DAFTAR PUSTAKA

[1] H. Fatima, G. N. Dash, and S. K. Pradhan, "Soft Computing applications in Cyber crimes," in *2017 2nd International Conference on Anti-Cyber Crimes, ICACC 2017*. IEEE, 2017, pp. 66–69.

[2] BSSN, "Laporan Tahunan 2020 Monitoring Keamanan Siber," 2020.

[3] P. Rosler, C. Mainka, and J. Schwenk, "More is Less : On the End-to-End Security of Group Chats in Signal, WhatsApp, and Threema," *2018 IEEE European Symposium on Security and Privacy More*, 2018.

[4] F. Salo, M. Injadat, A. B. Nassif, A. Shami, and A. Essex, "Data mining techniques in intrusion detection systems: A systematic literature review," *IEEE Access*, vol. 6, pp. 56 046–56 058, 2018.

[5] A. Nisioti, A. Mylonas, P. D. Yoo, and V. Katos, "From intrusion detection to attacker attribution: A comprehensive survey of unsupervised methods," *IEEE Communications Surveys and Tutorials Surveys & Tutorials*, vol. 20, no. 4, p. 3369, 2018.

[6] T. A. Alamiedy, M. Anbar, Z. N. Alqattan, and Q. M. Alzubi, "Anomaly-based intrusion detection system using multi-objective grey wolf optimisation algorithm," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, 2019.

[7] D. Sovilj, P. Budnarain, S. Sanner, G. Salmon, and M. Rao, "A comparative evaluation of unsupervised deep architectures for intrusion detection in sequential data streams," *Expert Systems with Applications*, vol. 159, 2020.

[8] H. Rajadurai and U. D. Gandhi, "A stacked ensemble learning model for intrusion detection in wireless network," *Neural Computing and Applications*, vol. 5, 2020. [Online]. Available: https://doi.org/10.1007/s00521-020-04986-5

[9] U. H. Rao and U. Nayak, *The InfoSec Handbook An Introduction to Information Security*. India: Apress Open, 2014, vol. 148.

[10] L. Hu, T. Li, N. Xie, and J. Hu, "False positive elimination in intrusion detection based on clustering," in *2015 12th International Conference on Fuzzy Systems and Knowledge Discovery, FSKD 2015*. IEEE, 2015, pp. 519–523.

[11] A. Sultana and M. A. Jabbar, "Intelligent network intrusion detection system using data mining techniques," in *2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT)*. IEEE, 2016. [Online]. Available: http://dx.doi.org/10.1109/icatcct.2016.7912017

[12] S. Thaseen Ikram and A. Kumar Cherukuri, "Intrusion detection model using fusion of chi-square feature selection and multi class SVM," *Journal of King Saud University - Computer and Information Sciences*, vol. 29, no. 4, pp. 462–472, 2017.

[13] S. Muller, J. Lancrenon, C. Harpes, Y. Le Traon, S. Gombault, and J.-M. M. Bonnin, "A training-resistant anomaly detection system," *Computers and Security*, vol. 76, pp. 1–11, 2018.

[14] F. Salo, A. B. Nassif, and A. Essex, "Dimensionality reduction with IG-PCA and ensemble classifier for network intrusion detection," *Computer Networks*, vol. 148, pp. 164–175, 2019.

[15] L. Chen, X. Kuang, A. Xu, S. Suo, and Y. Yang, "A Novel Network Intrusion Detection System Based on CNN," *Proceedings - 2020 8th International Conference on Advanced Cloud and Big Data, CBD 2020*, pp. 243–247, 2020.

[16] G. Yedukondalu, G. H. Bindu, J. Pavan, G. Venkatesh, and A. Saiteja, "Intrusion Detection System Framework Using Machine Learning," *Proceedings of the 3rd International Conference on Inventive Research in Computing Applications, ICIRCA 2021*, pp. 1224–1230, 2021.

[17] C. R. Wang, R. F. Xu, S. J. Lee, and C. H. Lee, "Network intrusion detection using equality constrained-optimization-based extreme learning machines," *Knowledge-Based Systems*, vol. 147, pp. 68–80, 2018.

[18] A. Amarudin, R. Ferdiana, and W. Widyawan, "A Systematic Literature Review of Intrusion Detection System for Network Security: Research Trends, Datasets and Methods," in *The 4th International Conference on Informatics and Computational Sciences*. IEEE Explore, 2020.

[19] X. An, J. Su, X. Lu, and F. Lin, "Hypergraph clustering model-based association analysis of DDOS attacks in fog computing intrusion detection system," *Eurasip Journal on Wireless Communications and Networking*, vol. 11, p. 249, 2018. [Online]. Available: https://dblp.uni-trier.de/db/journals/ejwcn/ejwcn2018.html#AnSLL18

[20] E. M. Roopa Devi and R. C. Suganthe, "Improved Relevance Vector Machine (IRVM) classifier for Intrusion Detection System," *Soft Computing*, vol. 23, no. 19, pp. 9111–9119, oct 2018. [Online]. Available: https://doi.org/10.1007/s00500-018-3621-z

[21] C. Callegari, S. Giordano, and M. Pagano, "An information-theoretic method for the detection of anomalies in network traffic," *Computers and Security*, vol. 70, pp. 351–365, 2017. [Online]. Available: https://doi.org/10.1016/j.cose.2017.07.004

[22] Y. Liu, L. Zhu, and F. Liu, "Design of Multimedia Education Network Security and Intrusion Detection System," *Multimedia Tools and Applications*, 2020.

