

DAFTAR PUSTAKA

- [1] D. Canavese, L. Mannella, L. Regano, and C. Basile, “Security at the Edge for Resource-Limited IoT Devices,” *Sensors*, vol. 24, no. 2, Jan. 2024, doi: 10.3390/s24020590.
- [2] E. Schiller, A. Aidoo, J. Fuhrer, J. Stahl, M. Ziörjen, and B. Stiller, “Landscape of IoT security,” *Comput Sci Rev*, vol. 44, p. 100467, 2022.
- [3] M. S. Rafsanjani, V. Suryani, and R. R. Pahlevi, “Deteksi Serangan Botnet Pada Jaringan Internet of Things Menggunakan Algoritma Random Forest (RF),” *e-Proceeding of Engineering*, vol. 9, no. 3, pp. 1862–1871, 2022.
- [4] S. 'Jose, “Zscaler ThreatLabz Finds a 400% Increase in IoT and OT Malware Attacks Year-over-Year, Underscoring Need for Better Zero Trust Security to Protect Critical Infrastructures.”
- [5] D. 'Kalinin, “WhatsApp spy mod spreads through Telegram, attacks Arabic-speaking users.”
- [6] C. Menteng, A. Setyanto, and H. Al Fatta, “MODEL DETEKSI SERANGAN SSH-BRUTE FORCE BERDASARKAN DEEP BELIEF NETWORK,” *Jurnal Teknologi Informasi*, vol. 17, no. 2, pp. 101–110, 2023, doi: 10.47111/JTI.
- [7] I. Alkhwaja *et al.*, “Password Cracking with Brute Force Algorithm and Dictionary Attack Using Parallel Programming,” *Applied Sciences (Switzerland)*, vol. 13, no. 10, May 2023, doi: 10.3390/app13105979.
- [8] F. Riza, “Sistem Deteksi Intrusi pada Server secara Realtime Menggunakan Seleksi Fitur dan Firebase Cloud Messaging,” *Jurnal Sistim Informasi dan Teknologi*, Sep. 2022, doi: 10.37034/jsisfotek.v5i1.161.
- [9] Suci Amaliah, M. Nusrang, and A. Aswi, “Penerapan Metode Random Forest Untuk Klasifikasi Varian Minuman Kopi di Kedai Kopi Konijiwa Bantaeng,” *VARIANSI: Journal of Statistics and Its application on Teaching and Research*, vol. 4, no. 3, pp. 121–127, Dec. 2022, doi: 10.35580/variantsium31.
- [10] H. Jeon and S. Oh, “Hybrid-recursive feature elimination for efficient feature selection,” *Applied Sciences (Switzerland)*, vol. 10, no. 9, May 2020, doi: 10.3390/app10093211.
- [11] E. Kharismadhany, M. Ruswiansari, and T. Harsono, “Brute-force Detection Using Ensemble Classification,” *INTEK Jurnal Penelitian*, vol. 9, no. 2, pp. 98–104, 2022, doi: 10.31963/intek.v9i2.3350.

- [12] A. A. Hamza and R. J. surayh Al-Janabi, "Detecting Brute Force Attacks Using Machine Learning," in *BIO Web of Conferences*, EDP Sciences, Apr. 2024. doi: 10.1051/bioconf/20249700045.
- [13] M. K. Riskilah, F. A. Yulianto, and E. M. Jadied, "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.
- [14] M. Rizal, D. E. Sondakh, I. F. Ashari, and M. A. Suryawan, *Konsep & Implementasi Internet of Things*. Kita Menulis, 2023.
- [15] G. M. I. Akbar, "DETEKSI SERANGAN PADA PROTOKOL MQTT IOT MENGGUNAKAN RANDOM FOREST," 2023.
- [16] D. Sawitri, "Internet Of Things Memasuki Era Society 5.0," *Jurnal Komputer, Informasi Teknologi, dan Elektro*, vol. 8, no. 1, 2023.
- [17] A. Junaidi, "INTERNET OF THINGS, SEJARAH, TEKNOLOGI DAN PENERAPANNYA : REVIEW," *Jurnal Ilmiah Teknologi Informasi Terapan*, vol. I, no. 3, 2015.
- [18] D. Hanes, G. Salgueiro, R. Barton, J. Henry, and P. Grossetete, *IoT fundamentals : networking technologies, protocols, and use cases for the Internet of Things*. Cisco Press, 2017.
- [19] F. Antony and R. Gustriansyah, "Deteksi Serangan Denial of Service pada Internet of Things Menggunakan Finite-State Automata," *MATRIK : Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer*, vol. 21, no. 1, pp. 43–52, Nov. 2021, doi: 10.30812/matrik.v21i1.1078.
- [20] S. Munawarah and E. Arip Winanto, "Jurnal Informatika Dan Rekayasa Komputer (JAKAKOM) Deteksi Serangan DDoS SYN Flood Pada Jaringan Internet of Things (IoT) Menggunakan Metode Deep Neural Network (DNN)," *Jurnal Informatika dan Rekayasa Komputer*, vol. 4, no. 1, pp. 982–990, 2024, doi: 10.33998/jakakom.v4i1.
- [21] S. Aprianti and H. Alamsyah, "Analisa Keamanan Jaringan Komputer Menggunakan Sistem Deteksi Intrusi Shorewall," *Jurnal Amplifier Mei*, vol. 13, 2023.
- [22] R. Manglik, *Intrusion Detection System*. EduGorilla Publication, 2024.
- [23] S. K. Wagh, V. K. Pachghare, and S. R. Kolhe, "Survey on Intrusion Detection System using Machine Learning Techniques," 2013.
- [24] C. John Ugochukwu and E. O. Bennett, "An Intrusion Detection System Using Machine Learning Algorithm," 2018. [Online]. Available: www.iiardpub.org
- [25] R. Bace, "An introduction to intrusion detection & assessment," *ICSA intrusion detection systems consortium white paper*, pp. 1–38, 1999.

