

DAFTAR PUSTAKA

- [1] E. D. T. R. Agustinus Rangga Respati, “99 persen kasus penipuan perbankan di indonesia karena ”social engineering”,” 2023. [Online]. Available: <https://money.kompas.com/read/2023/08/03/161100126/99-persen-kasus-penipuan-perbankan-di-indonesia-karena-social-engineering->
- [2] M. R. Muzzaki, “Kerugian akibat penipuan transaksi keuangan mencapai rp 2,5 triliun,” 2024. [Online]. Available: <https://www.tempo.co/ekonomi/kerugian-akibat-penipuan-transaksi-keuangan-mencapai-rp-2-5-triliun-1180226>
- [3] bjcoid2, “Serangan phishing di indonesia terus meningkat, berikut data lengkapnya.” [Online]. Available: <https://bankjombang.co.id/serangan-phishing-di-indonesia-terus-meningkat-berikut-data-lengkapnya/>
- [4] M. Chen and D. K. Halim, “Federated learning for scam classification in small indonesian language dataset: an initial study,” *Indonesian Journal of Electrical Engineering and Computer Science*, 2023. [Online]. Available: <https://api.semanticscholar.org/CorpusID:256253602>
- [5] A. Zamsuri, S. Defit, and G. Nurcahyo, “Classification of multiple emotions in indonesian text using the k-nearest neighbor method,” *Journal of Applied Engineering and Technological Science (JAETS)*, vol. 4, pp. 1012–1021, 06 2023.
- [6] A. Sitepu, W. Wanayumini, and Z. Situmorang, “Determining bullying text classification using naive bayes classification on social media,” *Jurnal Varian*, vol. 4, no. 2, pp. 133 – 140, Apr. 2021. [Online]. Available: <https://journal.universitasbumigora.ac.id/index.php/Varian/article/view/1086>
- [7] Y. P. Astuti, A. R. Wibowo, E. Kartikadarma, E. R. Subhiyakto, N. A. Sri Winarsih, and M. S. Rohman, “Penerapan metode naïve bayes classifier untuk klasifikasi sentimen pada judul berita,” *LogicLink*, vol. 1, no. 1, p. 1–12, Jun. 2024. [Online]. Available: <https://e-journal.uingusdur.ac.id/logiclink/article/view/7684>
- [8] Q. Li, H. Peng, J. Li, C. Xia, R. Yang, L. Sun, P. S. Yu, and L. He, “A survey on text classification: From traditional to deep learning,” *ACM Trans. Intell. Syst. Technol.*, vol. 13, no. 2, Apr. 2022. [Online]. Available: <https://doi.org/10.1145/3495162>
- [9] AWS, “What is text classification?” [Online]. Available: <https://aws.amazon.com/id/what-is/text-classification/>
- [10] H. Allam, L. Makubvure, B. Gyamfi, K. N. Graham, and K. Akinwolere, “Text classification: How machine learning is revolutionizing text

- categorization,” *Information*, vol. 16, no. 2, 2025. [Online]. Available: <https://www.mdpi.com/2078-2489/16/2/130>
- [11] K. Tjendrawinata, “Social engineering: Crisis in humanity,” *JATISI (Jurnal Teknik Informatika dan Sistem Informasi)*, vol. 9, 2022.
- [12] K. Chetioui, B. Bah, A. O. Alami, and A. Bahnasse, “Overview of social engineering attacks on social networks,” *Procedia Computer Science*, vol. 198, pp. 656–661, 2022, 12th International Conference on Emerging Ubiquitous Systems and Pervasive Networks / 11th International Conference on Current and Future Trends of Information and Communication Technologies in Healthcare. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S1877050921025412>
- [13] imperva, “Social engineering.” [Online]. Available: <https://www.imperva.com/learn/application-security/social-engineering-attack/>
- [14] IBM, “Types of social engineering attacks,” 2022. [Online]. Available: <https://www.ibm.com/think/topics/social-engineering>
- [15] M. Y. DM, A. Addermi, and J. Lim, “Kejahatan phishing dalam dunia cyber crime dan sistem hukum di indonesia,” *Jurnal Pendidikan dan Konseling (JPDK)*, vol. 4, no. 5, p. 8018–8023, Oct. 2022. [Online]. Available: <https://journal.universitaspahlawan.ac.id/index.php/jpdk/article/view/7977>
- [16] K. Z. Ansyafa, M. Fajarudin, M. Fadhil, and S. N. Neyman, “Analisis keamanan media sosial terhadap serangan phishing online menggunakan metode zphisher dan social engineering toolkit,” *Journal of Internet and Software Engineering*, vol. 1, no. 4, p. 10, Jun. 2024. [Online]. Available: <https://journal.pubmedia.id/index.php/pjise/article/view/2641>
- [17] N. Chauhan, “Naïve bayes algorithm: Everything you need to know,” *KDnuggets*, 2022.
- [18] geeksforgeeks, “Bayes’ theorem.” [Online]. Available: <https://www.geeksforgeeks.org/bayes-theorem/>
- [19] Rina, “Mengenal term frequency-inverse document frequency (tf-idf) pada model nlp,” 2024. [Online]. Available: <https://esairina.medium.com/mengenal-term-frequency-inverse-document-frequency-tf-idf-pada-model-nlp-e0cc571f7e37>
- [20] Y. Hamdaoui, “A guide to tf-idf,” 2024. [Online]. Available: <https://builtin.com/articles/tf-idf>
- [21] IBM, “Using countvectorizer for nlp feature extraction,” 2023. [Online]. Available: <https://www.ibm.com/reference/python/countvectorizer>

- [22] M. Zaynurrohan, Asriyanik, and A. Pambudi, "Perbandingan tf-idf dengan count vectorization dalam content-based filtering rekomendasi mobil listrik," *Explore IT: Jurnal Keilmuan dan Aplikasi Teknik Informatika*, vol. 15, pp. 8–15, 06 2023.
- [23] geeksforgeeks, "Using countvectorizer to extracting features from text," 2022. [Online]. Available: <https://www.geeksforgeeks.org/nlp/using-countvectorizer-to-extracting-features-from-text/>
- [24] scikit learn, "Gridsearchcv." [Online]. Available: https://scikit-learn.org/stable/modules/generated/sklearn.model_selection.GridSearchCV.html
- [25] G. L. E. Team, "Hyperparameter tuning with gridsearchcv," 2024. [Online]. Available: <https://www.mygreatlearning.com/blog/gridsearchcv/#what-is-gridsearchcv>
- [26] M. S. Saluja, "Gridsearchcv: Key concepts," 2024. [Online]. Available: <https://medium.com/@Mandeep2002/gridsearchcv-key-concepts-8f98ceb633e4>
- [27] M. Chen and D. K. Halim, "Scam classifier model training using federated learning method," 2023. [Online]. Available: <https://github.com/michaelchen27/scam-classifier>
- [28] Y. Wibisono, "Dataset for sms scam classification in indonesian language," 2018. [Online]. Available: https://bit.ly/yw_sms_spam_indonesia
- [29] S. Mishra and D. Soni, "Sms phishing dataset for machine learning and pattern recognition," 2022. [Online]. Available: <https://data.mendeley.com/datasets/f45bkkt8pr/1>