[23] I. Ghafir, M. Hammoudeh, V. Prenosil, L. Han, R. Hegarty, K. Rabie, and F. J. Aparicio-Navarro, "Detection of advanced persistent threat using machine-learning correlation analysis," *Future Generation Computer Systems*, vol. 89, pp. 349–359, 2018. [Online]. Available: https://doi.org/10.1016/j.future.2018.06.055

[24] J. Manan, A. Ahmed, I. Ullah, L. Merghem-Boulahia, and D. Gaiti, "Distributed intrusion detection scheme for next generation networks," *Journal of Network and Computer Applications*, vol. 147, p. 102422, 2019. [Online]. Available: https://doi.org/10.1016/j.jnca.2019.102422

[25] Y. Al-Hadhrami and F. K. Hussain, "Real time dataset generation framework for intrusion detection systems in IoT," *Future Generation Computer Systems*, vol. 108, pp. 414–423, jul 2020. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0167739X19322678

[26] Wenjuan Li, W. Meng, X. Luo, and L. F. Kwok, "MVPSys: Toward practical multi-view based false alarm reduction system in network intrusion detection," *Computers and Security*, vol. 60, pp. 177–192, 2016.

[27] H. Wang, J. Gu, and S. Wang, "An effective intrusion detection framework based on SVM with feature augmentation," *Knowledge-Based Systems*, vol. 136, pp. 130–139, 2017.

[28] G. Macia-Fernandez, J. Camacho, R. Magan-Carrion, P. Garcia-Teodoro, and R. Theron, "UGR16: A new dataset for the evaluation of cyclostationarity-based network IDSs," *Computers and Security*, vol. 73, pp. 411–424, 2018.

[29] S. C. Sethuraman, S. Dhamodara, and V. Vijayakumar, "Intrusion detection system for detecting wireless attacks in IEEE 802.11 networks," *IET Networks*, vol. 8, no. 4, pp. 219–232, 2019.

[30] P. Krishnan, S. Duttagupta, and K. Achuthan, "VARMAN: Multi-plane security framework for software defined networks," *Computer Communications*, vol. 148, no. July, pp. 215–239, 2019.

[31] S. Dwibedi, M. Pujari, and W. Sun, "A Comparative Study on Contemporary Intrusion Detection Datasets for Machine Learning Research," in *Proceedings - 2020 IEEE International Conference on Intelligence and Security Informatics, ISI 2020*, 2020, pp. 4–9.

[32] J. Liang, J. Chen, Y. Zhu, F. R. Yu, R. Yu, and F. R. Yu, "A novel Intrusion Detection System for Vehicular Ad Hoc Networks (VANETs) based on differences of traffic flow and position," *Applied Soft Computing Journal*, vol. 75, pp. 712–727, 2019.

[33] M. Gajewski, J. Mongay Batalla, A. Levi, C. Togay, C. X. Mavromoustakis, G. Mastorakis, J. M. Batalla, A. Levi, C. Togay, C. X. Mavromoustakis, and G. Mastorakis, "Two-tier anomaly detection based on traffic profiling of the home automation system," *Computer Networks*, vol. 158, pp. 46–60, 2019.

[34] F. H. Almasoudy, W. L. Al-Yaseen, and A. K. Idrees, "Differential Evolution Wrapper Feature Selection for Intrusion Detection System," in *Procedia Computer Science*, vol. 167, no. 2019. Elsevier B.V., 2020, pp. 1230–1239. [Online]. Available: https://doi.org/10.1016/j.procs.2020.03.438

[35] J. Zhang, H. Li, Q. Gao, H. Wang, and Y. Luo, "Detecting anomalies from big network traffic data using an adaptive detection approach," *Information Sciences*, vol. 318, pp. 91–110, 2015.

[36] N. Acharya and S. Singh, "An IWD-based feature selection method for intrusion detection system," *Soft Computing*, vol. 22, no. 13, pp. 4407–4416, 2018.

[37] Y. Zhou, G. Cheng, S. Jiang, and M. Dai, "Building an efficient intrusion detection system based on feature selection and ensemble classifier," *Computer Networks*, vol. 174, no. April, 2020.

[38] S.-H. Kang and K. J. Kim, "A feature selection approach to find optimal feature subsets for the network intrusion detection system," *Cluster Computing*, vol. 19, pp. 325–333, 2016.

[39] E. Popoola and A. Adewumi, "Efficient feature selection technique for network intrusion detection system using discrete differential evolution and decision tree," *International Journal of Network Security*, vol. 19, pp. 660–669, sep 2017.

[40] B. A. Tama and K. H. Rhee, "A combination of PSO-based feature selection and tree-based classifiers ensemble for intrusion detection systems," *Lecture Notes in Electrical Engineering*, vol. 373, pp. 489–495, 2015.

[41] A. I. Madbouly and T. Barakat, "Enhanced relevant feature selection model for intrusion detection systems," *International Journal of Intelligent Engineering Informatics*, vol. 4, no. 1, pp. 21–45, 2016.

[42] A. S. Alzahrani, R. A. Shah, Y. Qian, and M. Ali, "A novel method for feature learning and network intrusion classification," *Alexandria Engineering Journal*, 2020.

[43] M. Moukhafi, K. El Yasin, and S. Bri, "A novel hybrid GA and SVM with PSO feature selection for intrusion detection system," *ijasre*, vol. 4, no. 5, pp. 129–134, 2018.

[44] S. Mohammadi, H. Mirvaziri, M. Ghazizadeh-Ahsaee, and H. Karimipour, "Cyber intrusion detection by combined feature selection algorithm," *Journal of Information Security and Applications*, vol. 44, pp. 80–88, 2019.

