DAFTAR PUSTAKA

A. Binsaeed, K., & Hafez, A. M. (2023). Enhancing Intrusion Detection Systems with XGBoost Feature Selection and Deep Learning Approaches. *International Journal of Advanced Computer Science and Applications (IJACSA)*, *14*(5), 1084–1098. https://doi.org/10.14569/IJACSA.2023.01405112

Albulayhi, K., Al-Haija, Q. A., Alsuhibany, S. A., Jillepalli, A. A., Ashrafuzzaman, M., & Sheldon, F. T. (2022). IoT Intrusion Detection Using Machine Learning with a Novel High Performing Feature Selection Method. *Applied Sciences (Switzerland)*, *12*(10). https://doi.org/10.3390/app12105015

Aleesa, A. M., Zaidan, B. B., Zaidan, A. A., & Sahar, N. M. (2020). Review of intrusion detection systems based on deep learning techniques: coherent taxonomy, challenges, motivations, recommendations, substantial analysis and future directions. *Neural Computing and Applications*, *32*(14), 9827–9858. https://doi.org/10.1007/s00521-019-04557-3

Alqudah, N., & Yaseen, Q. (2020). Machine Learning for Traffic Analysis: A Review. *Procedia Computer Science*, *170*, 911–916. https://doi.org/10.1016/j.procs.2020.03.111

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

Alshahrani, N. D. (2026). Statistical reproducibility of correlation tests: Pearson, Spearman, and Kendall. *AIMS Mathematics*, *11*(1), 957–976. https://doi.org/10.3934/math.2026042

Alsharaiah, M. A., Abu-Shareha, A. A., Abualhaj, M., Baniata, L. H., Al-Saaidah, A., Kharma, Q. M., & Al-Zyoud, M. M. (2024). An innovative network intrusion detection system (NIDS): Hierarchical deep learning model based on Unsw-Nb15 dataset. *International Journal of Data and Network Science*, *8*(2), 709–722. https://doi.org/10.5267/j.ijdns.2024.1.007

Alzahrani, A. S., Shah, R. A., Qian, Y., & Ali, M. (2020). A novel method for feature learning and network intrusion classification. *Alexandria Engineering Journal*, *59*(3), 1159–1169. https://doi.org/10.1016/j.aej.2020.01.021

Amirjon, A., Gain, M., Kim, K. O., & Hong, C. S. (2025). An Enhanced Intrusion Detection Model with FeedForward Neural Network Classifier. *2025 27th*

International Conference on Advanced Communications Technology (ICACT), 88–93. https://doi.org/10.23919/ICACT63878.2025.10936304

Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, *54*(15), 2787–2805. https://doi.org/10.1016/j.comnet.2010.05.010

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2005). The value of intrusion detection systems in information technology security architecture. *Information Systems Research*, *16*(1), 28–46. https://doi.org/10.1287/isre.1050.0041

Chen, D., Wawrzynski, P., & Lv, Z. (2021). Cyber security in smart cities: A review of deep learning-based applications and case studies. *Sustainable Cities and Society*, *66*(March 2021). https://doi.org/10.1016/j.scs.2020.102655

Christen, P., Hand, D. J., & Kirielle, N. (2023). A Review of the F-Measure: Its History, Properties, Criticism, and Alternatives. *ACM Computing Surveys*, *56*(3). https://doi.org/10.1145/3606367

Cil, A. E., Yildiz, K., & Buldu, A. (2021). Detection of DDoS attacks with feed forward based deep neural network model. *Expert Systems with Applications*, *169*(May 2021). https://doi.org/10.1016/j.eswa.2020.114520

Committee on National Security Systems. (2022). *Committee on National Security Systems Committee on National Security Systems (CNSS) Glossary*. https://csrc.nist.gov/glossary/term/intrusion

Dao, T.-N., & Lee, H. (2022). Stacked Autoencoder-Based Probabilistic Feature Extraction for On-Device Network Intrusion Detection. *IEEE Internet of Things Journal*, *9*(16), 14438–14451. https://doi.org/10.1109/JIOT.2021.3078292

Das, A., Pramod, & B S, S. (2022). Anomaly-based Network Intrusion Detection using Ensemble Machine Learning Approach. *IJACSA) International Journal of Advanced Computer Science and Applications*, *13*(2), 635–645. www.ijacsa.thesai.org

De Donno, M., Dragoni, N., Giaretta, A., & Spognardi, A. (2018). DDoS-Capable IoT Malwares: Comparative Analysis and Mirai Investigation. *Security and Communication Networks*, *2018*(1). https://doi.org/10.1155/2018/7178164

Denning, D., & Neuman, P. G. (1985). *Requirements and model for IDES-A Real-time Intrusion-Detection Expert System*.

