DAFTAR PUSTAKA

Abadi, M., Barham, P., Chen, J., Chen, Z., & Davis, A. (2016). *TensorFlow: A System for Large-Scale Machine Learning*. 786. https://www.usenix.org/conference/osdi16/technical-sessions/presentation/abadi.

Adefemi, K. O., Mutanga, M. B., & Alimi, O. A. (2025). A Hybrid CNN–GRU Deep Learning Model for IoT Network Intrusion Detection. *Journal of Sensor and Actuator Networks*, *14*(5). https://doi.org/10.3390/jsan14050096.

Adesanya, O. M., Moradpoor, N., Maglaras, L., Lim, I. S., & Amine Ferrag, M. (2024). Assessment and Analysis of IoT Protocol Effectiveness in Data Exfiltration Scenario. *Proceedings - 2024 20th International Conference on Distributed Computing in Smart Systems and the Internet of Things, DCOSS-IoT 2024*, 556–563. https://doi.org/10.1109/DCOSS-IoT61029.2024.00087.

Adi, P. W., Kusumaningrum, R., Saputra, N. R., Setiawan, S. H., & Amrustian, M. A. (2026). *Lightweight and Accurate Deep Learning for Anomaly-Based IDS using Data-Driven Redundancy Reduction*. 1–6. https://doi.org/10.1109/icdxa69105.2025.11329716.

Adi, P. W., Sugiharto, A., Hakim, M. M., Saputra, N. R., & Setiawan, H. (2025). *Optimizing Machine Learning Models for Anomaly-based IDS using Intercorrelation Threshold*. https://dx.doi.org/10.62527/joiv.9.6.3355.

Alawi, Z. B. (2025). *A Comparative Survey of PyTorch vs TensorFlow for Deep Learning: Usability, Performance, and Deployment Trade-offs*. https://doi.org/10.48550/arXiv.2508.04035.

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Communications Surveys and Tutorials*, *17*(4), 2347–2376. https://doi.org/10.1109/COMST.2015.2444095.

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.

Alzubaidi, L., Zhang, J., Humaidi, A. J., Al-Dujaili, A., Duan, Y., Al-Shamma, O., Santamaría, J., Fadhel, M. A., Al-Amidie, M., & Farhan, L. (2021). Review of deep learning: concepts, CNN architectures, challenges, applications, future directions. *Journal of Big Data*, *8*(1). https://doi.org/10.1186/s40537-021-00444-8.

Bertino, E., & Islam, N. (2017). *Botnets and Internet of Things Security*. https://doi.org/10.1109/MC.2017.62.

Buczak, A. L., & Guven, E. (2016). A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. *IEEE Communications Surveys and Tutorials*, *18*(2), 1153–1176. https://doi.org/10.1109/COMST.2015.2494502.

Buda, M., Maki, A., & Mazurowski, M. A. (2018). *A systematic study of the class imbalance problem in convolutional neural networks*. https://doi.org/10.1016/j.neunet.2018.07.011.

Chetlur, S., Woolley, C., Vandermersch, P., Cohen, J., Tran, J., Catanzaro, B., & Shelhamer, E. (2014). *cuDNN: Efficient Primitives for Deep Learning*. http://arxiv.org/abs/1410.0759.

Cho, K., van Merrienboer, B., Gulcehre, C., Bahdanau, D., Bougares, F., Schwenk, H., & Bengio, Y. (2014). *Learning Phrase Representations using RNN Encoder-Decoder for Statistical Machine Translation*. http://arxiv.org/abs/1406.1078.

Chung, J., Gulcehre, C., Cho, K., & Bengio, Y. (2014). *Empirical Evaluation of Gated Recurrent Neural Networks on Sequence Modeling*. http://arxiv.org/abs/1412.3555.

Deshmukh, A. G., & Radhakrishnan, N. (2024). Analyzing Socioeconomic and Climatic Trends in Oman's Governorates Using Python Data Analysis Tools. *2024 2nd International Conference on Computing and Data Analytics, ICCDA 2024 - Proceedings*. https://doi.org/10.1109/ICCDA64887.2024.10867346.

Gueriani, A., Kheddar, H., Mazari, A. C., & Ghanem, M. C. (2025). A robust cross-domain IDS using BiGRU-LSTM-attention for medical and industrial IoT security. *ICT Express*. https://doi.org/10.1016/j.icte.2025.08.011.

