DAFTAR PUSTAKA

Abdulkadhum Abbas, S. A., & Abdu Ibrahim, A. (2024). Fortifying IoT Infrastructure Using Machine Learning for DDoS Attack within Distributed Computing-based Routing in Networks. *Qubahan Academic Journal*, *4*(2), 569–581. https://doi.org/10.48161/QAJ.V4N2A581

Abreu, S. (2019). *Automated Architecture Design for Deep Neural Networks*. http://arxiv.org/abs/1908.10714

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., Sugiharto, A., Hakim, M. M., Saputra, N. R., & Setiawan, S. H. (2025). Optimizing Machine Learning Models for Anomaly-based IDS using Intercorrelation Threshold. *JOIV : International Journal on Informatics Visualization*, *9*(6), 2327–2334. https://doi.org/10.62527/JOIV.9.6.3355

Airlangga, G. (2024). Predicting Student Performance Using Deep Learning Models: A Comparative Study of MLP, CNN, BiLSTM, and LSTM with Attention. *MALCOM: Indonesian Journal of Machine Learning and Computer Science*, *4*(4), 1561–1567. https://doi.org/10.57152/MALCOM.V4I4.1668

Akter, M., Moustafa, N., & Turnbull, B. (2024). SPEI-FL: Serverless Privacy Edge Intelligence-Enabled Federated Learning in Smart Healthcare Systems. *Cognitive Computation*, *16*(5), 2626–2641. https://doi.org/10.1007/S12559-024-10310-3

Al Jallad, K., Aljnidi, M., & Desouki, M. S. (2020). Anomaly detection optimization using big data and deep learning to reduce false-positive. *Journal of Big Data*, *7*(1). https://doi.org/10.1186/S40537-020-00346-1

Alam, Md. M., & Ansari, Mohd. S. (2022). A study on IoT-related security issues, challenges, and solutions. *International Journal of Smart Sensor and Adhoc Network.*, 50–60. https://doi.org/10.47893/IJSSAN.2022.1220

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

Al-Haija, Q. A., & Droos, A. (2024). A comprehensive survey on deep learning-based intrusion detection systems in Internet of Things (IoT). *Expert Systems*, *42*(2). https://doi.org/10.1111/EXSY.13726

Ali, M. L., Thakur, K., Schmeelk, S., Debello, J., & Dragos, D. (2025). Deep Learning vs. Machine Learning for Intrusion Detection in Computer Networks: A

Comparative Study. *Applied Sciences 2025, Vol. 15, Page 1903*, *15*(4), 1903. https://doi.org/10.3390/APP15041903

Awan, A. A., Subramoni, H., & Panda, D. K. (2017). An In-depth Performance Characterization of CPU- and GPU-based DNN Training on Modern Architectures. *Proceedings of MLHPC 2017: Machine Learning in HPC Environments - Held in conjunction with SC 2017: The International Conference for High Performance Computing, Networking, Storage and Analysis*. https://doi.org/10.1145/3146347.3146356

Ayad, A. G., Sakr, N. A., & Hikal, N. A. (2024). A hybrid approach for efficient feature selection in anomaly intrusion detection for IoT networks. *The Journal of Supercomputing 2024 80:19*, *80*(19), 26942–26984. https://doi.org/10.1007/S11227-024-06409-X

Azam, Z., Islam, M. M., & Huda, M. N. (2023). Comparative Analysis of Intrusion Detection Systems and Machine Learning-Based Model Analysis Through Decision Tree. *IEEE Access*, *11*, 80348–80391. https://doi.org/10.1109/ACCESS.2023.3296444

Azimjonov, J., & Kim, T. (2024). Designing accurate lightweight intrusion detection systems for IoT networks using fine-tuned linear SVM and feature selectors. *Computers & Security*, *137*, 103598. https://doi.org/10.1016/J.COSE.2023.103598

Bhavsar, M., Roy, K., Kelly, J., & Olusola, O. (2023). Anomaly-based intrusion detection system for IoT application. *Discover Internet of Things*, *3*(1). https://doi.org/10.1007/S43926-023-00034-5

