DAFTAR PUSTAKA

Abdulhammed, R., Musafer, H., Alessa, A., Faezipour, M., & Abuzneid, A. (2019). Features Dimensionality Reduction Approaches for Machine Learning Based Network Intrusion Detection. *electronics*.

Alalhareth, M., & Hong, S. C. (2023). An Improved Mutual Information Feature Selection Technique for Intrusion Detection Systems in the Internet of Medical Things. *Sensors*, *23*(10). https://doi.org/10.3390/s23104971

Alaudin Shalih, F., Akbar Ramadhan, R., & Syalaisa, N. (2025). *Tinjauan Komprehensif tentang Aplikasi dan Perkembangan Principal Component Analysis (PCA)* https://ejournal.upi.edu/index.php/JEM

Albalwy, F., & Almohaimeed, M. (2025). Advancing Artificial Intelligence of Things Security: Integrating Feature Selection and Deep Learning for Real-Time Intrusion Detection. *Systems*, *13*(4). https://doi.org/10.3390/systems13040231

Al-Garadi, M. A., Mohamed, A., Al-Ali, A. K., Du, X., Ali, I., & Guizani, M. (2020). A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security. *IEEE Communications Surveys and Tutorials*, *22*(3), 1646–1685. https://doi.org/10.1109/COMST.2020.2988293

Almaiah, M. A., Almomani, O., Alsaaidah, A., Al-Otaibi, S., Bani-Hani, N., Hwaitat, A. K. A., Al-Zahrani, A., Lutfi, A., Awad, A. B., & Aldhyani, T. H. H. (2022). Performance Investigation of Principal Component Analysis for

Intrusion Detection System Using Different Support Vector Machine Kernels. *Electronics (Switzerland)*,*11*(21). https://doi.org/10.3390/electronics1121357 1

Al-Marghilani, A. (2021). Comprehensive Analysis of IoT Malware Evasion Techniques. Dalam *Technology & Applied Science Research* (Vol. 11, Nomor 4). www.etasr.com

Almazarqi, H. A., Marnerides, A. K., Mursch, T., Woodyard, M., & Pezaros, D. (2021). Profiling IoT Botnet Activity in the Wild. *Proceedings - IEEE Global Communications Conference, GLOBECOM*. https://doi.org/10.1109/GLOBECOM46510.2021.9686012

Al-Sarem, M., Saeed, F., Alkhammash, E. H., & Alghamdi, N. S. (2022). An aggregated mutual information based feature selection with machine learning methods for enhancing iot botnet attack detection. *Sensors*, *22*(1). https://doi.org/10.3390/s22010185

Archana, J., & Aneetha, A. S. (2024). LSTM-MI: Revolutionizing Intrusion Detection Through Adaptive Learning and Mutual Information Analysis. *3rd IEEE International Conference on Distributed Computing and Electrical Circuits and Electronics, ICDCECE 2024*. https://doi.org/10.1109/ICDCECE60827.2024.10549671

Arfianti, U. I., Novitasari, D. C. R., Widodo, N., Hafiyusholeh, Moh., & Utami, W. D. (2021). Sunspot Number Prediction Using Gated Recurrent Unit (GRU) Algorithm. *IJCCS (Indonesian Journal of Computing and Cybernetics Systems)*, *15*(2), 141. https://doi.org/10.22146/ijccs.63676

Asghar, Nabeel, M., Asif, M., Murad, Zara, Alyahya, & Ahmed. (2024). *Detecting Malicious Botnets in IoT Networks Using Machine Learning Techniques*.

Balhareth, G., & Ilyas, M. (2024). Optimized Intrusion Detection for IoMT Networks with Tree-Based Machine Learning and Filter-Based Feature Selection. *Sensors*, *24*(17). https://doi.org/10.3390/s24175712

Cahyanto, T. A., Wahjuni, S., Sukoco, H., Rahmawan, H., & Neyman, S. N. (2022). Intelligent ubiquitous technology as a precision agri-food framework: A proposed framework. *IOP Conference Series: Earth and Environmental Science*, *1041*(1). https://doi.org/10.1088/1755-1315/1041/1/012022

Carvalho, M., Pinho, A. J., & Brás, S. (2025). Resampling approaches to handle class imbalance: a review from a data perspective. *Journal of Big Data*, *12*(1). https://doi.org/10.1186/s40537-025-01119-4

Chen, W., Yang, K., Yu, Z., Shi, Y., & Chen, C. L. P. (2024). A survey on imbalanced learning: latest research, applications and future directions. *Artificial Intelligence Review*, *57*(6). https://doi.org/10.1007/s10462-024-10759-6

De Diego, I. M., Redondo, A. R., Fernández, R. R., Navarro, J., & Moguerza, J. M. (2022). General Performance Score for classification problems. *Applied Intelligence*, *52*(10), 12049–12063. https://doi.org/10.1007/s10489-021-03041-7

