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 (Switzerland)*, *8*(3). https://doi.org/10.3390/electronics8030322

Al-Qatf, M., Lasheng, Y., Al-Habib, M., & Al-Sabahi, K. (2018). Deep Learning Approach Combining Sparse Autoencoder with SVM for Network Intrusion Detection. *IEEE Access*, *6*, 52843–52856. https://doi.org/10.1109/ACCESS.2018.2869577

Alabdulatif, A., & Rizvi, S. H. (2023). Network intrusion detection system using an optimized machine learning algorithm. *Mehran University Research Journal of Engineering and Technology*, *42*(1), 153. https://doi.org/10.22581/muet1982.2301.14

Alao, O. D., Alimi, S., Kuyoro, S. O., Amanze, R. C., Adio, A. K., & Agbaje, M. O. (2022). An Ensemble of Gaussian Mixture Model and Support Vector Machines for Network Intrusion Detection. *Journal of Computer Science*, *18*(9), 868–876. https://doi.org/10.3844/jcssp.2022.868.876

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/electronics11213571

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*(August), 80348–80391. https://doi.org/10.1109/ACCESS.2023.3296444

Bari, B. S., Yelamarthi, K., & Ghafoor, S. (2023). Intrusion Detection in Vehicle Controller Area Network (CAN) Bus Using Machine Learning: A Comparative Performance Study. *Sensors*, *23*(7). https://doi.org/10.3390/s23073610

Bouke, M. A., Abdullah, A., ALshatebi, S. H., & Abdullah, M. T. (2022). E2IDS: An Enhanced Intelligent Intrusion Detection System Based On Decision Tree Algorithm. *Journal of Applied Artificial Intelligence*, *3*(1), 1–16. https://doi.org/10.48185/jaai.v3i1.450

Chen, J., Zhao, Y., Li, Q., Feng, X., & Xu, K. (2022). *FedDef: Defense Against Gradient Leakage in Federated Learning-based Network Intrusion Detection Systems*. https://doi.org/10.1109/TIFS.2023.3297369

Cheng, H. T., Koc, L., Harmsen, J., Shaked, T., Chandra, T., Aradhye, H., Anderson, G., Corrado, G., Chai, W., Ispir, M., Anil, R., Haque, Z., Hong, L., Jain, V., Liu, X., & Shah, H. (2016). Wide & deep learning for recommender systems. *ACM International Conference Proceeding Series*, *15-Septemb*, 7–

10. https://doi.org/10.1145/2988450.2988454

Dahouda, M. K., & Joe, I. (2021). A Deep-Learned Embedding Technique for Categorical Features Encoding. *IEEE Access*, *9*, 114381–114391. https://doi.org/10.1109/ACCESS.2021.3104357

Deng, H., & Yang, T. (2021). Network Intrusion Detection Based on Sparse Autoencoder and IGA-BP Network. *Wireless Communications and Mobile Computing*, *2021*. https://doi.org/10.1155/2021/9510858

Figueiredo, J., Serrão, C., & de Almeida, A. M. (2023). Deep Learning Model Transposition for Network Intrusion Detection Systems. *Electronics (Switzerland)*, *12*(2). https://doi.org/10.3390/electronics12020293

Ganguly, S. (2021). Neural Networks. In *Quantum Machine Learning: An Applied Approach* (pp. 99–139). Apress. https://doi.org/10.1007/978-1-4842-7098-1_3

Ghojogh, B., Crowley, M., Karray, F., & Ghodsi, A. (2023). Uniform Manifold Approximation and Projection (UMAP). *Elements of Dimensionality Reduction and Manifold Learning*, 479–497. https://doi.org/10.1007/978-3-031-10602-6_17

Handika, V., Istiyanto, J. E., Ashari, A., Purnama, S. R., Rochman, S., & Dharmawan, A. (2022). Feature Representation for Network Intrusion Detection System Trough Embedding Neural Network. *Proceeding of the International Conference on Computer Engineering, Network and Intelligent Multimedia, CENIM 2022*, 349–352. https://doi.org/10.1109/CENIM56801.2022.10037425

Hassan, S. K., & Daneshwar, M. A. (2023). Anomaly-based Network Intrusion Detection System using Deep Intelligent Technique. *Polytechnic Journal*, *12*(2), 100–113. https://doi.org/10.25156/ptj.v12n2y2022.pp100-113

Hastie, T., Tibshirani, R., & Friedman, J. (2009). T. elements of statistical learning. (2009). The Elements of Statistical Learning. In *Journal of the Royal Statistical Society Series A: Statistics in Society* (Vol. 167, Issue 1). https://doi.org/10.1111/j.1467-985x.2004.298_11.x

Hewapathirana, I. U. (2025). *A Comparative Study of Two-Stage Intrusion Detection Using Modern Machine Learning Approaches on the*.