Bilal, M. A., Ji, Y., Wang, Y., Akhter, M. P., & Yaqub, M. (2022). Early Earthquake Detection Using Batch Normalization Graph Convolutional Neural Network (BNGCNN). *Applied Sciences (Switzerland)*, *12*(15). https://doi.org/10.3390/APP12157548

Bouke, M. A., & Abdullah, A. (2023). An empirical study of pattern leakage impact during data preprocessing on machine learning-based intrusion detection models reliability. *Expert Systems with Applications*, *230*, 120715. https://doi.org/10.1016/J.ESWA.2023.120715

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

Chen, C. C., Liu, Z., Yang, G., Wu, C. C., & Ye, Q. (2021). An improved fault diagnosis using 1d-convolutional neural network model. *Electronics (Switzerland)*, *10*(1), 1–19. https://doi.org/10.3390/ELECTRONICS10010059

Chen, G., Chen, P., Shi, Y., Hsieh, C.-Y., Liao, B., & Zhang, S. (2019). *Rethinking the Usage of Batch Normalization and Dropout in the Training of Deep Neural Networks*. https://arxiv.org/pdf/1905.05928

Chen, L., Li, S., Bai, Q., Yang, J., Jiang, S., & Miao, Y. (2021). Review of image classification algorithms based on convolutional neural networks. *Remote Sensing*, *13*(22). https://doi.org/10.3390/RS13224712

Cheng, S., Qiao, X., Shi, Y., & Wang, D. (2020). *Comparison of Machine Learning Methods for Predicting Karst Spring Discharge in North China*. https://arxiv.org/pdf/2007.12951

Ciuparu, A., Nagy-Dăbâcan, A., & Mureşan, R. C. (2020). Soft++, a multi-parametric non-saturating non-linearity that improves convergence in deep neural architectures. *Neurocomputing*, *384*, 376–388. https://doi.org/10.1016/J.NEUCOM.2019.12.014

Doshi, R., Apthorpe, N., & Feamster, N. (2018). Machine learning DDoS detection for consumer internet of things devices. *Proceedings - 2018 IEEE Symposium on Security and Privacy Workshops, SPW 2018*, 29–35. https://doi.org/10.1109/SPW.2018.00013

Elshewey, A. M., Abbas, S., Osman, A. M., Aldakheel, E. A., & Fouad, Y. (2025). DDoS classification of network traffic in software defined networking SDN using a hybrid convolutional and gated recurrent neural network. *Scientific Reports 2025 15:1*, *15*(1), 29122-. https://doi.org/10.1038/s41598-025-13754-1

Fei, X., Ye, M., Du, Z., & Miao, H. (2025). A comparative study of MLP and LSTM neural networks for shale gas production prediction based on numerical simulation data. *PLOS ONE*, *20*(11 November). https://doi.org/10.1371/JOURNAL.PONE.0336782

Ghaffari, A., Jelodari, N., pouralish, S., derakhshanfard, N., & Arasteh, B. (2024). Securing internet of things using machine and deep learning methods: a survey. *Cluster Computing*, *27*(7), 9065–9089. https://doi.org/10.1007/S10586-024-04509-0

Gong, J., Saadat, H., Gamaarachchi, H., Javaid, H., Hu, X. S., & Parameswaran, S. (2023). ApproxTrain: Fast Simulation of Approximate Multipliers for DNN Training and Inference. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, *42*(11), 3505–3518. https://doi.org/10.1109/TCAD.2023.3253045

Guimarães, L. C. B., & Couto, R. S. (2024). A Performance Evaluation of Neural Networks for Botnet Detection in the Internet of Things. *Journal of Network and Systems Management*, *32*(4). https://doi.org/10.1007/S10922-024-09875-Z

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. *IEEE Access*, *7*, 82721–82743. https://doi.org/10.1109/ACCESS.2019.2924045

Hodo, E., Bellekens, X., Hamilton, A., Tachtatzis, C., & Atkinson, R. (2017). *Shallow and Deep Networks Intrusion Detection System: A Taxonomy and Survey*. https://arxiv.org/pdf/1701.02145