[45] B. A. Tama and K. H. Rhee, "Performance Analysis of Multiple Classifier System in DoS Attack Detection," in *Springer International Publishing Switzerland*, vol. 9503, no. January 2016, 2016.

[46] X. Zou, J. Cao, Q. Guo, and T. Wen, "A novel network security algorithm based on improved support vector machine from smart city perspective," *Computers and Electrical Engineering*, vol. 65, no. 3, pp. 67–78, 2018. [Online]. Available: https://doi.org/10.1016/j.compeleceng.2017.09.028

[47] X. Gao, C. Shan, C. Hu, Z. Niu, and Z. Liu, "An Adaptive Ensemble Machine Learning Model for Intrusion Detection," *IEEE Access*, vol. 7, pp. 82 512–82 521, 2019. [Online]. Available: https://dblp.uni-trier.de/db/journals/access/access7.html#GaoSHNL19

[48] J. Zhao, J. Jin, S. Chen, R. Zhang, B. Yu, and Q. Liu, "A weighted hybrid ensemble method for classifying imbalanced data," *Knowledge-Based Systems*, vol. 203, p. 106087, 2020. [Online]. Available: https://doi.org/10.1016/j.knosys.2020.106087

[49] A. A. Aburomman and M. B. I. Reaz, "A novel SVM-kNN-PSO ensemble method for intrusion detection system," *Applied Soft Computing Journal*, vol. 38, pp. 360–372, 2016.

[50] T. Wisanwanichthan and M. Thammawichai, "A Double-Layered Hybrid Approach for Network Intrusion Detection System Using Combined Naive Bayes and SVM," *IEEE Access*, vol. 9, pp. 138 432–138 450, 2021.

[51] U. S. Musa, M. Chhabra, A. Ali, and M. Kaur, "Intrusion Detection System using Machine Learning Techniques: A Review," in *Proceedings of the International Conference on Smart Electronics and Communication (ICOSEC 2020)*, no. Icosec, 2020, pp. 61–71.

[52] M. Anbar, R. Abdullah, I. H. Hasbullah, Y.-W. W. Chong, and O. E. Elejla, "Comparative performance analysis of classification algorithms for intrusion detection system," in *Conference on Privacy, Security and Trust*, no. April. IEEE, 2016, pp. 282–288. [Online]. Available: https://ieeexplore.ieee.org/document/7906975

[53] M. Belhor and F. Jemili, "Intrusion Detection Based on Genetic Fuzzy Classification System," in *Proceedings of IEEE/ACS International Conference on Computer Systems and Applications, AICCSA*. IEEE, 2016, pp. 1–8.

[54] W. Chen, F. Kong, F. Mei, G. Yuan, and B. Li, "A Novel Unsupervised Anomaly Detection Approach for Intrusion Detection System," in *2017 IEEE 3rd International Conference on Big Data Security on Cloud*. IEEE, 2017, pp. 69–73.

[55] A. Yang, Y. Zhuansun, C. Liu, J. Li, and C. Zhang, "Design of Intrusion Detection System for Internet of Things Based on Improved BP Neural Network," *IEEE Access*, vol. 7, pp. 106 043–106 052, 2019.

[56] N. Chouhan, A. Khan, and H. u. R. Khan, "Network anomaly detection using channel boosted and residual learning based deep convolutional neural network," *Applied Soft Computing Journal*, vol. 83, p. 105612, 2019. [Online]. Available: https://doi.org/10.1016/j.asoc.2019.105612

[57] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed Analysis of the KDD CUP 99 Data Set," *IEEE Symposium on Computational Intelligence for Security and Defense Applications, CISDA 2009*, no. Cisda, pp. 1–6, 2009.

[58] M. V. Kotpalliwar and R. Wajgi, "Classification of attacks using support vector machine (SVM) on KDDCUP'99 IDS database," *Proceedings - 2015 5th International Conference on Communication Systems and Network Technologies, CSNT 2015*, pp. 987–990, 2015.

[59] G. Karatas and O. K. Sahingoz, "Neural network based intrusion detection systems with different training functions," pp. 1–6, 2018.

[60] D. Moon, H. Im, I. Kim, and J. H. Park, "DTB-IDS: an intrusion detection system based on decision tree using behavior analysis for preventing APT attacks," *The Journal of Supercomputing*, vol. 73, no. 7, pp. 2881–2895, 2017.

[61] Y. Wang, Y. Li, D. Tian, C. Wang, W. Wang, R. Hui, P. Guo, and H. Zhang, "A Novel Intrusion Detection System Based on Advanced Naive Bayesian Classification," *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, vol. 211, pp. 581–588, 2018.

[62] N. Farnaaz and M. A. Jabbar, "Random Forest Modeling for Network Intrusion Detection System," pp. 213–217, 2016.

[63] E. K. Boahen, B. E. Bouya-Moko, and C. Wang, "Network anomaly detection in a controlled environment based on an enhanced PSOGSARFC," *Computers and Security*, vol. 104, 2021.

[64] Kurniabudi, D. Stiawan, Darmawijoyo, M. Y. B. Bin Idris, A. M. Bamhdi, and R. Budiarto, "CICIDS-2017 Dataset Feature Analysis with Information Gain for Anomaly Detection," *IEEE Access*, vol. 8, pp. 132 911–132 921, 2020.