- [26] K. KR and A. Indra, "Intrusion detection tools and techniques—a survey," *International Journal of Computer Theory and Engineering*, vol. 2, no. 6, pp. 1793–8201, 2010.
- [27] I. E. Maulani and A. F. Umam, "EVALUASI EFEKTIVITAS SISTEM DETEKSI INTRUSI DALAM MENJAMIN KEAMANAN JARINGAN," *Jurnal Sosial dan Teknologi*, vol. 3, no. 8, 2023.
- [28] D. Rodrigues, *LEARN HYDRA Master Password Cracking via Brute Force Across Multiple Services (SSH, FTP, HTTP, RDP)*. 2025.
- [29] A. Z. Agghey, L. J. Mwinuka, S. M. Pandhare, M. A. Dida, and J. D. Ndibwile, "Detection of username enumeration attack on ssh protocol: Machine learning approach," *Symmetry (Basel)*, vol. 13, no. 11, Nov. 2021, doi: 10.3390/sym13112192.
- [30] K. A. Prasetyo, M. Idhom, and H. E. Wahanani, "SISTEM PENCEGAHAN SERANGAN BRUTEFORCE PADA MULTIPLE SERVER DENGAN MENGGUNAKAN FAIL2BAN," 2020.
- [31] S. Sandra, D. Stiawan, and A. Heryanto, "Visualisasi Serangan Brute Force Menggunakan Metode K-Means dan Naïve Bayes," 2016. [Online]. Available: <http://ars.ilkom.unsri.ac.id>
- [32] S. Kahara Wanjau, G. M. Wambugu, and G. Ndung'u Kamau, "SSH-Brute Force Attack Detection Model based on Deep Learning," 2021. [Online]. Available: www.ijcat.com
- [33] J. Park, J. Kim, B. B. Gupta, and N. Park, "Network Log-Based SSH Brute-Force Attack Detection Model," *Computers, Materials and Continua*, vol. 68, no. 1, pp. 887–901, Mar. 2021, doi: 10.32604/cmc.2021.015172.
- [34] J. M. Stewart, E. Tittel, and M. Chappie, *CISSP: Certified Information Systems Security Professional Study Guide*. Wiley, 2005.
- [35] T. Gautam and U. Singh, "AN APPROACH FOR DETECTING PASSWORD PATTERN IN DICTIONARY ATTACK," 2022.
- [36] T. V Geetha and S. Sendhilkumar, *Machine Learning Concepts, Techniques and Applications*. CRC Press, 2023.
- [37] F. Provost, "On Applied Research in Machine Learning," *Kluwer Academic Publisher*, 1998.
- [38] B. Mahesh, "Machine Learning Algorithms - A Review," *International Journal of Science and Research (IJSR)*, vol. 9, no. 1, pp. 381–386, Jan. 2020, doi: 10.21275/art20203995.
- [39] Roland. Vogl, *Research handbook on big data law*. Edward Elgar Publishing Limited, 2021.