Diro, A. A., & Chilamkurti, N. (2018). Distributed attack detection scheme using deep learning approach for Internet of Things. *Future Generation Computer*

Systems, *82*(May 2018), 761–768. https://doi.org/10.1016/j.future.2017.08.043

FortiGuard SE Team. (2019). *Cyber and Physical Convergence is Creating New Attack Opportunities for Cybercriminals*. https://www.fortinet.com/corporate/about-us/newsroom/press-releases/2019/cyber-and-physical-convergence-is-creating-new-attack-opportunit

Friha, O., Amine, M., Shu, L., Maglaras, L., Choo, R., & Nafaa, M. (2022). FELIDS : Federated learning-based intrusion detection system for agricultural Internet of Things. *Journal of Parallel and Distributed Computing*, *165*(July 2022), 17–31. https://doi.org/10.1016/j.jpdc.2022.03.003

Gaber, T., El-Ghamry, A., & Hassanien, A. E. (2022). Injection attack detection using machine learning for smart IoT applications. *Physical Communication*, *52*(June 2022), 101685. https://doi.org/10.1016/j.phycom.2022.101685

Gamage, S., & Samarabandu, J. (2020). Deep learning methods in network intrusion detection: A survey and an objective comparison. *Journal of Network and Computer Applications*, *169*(1 November 2020). https://doi.org/10.1016/j.jnca.2020.102767

Gavel, S., Raghuvanshi, A. S., & Tiwari, S. (2022). Maximum correlation based mutual information scheme for intrusion detection in the data networks. *Expert Systems with Applications*, *189*(1 March 2022). https://doi.org/10.1016/j.eswa.2021.116089

Gencturk, E., Ustubioglu, B., Ulutas, G., & Symeonidis, I. (2026). Class Imbalance in IoMT Datasets: Evaluating Balancing Strategies for Learning-Based Attack Detection. *Applied Sciences (Switzerland)*, *16*(10). https://doi.org/10.3390/app16104921

Gnatyuk, S., Berdibayev, R., Aleksander, M., Sydorenko, V., Zhyharevych, O., & Polozhentsev, A. (2024). Software System for Cybersecurity Events Correlation and Incident Management in Critical Infrastructure. In *Data-Centric Business and Applications: Advancements in Information and Knowledge Management, Volume 1* (pp. 247–269). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-62213-7_12

Gopi, R., Sathiyamoorthi, V., Selvakumar, S., Manikandan, R., Chatterjee, P., Jhanjhi, N. Z., & Luhach, A. K. (2022). Enhanced method of ANN based model for detection of DDoS attacks on multimedia internet of things. *Multimedia*

Tools and Applications, *81*(19), 26739–26757. https://doi.org/10.1007/s11042-021-10640-6

Gupta, S. K., Tripathi, M., & Grover, J. (2022). Hybrid optimization and deep learning based intrusion detection system. *Computers and Electrical Engineering*, *100*(May 2022), 107876. https://doi.org/10.1016/j.compeleceng.2022.107876

Gupta, S., & Singh, B. (2026). Lightweight ensemble learning based intrusion detection framework with explainable artificial intelligence. *Engineering Applications of Artificial Intelligence*, *163*(1 January 2026), 112936. https://doi.org/10.1016/j.engappai.2025.112936

Hakami, H., Faheem, M., & Bashir Ahmad, M. (2025). Machine Learning Techniques for Enhanced Intrusion Detection in IoT Security. *IEEE Access*, *13*, 31140–31158. https://doi.org/10.1109/ACCESS.2025.3542227

Hameed, K., Garg, S., Amin, M. B., Kang, B., & Khan, A. (2022). A context-aware information-based clone node attack detection scheme in Internet of Things. *Journal of Network and Computer Applications*, *197*. https://doi.org/10.1016/j.jnca.2021.103271

Haykin, S. (1999). *Simon Haykin-Neural Networks-A Comprehensive Foundation* (Second Edition). Prentice Hall.