[65] I. Dutt, S. Borah, and I. K. Maitra, "Immune System Based Intrusion Detection System (IS-IDS): A Proposed," *IEEE Access*, vol. 8, pp. 34 929–34 941, 2020. [Online]. Available: http://dx.doi.org/10.1109/access.2020.2973608

[66] M. F. A. Razak, N. B. Anuar, R. Salleh, and A. Firdaus, "The rise of malware: Bibliometric analysis of malware study," *Journal of Network and Computer Applications*, vol. 75, pp. 58–76, 2016. [Online]. Available: http://dx.doi.org/10.1016/j.jnca.2016.08.022

[67] A. Rejeb, S. Simske, K. Rejeb, H. Treiblmaier, and S. Zailani, "Internet of Things research in supply chain management and logistics: A bibliometric analysis," *Internet of Things*, vol. 12, p. 100318, 2020.

[68] M. Keepers and T. Wuest, "Smart trucking - Status of digital transformation of the trucking industry: A bibliometric analysis," *Procedia CIRP*, vol. 86, pp. 26–30, 2019. [Online]. Available: https://doi.org/10.1016/j.procir.2020.01.003

[69] M. Kamran, H. U. Khan, W. Nisar, M. Farooq, and S. U. Rehman, "Blockchain and Internet of Things: A bibliometric study," *Computers and Electrical Engineering*, vol. 81, p. 106525, 2020. [Online]. Available: https://doi.org/10.1016/j.compeleceng.2019.106525

[70] M. J. Cobo, A. G. López-Herrera, E. Herrera-Viedma, and F. Herrera, "An approach for detecting, quantifying, and visualizing the evolution of a research field: A practical application to the Fuzzy Sets Theory field," *Journal of Informetrics*, vol. 5, no. 1, pp. 146–166, 2011. [Online]. Available: http://dx.doi.org/10.1016/j.joi.2010.10.002

[71] J. Feng, X. Mu, W. Wang, and Y. Xu, "A topic analysis method based on a three-dimensional strategic diagram," *Journal of Information Science*, 2020.

[72] B. Kitchenham, S. Charters, D. Budgen, P. Brereton, M. Turner, S. Linkman, M. Jorgensen, E. Mendes, and G. Visaggio, *Guidelines for performing Systematic Literature Reviews in Software Engineering*. UK: Keele University, 2007.

[73] R. Vijayanand, D. Devaraj, and B. Kannapiran, "Intrusion detection system for wireless mesh network using multiple support vector machine classifiers with genetic-algorithm-based feature selection," *Computers & Security*, vol. 77, pp. 304–314, 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404818303766

[74] J. Gu, L. Wang, H. Wang, and S. Wang, "A novel approach to intrusion detection using SVM ensemble with feature augmentation," *Computers and Security*, vol. 86, pp. 53–62, 2019. [Online]. Available: https://doi.org/10.1016/j.cose.2019.05.022

[75] M. M. Rathore, A. Ahmad, and A. Paul, "Real time intrusion detection system for ultra-high-speed big data environments," *Journal of Supercomputing*, vol. 72, no. 9, pp. 3489–3510, 2016. [Online]. Available: https://link.springer.com/article/10.1007/s11227-015-1615-5

[76] W. L. Al-Yaseen, Z. A. Othman, and M. Z. A. Nazri, "Multi-level hybrid support vector machine and extreme learning machine based on modified K-means for intrusion detection system," *Expert Systems with Applications*, vol. 67, pp. 296–303, 2017. [Online]. Available: http://dx.doi.org/10.1016/j.eswa.2016.09.041

[77] E. Kabir, J. Hu, H. Wang, G. Zhuo, H. Wang, and G. Zhuo, "A novel statistical technique for intrusion detection systems," *Future Generation Computer Systems*, vol. 79, pp. 303–318, 2018. [Online]. Available: http://dx.doi.org/10.1016/j.future.2017.01.029

[78] M. Hawedi, C. Talhi, and H. Boucheneb, *Multi-tenant intrusion detection system for public cloud (MTIDS)*. Springer US, 2018, vol. 74, no. 10. [Online]. Available: https://doi.org/10.1007/s11227-018-2572-6

[79] G. Bhuvaneswari and G. Manikandan, "An intelligent intrusion detection system for secure wireless communication using IPSO and negative selection classifier," *Cluster Computing*, vol. 22, pp. 12 429–12 441, 2018. [Online]. Available: https://doi.org/10.1007/s10586-017-1643-4

[80] A. Nagaraja, B. Uma, and R. kumar Gunupudi, "UTTAMA: An Intrusion Detection System Based on Feature Clustering and Feature Transformation," *Foundations of Science*, no. 0123456789, 2019. [Online]. Available: https://doi.org/10.1007/s10699-019-09589-5

[81] P. Anitha and B. Kaarthick, "Oppositional based Laplacian grey wolf optimization algorithm with SVM for data mining in intrusion detection system," *Journal of Ambient Intelligence and Humanized Computing*, 2019. [Online]. Available: https://doi.org/10.1007/s12652-019-01606-6

[82] Q. M. Alzubi, M. Anbar, Z. N. M. Alqattan, M. A. Al-Betar, and R. Abdullah, "Intrusion detection system based on a modified binary grey wolf optimisation," *Neural Computing and Applications*, vol. 32, no. 10, pp. 6125–6137, 2019. [Online]. Available: https://doi.org/10.1007/s00521-019-04103-1

[83] W. Zhang, D. Han, K.-C. Li, and F. I. Massetto, "Wireless sensor network intrusion detection system based on MK-ELM," *Soft Computing*, jan 2020. [Online]. Available: http://link.springer.com/10.1007/s00500-020-04678-1

