REFERENCE

[1] A. Prajapati, A. Sakadasariya, and J. Patel, “Software defined network: Future of networking,” in *2018 2nd International Conference on Inventive Systems and Control (ICISC)*, IEEE, Jan. 2018, pp. 1351–1354. doi: 10.1109/ICISC.2018.8399028.

[2] A. Hakiri, A. Gokhale, P. Berthou, D. C. Schmidt, and T. Gayraud, “Software-defined networking: Challenges and research opportunities for future internet,” Dec. 24, 2014, *Elsevier B.V.* doi: 10.1016/j.comnet.2014.10.015.

[3] D. Firdaus, R. Munadi, and Y. Purwanto, “DDoS Attack Detection in Software Defined Network using Ensemble K-means++ and Random Forest,” in *2020 3rd International Seminar on Research of Information Technology and Intelligent Systems, ISRITI 2020*, Institute of Electrical and Electronics Engineers Inc., Dec. 2020, pp. 164–169. doi: 10.1109/ISRITI51436.2020.9315521.

[4] L. F. Eliyan and R. Di Pietro, “DoS and DDoS Attacks in Software Defined Networks: A Survey of Existing Solutions and Research Challenges,” *Future Generation Computer Systems*, vol. 122, pp. 149–171, Sep. 2021, doi: 10.1016/j.future.2021.03.011.

[5] A. J. Altamemi, A. Abdulhassan, and N. T. Obeis, “DDoS Attack Detection in Software Defined Networking Controller using Machine Learning Techniques,” *Bulletin of Electrical Engineering and Informatics*, vol. 11, no. 5, pp. 2836–2844, Oct. 2022, doi: 10.11591/eei.v11i5.4155.

[6] J. Pei, Y. Chen, and W. Ji, “A DDoS Attack Detection Method Based on Machine Learning,” in *Journal of Physics: Conference Series*, Institute of Physics Publishing, Jul. 2019. doi: 10.1088/1742-6596/1237/3/032040.

[7] M. S. Elsayed, N.-A. Le-Khac, S. Dev, and A. D. Jurcut, “Machine-Learning Techniques for Detecting Attacks in SDN,” Oct. 2019, [Online]. Available: http://arxiv.org/abs/1910.00817

[8] O. Rahman, M. A. G. Quraishi, and C. H. Lung, “DDoS Attacks Detection and Mitigation in SDN Using Machine Learning,” in *Proceedings - 2019 IEEE World Congress on Services, SERVICES 2019*, Institute of Electrical and Electronics Engineers Inc., Jul. 2019, pp. 184–189. doi: 10.1109/SERVICES.2019.00051.

[9] H. A. Alamri and V. Thayananthan, “Analysis of Machine Learning for Securing Software-Defined Networking,” in *Procedia Computer Science*, Elsevier B.V., 2021, pp. 229–236. doi: 10.1016/j.procs.2021.10.078.

[10] M. T. Kurniawan, S. Yazid, and Y. G. Sucahyo, “Comparison of Feature Selection Methods for DDoS Attacks on Software Defined Networks using Filter-Based, Wrapper-Based and Embedded-Based.” [Online]. Available: www.joiv.org/index.php/joiv

[11] K. Peffers and M. Rossi, “Design Science Research Process: A Model for Producing and Presenting Information Systems Research Cross-border Shopping View project Means-end Understanding of Consumer Decision Making View project,” 2020. [Online]. Available: https://www.researchgate.net/publication/341926962

[12] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, “Machine Learning in IoT Security: Current Solutions and Future Challenges,” *IEEE Communications Surveys and Tutorials*, vol. 22, no. 3, pp. 1686–1721, Jul. 2020, doi: 10.1109/COMST.2020.2986444.

[13] M. S. Elsayed, N. A. Le-Khac, and A. D. Jurcut, “InSDN: A Novel SDN Intrusion Dataset,” *IEEE Access*, vol. 8, pp. 165263–165284, 2020, doi: 10.1109/ACCESS.2020.3022633.

[14] O. Rahman, M. A. G. Quraishi, and C. H. Lung, “DDoS attacks detection and mitigation in SDN using machine learning,” in *Proceedings - 2019 IEEE World Congress on Services, SERVICES 2019*, Institute of Electrical and Electronics Engineers Inc., Jul. 2019, pp. 184–189. doi: 10.1109/SERVICES.2019.00051.