Hussain, F., Abbas, S. G., Pires, I. M., Tanveer, S., Fayyaz, U. U., Garcia, N. M., Shah, G. A., & Shahzad, F. (2021). A Two-Fold Machine Learning Approach to Prevent and Detect IoT Botnet Attacks. *IEEE Access*, *9*, 163412–163430. https://doi.org/10.1109/ACCESS.2021.3131014

Ilemobayo, J. A., Durodola, O., Alade, O., Awotunde, O. J., Olanrewaju, A. T., Falana, O., Ogungbire, A., Osinuga, A., Ogunbiyi, D., Ifeanyi, A., Odezuligbo, I. E., & Edu, O. E. (2024). Hyperparameter Tuning in Machine Learning: A Comprehensive Review. *Journal of Engineering Research and Reports*, *26*(6), 388–395. https://doi.org/10.9734/JERR/2024/V26I61188

Javid, A. M., Das, S., Skoglund, M., & Chatterjee, S. (2021). A relu dense layer to improve the performance of neural networks. *ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings*, *2021-June*, 2810–2814. https://doi.org/10.1109/ICASSP39728.2021.9414269

Jyothsna, V., & Munivara Prasad, K. (2020). Anomaly-Based Intrusion Detection System. *Computer and Network Security*. https://doi.org/10.5772/INTECHOPEN.82287

Kanimozhi, V., & Jacob, Dr. T. P. (2019a). Calibration of Various Optimized Machine Learning Classifiers In Network Intrusion Detection System on the Realistic Cyber Dataset CSE-CIC-IDS2018 Using Cloud Computing. *International Journal of Engineering Applied Sciences and Technology*, *04*(06), 209–213. https://doi.org/10.33564/IJEAST.2019.V04I06.036

Kanimozhi, V., & Jacob, T. P. (2019b). Artificial Intelligence based Network Intrusion Detection with hyper-parameter optimization tuning on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing. *ICT Express*, *5*(3), 211–214. https://doi.org/10.1016/J.ICTE.2019.03.003

Kenaza, R., Khemane, A., Bendjenna, H., Meraoumia, A., & Laimeche, L. (2022). Internet of Things (IoT): Architecture, Applications, and Security Challenges. *4th International Conference on Pattern Analysis and Intelligent Systems, PAIS 2022 - Proceedings*. https://doi.org/10.1109/PAIS56586.2022.9946918

Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: techniques, datasets and challenges. *Cybersecurity 2019 2:1*, *2*(1), 20-. https://doi.org/10.1186/S42400-019-0038-7

Khraisat, A., Gondal, I., Vamplew, P., Kamruzzaman, J., & Alazab, A. (2019). A Novel Ensemble of Hybrid Intrusion Detection System for Detecting Internet of Things Attacks. *Electronics 2019, Vol. 8, Page 1210*, *8*(11), 1210. https://doi.org/10.3390/electronics8111210

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/https://doi.org/10.1016/j.future.2019.05.041

Kukačka, J., Golkov, V., & Cremers, D. (2017). *Regularization for Deep Learning: A Taxonomy*. http://arxiv.org/abs/1710.10686

Kumar, A., & Lim, T. J. (2019). EDIMA: Early Detection of IoT Malware Network Activity Using Machine Learning Techniques. *IEEE 5th World Forum on Internet of Things, WF-IoT 2019 - Conference Proceedings*, 289–294. https://doi.org/10.1109/WF-IOT.2019.8767194

Labach, A., Salehinejad, H., & Valaee, S. (2019). *Survey of Dropout Methods for Deep Neural Networks*. https://arxiv.org/pdf/1904.13310

Li, H., Rajbahadur, G. K., Lin, D., Bezemer, C. P., & Jiang, Z. M. (2024). Keeping Deep Learning Models in Check: A History-Based Approach to Mitigate Overfitting. *IEEE Access*, *12*, 70676–70689. https://doi.org/10.1109/ACCESS.2024.3402543

Li, M., Bi, Z., Wang, T., Wen, Y., Niu, Q., Song, X., Jiang, Z., Liu, J., Peng, B., Zhang, S., Pan, X., Xu, J., Wang, J., Chen, K., Yin, C. H., Feng, P., & Liu, M. (2025). *Deep Learning and Machine Learning with GPGPU and CUDA: Unlocking the Power of Parallel Computing*. http://arxiv.org/abs/2410.05686