[84] A. Davahli, M. Shamsi, and G. Abaei, "Hybridizing genetic algorithm and grey wolf optimizer to advance an intelligent and lightweight intrusion detection system for IoT wireless networks," *Journal of Ambient Intelligence and Humanized Computing*, no. 0123456789, 2020. [Online]. Available: https://doi.org/10.1007/s12652-020-01919-x

[85] A. N. Jaber and S. U. Rehman, "FCM-SVM based intrusion detection system for cloud computing environment," *Cluster Computing*, vol. 6, 2020. [Online]. Available: https://doi.org/10.1007/s10586-020-03082-6

[86] P. Devan and N. Khare, "An efficient XGBoostDNN-based classification model for network intrusion detection system," *Neural Computing and Applications*, vol. 32, 2020. [Online]. Available: https://doi.org/10.1007/s00521-020-04708-x

[87] N. Upasani and H. Om, "A modified neuro-fuzzy classifier and its parallel implementation on modern GPUs for real time intrusion detection," *Applied Soft Computing Journal*, vol. 82, p. 105595, 2019. [Online]. Available: https://doi.org/10.1016/j.asoc.2019.105595

[88] X. F. Chen and S. Z. Yu, "CIPA: A collaborative intrusion prevention architecture for programmable network and SDN," *Computers and Security*, vol. 58, pp. 1–19, 2016. [Online]. Available: http://dx.doi.org/10.1016/j.cose.2015.11.008

[89] C. Azad and V. K. Jha, "Fuzzy minmax neural network and particle swarm optimization based intrusion detection system," *Microsystem Technologies*, vol. 23, no. 4, pp. 907–918, 2016. [Online]. Available: https://dl.acm.org/citation.cfm?id=3065308

[90] D. R. C. Canedo and A. R. S. R. Romariz, "Intrusion Detection System in Ad Hoc Networks with Artificial Neural Networks and Algorithm K-Means," *IEEE Latin America Transactions*, vol. 17, no. 7, pp. 1109–1115, 2019.

[91] E. Anthi, L. Williams, M. Slowinska, G. Theodorakopoulos, and P. Burnap, "A Supervised Intrusion Detection System for Smart Home IoT Devices," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 9042–9053, oct 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8753563/

[92] K. Wang, "Network data management model based on Naïve Bayes classifier and deep neural networks in heterogeneous wireless networks," *Computers and Electrical Engineering*, vol. 75, pp. 135–145, 2019. [Online]. Available: https://doi.org/10.1016/j.compeleceng.2019.02.015

[93] H. M. Song, J. Woo, and H. K. Kim, "In-vehicle network intrusion detection using deep convolutional neural network," *Vehicular Communications*, vol. 21, p. 100198, 2019. [Online]. Available: https://doi.org/10.1016/j.vehcom.2019.100198

[94] W. A. Ghanem and A. Jantan, "A new approach for intrusion detection system based on training multilayer perceptron by using enhanced Bat algorithm," *Neural Computing and Applications*, vol. 2, 2019. [Online]. Available: https://doi.org/10.1007/s00521-019-04655-2

[95] W. Elmasry, A. Akbulut, and A. H. Zaim, "Evolving deep learning architectures for network intrusion detection using a double PSO metaheuristic," *Computer Networks*, vol. 168, 2020.

[96] Y. Li, Y. Xu, Z. Liu, H. Hou, Y. Zheng, Y. Xin, Y. Zhao, and L. Cui, "Robust detection for network intrusion of industrial IoT based on multi-CNN fusion," *Measurement*, vol. 154, p. 107450, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S026322411931317X

[97] D. Moon, S. B. Pan, and I. Kim, "Host-based intrusion detection system for secure human-centric computing," *Journal of Supercomputing*, vol. 72, no. 7, pp. 2520–2536, 2016.

[98] B. Selvakumar, K. Muneeswaran, S. B, M. K, and B. Selvakumar, "Firefly algorithm based feature selection for network intrusion detection," *Computers and Security*, vol. 81, pp. 148–155, 2019. [Online]. Available: https://dblp.uni-trier.de/db/journals/compsec/compsec81.html{#}BK19

[99] V. Kumar, D. Sinha, A. K. Das, S. C. Pandey, and R. T. Goswami, "An integrated rule based intrusion detection system: analysis on UNSW-NB15 data set and the real time online dataset," *Cluster Computing*, vol. 23, 2019. [Online]. Available: https://doi.org/10.1007/s10586-019-03008-x

[100] K. Sethi, E. Sai Rupesh, R. Kumar, P. Bera, and Y. Venu Madhav, "A context-aware robust intrusion detection system: a reinforcement learning-based approach," *International Journal of Information Security*, no. 1, 2019. [Online]. Available: https://doi.org/10.1007/s10207-019-00482-7

[101] Y. Gao, H. Wu, B. Song, Y. Jin, X. Luo, and X. Zeng, "A distributed network intrusion detection system for distributed denial of service attacks in vehicular ad hoc network," *IEEE Access*, vol. 7, pp. 154 560–154 571, 2019.

[102] J. H. Lee and K. H. Park, "GAN-based imbalanced data intrusion detection system," *Personal and Ubiquitous Computing*, 2019.

[103] L. Li, H. Zhang, H. Peng, and Y. Yang, "Nearest neighbors based density peaks approach to intrusion detection," *Chaos Solitons & Fractals*, vol. 110, pp. 33–40, 2018. [Online]. Available: https://doi.org/10.1016/j.chaos.2018.03.010

[104] S. Sandosh, V. Govindasamy, and G. Akila, "Enhanced intrusion detection system via agent clustering and classification based on outlier detection," *Peer-to-Peer Networking and Applications*, 2020.