[15] D. Firdaus, R. Munadi, and Y. Purwanto, “DDoS Attack Detection in Software Defined Network using Ensemble K-means++ and Random Forest,” in *2020 3rd International Seminar on Research of Information Technology and Intelligent Systems, ISRITI 2020*, Institute of Electrical and Electronics Engineers Inc., Dec. 2020, pp. 164–169. doi: 10.1109/ISRITI51436.2020.9315521.

[16] H. A. Alamri and V. Thayananthan, “Analysis of Machine Learning for Securing Software-Defined Networking,” in *Procedia Computer Science*, Elsevier B.V., 2021, pp. 229–236. doi: 10.1016/j.procs.2021.10.078.

[17] A. J. Altamemi, A. Abdulhassan, and N. T. Obeis, “DDoS attack detection in software defined networking controller using machine learning techniques,” *Bulletin of Electrical Engineering and Informatics*, vol. 11, no. 5, pp. 2836–2844, Oct. 2022, doi: 10.11591/eei.v11i5.4155.

[18] S. Wang *et al.*, “Detecting Flooding DDoS Attacks in Software Defined Networks using Supervised Learning Techniques,” *Engineering Science and Technology, an International Journal*, vol. 35, Nov. 2022, doi: 10.1016/j.jestch.2022.101176.

[19] M. A. Mohsin and A. H. Hamad, “Performance Evaluation of SDN DDoS Attack Detection and Mitigation Based Random Forest and K-Nearest Neighbors Machine Learning Algorithms,” *Revue d’Intelligence Artificielle*, vol. 36, no. 2, pp. 233–240, Apr. 2022, doi: 10.18280/ria.360207.

[20] Z. Liu, Y. Wang, F. Feng, Y. Liu, Z. Li, and Y. Shan, “A DDoS Detection Method Based on Feature Engineering and Machine Learning in Software-Defined Networks,” *Sensors*, vol. 23, no. 13, Jul. 2023, doi: 10.3390/s23136176.

[21] O. R. Sanchez, M. Repetto, A. Carrega, and R. Bolla, “Evaluating ML-based DDoS Detection with Grid Search Hyperparameter Optimization,” in *2021 IEEE 7th International Conference on Network Softwarization (NetSoft)*, IEEE, Jun. 2021, pp. 402–408. doi: 10.1109/NetSoft51509.2021.9492633.

[22] J. Wu, X. Y. Chen, H. Zhang, L. D. Xiong, H. Lei, and S. H. Deng, “Hyperparameter Optimization for Machine Learning Models Based on Bayesian Optimization,” *Journal of Electronic Science and Technology*, vol. 17, no. 1, pp. 26–40, Mar. 2019, doi: 10.11989/JEST.1674-862X.80904120.

[23] M. Aghaabbasi, M. Ali, M. Jasiński, Z. Leonowicz, and T. Novák, “On Hyperparameter Optimization of Machine Learning Methods Using a Bayesian Optimization Algorithm to Predict Work Travel Mode Choice,” *IEEE Access*, vol. 11, pp. 19762–19774, 2023, doi: 10.1109/ACCESS.2023.3247448.

[24] J. A. Nichols, H. W. Herbert Chan, and M. A. B. Baker, “Machine learning: applications of artificial intelligence to imaging and diagnosis,” *Biophys Rev*, vol. 11, no. 1, pp. 111–118, Feb. 2019, doi: 10.1007/s12551-018-0449-9.

[25] P. K. Sharma* and Dr. S. S. Tyagi, “Improving Security through Software Defined Networking (SDN): AN SDN based Model,” *International Journal of Recent Technology and Engineering (IJRTE)*, vol. 8, no. 4, pp. 295–300, Nov. 2019, doi: 10.35940/ijrte.D6814.118419.

[26] K. Gaur, P. Choudhary, P. Yadav, A. Jain, and P. Kumar, “Software Defined Networking: A review on Architecture, Security and Applications,” *IOP Conf Ser Mater Sci Eng*, vol. 1099, no. 1, p. 012073, Mar. 2021, doi: 10.1088/1757-899x/1099/1/012073.