Henry, A., Gautam, S., Khanna, S., Rabie, K., Shongwe, T., Bhattacharya, P., Sharma, B., & Chowdhury, S. (2023). Composition of Hybrid Deep Learning Model and Feature Optimization for Intrusion Detection System. *Sensors*, *23*(2). https://doi.org/10.3390/s23020890

James, P. A., & Co. (1980). Computer Security Threat Monitoring and Surveillance. In *Box* (Vol. 42).

Jan, M. A., Cai, J., Gao, X. C., Khan, F., Mastorakis, S., Usman, M., Alazab, M., & Watters, P. (2021). Security and blockchain convergence with Internet of Multimedia Things: Current trends, research challenges and future directions. *Journal of Network and Computer Applications*, *175*(1 February 2021), 102918. https://doi.org/10.1016/j.jnca.2020.102918

Kasongo, S. M., & Sun, Y. (2020). A deep learning method with wrapper based feature extraction for wireless intrusion detection system. *Computers and Security*, *92*(May 2020), 101752. https://doi.org/10.1016/j.cose.2020.101752

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

Khaire, U. M., & Dhanalakshmi, R. (2022). Stability of feature selection algorithm: A review. *Journal of King Saud University - Computer and Information Sciences*, *34*(4), 1060–1073. https://doi.org/10.1016/j.jksuci.2019.06.012

Kou, G., Lu, Y., Peng, Y., & Shi, Y. (2012). Evaluation of classification algorithms using MCDM and rank correlation. *International Journal of Information Technology and Decision Making*, *11*(1), 197–225. https://doi.org/10.1142/S0219622012500095

Kovacs, E. (n.d.). *Many Hikvision Cameras Exposed to Attacks Due to Critical Vulnerability*. Retrieved July 15, 2022, from https://www.securityweek.com/many-hikvision-cameras-exposed-attacks-due-critical-vulnerability

Kozik, R. (2018). Distributed System for Botnet Traffic Analysis and Anomaly Detection. *Proceedings - 2017 IEEE International Conference on Internet of Things, IEEE Green Computing and Communications, IEEE Cyber, Physical and Social Computing, IEEE Smart Data, IThings-GreenCom-CPSCom-SmartData 2017*, *2018-January*, 330–335. https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData.2017.55

Kunang, Y. N., Nurmaini, S., Stiawan, D., & Suprapto, B. Y. (2021). Attack classification of an intrusion detection system using deep learning and hyperparameter optimization. *Journal of Information Security and Applications*, *58*(May 2021), 102804. https://doi.org/10.1016/j.jisa.2021.102804

Kuncheva, L. I., & Whitaker, C. J. (2003). Measures of Diversity in Classifier Ensembles and Their Relationship with the Ensemble Accuracy. *Machine Learning*, *51*(May 2023), 181–207. https://doi.org/10.1023/A:1022859003006

Lawall, M. A., Shaikh, R. A., & Hassan, S. R. (2021). A DDoS Attack Mitigation Framework for IoT Networks using Fog Computing. *Procedia Computer Science*, *182*, 13–20. https://doi.org/10.1016/j.procs.2021.02.003

Li, D., Deng, L., Lee, M., & Wang, H. (2019). IoT data feature extraction and intrusion detection system for smart cities based on deep migration learning.

International Journal of Information Management, *49*(December 2019), 533–545. https://doi.org/10.1016/j.ijinfomgt.2019.04.006

Li, J., Chen, H., Shahizan, M. O., & Yusuf, L. M. (2024). Enhancing IoT security: A comparative study of feature reduction techniques for intrusion detection system. *Intelligent Systems with Applications*, *23*(September 2024), 200407. https://doi.org/10.1016/j.iswa.2024.200407

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, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

Liu, H., & Lang, B. (2019). Machine learning and deep learning methods for intrusion detection systems: A survey. *Applied Sciences (Switzerland)*, *9*(20). https://doi.org/10.3390/app9204396

Liu, J., Yang, D., Lian, M., & Li, M. (2021). Research on intrusion detection based on particle swarm optimization in IoT. *IEEE Access*, *9*, 38254–38268. https://doi.org/10.1109/ACCESS.2021.3063671