[105] R. N. Wibowo, P. Sukarno, and E. M. Jadied, "Pendeteksian Serangan DoS Menggunakan Multiclassfier Pada NSL-KDD Dataset," in *e-Proceeding of Engineering*, vol. 5, no. 3, 2018, pp. 7885–7893.

[106] J. Joque, "Distributed Denial of Service:," in *Deconstruction Machines*, 2018, pp. 111–148.

[107] S. Paliwal and R. Gupta, "Denial-of-Service, Probing & Remote to User (R2L) Attack Detection using Genetic Algorithm," *International Journal of Computer Applications*, vol. 60, no. 19, pp. 975–8887, 2012.

[108] E. A. Winanto, A. Heryanto, and D. Stiawan, "Visualisasi Serangan Remote to Local (R2L) Dengan Clustering K-Means," *Annual Research Seminar 2016*, vol. 2, no. 1, pp. 359–362, 2016.

[109] M. Danuri and Suharnawi, "Trend cyber crime dan teknologi informasi di indonesia," *Infokam*, no. January, pp. 55–64, 2017.

[110] A. Borkar, A. Donode, and A. Kumari, "A survey on Intrusion Detection System (IDS) and Internal Intrusion Detection and protection system (IIDPS)," *Proceedings of the International Conference on Inventive Computing and Informatics, ICICI 2017*, no. Icici, pp. 949–953, 2017. [Online]. Available: http://dx.doi.org/10.1109/icici.2017.8365277

[111] G. Akman, "A Cryptographic Approach for Secure Client - Server Chat Application using Public Key Infrastructure (PKI)," in *The 11th International Conference for Internet Technology and Secured Transactions (ICITST-2016) A*, 2016, pp. 442–446.

[112] B. Siregar, R. F. Dwiputra Purba, Seniman, and F. Fahmi, "Intrusion Prevention System Against Denial of Service Attacks Using Genetic Algorithm," *2018 IEEE International Conference on Communication, Networks and Satellite, Comnetsat 2018 - Proceedings*, pp. 55–59, 2019.

[113] R. F. Pratama, N. A. Suwastika, and M. A. Nugroho, "Design and implementation adaptive Intrusion Prevention System (IPS) for attack prevention in software-defined network (SDN) architecture," *2018 6th International Conference on Information and Communication Technology, ICoICT 2018*, vol. 0, no. c, pp. 299–304, 2018.

[114] A. H. Al-hamami and G. M. W. Al-saadoon, "Development of a Network-based," *2013 Science and Information Conference*, pp. 641–644, 2013.

[115] M. MacAs, L. Lagla, W. Fuertes, G. Guerrero, and T. Toulkeridis, "Data Mining model in the discovery of trends and patterns of intruder attacks on the data network as a public-sector innovation," *2017 4th International Conference on eDemocracy and eGovernment, ICEDEG 2017*, pp. 55–62, 2017. [Online]. Available: https://ieeexplore.ieee.org/document/7962513/

[116] H. Wang, Y. Xiao, and Y. Long, "Research of intrusion detection algorithm based on parallel SVM on spark," *Proceedings of 2017 IEEE 7th International Conference on Electronics Information and Emergency Communication, ICEIEC 2017*, pp. 153–156, 2017.

[117] A. Sharma, A. Zaidi, R. Singh, S. Jain, and A. Sahoo, "Optimization of SVM classifier using Firefly algorithm," *2013 IEEE 2nd International Conference on Image Information Processing, IEEE ICIIP 2013*, pp. 198–202, 2013.

[118] R. Parihar, A. Jain, and U. Singh, "Support Vector Machine through Detecting Packet Dropping Misbehaving Nodes in MANET," in *International Conference on Electronics, Communication and Aerospace Technology (ICECA 2017)*, 2017, pp. 483–488.

[119] X. Wang, "Hyperscan and Snort* Integration," 2017. [Online]. Available: https://software.intel.com/content/www/us/en/develop/articles/hyperscan-and-snort-integration.html

[120] Dnsstuff, "7 Best Intrusion Detection Software 2020 - IDS Systems - DNSstuff," 2020. [Online]. Available: https://www.dnsstuff.com/network-intrusion-detection-software

[121] Ariyus and Dony, *Intrusion Detection System, Sistem Pendeteksi Penyusup Pada Jaringan Komputer*. Yogyakarta: Andi OFFSET, 2007.

[122] M. Ulfa and Megawaty, "Perancangan dan Implementasi Sistem Keamanan Berbasis IDS di Jaringan Internet Universitas Bina Darma," *Jurnal Nasional Pendidikan Teknik Informatika (JANAPATI)*, vol. 4, no. 2, p. 45, 2015.

[123] R. Bejtlich, A. Reviewer, S. Northcutt, and C. Hill, *Snort 2.1 Intrusion Detection*. Syngress, 2004.

[124] A. S. Ashoor and P. S. Gore, "Difference between intrusion detection system (ids) & intrusion prevention system (ips)," in *CNSA 2011*, vol. 2, no. 7, 2011, pp. 1–3.

[125] D. T. Larose, *Discovering Knowledge in Data: An Introduction to Data Mining*. Wiley Interscience, 2005.

[126] L. Rokach and O. Maimon, *Data Mining With Decision Trees-Theory and Applications*. World Scientific, 2014.

[127] C. Maione, E. S. de Paula, M. Gallimberti, L. B. Batista, D. A. Campiglia, F. Jr Barbosa, and R. M. Barbosa, "Comparative study of data mining techniques for the authentication of organic grape juice based on ICP-MS analysis," *Expert Systems with Applications*, vol. 49, pp. 60–73, 2016.

