REFERENCES

[1] A. Reurink, "Financial Fraud: a Literature Review," *J. Econ. Surv.*, vol. 32, no. 5, pp. 1292–1325, 2018, doi: 10.1111/joes.12294.

[2] A. Ali *et al.*, "Financial Fraud Detection Based on Machine Learning: A Systematic Literature Review," *Appl. Sci.*, vol. 12, no. 19, 2022, doi: 10.3390/app12199637.

[3] Otoritas Jasa Keuangan, "Peraturan Otoritas Jasa Keuangan Republik Indonesia Nomor 39/POJK.03/2019 tentang Penerapan Strategi Anti Fraud Bagi Bank Umum," p. 2, 2019, [Online]. Available: https://www.ojk.go.id/id/regulasi/Pages/Penerapan-Strategi-Anti-Fraud-Bagi-Bank-Umum.aspx

[4] M. Lal Bhasin, "Corporate Accounting Fraud: A Case Study of Satyam Computers Limited," *Open J. Account.*, vol. 02, no. 02, pp. 26–38, 2013, doi: 10.4236/OJACCT.2013.22006.

[5] S. Ramamoorti, "The Psychology and Sociology of Fraud : Integrating the Behavioral Sciences," *Issues Account. Educ.*, vol. 23, no. 4, pp. 521–533, 2008.

[6] D. Bholat *et al.*, "Centre for Central Banking Studies Text mining for central banks Text mining for central banks," *Cent. Cent. Bank. Stud.*, 2015.

[7] S. Bhattacharyya, S. Jha, K. Tharakunnel, and J. C. Westland, "Data mining for credit card fraud: A comparative study," *Decis. Support Syst.*, vol. 50, no. 3, pp. 602–613, Feb. 2011, doi: 10.1016/J.DSS.2010.08.008.

[8] "How to Use Machine Learning in Fraud Detection and Prevention - Intellias." https://intellias.com/how-to-use-machine-learning-in-fraud-detection/ (accessed Mar. 24, 2022).

[9] E. Kirkos, C. Spathis, and Y. Manolopoulos, "Data Mining techniques for the detection of fraudulent financial statements," *Expert Syst. Appl.*, vol. 32, no. 4, pp. 995–1003, May 2007, doi: 10.1016/J.ESWA.2006.02.016.

[10] N. K. Gyamfi and J. D. Abdulai, "Bank Fraud Detection Using Support Vector Machine," *2018 IEEE 9th Annu. Inf. Technol. Electron. Mob. Commun. Conf. IEMCON 2018*, no. May 2019, pp. 37–41, 2019, doi: 10.1109/IEMCON.2018.8614994.

[11] A. Kurniawan and Y. Yulianingsih, "Pendugaan Fraud Detection pada kartu kredit dengan Machine Learning," *Kilat*, vol. 10, no. 2, pp. 320–325, 2021, doi: 10.33322/kilat.v10i2.1482.

[12] H. Sunata, "Komparasi Tujuh Algoritma Identifikasi Fraud ATM Pada PT. Bank Central Asia Tbk," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 7, no. 3, pp. 441–450, 2020, doi: 10.35957/jatisi.v7i3.471.

[13] "Credit Card Fraud Detection Using Machine Learning Final Research Paper | PDF | Sensitivity And Specificity | Machine Learning." https://www.scribd.com/document/512495759/Credit-Card-Fraud-Detection-using-Machine-Learning-Final-Research-Paper (accessed Mar. 24, 2022).

[14] "Random Forest For Credit Card Fraud Detection | PDF | Accuracy And Precision | Applied Mathematics." https://www.scribd.com/document/512809270/random-forest-for-credit-