Jia, Z., Shen, C., Yi, X., Chen, Y., Yu, T., & Guan, X. (2018). Big-data analysis of multi-source logs for anomaly detection on network-based system. *IEEE International Conference on Automation Science and Engineering*, *2017-Augus*, 1136–1141. https://doi.org/10.1109/COASE.2017.8256257

Juseong Kim, Jinsun Park, G. S. (2021). *Salt : Sharing Attention Between Linear Layer and Transformer for Tabular Dataset*. 1–11.

Kayode Saheed, Y., Idris Abiodun, A., Misra, S., Kristiansen Holone, M., & Colomo-Palacios, R. (2022). A machine learning-based intrusion detection for detecting internet of things network attacks. *Alexandria Engineering Journal*, *61*(12), 9395–9409. https://doi.org/10.1016/j.aej.2022.02.063

Khammassi, C., & Krichen, S. (2017). A GA-LR wrapper approach for feature selection in network intrusion detection. *Computers and Security*, *70*, 255–

277. https://doi.org/10.1016/j.cose.2017.06.005

Khan, M. A., & Kim, J. (2020). Toward developing efficient Conv-AE-based intrusion detection system using heterogeneous dataset. *Electronics (Switzerland)*, *9*(11), 1–17. https://doi.org/10.3390/electronics9111771

Kim, T., & Pak, W. (2023). Deep Learning-Based Network Intrusion Detection Using Multiple Image Transformers. *Applied Sciences (Switzerland)*, *13*(5). https://doi.org/10.3390/app13052754

Kumar, Y. P., & Babu, B. V. (2022). Stabbing of Intrusion with Learning Framework Using Auto Encoder Based Intellectual Enhanced Linear Support Vector Machine for Feature Dimensionality Reduction. *Revue d'Intelligence Artificielle*, *36*(5), 737–743. https://doi.org/10.18280/ria.360511

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

Li, Z., B, Z. Q., & Shen, P. (2019). *Intrusion Detection via Wide and Deep Model*. 717–730.

Maseer, Z. K., Yusof, R., Bahaman, N., Mostafa, S. A., & Foozy, C. F. M. (2021). Benchmarking of Machine Learning for Anomaly Based Intrusion Detection Systems in the CICIDS2017 Dataset. *IEEE Access*, *9*, 22351–22370. https://doi.org/10.1109/ACCESS.2021.3056614

Niyaz, Q., Sun, W., Javaid, A. Y., & Alam, M. (2015). A deep learning approach for network intrusion detection system. *EAI International Conference on Bio-Inspired Information and Communications Technologies (BICT)*. https://doi.org/10.4108/eai.3-12-2015.2262516

Pamungkas, I. G. A. K., Ahmad, T., & Ijtihadie, R. M. (2022). Analysis of Autoencoder Compression Performance in Intrusion Detection System. *International Journal of Safety and Security Engineering*, *12*(3), 395–401. https://doi.org/10.18280/ijsse.120314

Plaka, R. (2021). *Intrusion Detection Using Machine Learning for Industrial Control Systems*. *PG-*. NS -

Pu, G., Wang, L., Shen, J., & Dong, F. (2021). A hybrid unsupervised clustering-based anomaly detection method. *Tsinghua Science and Technology*, *26*(2), 146–153. https://doi.org/10.26599/TST.2019.9010051

Qazi, E. U. H., Almorjan, A., & Zia, T. (2022). A One-Dimensional Convolutional Neural Network (1D-CNN) Based Deep Learning System for Network Intrusion Detection. *Applied Sciences (Switzerland)*, *12*(16). https://doi.org/10.3390/app12167986

Rajendran, P., & Ganapathy, K. (2022). Neural network based seizure detection system using statistical package analysis. *Bulletin of Electrical Engineering and Informatics*, *11*(5), 2547–2554. https://doi.org/10.11591/eei.v11i5.3771