De Keersmaeker, F., Cao, Y., Ndonda, G. K., & Sadre, R. (2023). A Survey of Public IoT Datasets for Network Security Research. *Commun. Surveys Tuts.*, *25*(3), 1808–1840. https://doi.org/10.1109/COMST.2023.3288942

Elrawy, M. F., Awad, A. I., & Hamed, H. F. A. (2018). Intrusion detection systems for IoT-based smart environments: a survey. Dalam *Journal of Cloud Computing* (Vol. 7, Nomor 1). Springer Verlag. https://doi.org/10.1186/s13677-018-0123-6

Ferrag, M. A., Friha, O., Hamouda, D., Maglaras, L., & Janicke, H. (2022). Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning. *IEEE Access*, *10*, 40281–40306. https://doi.org/10.1109/ACCESS.2022.3165809

G., S., & K., P. (2025). A GRU-based approach for botnet detection using deep learning technique. *Indonesian Journal of Electrical Engineering and Computer Science*, *38*(2), 1098. https://doi.org/10.11591/ijeecs.v38.i2.pp1098-1105

Hamarashid, H. K. (2021). Utilizing Statistical Tests for Comparing Machine Learning Algorithms. *Kurdistan Journal of Applied Research*.

Hartinah, Wahyudi;Paundu;Ady, & Ilham; Ahmad;Amil. (2023). *Deteksi Malware Ransomware Berdasarkan Panggilan API dengan Metode Ekstraksi Fitur N-gram dan TF-IDF*.

Hasan, B. M. S., & Abdulazeez, A. M. (2021). A Review of Principal Component Analysis Algorithm for Dimensionality Reduction. *Journal of Soft Computing*

and Data Mining, *2*(1), 20–30. https://doi.org/10.30880/jscdm.2021.02.01.003

Huang, L., Zhou, X., Shi, L., & Gong, L. (2024). Time Series Feature Selection Method Based on Mutual Information. *Applied Sciences (Switzerland)*, *14*(5). https://doi.org/10.3390/app14051960

IoT Analytics. (2025, Oktober 28). *State of IoT 2025: Number of connected IoT devices growing 14% to 21.1 billion globally*. IoT Analytics. https://iot-analytics.com/number-connected-iot-devices/

John, A., Isnin, I. F. Bin, Madni, S. H. H., & Muchtar, F. B. (2024). Enhanced intrusion detection model based on principal component analysis and variable ensemble machine learning algorithm. *Intelligent Systems with Applications*, *24*. https://doi.org/10.1016/j.iswa.2024.200442

Kaushik, S., Bhadrdwaj, A., Rehman, A. U., Bharany, S., Harguem, S., Kukunuru, S., & Thawabeh, O. A. (2022). Designing an MI-PCA based Agile Intrusion Detection System. *International Conference on Cyber Resilience, ICCR 2022*. https://doi.org/10.1109/ICCR56254.2022.9995863

Kilichev, D., Turimov, D., & Kim, W. (2024). Next–Generation Intrusion Detection for IoT EVCS: Integrating CNN, LSTM, and GRU Models. *Mathematics*, *12*(4). https://doi.org/10.3390/math12040571

Li, J., Othman, M. S., Chen, H., & Yusuf, L. M. (2024). Optimizing IoT intrusion detection system: feature selection versus feature extraction in machine

learning. *Journal of Big Data*, *11*(1). https://doi.org/10.1186/s40537-024-00892-y

Lu, Y., & Hu, L. (2023). *Technology Stock Forecasting Based on Hybrid Model and Data Migration* (hlm. 383–394). https://doi.org/10.2991/978-94-6463-304-7_41

Mahjoub, S., Chrifi-Alaoui, L., Marhic, B., & Delahoche, L. (2022). Predicting Energy Consumption Using LSTM, Multi-Layer GRU and Drop-GRU Neural Networks. *Sensors*, *22*(11). https://doi.org/10.3390/s22114062

Mienye, I. D., Swart, T. G., & Obaido, G. (2024). Recurrent Neural Networks: A Comprehensive Review of Architectures, Variants, and Applications. *Information*, *15*(9), 517. https://doi.org/10.3390/info15090517

Mohsen, S. (2023). Recognition of human activity using GRU deep learning algorithm. *Multimedia Tools and Applications*, *82*(30), 47733–47749. https://doi.org/10.1007/s11042-023-15571-y

Mondragon, J. C., Branco, P., Jourdan, G. V., Gutierrez-Rodriguez, A. E., & Biswal, R. R. (2025). Advanced IDS: a comparative study of datasets and machine learning algorithms for network flow-based intrusion detection systems. *Applied Intelligence*, *55*(7). https://doi.org/10.1007/s10489-025-06422-4