[27] U. I. & Sunday and S. D. Akhibi, “Application of Software-Defined Networking,” 2022.

[28] Nilesh Kumar Jadav *et al.*, “AI-Driven Network Softwarization Scheme for Efficient Message Exchange in IoT Environment Beyond 5G,” *ResearchGate*, Nov. 2022.

[29] Z. Zhang, H. Li, S. Dong, and L. Hu, “Software Defined Networking (SDN) Research Review,” 2018.

[30] R. Wazirali, R. Ahmad, and S. Alhiyari, “SDN-Openflow Topology Discovery: An Overview of Performance Issues,” Aug. 01, 2021, *MDPI AG*. doi: 10.3390/app11156999.

[31] S. Askar and F. Keti, “Performance Evaluation of Different SDN Controllers: A Review,” 2021, doi: 10.5281/zenodo.4742771.

[32] S. Ray, “A Quick Review of Machine Learning Algorithms,” in *2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon)*, IEEE, Feb. 2019, pp. 35–39. doi: 10.1109/COMITCon.2019.8862451.

[33] J. A. Nichols, H. W. Herbert Chan, and M. A. B. Baker, “Machine learning: applications of artificial intelligence to imaging and diagnosis,” Feb. 07, 2019, *Springer Verlag*. doi: 10.1007/s12551-018-0449-9.

[34] Aurelien Geron, *Hands-On Machine Learning with Scikit-Learn & TensorFlow : Concept, Tools, and Technique to Build Intelligent System*, 2ns Edition. Beijing: O’Reilly Media, 2019.

[35] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, “Machine Learning in IoT Security: Current Solutions and Future Challenges,” *IEEE Communications Surveys and Tutorials*, vol. 22, no. 3, pp. 1686–1721, Jul. 2020, doi: 10.1109/COMST.2020.2986444.

[36] P. Monika, C. Kulkarni, N. Harish Kumar, S. Shruthi, and V. Vani, “Machine Learning Approaches for Sentiment Analysis,” *Int J Health Sci (Qassim)*, pp. 1286–1300, Apr. 2022, doi: 10.53730/ijhs.v6ns4.6119.

[37] N. M. Abdulkareem and A. M. Abdulazeez, “Machine Learning Classification Based on Radom Forest Algorithm: A Review,” *International Journal of Science and Business, IJSAB International*, vol. 5, no. 2, 2021.

[38] M. I. Prasetiyowati, N. U. Maulidevi, and K. Surendro, “Feature Selection to Increase the Random Forest Method Performance on High Dimensional Data,” *International Journal of Advances in Intelligent Informatics*, vol. 6, no. 3, pp. 303–312, 2020, doi: 10.26555/ijain.v6i3.471.

[39] G. S. Saragih, Z. Rustam, D. Aldila, R. Hidayat, R. E. Yunus, and J. Pandelaki, “Ischemic Stroke Classification using Random Forests Based on Feature Extraction of Convolutional Neural Networks,” vol. 10, no. 5, 2020.

[40] E. M. S. Rochman, A. Rachmad, D. A. Fatah, W. Setiawan, and Y. Kustiyahningsih, “Classification of Salt Quality based on Salt-Forming Composition using Random Forest,” in *Journal of Physics: Conference Series*, Institute of Physics, 2022. doi: 10.1088/1742-6596/2406/1/012021.

[41] N. Mahdi Abdulkareem and A. Mohsin Abdulazeez, “Machine Learning Classification Based on Radom Forest Algorithm: A Review,” 2021, doi: 10.5281/zenodo.4471118.

[42] E. Bartz, T. Bartz-Beielstein, M. Zaefferer, and O. Mersmann, “Hyperparameter Tuning for Machine and Deep Learning with R A Practical Guide.”

[43] E. Elgeldawi, A. Sayed, A. R. Galal, and A. M. Zaki, “Hyperparameter Tuning for Machine Learning Algorithms used for Arabic Sentiment Analysis,” *Informatics*, vol. 8, no. 4, Dec. 2021, doi: 10.3390/informatics8040079.

[44] L. Yang and A. Shami, “On Hyperparameter optimization of machine learning algorithms: Theory and practice,” *Neurocomputing*, vol. 415, pp. 295–316, Nov. 2020, doi: 10.1016/j.neucom.2020.07.061.

