DAFTAR PUSTAKA

[1] A. Banitalebi Dehkordi, M. Soltanaghaei, and F. Z. Boroujeni, "The DDoS attacks detection through machine learning and statistical methods in SDN," *J. Supercomput.*, vol. 77, no. 3, pp. 2383–2415, Mar. 2021.

[2] M. Security, "What is a ddos attack?: Microsoft security." [Online]. Available: https://www.microsoft.com/en/security/business/security-101/what-is-a-ddos-attack

[3] S. Priya, M. Sivaram, D. Yuvaraj, and A. Jayanthiladevi, "Machine learning based ddos detection," in *2020 International Conference on Emerging Smart Computing and Informatics (ESCI)*, 2020, pp. 234–237.

[4] R. Vishwakarma and A. K. Jain, "A survey of DDoS attacking techniques and defence mechanisms in the IoT network," *Telecommun. Syst.*, vol. 73, no. 1, pp. 3–25, Jan. 2020.

[5] F. S. d. Lima Filho, F. A. F. Silveira, A. de Medeiros Brito Junior, G. Vargas-Solar, and L. F. Silveira, "Smart detection: An online approach for dos/ddos attack detection using machine learning," *Security and Communication Networks*, vol. 2019, p. 1574749, Oct 2019. [Online]. Available: https://doi.org/10.1155/2019/1574749

[6] A. Praseed and P. S. Thilagam, "Http request pattern based signatures for early application layer ddos detection: A firewall agnostic approach," *Journal of Information Security and Applications*, vol. 65, p. 103090, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2214212621002696

[7] K. Vos, Z. Peng, C. Jenkins, M. R. Shahriar, P. Borghesani, and W. Wang, "Vibration-based anomaly detection using lstm/svm approaches," *Mechanical Systems and Signal Processing*, vol. 169, p. 108752, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0888327021010682

[8] H. Xu, G. Pang, Y. Wang, and Y. Wang, "Deep isolation forest for anomaly detection," *IEEE Transactions on Knowledge and Data Engineering*, vol. 35, no. 12, pp. 12 591–12 604, 2023.

[9] K. S. Sahoo, B. K. Tripathy, K. Naik, S. Ramasubbareddy, B. Balusamy, M. Khari, and D. Burgos, "An evolutionary svm model for ddos attack detection in software defined networks," *IEEE access*, vol. 8, pp. 132 502–132 513, 2020.

[10] Z. Ma and Z. Li, "Research on ddos attack detection based on isolation forest and kmeans algorithm in sdn."

[11] L. Hefei, H. Xinli, and Z. Zhengqi, "Detection method of ddos attack based on software defined network and its application [j]," *Computer Engineering*, vol. 42, no. 2, pp. 118–123, 2016.

[12] J. Lesouple, C. Baudoin, M. Spigai, and J.-Y. Tourneret, "Generalized isolation forest for anomaly detection," *Pattern Recognition Letters*, vol. 149, pp. 109–119, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167865521002063

[13] S. Mazzanti, ""Isolation Forest": The Anomaly Detection Algorithm Any Data Scientist Should Know — towardsdatascience.com," [Accessed 06-02-2024].

[14] Y. Mirsky, T. Doitshman, Y. Elovici, and A. Shabtai, "Kitsune: An ensemble of autoencoders for online network intrusion detection," in *The Network and Distributed System Security Symposium (NDSS) 2018*, 2018.

[15] S. S. A. Naqvi, Y. Li, and M. Uzair, "DDoS attack detection in smart grid network using reconstructive machine learning models," *PeerJ Comput. Sci.*, vol. 10, no. e1784, p. e1784, Jan. 2024.

[16] G. Pang, C. Shen, L. Cao, and A. V. D. Hengel, "Deep learning for anomaly detection: A review," *ACM Comput. Surv.*, vol. 54, no. 2, mar 2021. [Online]. Available: https://doi.org/10.1145/3439950

[17] B. Mahesh, "Machine learning algorithms -a review," 01 2019.

[18] M. Alloghani, D. Al-Jumeily, J. Mustafina, A. Hussain, and A. J. Aljaaf, *A Systematic Review on Supervised and Unsupervised Machine Learning Algorithms for Data Science*. Cham: Springer International Publishing, 2020, pp. 3–21. [Online]. Available: https://doi.org/10.1007/978-3-030-22475-2_1

[19] C. Maklin, "Isolation Forest — corymaklin," https://medium.com/@corymaklin/isolation-forest-799fceacdda4, [Accessed 08-02-2024].

[20] X. Yuan, J. Yu, J. Xi, L. Yang, J. Shang, Z. Li, and J. Duan, "An isolation forest and total variation-based detection of cnvs from short-read sequencing data," *IEEE / ACM Transactions on Computational Biology and Bioinformatics*, vol. 18, no. 2, pp. 539–549, 2021.

[21] M. Hosseinzadeh, A. M. Rahmani, B. Vo, M. Bidaki, M. Masdari, and M. Zangakani, "Improving security using svm-based anomaly detection: issues and challenges," *Soft Computing*, vol. 25, no. 4, pp. 3195–3223, Feb 2021. [Online]. Available: https://doi.org/10.1007/s00500-020-05373-x

[22] A. Al Shorman, H. Faris, and I. Aljarah, "Unsupervised intelligent system based on one class support vector machine and grey wolf optimization for iot botnet detection," *Journal of Ambient Intelligence and Humanized*

Computing, vol. 11, no. 7, pp. 2809–2825, Jul 2020. [Online]. Available: https://doi.org/10.1007/s12652-019-01387-y

[23] S. Reddi and G. Eswar, "Chapter 9 - fake news in social media recognition using modified long short-term memory network," in *Security in IoT Social Networks*, ser. Intelligent Data-Centric Systems, F. Al-Turjman and B. Deebak, Eds. Academic Press, 2021, pp. 205–227. [Online]. Available: https://www.sciencedirect.com/science/article/pii/B9780128215999000091

[24] S. Zhong, S. Fu, L. Lin, X. Fu, Z. Cui, and R. Wang, "A novel unsupervised anomaly detection for gas turbine using isolation forest," in *2019 IEEE International Conference on Prognostics and Health Management (ICPHM)*, 2019, pp. 1–6.

UMN
UNIVERSITAS
MULTIMEDIA
NUSANTARA