## DAFTAR PUSTAKA


Agustina, T., Masrizal, M., & Irmayanti, I. (2024). Performance Analysis of Random Forest Algorithm for Network Anomaly Detection using Feature Selection. *Sinkron*, *8*(2). https://doi.org/10.33395/sinkron.v8i2.13625

Almaiah, M. A., & Kadel, R. (2025). Leveraging ACO, GA, and GWO for Enhancing Port Scan Attack Detection Using Machine Learning. *Journal of Cyber Security and Risk Auditing*, *2025*(4), 306–326. https://doi.org/10.63180/j

Azhari, F., Hananto, B., & Ernawati, I. (2025). Perbandingan Kinerja Algoritma dalam Klasifikasi Serangan DDoS Berdasarkan Data CIC IoMT Dataset. *Jurnal Informatic*, *21*(2), 115–127. https://doi.org/https://doi.org/10.52958/iftk.v21i2.11467

Bourgeois, D., Mortati, J., Wang, S., & Smith, J. (2019). *Information Systems for Business and Beyond (2019)*.

Brownlee, J. (2020). *Imbalanced Classification with Python Choose Better Metrics, Balance Skewed Classes, and Apply Cost-Sensitive Learning*.

Chan, Y. Y., Ismail, I. B., & Khammas, B. M. (2021). Online Traffic Classification for Malicious Flows using Efficient Machine Learning Techniques. *Telkomnika (Telecommunication Computing Electronics and Control)*, *19*(4), 1396–1406. https://doi.org/10.12928/TELKOMNIKA.v19i4.20402

Chandra, S. D., Oktavianto, H., & Wardoyo, A. E. (2024). Klasifikasi Malware Menggunakan Metode Convolutional Neural Network (CNN) Berbasis Website. *Jurnal Penelitian Teknologi Informasi dan Sains*, *2*(2), 84–99. https://doi.org/10.54066/jptis.v2i2.1931

Dei, H., Shvets, D., Lytvyn, N., Sytnichenko, O., & Kobus, O. (2024). Legal Challenges and Perspectives of Cybersecurity in the System of State Governance of Educational Institutions in Ukraine. *Journal of Cyber Security and Mobility*, *13*(5), 963–982. https://doi.org/10.13052/jcsm2245-1439.1357

Diogenes, Y., & Ozkaya, E. (2018). *Cybersecurity, Attack and Defense Strategies : Infrastructure Security with Red Team and Blue Team tactics*. Packt Publishing.

Duarte, J. D., Bispo, G. D., Pimenta Rodrigues, G. A., Marques Serrano, A. L., Mayumi Saiki, G., & Gonçalves, V. P. (2025). Synthetic Minority Over-sampling Technique for detecting Malicious Traffic targeting Internet of Things' devices. *Journal of Internet Services and Applications*, *16*(1), 332–344. https://doi.org/10.5753/jisa.2025.5251

Géron, A. (2019). *Hands on Machine Learning with Scikit-Learn, Keras, and TensorFlow : Concepts, Tools, and Techniques to Build Intelligent systems*. O'Reilly Media, Inc.

Hartono, Khotimah, K., & Maharjan, R. (2025). Improving Detection Accuracy of Brute-Force Attacks on MariaDB Using Standard Isolation Forest: A Comparative Analysis with RotatedVariant. *Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer*, *25*(1), 145–160. https://doi.org/10.30812/matrik.v25i1.5817

Inayah, K., & Ramli, K. (2024). Analisis Kinerja Intrusion Detection Sistem Berbasis Algoritma Random Forest Menggunakan Dataset Unbalanced Honeynet BSSN. *Jurnal Teknologi Informasi dan Ilmu Komputer*, *4*(11), 867–876. https://doi.org/10.25126/jtiik1148911

Islamey, R., Winiarti, S., & Riadi, I. (2026). Analisis Komparatif Random Forest dan Support Vector Machine untuk Klasifikasi Tingkat Keparahan Serangan Siber. *Euler : Jurnal Ilmiah Matematika, Sains dan Teknologi*, *14*(1), 1–14. https://doi.org/10.37905/euler.v14i1.36558

Jariwala, M. (2023). *The Cyber Security Roadmap A Comprehensive Guide to Cyber Threats, Cyber Laws, and Cyber Security Training for a Safer Digital World Content at a Glance*.

Kumar, J., Rajendran, B., & Sudarsan, S. D. (2024). Zero-Day Malware Classification and Detection Using Machine Learning. *SN Computer Science*, *5*(1). https://doi.org/10.1007/s42979-023-02404-w

Lanka, P., Gupta, K., & Varol, C. (2024). Intelligent Threat Detection—AI-Driven Analysis of Honeypot Data to Counter Cyber Threats. *Electronics*, *13*(13). https://doi.org/10.3390/electronics13132465

Lanz, S., Pignol, S. L. R., Schmitt, P., Wang, H., Papaioannou, M., Choudhary, G., & Dragoni, N. (2025). Optimizing Internet of Things Honeypots with Machine Learning: A Review. Dalam *Applied Sciences (Switzerland)* (Vol. 15, Nomor 10). Multidisciplinary Digital Publishing Institute (MDPI). https://doi.org/10.3390/app15105251

Li, Y., Yin, J., & Chen, L. (2023). Informative pseudo-labeling for graph neural networks with few labels. *Data Mining and Knowledge Discovery*, *37*(1), 228–254. https://doi.org/10.1007/s10618-022-00879-4

Ma, Y., & Tang, J. (2020). *Deep Learning on Graphs*. https://yaoma24.github.io/dlg_book/

Mc Cabe, M., & Houmb, S. H. (2026). Enhancing the MITRE ATT&CK® Framework for Cyber-Physical Systems Using Insights from Advanced Persistent Threats. *Applied Sciences*, *16*(4), 1815. https://doi.org/10.3390/app16041815

Morić, Z., Dakić, V., & Regvart, D. (2025). Advancing Cybersecurity with Honeypots and Deception Strategies. *Informatics*, *12*(1). https://doi.org/10.3390/informatics12010014

NIST. (2012). *Guide for Conducting Risk Assessments*. https://doi.org/10.6028/NIST.SP.800-30r1

Oosterhof, M. (2026). *Cowrie Documentation*.