[45] R. Gomes Mantovani, “Use of Meta-Learning for Hyperparameter Tuning of Classification Problems.” [Online]. Available: https://www.researchgate.net/publication/346044422

[46] N. Decastro-García, Á. L. Muñoz Castañeda, D. Escudero García, and M. V. Carriegos, “Effect of the Sampling of a Dataset in the Hyperparameter Optimization Phase over the Efficiency of a Machine Learning Algorithm,” *Complexity*, vol. 2019, 2019, doi: 10.1155/2019/6278908.

[47] K. M. Kelkar and J. W. Bakal, “Hyperparameter Tuning of Random Forest Algorithm or Affective Learning System,” in *Proceedings of the 3rd International Conference on Smart Systems and Inventive Technology, ICSSIT 2020*, Institute of Electrical and Electronics Engineers Inc., Aug. 2020, pp. 1192–1195. doi: 10.1109/ICSSIT48917.2020.9214213.

[48] J. Bergstra, J. B. Ca, and Y. B. Ca, “Random Search for Hyper-Parameter Optimization Yoshua Bengio,” 2012. [Online]. Available: http://scikit-learn.sourceforge.net.

[49] Z. Wang, M. Agung, R. Egawa, R. Suda, and H. Takizawa, “Automatic Hyperparameter Tuning of Machine Learning Models under Time Constraints,” in *2018 IEEE*

International Conference on Big Data (Big Data), IEEE, Dec. 2018, pp. 4967–4973. doi: 10.1109/BigData.2018.8622384.

[50] O. R. Sanchez, M. Repello, A. Carrega, and R. Bolla, "Evaluating ML-based DDoS Detection with Grid Search Hyperparameter Optimization," in *Proceedings of the 2021 IEEE Conference on Network Softwarization: Accelerating Network Softwarization in the Cognitive Age, NetSoft 2021*, Institute of Electrical and Electronics Engineers Inc., Jun. 2021, pp. 402–408. doi: 10.1109/NetSoft51509.2021.9492633.

[51] R. K. Batchu and H. Seetha, "A Generalized Machine Learning Model For DDoS Attacks Detection using Hybrid Feature Selection and Hyperparameter Tuning," *Computer Networks*, vol. 200, p. 108498, Dec. 2021, doi: 10.1016/j.comnet.2021.108498.

[52] Vimal Gaur and Rajneesh Kumar, "HPDDoS: A Hyper Parameter Model for Detection of Multiclass DDoS Attacks," *Mathematical Statistician and Engineering Applications*, vol. 71, no. 3s2, Jul. 2022.

[53] N. Sivanesan, A. Rajesh, S. Anitha, and K. S. Archana, "Detecting Distributed Denial of Service (DDoS) in MANET Using Ad Hoc On-Demand Distance Vector (AODV) with Extra Tree Classifier (ETC)," *Iranian Journal of Science and Technology, Transactions of Electrical Engineering*, Dec. 2023, doi: 10.1007/s40998-023-00678-7.

[54] M. A. Setitra, M. Fan, B. L. Y. Agbley, and Z. E. A. Bensalem, "Optimized MLP-CNN Model to Enhance Detecting DDoS Attacks in SDN Environment," *Network*, vol. 3, no. 4, pp. 538–562, Dec. 2023, doi: 10.3390/network3040024.

[55] R. V. Deshmukh and K. K. Devadkar, "Understanding DDoS Attack and Its Effect in Cloud Environment," in *Procedia Computer Science*, Elsevier B.V., 2015, pp. 202–210. doi: 10.1016/j.procs.2015.04.245.

[56] A. Sanmorino, "A Study for DDOS Attack Classification Method," in *Journal of Physics: Conference Series*, Institute of Physics Publishing, Jun. 2019. doi: 10.1088/1742-6596/1175/1/012025.

[57] B. H. A. N. Lawal, *Real-Time Detection and Mitigation of Distributed Denial of Service (DDoS) Attacks in Software Defined Networking (SDN)*. IEEE, 2018.