card-fraud-detection (accessed Mar. 24, 2022).
[15] N. Made and W. Arie, "The Effect of Red Flags and Internal Bank Auditor Professional Skepticism on Fraud Detection in Denpasar," vol. 23, no. 8, pp. 36–43, 2023, doi: 10.9734/AJEBA/2023/v23i8952.
[16] M. Carminati, M. Polino, A. Continella, A. Lanzi, F. Maggi, and S. Zanero, "Security Evaluation of a Banking Fraud Analysis System," *ACM Trans. Priv. Secur.*, vol. 21, no. 3, Apr. 2018, doi: 10.1145/3178370.
[17] O. Syniavska, N. Dekhtyar, O. Deyneka, T. Zhukova, and O. Syniavska, "Security of e-banking systems: modelling the process of counteracting e-banking fraud," *SHS Web Conf.*, vol. 65, p. 03004, 2019, doi: 10.1051/SHSCONF/20196503004.
[18] L. Gabudeanu, I. Brici, C. Mare, I. C. Mihai, and M. C. Scheau, "Privacy Intrusiveness in Financial-Banking Fraud Detection," *Risks 2021, Vol. 9, Page 104*, vol. 9, no. 6, p. 104, Jun. 2021, doi: 10.3390/RISKS9060104.
[19] S. Nyakarimi, "Probable earning manipulation and fraud in banking sector. Empirical study from East Africa," *http://www.editorialmanager.com/cogentecon*, vol. 10, no. 1, 2022, doi: 10.1080/23322039.2022.2083477.
[20] "Skimming : a transactional card fraud monster | Acta Criminologica : African Journal of Criminology & Victimology." https://journals.co.za/doi/epdf/10.10520/EJC150915 (accessed Jun. 15, 2023).
[21] "Chip and Skim: Cloning EMV Cards with the Pre-play Attack | IEEE Conference Publication | IEEE Xplore." https://ieeexplore.ieee.org/abstract/document/6956556 (accessed Jun. 15, 2023).
[22] K. J. Barker, J. D'Amato, and P. Sheridon, "Credit card fraud: awareness and prevention," *J. Financ. Crime*, vol. 15, no. 4, pp. 398–410, Oct. 2008, doi: 10.1108/13590790810907236/FULL/XML.
[23] J. O. Adeoti, "Automated Teller Machine (ATM) Frauds in Nigeria: The Way Out," *Kamla Raj Enterp.*, vol. 27, no. 1, pp. 53–58, Apr. 2017, doi: 10.1080/09718923.2011.11892905.
[24] "415457304-McGraw-Hill-series-in-computer-science-Tom-M-Mitchell-Machine-Learning-1997-McGraw-Hill-pdf.pdf."
[25] S. B. Kotsiantis, "Supervised Machine Learning: A Review of Classification Techniques," *Informatica*, vol. 31, pp. 249–268, 2007.
[26] I. H. Witten, E. Frank, and M. A. Hall, "Data Mining: Practical Machine Learning Tools and Techniques, Third Edition," *Data Min. Pract. Mach. Learn. Tools Tech. Third Ed.*, pp. 1–629, Jan. 2011, doi: 10.1016/C2009-0-19715-5.
[27] V. J. Hodge and J. Austin, "A Survey of Outlier Detection Methodologies," *Artif. Intell. Rev. 2004 222*, vol. 22, no. 2, pp. 85–126, Oct. 2004, doi: 10.1007/S10462-004-4304-Y.
[28] J. Ha, M. Kambe, and J. Pe, "Data Mining: Concepts and Techniques," *Data Min. Concepts Tech.*, pp. 1–703, Jan. 2011, doi: 10.1016/C2009-0-61819-5.
[29] P.-N. Tan, M. Steinbach, and V. Kumar, "Introduction to Data Mining Instructor's Solution Manual".

[30] K. Arulkumaran, M. P. Deisenroth, M. Brundage, and A. A. Bharath, "IEEE SIGNAL PROCESSING MAGAZINE, SPECIAL ISSUE ON DEEP LEARNING FOR IMAGE UNDERSTANDING (ARXIV EXTENDED VERSION) 1 A Brief Survey of Deep Reinforcement Learning."
[31] I. G. and Y. B. and A. Courville, "Deep learning by Ian Goodfellow,Yoshua Bengio, Aaron Courville," *Nature*, vol. 29, no. 7553, pp. 1–73, 2016.
[32] C. Cortes and V. Vapnik, "Support-vector networks," *Mach. Learn.*, vol. 20, no. 3, pp. 273–297, Sep. 1995, doi: 10.1007/BF00994018.
[33] S. Wang, "A comprehensive survey of data mining-based accounting-fraud detection research," *2010 Int. Conf. Intell. Comput. Technol. Autom. ICICTA 2010*, vol. 1, pp. 50–53, 2010, doi: 10.1109/ICICTA.2010.831.
[34] L. Breiman, "Random forests," *Mach. Learn.*, vol. 45, no. 1, pp. 5–32, Oct. 2001, doi: 10.1023/A:1010933404324.
[35] C. Dombry and J.-J. Duchamps, "A large sample theory for infinitesimal gradient boosting," 2022.
[36] M. J. Saberian and N. Vasconcelos, "Multiclass Boosting: Theory and Algorithms".
[37] T. Chen and C. Guestrin, "XGBoost: A Scalable Tree Boosting System," *Proc. 22nd ACM SIGKDD Int. Conf. Knowl. Discov. Data Min.*, doi: 10.1145/2939672.
[38] A. Dal Pozzolo, O. Caelen, Y.-A. Le Borgne, S. Waterschoot, and G. Bontempi, "Learned lessons in credit card fraud detection from a practitioner perspective," *Expert Syst. Appl.*, vol. 41, pp. 4915–4928, 2014, doi: 10.1016/j.eswa.2014.02.026.
[39] "Glossary of Terms Journal of Machine Learning." https://ai.stanford.edu/~ronnyk/glossary.html (accessed Jun. 16, 2023).
[40] A. Tharwat, "Classification assessment methods," *Appl. Comput. Informatics*, vol. 17, no. 1, pp. 168–192, 2018, doi: 10.1016/J.ACI.2018.08.003.
[41] T. Fawcett, "An introduction to ROC analysis," *Pattern Recognit. Lett.*, vol. 27, no. 8, pp. 861–874, Jun. 2006, doi: 10.1016/J.PATREC.2005.10.010.
[42] D. M. W. Powers, "Evaluation: from precision, recall and F-measure to ROC, informedness, markedness and correlation," Oct. 2020, Accessed: Jun. 16, 2023. [Online]. Available: https://arxiv.org/abs/2010.16061v1
[43] B. M. Ololade, M. K. Salawu, and A. D. Adekanmi, "E-Fraud in Nigerian Banks: Why and How?," *J. Financ. Risk Manag.*, vol. 09, no. 03, pp. 211–228, 2020, doi: 10.4236/JFRM.2020.93012.