Harris, C. R., Millman, K. J., van der Walt, S. J., Gommers, R., Virtanen, P., Cournapeau, D., Wieser, E., Taylor, J., Berg, S., Smith, N. J., Kern, R., Picus, M., Hoyer, S., van Kerkwijk, M. H., Brett, M., Haldane, A., del Río, J. F., Wiebe, M., Peterson, P., … Oliphant, T. E. (2020). Array programming with NumPy. Dalam *Nature* (Vol. 585, Nomor 7825, hlm. 357–362). Nature Research. https://doi.org/10.1038/s41586-020-2649-2.

Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, B. (2019). A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures. Dalam *IEEE Access* (Vol. 7, hlm. 82721–82743). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ACCESS.2019.2924045.

Hossin, M., & Sulaiman, M. N. (2015). A Review on Evaluation Metrics for Data Classification Evaluations. *International Journal of Data Mining & Knowledge Management Process*, *5*(2), 01–11. https://doi.org/10.5121/ijdkp.2015.5201.

Hunter, J. D. (2007). *Matplotlib: A 2D Graphics Environment*.

Ioffe, S., & Szegedy, C. (2015). *Batch Normalization: Accelerating Deep Network Training by Reducing Internal Covariate Shift*. http://arxiv.org/abs/1502.03167.

Kamal, H., & Mashaly, M. (2025). Robust Intrusion Detection System Using an Improved Hybrid Deep Learning Model for Binary and Multi-Class Classification in IoT Networks. *Technologies*, *13*(3). https://doi.org/10.3390/technologies13030102.

Khalid, S., Khalil, T., & Nasreen, S. (2014). *A Survey of Feature Selection and Feature Extraction Techniques in Machine Learning*. *372*. https://doi.org/10.1109/SAI.2014.6918213.

Khokher, B., Singh, P., Chaudhary, S., Joshi, N., & Vishnoi, V. (2024). Applications and Use Cases of Internet of Things (IoT) with Case Study. *2nd IEEE International Conference on IoT, Communication and Automation Technology, ICICAT 2024*, 1575–1581. https://doi.org/10.1109/ICICAT62666.2024.10923465.

Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: techniques, datasets and challenges. *Cybersecurity*, *2*(1). https://doi.org/10.1186/s42400-019-0038-7.

Koroniotis, N., Moustafa, N., Sitnikova, E., & Turnbull, B. (2019). Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset. *Future Generation Computer Systems*, *100*, 779–796. https://doi.org/10.1016/j.future.2019.05.041.

Kurniawan, R., & Prakoso, F. (2020). *Implementasi Metode IPS (Intrusion Prevention System) dan IDS (Intrusion Detection System) untuk Meningkatkan Keamanan Jaringan* (Vol. 2, Nomor 02).

Lee, C. K. (2020). *Deep Learning Creativity in EDA*. https://doi.org/10.1109/VLSI-DAT49148.2020.9196288.

Liao, H. J., Richard Lin, C. H., Lin, Y. C., & Tung, K. Y. (2013). Intrusion detection system: A comprehensive review. Dalam *Journal of Network and Computer Applications* (Vol. 36, Nomor 1, hlm. 16–24). https://doi.org/10.1016/j.jnca.2012.09.004.

Maggu, J., Aggarwal, A., Saini, J. K., & Verma, P. (2025). Non-linear Analysis Dictionary Learning with Orthogonal Constraint for Fault Detection. *International Conference on Electronics, AI, and Computing: Innovating for a Sustainable and Connected Future, EAIC 2025*. https://doi.org/10.1109/EAIC66483.2025.11101443.

Maji, A. K., Gorenstein, L., & Lentner, G. (2020). *Demystifying Python Package Installation with conda-env-mod*. https://doi.org/10.1109/HUSTProtools51951.2020.00011.

Mckinney, W. (2010). Data Structures for Statistical Computing in Python. *scipy*, 445(1), 51–56.

Mishra, P., Pilli, E. S., Varadharajan, V., & Tupakula, U. (2017). Intrusion detection techniques in cloud environment: A survey. Dalam *Journal of Network and Computer Applications* (Vol. 77, hlm. 18–47). Academic Press. https://doi.org/10.1016/j.jnca.2016.10.015.

Pedregosa, F., Varoquaux, G., Gramfort, A., Michel, V., Thirion, B., & Grisel, O. (2011). Scikit-learn: Machine Learning in Python. *Journal of Machine Learning Research*, *12*, 2825–2830. http://scikit-learn.sourceforge.net.

Rohit, H. M., Fahim, S. M., & Khan, A. H. A. (2019). *Mitigating and Detecting DDoS attack on IoT Environment*. https://doi.org/10.1109/RAAICON48939.2019.5.

Roopak, M., Tian, G. Y., & Chambers, J. (2019). *Deep Learning Models for Cyber Security in IoT Networks*. https://doi.org/10.1109/CCWC.2019.8666588.