Nogales, R. E., & Benalcázar, M. E. (2023). Analysis and Evaluation of Feature Selection and Feature Extraction Methods. *International Journal of*

Computational Intelligence Systems, *16*(1). https://doi.org/10.1007/s44196-023-00319-1

Pai, V., Karthik Pai, B. H., Sudhiksha, G. S., Kamath, V., Varsha, K., & Manjunatha, S. (2025). Systematic Approach for Malware Detection in IoT Devices: Enhancing Security and Performance. *International Journal of Computational Intelligence Systems*, *18*(1). https://doi.org/10.1007/s44196-025-00939-9

Quy, V. K., Hau, N. Van, Anh, D. Van, Quy, N. M., Ban, N. T., Lanza, S., Randazzo, G., & Muzirafuti, A. (2022). IoT-Enabled Smart Agriculture: Architecture, Applications, and Challenges. Dalam *Applied Sciences (Switzerland)* (Vol. 12, Nomor 7). MDPI. https://doi.org/10.3390/app12073396

Rainio, O., Teuho, J., & Klén, R. (2024). Evaluation metrics and statistical tests for machine learning. *Scientific Reports*, *14*(1). https://doi.org/10.1038/s41598-024-56706-x

Sagu, A., Gill, N. S., Gulia, P., Alduaiji, N., Shukla, P. K., & Shah, M. A. (2025). Advances to IoT security using a GRU-CNN deep learning model trained on SUCMO algorithm. *Scientific Reports*, *15*(1). https://doi.org/10.1038/s41598-025-99574-9

Sarhan, M., Layeghy, S., Moustafa, N., Gallagher, M., & Portmann, M. (2022). *Feature Extraction for Machine Learning-based Intrusion Detection in IoT Networks*. https://doi.org/10.1016/j.dcan.2022.08.012

Sarwar, N., Alharthi, R. S., Aljohani, M., & Elhosseini, M. A. (2025). Securing IoT networks: a machine learning approach for detecting unusual traffic patterns. *Scientific Reports*. https://doi.org/10.1038/s41598-025-33447-z

Sathyanarayanan, S. (2024). Confusion Matrix-Based Performance Evaluation Metrics. *African Journal of Biomedical Research*, 4023–4031. https://doi.org/10.53555/ajbr.v27i4s.4345

Sazzed, S., & Ullah, S. (2023). *Enhancing Efficiency and Privacy in Memory-Based Malware Classification through Feature Selection*.

Shaikh, J. A., Wang, C., Sima, M. W. U., Arshad, M., Owais, M., Hassan, D. S. M., Alkanhel, R., & Muthanna, M. S. A. (2025). A deep Reinforcement learning-based robust Intrusion Detection System for securing IoMT Healthcare Networks. *Frontiers in Medicine*, *12*. https://doi.org/10.3389/fmed.2025.1524286

Sheheryar, M. A., & Sharma, S. (2025). Ensemble Feature Engineering and Deep Learning for Botnet Attacks Detection in the Internet of Things. *Transactions on Emerging Telecommunications Technologies*, *36*(3). https://doi.org/10.1002/ett.70099

Shoab, M., & Alsbatin, L. (2024). GRU Enabled Intrusion Detection System for IoT Environment with Swarm Optimization and Gaussian Random Forest Classification. *Computers, Materials and Continua*, *81*(1), 625–642. https://doi.org/10.32604/cmc.2024.053721

Syifa, M. A., Retno, D., & Saputro, S. (2023). *Stance Detection Dengan Algoritme Gated Recurrent Unit (GRU)*.

Talukder, M. A., Khalid, M., & Sultana, N. (2025). A hybrid machine learning model for intrusion detection in wireless sensor networks leveraging data balancing and dimensionality reduction. *Scientific Reports*, *15*(1). https://doi.org/10.1038/s41598-025-87028-1

Tian, Y., Xu, S., Cao, Y., Wang, Z., & Wei, Z. (2025). An Empirical Comparison of Machine Learning and Deep Learning Models for Automated Fake News Detection. *Mathematics*, *13*(13). https://doi.org/10.3390/math13132086

Westphal, C., Hailes, S., & Musolesi, M. (2025). Feature Selection for Network Intrusion Detection. *Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, *1*, 1599–1610. https://doi.org/10.1145/3690624.3709339

Yousefi-Azar, M., Varadharajan, V., Hamey, L., & Chen, S. (2021). Mutual Information and Feature Importance Gradient Boosting: Automatic byte n-gram feature reranking for Android malware detection. *Software - Practice and Experience*, *51*(7), 1518–1539. https://doi.org/10.1002/spe.2971

Zeng, G. (2025). Invariance Properties and Evaluation Metrics Derived from the Confusion Matrix in Multiclass Classification. *Mathematics*, *13*(16). https://doi.org/10.3390/math13162609