[58] I. Masud, K. Kusrini, and A. B. Prasetio, "Distributed Denial Of Service (DDOS) Attack Detection On Zigbee Protocol Using Naive Bayes Algoritm," *International Journal of Artificial Intelligence Research*, vol. 5, no. 2, Jun. 2021, doi: 10.29099/ijair.v5i2.214.

[59] M. Aqil *et al.*, “Feature Selection Approach to Detect DDoS Attack Using Machine Learning Algorithms.”

[60] S. Dong, K. Abbas, and R. Jain, “A Survey on Distributed Denial of Service (DDoS) Attacks in SDN and Cloud Computing Environments,” *IEEE Access*, vol. 7, pp. 80813–80828, 2019, doi: 10.1109/ACCESS.2019.2922196.

[61] B. N. Ramkumar and T. Subbulakshmi, “Tcp Syn Flood Attack Detection and Prevention System using Adaptive Thresholding Method,” *ITM Web of Conferences*, vol. 37, p. 01016, 2021, doi: 10.1051/itmconf/20213701016.

[62] S. Iswandi Walad, M. Zarlis, and M. I. T. Syahril Efendi, “Analysis of Denial of Service Attack on Web Security Systems,” in *Journal of Physics: Conference Series*, IOP Publishing Ltd, 2021. doi: 10.1088/1742-6596/1811/1/012127.

[63] T. Tun, “A Forensics Analysis of ICMP Flooded DDoS Attack using WireShark,” *Transactions on Networks and Communications*, vol. 8, no. 3, pp. 08–15, Jun. 2020, doi: 10.14738/tnc.83.8250.

[64] S. Q. Ali Shah, F. Zeeshan Khan, and M. Ahmad, “The Impact and Mitigation of ICMP Based Economic Denial of Sustainability Attack in Cloud Computing Environment using Software Defined Network,” *Computer Networks*, vol. 187, Mar. 2021, doi: 10.1016/j.comnet.2021.107825.

[65] K. D. G. Na. P. S. H. B. V, *Detection of DDoS Attacks in Software Defined Networks*. IEEE, 2018.

[66] M. S. ElSayed, N. A. Le-Khac, M. A. Albahar, and A. Jurcut, “A Novel Hybrid Model for Intrusion Detection Systems in SDNs Based on CNN and A New Regularization Technique,” *Journal of Network and Computer Applications*, vol. 191, Oct. 2021, doi: 10.1016/j.jnca.2021.103160.

[67] M. Hammad, N. Hewahi, and W. Elmedany, “Enhancing Network Intrusion Recovery in SDN with machine learning: an innovative approach,” *Arab J Basic Appl Sci*, vol. 30, no. 1, pp. 561–572, 2023, doi: 10.1080/25765299.2023.2261219.

[68] N. Ahuja, G. Singal, and D. Mukhopadhyay, “DLSDN: Deep Learning for DDOS Attack Detection in Software Defined Networking,” in *Proceedings of the Confluence 2021: 11th International Conference on Cloud Computing, Data Science and Engineering*, Institute of Electrical and Electronics Engineers Inc., Jan. 2021, pp. 683–688. doi: 10.1109/Confluence51648.2021.9376879.

[69] A. A. Elngar, D. A. El A Mohamed, and F. F. M Ghaleb, “A Fast Accurate Network Intrusion Detection System.” [Online]. Available: http://sites.google.com/site/ijcsis/

[70] J. Cai, J. Luo, S. Wang, and S. Yang, “Feature selection in machine learning: A new perspective,” *Neurocomputing*, vol. 300, pp. 70–79, Jul. 2018, doi: 10.1016/j.neucom.2017.11.077.

[71] R. Medar, V. S. Rajpurohit, and B. Rashmi, “Impact of Training and Testing Data Splits on Accuracy of Time Series Forecasting in Machine Learning,” in *2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA)*, IEEE, Aug. 2017, pp. 1–6. doi: 10.1109/ICCUBEA.2017.8463779.

[72] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, “A detailed analysis of the KDD CUP 99 data set,” in *2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications*, IEEE, Jul. 2009, pp. 1–6. doi: 10.1109/CISDA.2009.5356528.