Lu, Y., Chai, S., Suo, Y., Yao, F., & Zhang, C. (2024). Intrusion detection for Industrial Internet of Things based on deep learning. *Neurocomputing*, *564*(7 January 2024), 126886. https://doi.org/10.1016/j.neucom.2023.126886

Ma, H., Zhang, W., Zhang, D., & Chen, B. (2025). An IoT intrusion detection framework based on feature selection and large language models fine-tuning. *Scientific Reports*, *15*(1). https://doi.org/10.1038/s41598-025-08905-3

Madan, S., Sofat, S., & Bansal, D. (2022). Tools and Techniques for Collection and Analysis of Internet-of-Things malware: A systematic state-of-art review. *Journal of King Saud University - Computer and Information Sciences*, *34*(10), 9867–9888. https://doi.org/10.1016/j.jksuci.2021.12.016

Martins, I., Resende, J. S., Sousa, P. R., Silva, S., Antunes, L., & Gama, J. (2022). Host-based IDS: A review and open issues of an anomaly detection system in IoT. *Future Generation Computer Systems*, *133*(August 2022), 95–113. https://doi.org/10.1016/j.future.2022.03.001

Mirkes, E. M., Allohibi, J., & Gorban, A. (2020). Fractional norms and quasinorms do not help to overcome the curse of dimensionality. *Entropy*, *22*(10), 1–31. https://doi.org/10.3390/e22101105

Moustafa, N., & Slay, J. (2015, December 7). UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). *2015 Military Communications and Information Systems Conference, MilCIS 2015 - Proceedings*. https://doi.org/10.1109/MilCIS.2015.7348942

Moustafa, N., & Slay, J. (2016). The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set. *Information Security Journal: A Global Perspective*, *25*(1–3), 18–31. https://doi.org/10.1080/19393555.2015.1125974

Nath N, R., & V Nath, H. (2022). Critical analysis of the layered and systematic approaches for understanding IoT security threats and challenges. *Computers and Electrical Engineering*, *100*(May 2022), 107997. https://doi.org/10.1016/j.compeleceng.2022.107997

Nauman, A., Qadri, Y. A., Amjad, M., Zikria, Y. bin, Afzal, M. K., & Kim, S. W. (2020). Multimedia internet of things: A comprehensive survey. *IEEE Access*, *8*, 8202–8250. https://doi.org/10.1109/ACCESS.2020.2964280

Nguyen, G. L., Dumba, B., Ngo, Q., Le, H., & Nguyen, T. N. (2022). A collaborative approach to early detection of IoT Botnet ☆. *Computers and Electrical Engineering*, *97*(January 2022), 107525. https://doi.org/10.1016/j.compeleceng.2021.107525

Omolara, A. E., Alabdulatif, A., Abiodun, O. I., Alawida, M., Alabdulatif, A., Alshoura, W. H., & Arshad, H. (2022). The internet of things security: A survey encompassing unexplored areas and new insights. *Computers and Security*, *112*, 102494. https://doi.org/10.1016/j.cose.2021.102494

Osa, E., Orukpe, P. E., & Iruansi, U. (2024). Design and implementation of a deep neural network approach for intrusion detection systems. *E-Prime - Advances in Electrical Engineering, Electronics and Energy*, *7*(March 2024), 100434. https://doi.org/10.1016/j.prime.2024.100434

Pao, W. (2021, December 24). *Top cyber threats against IP cameras and ways to prevent them*. https://www.asmag.com/showpost/32708.aspx

Patil, N. V., Rama Krishna, C., Kumar, K., & Behal, S. (2022). E-Had: A distributed and collaborative detection framework for early detection of DDoS attacks. *Journal of King Saud University - Computer and Information Sciences*, *34*(4), 1373–1387. https://doi.org/10.1016/j.jksuci.2019.06.016

Popoola, S. I., Adebisi, B., Hammoudeh, M., Gui, G., & Gacanin, H. (2021). Hybrid Deep Learning for Botnet Attack Detection in the Internet-of-Things Networks. *IEEE Internet of Things Journal*, *8*(6), 4944–4956. https://doi.org/10.1109/JIOT.2020.3034156

Pramanick, N., Mathew, J., Selvarajan, S., & Agarwal, M. (2025). Leveraging stacking machine learning models and optimization for improved cyberattack detection. *Scientific Reports*, *15*(1). https://doi.org/10.1038/s41598-025-01052-9