Permana, A. A., S Wahyuddin, Santoso, L. W., Wibowo, G. W. N., Wardhani, A. K., Rahmaddeni, Wahidin, A. J., Yuliastuti, G. E., Elisawati, Wijayanti, R. R., Abdurrasyid, Elisawati, Y., Rizqi, R., & Abdurrasyid, W. (2023). *Machine Learning*. www.globaleksekutifteknologi.co.id

Purnomo, A., Kurniasih, A., Nuarminah, A., & Hartati, S. (2024). Peran Artificial Intelligence dalam Deteksi Dini Ancaman Keamanan Jaringan. *Jurnal Minfo Polgan*, *13*(2), 2044–2048. https://doi.org/10.33395/jmp.v13i2.14356

Ragsdale, J., & Boppana, R. V. (2023). On Designing Low-Risk Honeypots Using Generative Pre-Trained Transformer Models with Curated Inputs. *IEEE Access*, *11*, 117528–117545. https://doi.org/10.1109/ACCESS.2023.3326104

Rahayu Ade. (2025). Metode Penelitian dan Pengembangan (R&D) : Pengertian, Jenis dan Tahapan. *DIAJAR: Jurnal Pendidikan dan Pembelajaran*, *4*(3), 459–470. https://doi.org/10.54259/diajar.v4i3.5092

Raza, M. N. (2024). Sistem Deteksi Berita Hoax menggunakan Algoritma Naive Bayes dan Random Forest pada Machine Learning. *Pondasi: Journal of Applied Science Engineering*, *1*(2), 43–57. https://journal.alshobar.or.id/index.php/pondasi/article/view/221

Reiber, J., & Wright, C. (2021). *MITRE ATT&CK for Dummies*.

Rinandi, F. R., Heryanto, H., & Wiyatmoko, K. (2023). Deteksi Dini Siswa Bermasalah menggunakan Metode Random Forest di SMK Muhammadiyah 3 Banjarmasin. *Jurnal Sistem dan Teknologi Informasi*, *9*(1), 1–7.

Risal, Z., Hakim, R., & Abdullah, A. R. (2022). *Metode Penelitian dan Pengembangan Research and Development (R&D) Konsep, Teori-Teori, dan Desain Penelitian* (Z. R. Bahar, Ed.).

Saadon, M., & Behadili, S. F. (2026). One-Class and Multi-Class Malware Classification Using Hybrid and Supervised Machine Learning Techniques. *Iraqi Journal of Science*, *67*(2), 1110–1124. https://doi.org/10.24996/ijs.2025.67.2.37

Sargsyan, G., Kavallieros, D., & Kolokotronis, N. (2022). Security Technologies and Methods for Advanced Cyber Threat Intelligence, Detection and Mitigation. Dalam *Security Technologies and Methods for Advanced Cyber Threat Intelligence, Detection and Mitigation*. Now Publishers. https://doi.org/10.1561/9781680838350

Sinaga, N. H., Irmayani, D., & Hasibuan, M. N. S. (2024). Mengoptimalkan Keamanan Jaringan: Memanfaatkan Kecerdasan Buatan Untuk Meningkatkan Deteksi Dan Respon Ancaman. *Jurnal Ilmu Komputer Dan Sistem Informasi (JIKOMSI)*, *7*(2), 364–369. https://ejournal.sisfokomtek.org/index.php/jikom/article/view/3582

Takur, A. (2020). *Approaching (Almost) Any Machine Learning Problem*. https://github.com/abhishekkrthakur/approachingalmost/blob/master/AAAMLP.pdf

Tjahjono, B., Ardiansyah, M., Firmansyah, G., & Akbar, H. (2023). *Risk Management of Information System in DISKOMINFO Statistic and Encoding using NIST SP 800-30*. *9*(1). https://doi.org/10.33480/jitk.v9i1.4080

Vaasudevan, J., Manukonda, H., Pallakonda, A., Raj, R. D. A., Yanamala, R. M. R., Nazari, R., & Krishna Prakasha, K. (2025). A Holistic Framework for Cyber Attack Detection, Classification, and Security Enhancement of DNP3 Protocol in Smart Grids. *IEEE Access*. https://doi.org/10.1109/ACCESS.2025.3636010

Verdonck, T., Baesens, B., Óskarsdóttir, M., & vanden Broucke, S. (2024). Special issue on feature engineering editorial. *Machine Learning*, *113*(7), 3917–3928. https://doi.org/10.1007/s10994-021-06042-2

Verizon. (2024). *2024 Data Breach Investigations Report*.

Wang, S., Tu, C., Zhang, Y., Zhang, M., & Xue, P. (2025). Mapping Cyber Bot Behaviors: Understanding Payload Patterns in Honeypot Traffic. *Sensors*, *26*(1). https://doi.org/10.3390/s26010011

Zheng, A. (2015). *Evaluating Machine Learning Models A Beginner's Guide to Key Concepts and Pitfalls*.