[73] S. Revathi and A. Malathi, “A Detailed Analysis on NSL-KDD Dataset Using Various Machine Learning Techniques for Intrusion Detection.” [Online]. Available: www.ijert.org

[74] Kurniabudi, D. Stiawan, Darmawijoyo, M. Y. Bin Bin Idris, A. M. Bamhdi, and R. Budiarto, “CICIDS-2017 Dataset Feature Analysis with Information Gain for Anomaly Detection,” *IEEE Access*, vol. 8, pp. 132911–132921, 2020, doi: 10.1109/ACCESS.2020.3009843.

[75] Y. Ayachi, Y. Mellah, J. Berrich, and T. Bouchentouf, “Increasing the Performance of an IDS using ANN model on the realistic cyber dataset CSE-CIC-IDS2018,” in *2020 International Symposium on Advanced Electrical and Communication Technologies (ISAECT)*, IEEE, Nov. 2020, pp. 1–4. doi: 10.1109/ISAECT50560.2020.9523662.

[76] C. V. Gonzalez Zelaya, “Towards Explaining the Effects of Data Preprocessing on Machine Learning,” in *Proceedings - International Conference on Data Engineering*, IEEE Computer Society, Apr. 2019, pp. 2086–2090. doi: 10.1109/ICDE.2019.00245.

[77] A. R. Khan *et al.*, “Feature Selection Mechanism for Attention Classification using Gaze Tracking Data,” in *2022 29th IEEE International Conference on Electronics, Circuits and Systems (ICECS)*, IEEE, Oct. 2022, pp. 1–4. doi: 10.1109/ICECS202256217.2022.9970936.

[78] X. Zeng, Y.-W. Chen, and C. Tao, “Feature Selection Using Recursive Feature Elimination for Handwritten Digit Recognition,” in *2009 Fifth International*

Conference on Intelligent Information Hiding and Multimedia Signal Processing, IEEE, Sep. 2009, pp. 1205–1208. doi: 10.1109/IIH-MSP.2009.145.

[79] G. Konig, C. Molnar, B. Bischl, and M. Grosse-Wentrup, "Relative Feature Importance," in *2020 25th International Conference on Pattern Recognition (ICPR)*, IEEE, Jan. 2021, pp. 9318–9325. doi: 10.1109/ICPR48806.2021.9413090.

[80] A. Baita, I. A. Prasetyo, and N. Cahyono, "Hyperparameter Tuning on Random Forest for Diagnose COVID-19," *JIKO (Jurnal Informatika dan Komputer)*, vol. 6, no. 2, Aug. 2023, doi: 10.33387/jiko.v6i2.6389.

[81] L. Barki, A. Shidling, N. Meti, D. G. Narayan, and M. M. Mulla, "Detection of distributed denial of service attacks in software defined networks," in *2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, IEEE, Sep. 2016, pp. 2576–2581. doi: 10.1109/ICACCI.2016.7732445.

[82] L. Yang and H. Zhao, "DDoS Attack Identification and Defense using SDN Based on Machine Learning Method," in *Proceedings - 2018 15th International Symposium on Pervasive Systems, Algorithms and Networks, I-SPAN 2018*, Institute of Electrical and Electronics Engineers Inc., Jul. 2019, pp. 174–178. doi: 10.1109/I-SPAN.2018.00036.

[83] J. A. Perez-Diaz, I. A. Valdovinos, K. K. R. Choo, and D. Zhu, "A Flexible SDN-Based Architecture for Identifying and Mitigating Low-Rate DDoS Attacks Using Machine Learning," *IEEE Access*, vol. 8, pp. 155859–155872, 2020, doi: 10.1109/ACCESS.2020.3019330.

[84] H. M and S. M.N, "A Review on Evaluation Metrics for Data Classification Evaluations," *International Journal of Data Mining & Knowledge Management Process*, vol. 5, no. 2, pp. 01–11, Mar. 2015, doi: 10.5121/ijdkp.2015.5201.

[85] M. S. Elsayed, N.-A. Le-Khac, and A. D. Jurcut, "InSDN: A Novel SDN Intrusion Dataset," *IEEE Access*, vol. 8, pp. 165263–165284, 2020, doi: 10.1109/ACCESS.2020.3022633.

[86] N. Moustafa and J. Slay, "UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," in *2015 Military Communications and Information Systems Conference (MilCIS)*, IEEE, Nov. 2015, pp. 1–6. doi: 10.1109/MilCIS.2015.7348942.