Radanliev, P., De Roure, D. C., Nicolescu, R., Huth, M., Montalvo, R. M., Cannady, S., & Burnap, P. (2018). Future developments in cyber risk assessment for the internet of things. *Computers in Industry*, *102*(November 2018), 14–22. https://doi.org/10.1016/j.compind.2018.08.002

Rashid, M. M., Kamruzzaman, J., Hassan, M. M., Imam, T., & Gordon, S. (2020). Cyberattacks detection in iot-based smart city applications using machine learning techniques. *International Journal of Environmental Research and Public Health*, *17*(24), 1–21. https://doi.org/10.3390/ijerph17249347

Rokach, L., & Maimon, O. (2015). *DATA MINING WITH DECISION TREES* (A. Yun, Ed.; 2nd ed., Vol. 81). World Scientific Publishing Co. Pte. Ltd. http://www.worldscientific.com/series/smpai

Saeys, Y., Abeel, T., & Van de Peer, Y. (2008). Robust Feature Selection Using Ensemble Feature Selection Techniques. *Machine Learning and Knowledge Discovery in Databases*, *5212*(1), 313–325. https://doi.org/10.1007/978-3-540-87481-2_21

Safi, A., & Singh, S. (2023). A systematic literature review on phishing website detection techniques. *Journal of King Saud University - Computer and Information Sciences*, *35*(2), 590–661. https://doi.org/10.1016/j.jksuci.2023.01.004

Salman, R., Alzaatreh, A., & Sulieman, H. (2026). Review of Feature Selection Methods and Their Ensembles. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *16*(2), 1–26. https://doi.org/10.1002/widm.70085

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

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

Sedrakyan, H., & Sedrakyan, N. (2018). The Cauchy–Bunyakovsky–Schwarz Inequality. In P. Winkler (Ed.), *Problem Books in Mathematics* (1st ed., pp. 45–57). Springer, Cham. https://doi.org/10.1007/978-3-319-77836-5_4

Sehrawat, S., & Singh, D. (2023). Deep Learning Approach to Enhance IDS Accuracy using Hybrid LSTM Algorithm. *2023 14th International Conference on Computing Communication and Networking Technologies, ICCCNT 2023*, 56998. https://doi.org/10.1109/ICCCNT56998.2023.10307354

Shahin, M., Maghanaki, M., Hosseinzadeh, A., & Chen, F. F. (2024). Advancing Network Security in Industrial IoT: A Deep Dive into AI-Enabled Intrusion Detection Systems. *Advanced Engineering Informatics*, *62*(October 2024), 102685. https://doi.org/10.1016/j.aei.2024.102685

Sharif, R. Al, & Pokharel, S. (2022). Smart City Dimensions and Associated Risks: Review of literature. *Sustainable Cities and Society*, *77*(February 2022). https://doi.org/10.1016/j.scs.2021.103542

Sharma, B., Sharma, L., Lal, C., & Roy, S. (2023). Anomaly based network intrusion detection for IoT attacks using deep learning technique. *Computers and Electrical Engineering*, *107*(April 2023), 108626. https://doi.org/10.1016/j.compeleceng.2023.108626

Sharma, H. S., & Singh, K. J. (2024). A feed forward deep neural network model using feature selection for cloud intrusion detection system. *Concurrency and Computation: Practice and Experience*, *36*(9). https://doi.org/10.1002/cpe.8001

Sikos, L. F. (2020). Packet analysis for network forensics: A comprehensive survey. *Forensic Science International: Digital Investigation*, *32*(March 2020), 200892. https://doi.org/10.1016/j.fsidi.2019.200892

Soflaei, M. R. A. B., Salehpour, A., & Samadzamini, K. (2024). Enhancing network intrusion detection: a dual-ensemble approach with CTGAN-balanced data and weak classifiers. *The Journal of Supercomputing*, *80*(11), 16301–16333. https://doi.org/10.1007/s11227-024-06108-7

SonicWall. (2019). *SonicWall Cyber Threat Report*. https://www.sonicwall.com/medialibrary/en/white-paper/2019-sonicwall-cyber-threat-report.pdf

Spearman, C. (1904). The Proof and Measurement of Association between Two Things. *The American Journal of Psychology*, *15*(1), 72–101.

Suyanto. (2019). *Data Mining : untuk Klasifikasi dan Klasterisasi Data* (first). Penerbit Informatika.