Riadi, S., & Fawaiq, M. N. (2024). *Intrusion Detection System in Network Security Using Naive Bayes and Support Vector Machine*. *November*. https://doi.org/10.70687/ijimatic.v1.i1.24

Saheed, Y. K., Arowolo, M. O., & Tosho, A. U. (2022). An Efficient Hybridization of K-Means and Genetic Algorithm Based on Support Vector Machine for Cyber Intrusion Detection System. *International Journal on Electrical Engineering and Informatics*, *14*(2), 426–442. https://doi.org/10.15676/ijeei.2022.14.2.11

Sarhan, M., Layeghy, S., Moustafa, N., Gallagher, M., & Portmann, M. (2024). Feature extraction for machine learning-based intrusion detection in IoT networks. *Digital Communications and Networks*, *10*(1), 205–216. https://doi.org/10.1016/j.dcan.2022.08.012

Sarumi, O. A., Adetunmbi, A. O., & Adetoye, F. A. (2020). Discovering computer networks intrusion using data analytics and machine intelligence. *Scientific African*, *9*, e00500. https://doi.org/10.1016/j.sciaf.2020.e00500

Thamilarasu, G., & Chawla, S. (2019). Towards deep-learning-driven intrusion detection for the internet of things. *Sensors (Switzerland)*, *19*(9). https://doi.org/10.3390/s19091977

Umar, M. A., & Zhanfang, C. (2020). *Effects of Feature Selection and Normalization on Network Intrusion Detection*. 1–25. https://doi.org/10.36227/techrxiv.12480425

Verma, A., Paneru, E., & Baaniya, B. (2022). Anomaly-Based Network Intrusion Detection System. *Journal of Lumbini Engineering College*, *4*(1), 38–42. https://doi.org/10.3126/lecj.v4i1.49364

Vojinovic, I. (2023). *Data Breach Statistics That Will Make You Think Twice Before Filling Out an Online Form*. Dataprot. https://dataprot.net/statistics/data-breach-statistics/

Wiens, C. (2021). *The Top 5 Zero-Day Attacks of the 21st Century*. Security Boulevard. https://securityboulevard.com/2021/07/the-top-5-zero-day-attacks-of-the-21st-century/

Xiaopeng, C., & Hongyan, Q. (2020). *Deep Feature Extraction via Sparse Autoencoder for Intrusion Detection System*. 61–73. https://doi.org/10.5121/csit.2020.101906

Xu, C., Shen, J., Du, X., & Zhang, F. (2018). An Intrusion Detection System Using a Deep Neural Network with Gated Recurrent Units. *IEEE Access*, *6*, 48697–48707. https://doi.org/10.1109/ACCESS.2018.2867564

Yan, B., & Han, G. (2018). Effective Feature Extraction via Stacked Sparse Autoencoder to Improve Intrusion Detection System. *IEEE Access*, *6*, 41238–41248. https://doi.org/10.1109/ACCESS.2018.2858277

Yan, J., Jin, D., Lee, C. W., & Liu, P. (2018). A Comparative Study of Off-Line Deep Learning Based Network Intrusion Detection. *International Conference on Ubiquitous and Future Networks, ICUFN*, *2018-July*, 299–304. https://doi.org/10.1109/ICUFN.2018.8436774

Zare, F., & Mahmoudi-Nasr, P. (2023). Feature Engineering Methods in Intrusion Detection System: A Performance Evaluation. *International Journal of Engineering, Transactions B: Applications*, *36*(7), 1343–1353. https://doi.org/10.5829/ije.2023.36.07a.15

Zarzoor, A. R., Al-Jamali, N. A. S., & Abdul Qader, D. A. (2023). Intrusion detection method for internet of things based on the spiking neural network and decision tree method. *International Journal of Electrical and Computer Engineering*, *13*(2), 2278–2288. https://doi.org/10.11591/ijece.v13i2.pp2278-2288

Zhang, Y., Muniyandi, R. C., & Qamar, F. (2025). A Review of Deep Learning Applications in Intrusion Detection Systems: Overcoming Challenges in Spatiotemporal Feature Extraction and Data Imbalance. *Applied Sciences (Switzerland)*, *15*(3), 1–20. https://doi.org/10.3390/app15031552

Zong, W., B, Y. C., & Susilo, W. (2019). *Dimensionality Reduction and Visualization of Network Intrusion Detection Data*. Springer International Publishing. https://doi.org/10.1007/978-3-030-21548-4