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

Liu, X., Li, T., Zhang, R., Wu, D., Liu, Y., & Yang, Z. (2021). A GAN and Feature Selection-Based Oversampling Technique for Intrusion Detection. *Security and Communication Networks*, *2021*. https://doi.org/10.1155/2021/9947059

Liu, Z., Xu, Z., Jin, J., Shen, Z., & Darrell, T. (2023). Dropout Reduces Underfitting. *Proceedings of Machine Learning Research*, *202*, 21715–21729. https://arxiv.org/pdf/2303.01500

Logeswari, G., Purbia, R., Tamilarasi, K., & Bose, S. (2025). IA-IDS: an intelligent adaptive intrusion detection system for IoT security using CNN, BiLSTM, and attention mechanism. *Peer-to-Peer Networking and Applications 2025 19:1*, *19*(1), 32-. https://doi.org/10.1007/S12083-025-02177-4

Lone, A. N., Mustajab, S., & Alam, M. (2023). A comprehensive study on cybersecurity challenges and opportunities in the IoT world . *SECURITY AND PRIVACY*, *6*(6). https://doi.org/10.1002/SPY2.318

Luqman, M., Zeeshan, M., Riaz, Q., Hussain, M., Tahir, H., Mazhar, N., & Khan, M. S. (2025). Intelligent parameter-based in-network IDS for IoT using UNSW-NB15 and BoT-IoT datasets. *Journal of the Franklin Institute*, *362*(1). https://doi.org/10.1016/j.jfranklin.2024.107440

Mahendra Achari, B., & Sreedevi, M. (2025). Network Intrusion Detection Using Supervised Machine Learning Technique with Feature Selection. *International Journal of Science and Research (IJSR)*, 208–212. https://doi.org/10.21275/SR25701121911

Manai, E., Mejri, M., & Fattahi, J. (2024). Confusion Matrix Explainability to Improve Model Performance: Application to Network Intrusion Detection. *10th 2024 International Conference on Control, Decision and Information Technologies, CoDIT 2024*, 587–591. https://doi.org/10.1109/CODIT62066.2024.10708595

Manzano Sanchez, R. A., Zaman, M., Goel, N., Naik, K., & Joshi, R. (2022). Towards Developing a Robust Intrusion Detection Model Using Hadoop–Spark and Data Augmentation for IoT Networks. *Sensors 2022, Vol. 22, Page 7726*, *22*(20), 7726. https://doi.org/10.3390/S22207726

Markov, K. (2023). Multilayer Perceptron with Backpropagation, HDL Coder, and FPGA Technology: An Integrated Approach for Efficient Neural Network Implementation. *Problems of Engineering Cybernetics and Robotics*, *80*. https://doi.org/10.7546/PECR.80.23.02

Mendez Mena, D., Papapanagiotou, I., & Yang, B. (2018). Internet of things: Survey on security. *Information Security Journal*, *27*(3), 162–182. https://doi.org/10.1080/19393555.2018.1458258

Mohy-eddine, M., Guezzaz, A., Benkirane, S., & Azrour, M. (2023). An Intrusion Detection Model using election-Based Feature Selection and K-NN. *Microprocessors and Microsystems*, 104966. https://doi.org/10.1016/j.micpro.2023.104966

Monani, U. J., Yun, T. S., Sain, M., & Pattnaik, P. K. (2025). Improved classification of oral cancer through a personalized transfer learning CNN architecture. *Journal of Oral Biology and Craniofacial Research*, *15*(6), 1779–1785. https://doi.org/10.1016/J.JOBCR.2025.10.002

Musthafa, M. B., Huda, S., Kodera, Y., Ali, M. A., Araki, S., Mwaura, J., & Nogami, Y. (2024). Optimizing IoT Intrusion Detection Using Balanced Class Distribution, Feature Selection, and Ensemble Machine Learning Techniques. *Sensors 2024, Vol. 24, Page 4293*, *24*(13), 4293. https://doi.org/10.3390/s24134293