Swarna Priya, R. M., Maddikunta, P. K. R., Parimala, M., Koppu, S., Gadekallu, T. R., Chowdhary, C. L., & Alazab, M. (2020). An effective feature engineering for DNN using hybrid PCA-GWO for intrusion detection in IoMT architecture. *Computer Communications*, *160*(1 July 2020), 139–149. https://doi.org/10.1016/j.comcom.2020.05.048

Thakkar, A., & Lohiya, R. (2021a). A Review on Machine Learning and Deep Learning Perspectives of IDS for IoT: Recent Updates, Security Issues, and Challenges. *Archives of Computational Methods in Engineering*, *28*(4), 3211–3243. https://doi.org/10.1007/s11831-020-09496-0

Thakkar, A., & Lohiya, R. (2021b). Analyzing fusion of regularization techniques in the deep learning-based intrusion detection system. *International Journal of Intelligent Systems*, *36*(12), 7340–7388. https://doi.org/10.1002/int.22590

Thakkar, A., & Lohiya, R. (2023). Fusion of statistical importance for feature selection in Deep Neural Network-based Intrusion Detection System. *Information Fusion*, *90*(February 2023), 353–363. https://doi.org/10.1016/j.inffus.2022.09.026

Tidjon, L. N., Frappier, M., & Mammar, A. (2019). Intrusion Detection Systems : A Cross-Domain Overview. *IEEE Communications Surveys & Tutorials*, *21*(4), 3639–3681.

Tseng, C. H., & Chang, Y. T. (2023). EBDM: Ensemble binary detection models for multi-class wireless intrusion detection based on deep neural network. *Computers and Security*, *133*(October 2023). https://doi.org/10.1016/j.cose.2023.103419

Vigneswaran, R., Kp, S., & Poornachandran, P. (2018, July 10). Evaluating Shallow and Deep Neural Networks for Network Intrusion Detection Systems in Cyber Security. *2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*. https://doi.org/10.1109/ICCCNT.2018.8494096

Wang, Z., Liu, Y., He, D., & Chan, S. (2021). Intrusion detection methods based on integrated deep learning model. *Computers and Security*, *103*(April 2021), 102177. https://doi.org/10.1016/j.cose.2021.102177

Yang, Z., Liu, X., Li, T., Wu, D., Wang, J., Zhao, Y., & Han, H. (2022). A systematic literature review of methods and datasets for anomaly-based network

intrusion detection. *Computers & Security*, *116*(May 2022), 102675. https://doi.org/10.1016/j.cose.2022.102675

Ye, Z., Luo, J., Zhou, W., Wang, M., & He, Q. (2024). An ensemble framework with improved hybrid breeding optimization-based feature selection for intrusion detection. *Future Generation Computer Systems*, *151*(February 2024), 124–136. https://doi.org/10.1016/j.future.2023.09.035

Yousuf, O., & Mir, R. N. (2022). DDoS attack detection in Internet of Things using recurrent neural network. *Computers and Electrical Engineering*, *101*(July 2022), 108034. https://doi.org/10.1016/j.compeleceng.2022.108034

Yu, H., & Hutson, A. D. (2024). A robust Spearman correlation coefficient permutation test. *Communications in Statistics - Theory and Methods*, *53*(6), 2141–2153. https://doi.org/10.1080/03610926.2022.2121144

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

Zhang, L., Liu, K., Xie, X., Bai, W., Wu, B., & Dong, P. (2023). A data-driven network intrusion detection system using feature selection and deep learning. *Journal of Information Security and Applications*, *78*(November 2023), 103606. https://doi.org/10.1016/j.jisa.2023.103606

Zhao, Z. (2017). *Ensemble Methods for Anomaly Detection* [Dissertations, Syracuse University]. https://surface.syr.edu/etd/817

Zhou, P., Xie, X., Lin, Z., & Yan, S. (2024). Towards Understanding Convergence and Generalization of AdamW. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *46*(9), 6486–6493. https://doi.org/10.1109/TPAMI.2024.3382294

Zhu, H., You, X., & Liu, S. (2019). Multiple Ant Colony Optimization Based on Pearson Correlation Coefficient. *IEEE Access*, *7*, 61628–61638. https://doi.org/10.1109/ACCESS.2019.2915673