[128] F. N. Ogwueleka, "Data Mining Application in Credit Card Fraud Detection System," *Journal of Engineering Science and Technology*, vol. 6, no. 3, pp. 311–322, 2011.

[129] T. Hendrickx, B. Cule, P. Meysman, S. Naulaerts, K. Laukens, and B. Goethals, "From data mining to knowledge discovery in databases," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 9078, no. 3, pp. 637–648, 1996.

[130] "NSL-KDD Datasets," 2018. [Online]. Available: https://www.unb.ca/cic/datasets/nsl.html

[131] H. Liu and H. Motoda, *Feature selection for knowledge discovery and data mining*. Library of Congress Cataloging.in.Publication Data, 1998.

[132] S. Cateni, V. Colla, and M. Vannucci, "A Fuzzy System for Combining Filter Features Selection Methods," *International Journal of Fuzzy Systems*, vol. 19, no. 4, pp. 1168–1180, 2017.

[133] F. F. Firdaus, H. A. Nugroho, and I. Soesanti, "A Review of Feature Selection and Classification Approaches for Heart Disease Prediction," *IJITEE*, vol. 4, no. 3, pp. 75–83, 2020.

[134] R. A. R. Mahmood, A. Abdi, and M. Hussin, "Performance Evaluation of Intrusion Detection System using Selected Features and Machine Learning Classifiers," *Baghdad Science Journal*, vol. 18, no. 2(Suppl.), p. 0884, 2021.

[135] M. Masdari and H. Khezri, "A survey and taxonomy of the fuzzy signature-based Intrusion Detection Systems," *Applied Soft Computing Journal*, vol. 92, p. 106301, 2020. [Online]. Available: https://doi.org/10.1016/j.asoc.2020.106301

[136] Suyanto, *Data mining untuk klasifikasi dan klasterisasi data*. Bandung: Informatika Bandung, 2019.

[137] J. Brownlee, "Recursive Feature Elimination (RFE) for Feature Selection in Python," 2020. [Online]. Available: https://machinelearningmastery.com/rfe-feature-selection-in-python/

[138] Z. Pawlak, "Rough Sets," *International Journal of Computer and Information Science*, vol. 11, no. 5, pp. 341–356, 1982.

[139] A. Prajana, F. Sains, T. Universitas, I. Negeri, A. Raniry, and B. Aceh, "Penerapan Teory Rough Set Untuk Memprediksi Tingkat Kelulusan Siswa Dalam Ujian Nasional Pada Sma Negeri 5 Kota Banda Aceh," *Journal of Islamic Science and Technology*, vol. 2, no. 1, pp. 75–88, 2016. [Online]. Available: www.jurnal.ar-raniry.com/index.php/elkawnie

[140] Suhardi, N. A. Setiawan, and I. Hidayah, "Seleksi Rule Menggunakan Rough Set Theory Untuk Diagnosis Penyakit Tuberkulosis," in *Seminar Nasional ke 9: Rekayasa Teknologi Industri dan Informasi*, 2014, pp. 97–102.

[141] T. H. Dwiputranto and N. A. Setiawan, "Rough-Set-Theory-Based Classification with Optimized k -Means Discretization," *technologies*, 2022.

[142] R. Takdirillah, "Apa itu Machine Learning? Beserta Pengertian dan Cara Kerjanya," 2020. [Online]. Available: https://www.dicoding.com/blog/machine-learning-adalah/

[143] J. Brownlee, "Machine Learning Algorithm," 2021. [Online]. Available: https://tinyurl.com/ML-Algorithm-Main-Map

[144] Scikit-learn, "Choosing the right estimator," 2022. [Online]. Available: https://scikit-learn.org/stable/tutorial/machine_learning_map/index.html

[145] A. S. Nugroho, A. B. Witarto, and D. Handoko, "Support Vector Machine," in *Proceeding of Indonesian Scientific Meeting in Central Japan*, 2003, pp. 842–847.

[146] Trivusi, "Penjelasan Lengkap Algoritma Support Vector Machine (SVM)," 2022. [Online]. Available: https://www.trivusi.web.id/2022/04/algoritma-svm.html

[147] ——, "Decision Tree: Pengertian, Cara Kerja, Kelebihan, dan Kekurangannya," 2022. [Online]. Available: https://www.trivusi.web.id/2022/06/algoritma-decision-tree.html

[148] B. S. Bhati, G. Chugh, F. Al-Turjman, and N. S. Bhati, "An improved ensemble based intrusion detection technique using XGBoost," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 6, pp. 1–15, 2020.

[149] G. Kumar, K. Thakur, and M. R. Ayyagari, "MLEsIDSs: machine learning-based ensembles for intrusion detection systemsa review," *Journal of Supercomputing*, vol. 76, no. 11, pp. 8938–8971, 2020. [Online]. Available: https://doi.org/10.1007/s11227-020-03196-z

[150] A. A. Aburomman and M. B. I. Reaz, "A survey of intrusion detection systems based on ensemble and hybrid classifiers," *Computers and Security*, vol. 65, pp. 135–152, 2017. [Online]. Available: http://dx.doi.org/10.1016/j.cose.2016.11.004

[151] D. P. Gaikwad and R. C. Thool, "Intrusion detection system using Bagging with Partial Decision Tree base classifier," *Procedia Computer Science*, vol. 49, no. 1, pp. 92–98, 2015.

