DAFTAR PUSTAKA

Rafi, F., Anugrah, T. D., & Yanuarsyah, R. (2023). Analisis *Malicious* URL pada File Menggunakan Metode K-Means Clustering Berbasis Host-Based Feature Extraction (Tugas Akhir).

Do, T. X., Nguyen, T. X., Nguyen, V. H., & Nguyen, D. V. (2020). *Malicious* URL Detection based on Machine Learning. International Journal of Computer Science and Network Security, 20(1), 74-81.

Nguyen, T. T., Nguyen, T. D., & Nguyen, N. T. (2020). Detecting abnormal DNS traffic using unsupervised machine learning. Journal of Science and Technology, 58(1), 101-112.

Tiwari, V. (2019). Suspicious URL Detection using Dynamic Learning Model with Machine Learning. International Journal of Research and Analytical Reviews (IJRAR), 6(1), 606-611. (DOI: 10.13140/RG.2.2.33962.36803)

Singh, J., & Roy, S. (2020). Detecting *Malicious* DNS over HTTPS Traffic Using Machine Learning. IEEE Xplore. (DOI: 10.1109/ICCCI50885.2020.9160533)

Toprak, N., & Yavuz, A. A. (2022). Web Application Firewall Based on Anomaly Detection using Deep Learning. Journal of Information Security and Applications, 67, 103173. (DOI: 10.1016/j.jisa.2022.103173)

Castell-Uroz, F. A., Pérez-Rosell, M., Soria-Olivas, E., & Ferrer-Coll, J. (n.d.). URL-based Web Tracking Detection Using Deep Learning. Procedia Computer Science.

Ngurah, D., Nanda, K. W., & Pradnyana, G. (2021). K-Means Clustering Algorithm in Web-Based Applications for Grouping Data on Scholarship

Selection Results. Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK), 8(6), 1187-1194. (DOI: 10.25126/jtiik.202186510)

Kulkarni, A. P., & Brown, T. L. (2019). Phishing Websites Detection using Machine Learning. Journal of Cyber Security Technology, 3(1), 1-10. (DOI: 10.1080/23742917.2019.1678912)

Shaheed, Z., & Kurdy, M. (2022). Web Application Firewall Using Machine Learning and Features Engineering. International Journal of Engineering Research & Technology (IJERT), 11(9), 1-8. (DOI: 10.17577/IJERTV11IS090001)

Hilal, I., Abdo, R. A., El-Hameed, M. A., & Alshami, M. A. (2023). *Malicious* URL Classification Using Artificial Fish Swarm Optimization and Deep Learning. Computers, Materials & Continua, 74(2), 3467-3484. (DOI: 10.32604/cmc.2023.033621)

Muzaki, H., Wicaksono, H. D., & Purwiantono, P. (2020). Improving Security of Web-Based Application Using ModSecurity and Reverse Proxy in Web Application Firewall. Jurnal Rekayasa Informasi, 9(1), 1-10. (DOI: 10.30649/jri.v9i1.116)

Sim, J., & Kim, M. (2023). *Malicious* URL Detection based on Supervised and Unsupervised Learning using MobileBERT Embedding. Sensors, 23(13), 6061. (DOI: 10.3390/s23136061)

Vanitha, N., & Vinodhini, V. (2019). *Malicious*-URL Detection using Logistic Regression Technique. International Journal of Pure and Applied Mathematics, 120(6), 9205-9216.

Bezas, K., & Filippidou, F. (2023).

Comparative Analysis of Open Source *Security Information & Event Management* Systems (SIEMs). *Indonesian Journal of Computer Science*. https://doi.org/10.33022/ijcs.v12i2.3182

Bommasani, R., Hudson, D. A., Adeli, E., Altman, R., Arora, S., von Arx, S., ... & Liang, P. (2022). On the Opportunities and Risks of Foundation Models. arXiv preprint arXiv:2108.07258.

Zhao, W., Chang, M., Liu, J., & Guo, Y. (2023). A Survey of Large Language Models. *arXiv preprint arXiv:2303.18223*.

Elsadig, M., Ibrahim, A. O., Basheer, S., Alohali, M. A., Alshunaifi, S., Alqahtani, H. A., Alharbi, N., & Nagmeldin, W. (2022). Intelligent Deep Machine Learning Cyber Phishing URL Detection Based on BERT Features Extraction. *Electronics*, *11*(22), 3647. https://doi.org/10.3390/electronics11223647

Devlin, J., Chang, M. W., Lee, K., & Toutanova, K. (2019). BERT: Pre-training of deep bidirectional transformers for language understanding. *Proceedings of the 2019 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, Volume 1 (Long and Short Papers)*, 4171-4186.

Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., ... & Polosukhin, I. (2017). Attention Is All You Need. *Advances in Neural Information Processing Systems*, *30*.

Guo, J. (2019). The Advantages of Python Language in Big Data Processing. *Journal of Physics: Conference Series*, *1237*(3), 032014. https://doi.org/10.1088/1742-6596/1237/3/032014

Liu, R., Du, X., & Chen, G. (2020). Research on Python Programming Language Characteristics and Application. *Journal of Physics: Conference Series*, *1684*(1), 012093. https://doi.org/10.1088/1742-6596/1684/1/012093

Ouyang, L., Wu, J., Jiang, X., Almeida, D., Wainwright, C. L., Mishkin, P., Zhang, C., Agarwal, S., Slama, K., Ray, A., Schulman, J., Hilton, J., Kelton, F., Miller, L., Simens, M., Askell, A., Welinder, P., Christiano, P., Leike, J., & Lowe, R. (2022). *Training language models to follow instructions with human feedback*. arXiv. https://arxiv.org/abs/2203.02155

Almasri, M. N., Al-Rubaie, M., Al-Rubaie, A., & Al-Qurashi, M. (2024). *Detecting Phishing URLs using the BERT Transformer Model*. ResearchGate. Retrieved from https://www.researchgate.net/publication/377612023_Detecting_Phishing_URLs_using_the_BERT_Transformer_Model

Liu, Z., Wang, J., & Shi, T. (2024). Research on Malicious URL Detection Using a Multi-Channel Neural Network that Integrates Adversarial Training with BERT-CNN-BiLSTM. *Netinfo Security, 24*(12), 1922-1932. doi:10.3969/j.issn.1671-1122.2024.12.010