- [40] M. Pal and S. Parija, “Prediction of Heart Diseases using Random Forest,” in *Journal of Physics: Conference Series*, IOP Publishing Ltd, Mar. 2021. doi: 10.1088/1742-6596/1817/1/012009.
- [41] L. Breiman, “Random Forests,” *Kluwer Academic Pblisher*, vol. 45, pp. 5–32, 2001.
- [42] H. A. Salman, A. Kalakech, and A. Steiti, “Random Forest Algorithm Overview,” *Babylonian Journal of Machine Learning*, vol. 2024, pp. 69–79, Jun. 2024, doi: 10.58496/bjml/2024/007.
- [43] R. Genuer and J. M. Poggi, *Random Forests with R*. Springer International Publishing, 2020.
- [44] V. B. Canedo and A. A. Betanzos, *Recent Advances in Ensembles for Feature Selection*. Springer International Publishing, 2018.
- [45] P. Dhal and C. Azad, “A comprehensive survey on feature selection in the various fields of machine learning,” *Applied Intelligence*, vol. 52, no. 4, pp. 4543–4581, Mar. 2022, doi: 10.1007/s10489-021-02550-9.
- [46] E. Odhiambo Omuya, G. Onyango Okeyo, and M. Waema Kimwele, “Feature Selection for Classification using Principal Component Analysis and Information Gain,” *Expert Syst Appl*, vol. 174, Jul. 2021, doi: 10.1016/j.eswa.2021.114765.
- [47] N. Pudjihartono, T. Fadason, A. W. Kempa-Liehr, and J. M. O’Sullivan, “A Review of Feature Selection Methods for Machine Learning-Based Disease Risk Prediction,” 2022, *Frontiers Media SA*. doi: 10.3389/fbinf.2022.927312.
- [48] P. Agrawal, H. F. Abutarboush, T. Ganesh, and A. W. Mohamed, “Metaheuristic algorithms on feature selection: A survey of one decade of research (2009-2019),” *IEEE Access*, vol. 9, pp. 26766–26791, 2021, doi: 10.1109/ACCESS.2021.3056407.
- [49] Y. Han, L. Huang, and F. Zhou, “A dynamic recursive feature elimination framework (dRFE) to further refine a set of OMIC biomarkers,” *Bioinformatics*, vol. 37, no. 15, pp. 2183–2189, Aug. 2021, doi: 10.1093/bioinformatics/btab055.
- [50] H. M. Alshanbari, T. Mehmood, W. Sami, W. Alturaiki, M. A. Hamza, and B. Alosaimi, “Prediction and Classification of COVID-19 Admissions to Intensive Care Units (ICU) Using Weighted Radial Kernel SVM Coupled with Recursive Feature Elimination (RFE),” *Life*, vol. 12, no. 7, Jul. 2022, doi: 10.3390/life12071100.
- [51] C. A. Ramezan, “Transferability of Recursive Feature Elimination (RFE)-Derived Feature Sets for Support Vector Machine Land Cover Classification,” *Remote Sens (Basel)*, vol. 14, no. 24, Dec. 2022, doi: 10.3390/rs14246218.

- [52] I. Guyon and S. Gunn, *Feature Extraction Foundations and Applications*. Springer Berlin Heidelberg, 2008.
- [53] N. S. Azman *et al.*, “Support Vector Machine – Recursive Feature Elimination for Feature Selection on Multi-omics Lung Cancer Data,” *Progress in Microbes and Molecular Biology*, vol. 6, no. 1, 2023, doi: 10.36877/pmmb.a0000327.
- [54] T. Hastie, R. Tibshirani, and J. Friedman, *Springer Series in Statistics The Elements of Statistical Learning Data Mining, Inference, and Prediction*. Springer, 2013.
- [55] M. Kuhn and K. Johnson, *Applied Predictive Modeling*. Springer, 2013.
- [56] G. M. I. Akbar, M. A. Hariyadi, and A. Hanani, “Detection of Brute force Attacks on the MQTT Protocol Using Random Forest Algorithm,” *Internet of Things and Artificial Intelligence Journal*, vol. 3, no. 3, pp. 250–272, Aug. 2023, doi: 10.31763/iota.v3i3.630.
- [57] A. S. Hermiati, R. Herteno, F. Indriani, T. H. Saragih, Muliadi, and Triwiyanto, “A Comparative Study: Application of Principal Component Analysis and Recursive Feature Elimination in Machine Learning for Stroke Prediction,” *Journal of Electronics, Electromedical Engineering, and Medical Informatics*, vol. 6, no. 3, pp. 231–242, Jul. 2024, doi: 10.35882/jeeemi.v6i3.446.