[152] G. Folino, C. Pizzuti, and G. Spezzano, "An ensemble-based evolutionary framework for coping with distributed intrusion detection," *Genetic Programming and Evolvable Machines*, vol. 11, no. 2, pp. 131–146, 2010.

[153] E. Bahri, N. Harbi, and H. N. Huu, "Approach Based Ensemble Methods for Better and Faster Intrusion Detection," in *Greedy-Boost for Intrusion Detection*. Springer, Berlin, Heidelberg, 2011, pp. 17–24. [Online]. Available: http://link.springer.com/10.1007/978-3-642-21323-6{_}3

[154] I. Syarif, E. Zaluska, A. Prugel-Bennett, and G. Wills, "Application of Bagging, Boosting and Stacking to Intrusion Detection," *MLDM*, pp. 593–602, 2012.

[155] L. Breiman, "Bagging predictors," *Machine Learning*, vol. 24, no. 2, pp. 123–140, aug 1996. [Online]. Available: http://link.springer.com/10.1007/BF00058655

[156] C. Zhang and Y. M, *Ensemble Machine Learning Methods and Applications*. Springer London, 2012. [Online]. Available: https://link.springer.com/10.1007/978-1-4419-9326-7

[157] M. Graczyk, T. Lasota, B. Trawiński, and K. Trawiński, "Comparison of Bagging, Boosting and Stacking Ensembles Applied to Real Estate Appraisal," *Asian Conference on Intelligent Information and Database Systems*, pp. 340–350, 2010.

[158] K. S. Nugroho, "Validasi Model Klasifikasi Machine Learning pada RapidMiner," 2020. [Online]. Available: https://medium.com/@ksnugroho/validasi-model-machine-learning-pada-rapidminer-50be0080df14

[159] M. Stojiljković, "Split Your Dataset With scikit-learn's train_test_split()," 2022. [Online]. Available: https://realpython.com/train-test-split-python-data/

[160] S. S. Gopalan, D. Ravikumar, D. Linekar, A. Raza, and M. Hasib, "Balancing Approaches towards ML for IDS: A Survey for the CSE-CIC IDS Dataset," in *2020 International Conference on Communications, Signal Processing, and their Applications (ICCSPA)*. IEEE Explore, 2020.

[161] E. Tufan, C. Tezcan, and C. Acartürk, "Anomaly-based intrusion detection by machine learning: A case study on probing attacks to an institutional network," *IEEE Access*, vol. 9, pp. 50 078–50 092, 2021.

[162] Jupriyadi, "Implementasi Seleksi Fitur Menggunakan Algoritma FVBRM Untuk Klasifikasi Serangan Pada Intrusion Detection System (Ids)," in *Seminar Nasional Teknologi Informasi (SEMNASTEK)*, vol. 17, 2018, pp. 1–6.

[163] K. Kristiawan and A. Widjaja, "Perbandingan Algoritma Machine Learning dalam Menilai Sebuah Lokasi Toko Ritel," *Jurnal Teknik Informatika dan Sistem Informasi*, vol. 7, no. 1, pp. 35–46, 2021.

[164] O. Purbo, "Istilah Istilah di IDS," 2020. [Online]. Available: https://lms.onnocenter.or.id/wiki/index.php/Intrusion_Detection_System

[165] J. R. Landis and G. G. Koch, "The measurement of observer agreement for categorical data," *Biometrics*, vol. 33, no. 1, pp. 159–174, 1977.

[166] B. Shmueli, "Multi-Class Metrics Made Simple, Part III: the Kappa Score (aka Cohen's Kappa Coefficient) Measure The Agreement Between Predicted and True Values," 2019. [Online]. Available: https://tinyurl.com/kappa-score

[167] H. Takaki, "Statistical tests for computational intellegence research and human subjective tests," 2013.

[168] Q. McNemar, "Note on the sampling error of the difference between correlated proportions or percentages," *Psychometrika*, vol. 12, no. 2, pp. 153–157, 1947.

[169] J. Brownlee, "How to Calculate McNemar's Test to Compare Two Machine Learning Classifiers," 2019. [Online]. Available: https://machinelearningmastery.com/mcnemars-test-for-machine-learning/

[170] A. L. Edwards, "Note on the "correction for continuity" in testing the significance of the difference between correlated proportions," *Psychometrika*, vol. 13, no. 3, pp. 185–187, 1948.

[171] S. Ahmed, A. Mahbub, F. Rayhan, R. Jani, S. Shatabda, and D. M. Farid, "Hybrid Methods for Class Imbalance Learning Employing Bagging with Sampling Techniques," *2nd International Conference on Computational Systems and Information Technology for Sustainable Solutions, CSITSS 2017*, pp. 1–5, 2017.

[172] Kunal and M. Dua, "Attribute Selection and Ensemble Classifier based Novel Approach to Intrusion Detection System," *Procedia Computer Science*, vol. 167, no. 2019, pp. 2191–2199, 2020. [Online]. Available: https://doi.org/10.1016/j.procs.2020.03.271

[173] I. Duntsch and G. Gediga, "Indices for rough set approximation and the application to confusion matrices," *International Journal of Approximate Reasoning*, vol. 118, pp. 155–172, 2020. [Online]. Available: https://doi.org/10.1016/j.ijar.2019.12.008

[174] H. Wang, H. Sun, C. Li, S. Rahnamayan, and J. S. Pan, "Diversity enhanced particle swarm optimization with neighborhood search," *Information Sciences*, vol. 223, pp. 119–135, 2013. [Online]. Available: http://dx.doi.org/10.1016/j.ins.2012.10.012