[22] H. Zhao, Z. Chang, G. Bao, and X. Zeng, "Malicious Domain Names Detection Algorithm Based on N -Gram," vol. 2019, 2019.
[23] W. B. Cavnar and J. M. Trenkle, "N-Gram-Based Text Categorization N-Gram-Based Text Categorization," *Proc. Third Annu. Symp. Doc. Anal. Inf. Retr.*, no. May, pp. 1–14, 2001.
[24] J. Daniel and J. H. Martin, "stanford n-gram_Speech and Language Processing," 2021.
[25] F. Angiulli, L. Argento, and A. Furfaro, "Exploiting n-gram location for intrusion detection," *CS.CR*, vol. 3, no. Cornell University, pp. 1–6, 2016, doi: 10.1109/ICTAI.2015.155.
[26] Z. Bazrafshan, H. Hashemi, S. M. H. Fard, and A. Hamzeh, "A survey on heuristic malware detection techniques," *IKT 2013 - 2013 5th Conf. Inf. Knowl. Technol.*, no. May, pp. 113–120, 2013, doi: 10.1109/IKT.2013.6620049.
[27] W. Halim, "Deteksi Malware dengan Menggunakan API Calls," *Paper*, p. 15, 2020.
[28] A. Shabtai, R. Moskovitch, C. Feher, S. Dolev, and Y. Elovici, "Detecting unknown malicious code by applying classification techniques on OpCode patterns," *Secur. Inform.*, vol. 1, no. 1, p. 1, 2012, doi: 10.1186/2190-8532-1-1.
[29] T. Abou-Assaleh, N. Cercone, V. Keselj, and R. Sweidan, "N-gram-based detection of new malicious code," in *Proc of the 28th Annual International Computer Software and Applications Conference, IEEE Computer Society*, 2004, vol. 2, pp. 41–42 vol.2, doi: 10.1109/CMPSAC.2004.1342667.
[30] I. Journal, O. F. Engineering, C. Of, M. Virus, and U. N. Gram, "International journal of engineering sciences & research technology classification of metamorphic virus using n gram analysis," vol. 6, no. 2, pp. 364–370, 2017.
[31] L. Tan, "The worst-case execution time tool challenge 2006," *STTT*, vol. 11, pp. 133–152, 2009, doi: 10.1109/ISoLA.2006.72.
[32] T. McCabe, "A Complexity Measure," *IEEE Trans. Softw. Eng.*, vol. SE-2, pp. 308–320, 1976.
[33] P. Jalote, *An Integrated Approach to Software Engineering*. 1997.
[34] M. A. H. Azmi, C. F. M. Foozy, K. A. M. Sukri, N. A. Abdullah, I. R. A. Hamid, and H. Amnur, "Feature Selection Approach to Detect DDoS Attack Using Machine Learning Algorithms," *Int. J. Informatics Vis.*, vol. 5, no. 4, pp. 395–401, 2021, doi: 10.30630/JOIV.5.4.734.
[35] A. Martín, R. Lara-Cabrera, and D. Camacho, "Android malware detection through hybrid features fusion and ensemble classifiers: The AndroPyTool framework and the OmniDroid dataset," *Inf. Fusion*, vol. 52, no. December, pp. 128–142, 2019, doi: 10.1016/j.inffus.2018.12.006.
[36] S. Almutairi, S. Mahfoudh, S. Almutairi, and J. S. Alowibdi, "Hybrid Botnet Detection Based on Host and Network Analysis," *J. Comput. Networks Commun.*, vol. 2020, no. Hindawi, pp. 1–16, 2020, doi: 10.1155/2020/9024726.
[37] C. Ma, X. Du, and L. Cao, "Analysis of multi-Types of flow features based on hybrid neural network for improving network anomaly detection," *IEEE Access*, vol. 7, pp. 148363–148380, 2019, doi: 10.1109/ACCESS.2019.2946708.
[38] Z. Chiba, N. Abghour, K. Moussaid, A. El, and M. Rida, "Intelligent and Improved Self-Adaptive Anomaly based Intrusion Detection System for Networks," vol. 11, no. 2, pp. 312–330, 2019.
[39] T. Mahjabin, Y. Xiao, G. Sun, and W. Jiang, "A survey of distributed denial-of-service attack, prevention, and mitigation techniques," *Int. J. Distrib. Sens. Networks*, vol. 13, no. 12, 2017, doi: 10.1177/1550147717741463.