DAFTAR PUSTAKA

[1] Kominfo, "29 Juta Serangan Siber Diblokir di Indonesia Selama 2023." [Online]. Available: https://kominfo.lhokseumawekota.go.id/berita/read/29-juta-serangan-siber-diblokir-di-indonesia-selama-2023-202402291709170453

[2] F. Haddadi, J. Morgan, E. G. Filho, and A. N. Zincir-Heywood, "Botnet behaviour analysis using ip flows: With http filters using classifiers," in *2014 28th International Conference on Advanced Information Networking and Applications Workshops*, 2014, pp. 7–12.

[3] A. Coluccia, A. D'Alconzo, and F. Ricciato, "Distribution-based anomaly detection via generalized likelihood ratio test: A general maximum entropy approach," *Computer Networks*, vol. 57, no. 17, pp. 3446–3462, 2013.

[4] riskrecon, "Malicious Traffic Detection: A Guide For Businesses." [Online]. Available: https://blog.riskrecon.com/malicious-traffic-detection-a-guide-for-businesses#:~:text=Malicious%20traffic%20is%20any%20network,data%2C%20or%20compromise%20system%20integrity.

[5] J. Wang, L. Yang, J. Wu, and J. H. Abawajy, "Clustering analysis for malicious network traffic," in *2017 IEEE International Conference on Communications (ICC)*, 2017, pp. 1–6.

[6] A. Delplace, S. Hermoso, and K. Anandita, "Cyber attack detection thanks to machine learning algorithms," 2020.

[7] C.-I. A. A. A. L. M. B. C. V. K. Arnaldo, I., "Learning Representations for Log Data in Cybersecurity," *IEEE Transactions on Power Systems*, 2017.

[8] G. M. I. Lambert, "Security Analytics: Using Deep Learning to Detect Cyber Attacks," *UNF Graduate Theses and Dissertations. 728.*, 2017. [Online]. Available: https://digitalcommons.unf.edu/etd/728

[9] M. Stevanovic and J. M. Pedersen, "Detecting bots using multi-level traffic analysis." *Int. J. Cyber Situational Aware.*, vol. 1, no. 1, pp. 182–209, 2016.

[10] M. Koca, Avcı, and M. A. S. Al-hayani, "Classification of malicious urls using naive bayes and genetic algorithm," *Sakarya University Journal of Computer and Information Sciences*, vol. 6, no. 2, p. 80–90, 2023.

[11] M. Kruczkowski and E. N. Szynkiewicz, "Support vector machine for malware analysis and classification," in *2014 IEEE/WIC/ACM International Joint Conferences on Web Intelligence (WI) and Intelligent Agent Technologies (IAT)*, vol. 2, 2014, pp. 415–420.

[12] A. Ehsan, C. Catal, and A. Mishra, "Detecting malware by analyzing app permissions on android platform: A systematic literature review," *Sensors*, vol. 22, no. 20, 2022. [Online]. Available: https://www.mdpi.com/1424-8220/22/20/7928

[13] A. Basit, M. Zafar, X. Liu, A. R. Javed, Z. Jalil, and K. Kifayat, "A comprehensive survey of AI-enabled phishing attacks detection techniques," *Telecommunication Systems*, vol. 76, no. 1, pp. 139–154, Jan. 2021.

[14] J. G. Almaraz-Rivera, J. A. Perez-Diaz, and J. A. Cantoral-Ceballos, "Transport and application layer ddos attacks detection to iot devices by using machine learning and deep learning models," *Sensors*, vol. 22, no. 9, 2022. [Online]. Available: https://www.mdpi.com/1424-8220/22/9/3367

[15] J. Gardiner, M. Cova, and S. Nagaraja, "Command control: Understanding, denying and detecting - a review of malware c2 techniques, detection and defences," 2015.

[16] P. J. Cho YC, "Vulnerability assessment of ipv6 websites to sql injection and other application level attacks," *ScientificWorldJournal*, 2013.

[17] D. A. Pisner and D. M. Schnyer, "Support vector machine," in *Machine learning*. Elsevier, 2020, pp. 101–121.

[18] M. Mohammadi, T. A. Rashid, S. H. T. Karim, A. H. M. Aldalwie, Q. T. Tho, M. Bidaki, A. M. Rahmani, and M. Hosseinzadeh, "A comprehensive survey and taxonomy of the svm-based intrusion detection systems," *Journal of Network and Computer Applications*, vol. 178, p. 102983, 2021.

[19] V. Kecman, "Support vector machines–an introduction," in *Support vector machines: theory and applications*. Springer, 2005, pp. 1–47.

[20] G. M. B. T. Valkenborg D, Rousseau AJ, "Support vector machines," *Am J Orthod Dentofacial Orthop*, 2023.

[21] G. I. Webb, E. Keogh, and R. Miikkulainen, "Naïve bayes." *Encyclopedia of machine learning*, vol. 15, no. 1, pp. 713–714, 2010.

[22] A. McCallum, K. Nigam *et al.*, "A comparison of event models for naive bayes text classification," in *AAAI-98 workshop on learning for text categorization*, vol. 752, no. 1. Madison, WI, 1998, pp. 41–48.

[23] P. J. M. Ali, R. H. Faraj, E. Koya, P. J. M. Ali, and R. H. Faraj, "Data normalization and standardization: a technical report," *Mach Learn Tech Rep*, vol. 1, no. 1, pp. 1–6, 2014.

[24] "Classification: Roc curve and auc." [Online]. Available: https://developers.google.com/machine-learning/crash-course/classification/roc-and-auc

[25] a. M. J. E. Sebastian Garcia, Agustin Parmisano, "Malware detection in network traffic data," 2023. [Online]. Available: https://www.kaggle.com/dsv/7285844

[26] V. Gholamy, Afshin; Kreinovich and O. Kosheleva, "Why 70/30 or 80/20 relation between training and testing sets: A pedagogica explanation," *Departmental Technical Reports (CS).*, 2018. [Online]. Available: https://scholarworks.utep.edu/cs_techrep/1209