Future Internet. 13(6), 2021, 1–15, doi: https://doi.org/10.3390/fi13060154.
[24] Bagui, S., Nandi, D. and White, R. J. Machine Learning and Deep Learning for Phishing Email Classification using One-Hot Encoding, Journal of Computer Science. 17(7), 2021, 610–623, doi: https://doi.org/10.3844/jcssp.2021.610.623.
[25] Zhu, E., Chen, Y., Ye, C., Li, X. and Liu, F. OFS-NN: an effective phishing websites detection model based on optimal feature selection and neural network, IEEE Access. 7, 2019, 73271–73284, doi: 10.1109/ACCESS.2019.2920655.
[26] Ali, W. and Malebary, S. Particle swarm optimization-based feature weighting for improving intelligent phishing website detection, IEEE Access, 8, 2020, 116766–116780, doi: 10.1109/ACCESS.2020.3003569.
[27] Mao, J., Bian, J., Tian, W., Zhu, S., Wei, T., Li, A., and Liang, Z. Phishing page detection via learning classifiers from page layout feature, EURASIP Journal on Wireless Communications and Networking, 1, 2019, 1–14, doi: https://doi.org/10.1186/s13638- 019-1361-0.
[28] Acharya, B. and Vadrevu, P. PhishPrint: Evading Phishing Detection Crawlers by Prior Profiling, In: 30th USENIX Security Symposium, 2021, 3775–3792.
[29] Rasool, R. U., Ahmed, K., Anwar, Z., Wang, H., Ashraf, U., & Rafique, W. CyberPulse++: A machine learning-based security framework for detecting link flooding attacks in software defined networks. International Journal of Intelligent Systems, 36(8), 2021, 3852-3879.
[30] Vimalachandran, P., Liu, H., Lin, Y., Ji, K., Wang, H., & Zhang, Y. Improving accessibility of the Australian My Health Records while preserving privacy and security of the system. Health Information Science and Systems, 8(1), 2020, 1-9.
[31] Patil, D. R., Patil, J. B. Malicious web pages detection using feature selection techniques and machine learning, International Journal of High Performance Computing and Networking., 14(4), 2019, 473–488., doi: 10.1504/IJHPCN.2019.102355.
[32] Patil, D. R., Patil and J. B. Malicious URLs detection using decision tree classifiers and majority voting technique, Cybernetics and Information Technologies, 18(1), 2018, 11–29, doi: https://doi.org/10.2478/cait-2018-0002.
[33] Verma R., Das A, What's in a URL: Fast Feature Extraction and Malicious URL Detection, In: 3rd International Workshop on Security and Privacy Analytics, (Scottsdale, AZ, United States, 2017, 55–63.
[34] Evans, S. C., Hershey, J. E and Saulnier, G. Kolmogorov complexity estimation and analysis, In: Sixth World Conference on Systemics, Cybernetics and Informatics, (Orlando, Fla,), 2002.
[35] Pao, H. K., Chou, Y. L. and Lee, Y. J. Malicious URL detection based on Kolmogorov complexity estimation, In: IEEE/WIC/ACM International Joint Conferences on Web Intelligence and Intelligent Agent Technology, (Macau, China), 2012, 380– 387.
[36] Moffat, A. Huffman coding, In: ACM Computing Surveys (CSUR), 2019, 31–35.
[37] Dredze, M., Crammer, K. and Pereira, F. Confidence-weighted linear classification, In: 25th International Conference on Machine learning, (Helsinki Finland), 2008, 264–271.
[38] Dahlmeier D., Ng H. T. and Ng E. J. F. NUS at the HOO 2012 Shared Task, In: Seventh Workshop on Building Educational Applications Using NLP, 2008, 216– 224.
[39] Confidence-weighted (CW) learning. (2019), http://www.comp.nus.edu.sg/nlp/ software.html
[40] Crammer, K., Kulesza, A. and Dredze, M. Adaptive regularization of weight vectors, In: Advances in Neural Information Processing Systems, 2009, 414–422.
[41] AROW++: An implementation of the efficient confidence-weighted classifier. (2019), https://github.com/tetsuok/arowpp
[42] Alexa: Alexa top global websites. (2021), http://www.alexa.com/topsites
[43] Phishtank: Join the fight against phishing. (2021), https://www.phishtank.com
[44] OpenPhish - Phishing Intelligence. (2021), https://openphish.com
[45] Sokolova M. and Lapalme G. A systematic analysis of performance measures for classification tasks, Information Processing and Management, 45(4), 2009, 427–437, doi: 10.1016/j.ipm.2009.03.002.
[46] Xiang, J. Hong, C. P. Rose and L. Cranor. Cantina+: a feature-rich machine learning framework for detecting phishing web sites, ACM Transactions on Information and System Security (TISSEC), 14(2), 2011, 1–28, doi: https://doi.org/10.1145/2019599.2019606.