Nabila Putri Listyanto, & Yustanti, W. (2025). Comparative Study of Time Series Forecasting on Iron Sales Using CNN, MLP, and LSTM. *Journal of Emerging Information Systems and Business Intelligence (JEISBI)*, *6*(3). https://doi.org/10.26740/JEISBI.V6I3.71361

Pahl, C. (2015). Containerization and the PaaS Cloud. *IEEE Cloud Computing*, *2*(3), 24–31. https://doi.org/10.1109/MCC.2015.51

Pham, V. T., Huu, T. V., Nguyen, M. T., & Le, H. C. (2023). Advanced Feature Processing for IoT-Based Intrusion Detection System. *RIVF International Conference on Computing and Communication Technologies*, 37–42. https://doi.org/10.1109/RIVF60135.2023.10471837

Pimentel, J. F., Murta, L., Braganholo, V., & Freire, J. (2019). A large-scale study about quality and reproducibility of jupyter notebooks. *IEEE International Working*

Conference on Mining Software Repositories, *2019-May*, 507–517. https://doi.org/10.1109/MSR.2019.00077

Protić, D. (2020). Influence of pre-processing on anomaly-based intrusion detection. *Vojnotehnicki glasnik*, *68*(3), 598–611. https://doi.org/10.5937/VOJTEHG68-27319

Rafique, S. H., Abdallah, A., Musa, N. S., & Murugan, T. (2024). Machine Learning and Deep Learning Techniques for Internet of Things Network Anomaly Detection—Current Research Trends. *Sensors*, *24*(6). https://doi.org/10.3390/S24061968

Ramotsoela, D., Abu-Mahfouz, A. M., Silva, B., Mujtaba Qureshi, U., Umair, Z., Butt, N., Shahid, A., Naseer Qureshi, K., Haider, S., Osman Ibrahim, A., Binzagr, F., & Arshad, N. (2022). Intelligent Deep Learning for Anomaly-Based Intrusion Detection in IoT Smart Home Networks. *Mathematics 2022, Vol. 10, Page 4598*, *10*(23), 4598. https://doi.org/10.3390/MATH10234598

Ray, P. P. (2018). A survey on Internet of Things architectures. *Journal of King Saud University - Computer and Information Sciences*, *30*(3), 291–319. https://doi.org/10.1016/J.JKSUCI.2016.10.003

Razzaque, M. A., Milojevic-Jevric, M., Palade, A., & Cla, S. (2016). Middleware for internet of things: A survey. *IEEE Internet of Things Journal*, *3*(1), 70–95. https://doi.org/10.1109/JIOT.2015.2498900

Rihan , S. D. A., Anbar , M., & Alabsi, B. A. (2023). Approach for Detecting Attacks on IoT Networks Based on Ensemble Feature Selection and Deep Learning Models. *Sensors*, *23*(17). https://doi.org/10.3390/S23177342

Robacky Mbongo, K. H., Ahmed, K., Mamyrbayev, O., Wang, G., Zuo, F., Akhmediyarova, A., Mukazhanov, N., & Ayapbergenova, A. (2025). Conv1D-GRU-Self Attention: An Efficient Deep Learning Framework for Detecting Intrusions in Wireless Sensor Networks. *Future Internet 2025, Vol. 17, Page 301*, *17*(7), 301. https://doi.org/10.3390/FI17070301

Rohit, M. H., Fahim, S. M., & Khan, A. H. A. (2019). Mitigating and Detecting DDoS attack on IoT Environment. *2019 IEEE International Conference on Robotics, Automation, Artificial-Intelligence and Internet-of-Things, RAAICON 2019*, 5–8. https://doi.org/10.1109/RAAICON48939.2019.5

Rumelhart, D. E., Hinton, G. E., & Williams, R. J. (1986). Learning representations by back-propagating errors. *Nature*, *323*(6088), 533–536. https://doi.org/10.1038/323533A0;KWRD

Scarfone, K., & Mell, P. (2002). *Special Publication 800-94 Guide to Intrusion Detection and Prevention Systems (IDPS) Recommendations of the National Institute of Standards and Technology*. https://doi.org/10.6028/NIST.SP.800-94