Scarfone, K. A., & Mell, P. M. (2007). *Guide to Intrusion Detection and Prevention Systems (IDPS)*. https://doi.org/10.6028/NIST.SP.800-94.

Shafiq, M., Tian, Z., Sun, Y., Du, X., & Guizani, M. (2020). Selection of effective machine learning algorithm and Bot-IoT attacks traffic identification for internet of things in smart city. *Future Generation Computer Systems*, *107*, 433–442. https://doi.org/10.1016/j.future.2020.02.017.

Sharma, N., & Jain, C. (2019). *Characterization of Facial Expression using Deep Neural Networks*. https://doi.org/https://doi.org/10.1109/ICACCS.2019.8728386.

Shrestha, A., & Mahmood, A. (2019). Review of deep learning algorithms and architectures. Dalam *IEEE Access* (Vol. 7, hlm. 53040–53065). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ACCESS.2019.2912200.

Shyaa, M. A., Ibrahim, N. F., Zainol, Z., Abdullah, R., Anbar, M., & Alzubaidi, L. (2024). Evolving cybersecurity frontiers: A comprehensive survey on concept drift and feature dynamics aware machine and deep learning in intrusion detection systems. Dalam *Engineering Applications of Artificial Intelligence* (Vol. 137). Elsevier Ltd. https://doi.org/10.1016/j.engappai.2024.109143.

Tarigan, G. A., Hermawan, E., & Girsang, A. S. (2024). Parallelization of LSTM-GRU Architectures for Multivariate Prediction of Stock Prices. *Proceedings of 2024 International Conference on Information Management and Technology, ICIMTech 2024*, 311–315. https://doi.org/10.1109/ICIMTech63123.2024.10780885.

Tsai, M. F., Lan, C. Y., Wang, N. C., & Chen, L. W. (2023). Time Series Feature Extraction Using Transfer Learning Technology for Crop Pest Prediction. *Agronomy*, *13*(3). https://doi.org/10.3390/agronomy13030792.

Ullah, I., & Mahmoud, Q. H. (2022). Design and Development of RNN Anomaly Detection Model for IoT Networks. *IEEE Access*, *10*, 62722–62750. https://doi.org/10.1109/ACCESS.2022.3176317.

Ullah, I., Ullah, A., & Sajjad, M. (2021). Towards a Hybrid Deep Learning Model for Anomalous Activities Detection in Internet of Things Networks. *Internet of Things*, *2*(3), 428–448. https://doi.org/10.3390/iot2030022.

Uroz, D., & Rodriguez, R. J. (2022). Characterization and Evaluation of IoT Protocols for Data Exfiltration. Dalam *IEEE Internet of Things Journal* (Vol. 9, Nomor 19, hlm. 19062–19072). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/JIOT.2022.3163469.

Wensheng, L., Hongshi, Z., Kun, W., Zhen, W., & Weilong, C. (2024). Short-term Net Load Forecasting Model Based on GRU Neural Network Optimized by Improved Arithmetic Optimization Algorithm. *2024 IEEE 7th International Conference on Information Systems and Computer Aided Education, ICISCAE 2024*, 52–56. https://doi.org/10.1109/ICISCAE62304.2024.10761548.

Xiang, Y., Li, D., Meng, X., Dong, C., & Qin, G. (2024). ResNeSt-biGRU: An Intrusion Detection Model Based on Internet of Things. *Computers, Materials and Continua*, *79*(1), 1005–1023. https://doi.org/10.32604/cmc.2024.047143.

Ying, X. (2019). An Overview of Overfitting and its Solutions. *Journal of Physics: Conference Series*, *1168*(2). https://doi.org/10.1088/1742-6596/1168/2/022022.

Zahra Anwar, Y., & Sanmorino, A. (2024). Hukum dan Kebijakan Keamanan Siber: Tantangan Regulasi Perangkat IoT. *Jurnal Ilmiah Informatika Global, 15(3), 95-99*. https://doi.org/10.36982/jiig.v15i3.4773.

Zhang, L. (2021). A Feature Selection Algorithm Integrating Maximum Classification Information and Minimum Interaction Feature Dependency Information. *Computational Intelligence and Neuroscience*, *2021*. https://doi.org/10.1155/2021/3569632.

Zhao, J. (2023). Design and implementation of quickly building artificial intelligence training environment on high-performance server. *2023 IEEE International Conference on Control, Electronics and Computer Technology, ICCECT 2023*, 478–483. https://doi.org/10.1109/ICCECT57938.2023.10141127.