARIZATION NEURAL NETWORK (RBNN)," 2017.

[38] M. Johnston and C. H. Liu, "A Raspberry Pi Based Intrusion Detection System for Smart Home IoT Networks," in *2022 IEEE International Conference on Consumer Electronics (ICCE)*, Las Vegas, NV, USA, Jan. 2022, pp. 1–6. doi: 10.1109/ICCE50685.2021.9427586.

[39] J. Wunder, A. Gropengiesser, A. Hotop, C. Eichenmüller, and F. Freiling, "Shedding Light on CVSS Scoring Inconsistencies: A User-Centric Study on Evaluating Widespread Security Vulnerabilities," in *2024 IEEE Symposium on Security and Privacy (SP)*, 2024, pp. 1–18. doi: 10.1109/SP54263.2024.00131.

[40] A. P. Singh and J. Kaur, "A Study of CVSS v4.0: A CVE Scoring System," in *2024 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS)*, 2024, pp. 1–6. doi: 10.1109/SCEECS61402.2024.10397701.

[41] D. R. Tisna, T. Maharani, and K. T. Nugroho, "PEMANFAATAN CHATBOT TELEGRAM UNTUK MONITORING DAN KONTROL KUALITAS AIR MENGGUNAKAN ESP32," *JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, vol. 9, no. 3, pp. 1292–1306, Aug. 2024, doi: 10.29100/jipi.v9i3.5329.

[42] R. W. Beggs, *Mastering Kali Linux for Advanced Penetration Testing*, 4th ed. Packt Publishing, 2023.

[43] G. Najera-Gu*Tier*rez and J. A. Ansari, "A Review of Kali Linux as a Penetration Testing Platform," in *2023 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*, 2023, pp. 396–401. doi: 10.1109/ICCCIS60361.2023.10425053.

[44] M. S. Hawari and I. F. Kurniawan, "PENERAPAN IPTABLES FIREWALL PADA LINUX DENGAN MENGGUNAKAN FEDORA," 2016.

[45] A. Hussain and others, “A Systematic Approach of Analysing Network Traffic Using Packet Sniffing with Scapy Framework,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 15, no. 4, pp. 234–245, 2024, doi: 10.14569/IJACSA.2024.01504025.
[46] Scapy Project, “Scapy: the Python-based interactive packet manipulation program & library,” 2025.
[47] V. Mavani and others, “Automated Network Vulnerability Assessment with Nmap: A Comprehensive Approach,” in *2025 IEEE International Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation (IATMSI)*, 2025, pp. 1–6. doi: 10.1109/IATMSI60426.2025.10918528.
[48] M. K. Viswanath, M. V Saritha, and R. M. Ponnuvel, “A Case Study Using Companies to Examine the Nmap Tool’s Applicability for Network Security Assessment,” in *2023 7th International Conference on Electronics, Communication and Aerospace Technology (ICECA)*, 2023, pp. 1–6. doi: 10.1109/ICECA58529.2023.10249544.
[49] S. Sanfilippo, “hping3 – Active Network Security Tool,” 2024.
[50] C. Kemp, C. Calvert, T. M. Khoshgoftaar, and J. L. Leevy, “An Approach to Application-Layer DoS Detection,” *J. Big Data*, vol. 10, pp. 1–30, 2023, doi: 10.1186/s40537-023-00699-3.
[51] S. Sood and N. Hubballi, “slowTrack: Detecting Slow *Rate* Denial of Service Attacks Against HTTP with Behavioral Parameters,” *J. Supercomput.*, vol. 80, pp. 1788–1817, 2024, doi: 10.1007/s11227-023-05453-3.