Shafiq, M., Tian, Z., Bashir, A. K., Du, X., & Guizani, M. (2020). IoT malicious traffic identification using wrapper-based feature selection mechanisms. *Computers and Security*, *94*. https://doi.org/10.1016/j.cose.2020.101863

Sharma, A., Rani, S., Sah, D. K., Khan, Z., & Boulila, W. (2023). HOMLC-Hyperparameter Optimization for Multi-Label Classification of Intrusion Detection Data for Internet of Things Network. *Sensors*, *23*(19). https://doi.org/10.3390/S23198333

Tipu, R., Rathi, P., Pandya, K., & Panchal, V. (2025). Optimizing sustainable blended concrete mixes using deep learning and multi-objective optimization. *Scientific Reports*, *15*. https://doi.org/10.1038/s41598-025-00943-1

Turner, R., Eriksson, D., McCourt, M., Kiili, J., Laaksonen, E., Xu, Z., & Guyon, I. (2021). Bayesian Optimization is Superior to Random Search for Machine Learning Hyperparameter Tuning: Analysis of the Black-Box Optimization Challenge 2020. *Proceedings of Machine Learning Research*, *133*, 3–26. https://arxiv.org/pdf/2104.10201

Umar, M. A., Chen, Z., Shuaib, K., & Liu, Y. (2025). Effects of feature selection and normalization on network intrusion detection. *Data Science and Management*, *8*(1), 23–39. https://doi.org/10.1016/J.DSM.2024.08.001

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

Varala, C. R. (2025). The Role of GPUs in Artificial Intelligence and Machine Learning. *Journal of e-Science Letters*, *6*(2), 9–12. https://doi.org/10.51470/ESL.2025.6.1.22

Vasudev Karthik Ravindran, Sharad Shyam Ojha, & Arvind Kamboj. (2025). A Comparative Analysis of Signature-Based and Anomaly-Based Intrusion Detection Systems. *International Journal of Latest Technology in Engineering Management & Applied Science*, *14*(5), 209–214. https://doi.org/10.51583/IJLTEMAS.2025.140500026

Verma, N., Kumar, N., Singh, K., Aljohani, A., Sinha, A., & Hussain, S. A. (2025). A novel univariate feature selection with ANOVA F-test-based machine learning model for Intrusion Detection Framework of Robotics system. *Applied Artificial Intelligence*, *39*(1), 2539395. https://doi.org/10.1080/08839514.2025.2539395

Vijayaraj, A., Vasanth Raj, P. T., Jebakumar, R., Gururama Senthilvel, P., Kumar, N., Suresh Kumar, R., & Dhanagopal, R. (2022). Deep Learning Image Classification for Fashion Design. *Wireless Communications and Mobile Computing*, *2022*. https://doi.org/10.1155/2022/7549397

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

Zeeshan, M., Riaz, Q., Bilal, M. A., Shahzad, M. K., Jabeen, H., Haider, S. A., & Rahim, A. (2022). Protocol-Based Deep Intrusion Detection for DoS and DDoS Attacks Using UNSW-NB15 and Bot-IoT Data-Sets. *IEEE Access*, *10*, 2269–2283. https://doi.org/10.1109/ACCESS.2021.3137201

Zhang, Q., Liu, L., Pu, C., Dou, Q., Wu, L., & Zhou, W. (2018). A Comparative Study of Containers and Virtual Machines in Big Data Environment. *IEEE International Conference on Cloud Computing, CLOUD*, *2018-July*, 178–185. https://doi.org/10.1109/CLOUD.2018.00030

Zhang, X. (2017). Melanoma segmentation based on deep learning. *Computer Assisted Surgery*, *22*, 267–277. https://doi.org/10.1080/24699322.2017.1389405

Zhang, Z., & Xu, Z. Q. J. (2024). Implicit Regularization of Dropout. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *46*(6), 4206–4217. https://doi.org/10.1109/TPAMI.2024.3357172

Zhao, X., Wang, L., Zhang, Y., Han, X., Deveci, M., & Parmar, M. (2024). A review of convolutional neural networks in computer vision. *Artificial Intelligence Review*, *57*(4). https://doi.org/10.1007/S10462-024-10721-6