REFERENCES

[1] S P Maniraj, Aditya Saini, Swarna Deep Sarkar Shadab Ahmed; Credit Card Fraud Detection using Machine Learning and Data Science (September-2019); International Journal of Engineering Research & Technology (IJERT); ISSN: 2278-0181 Vol. 8 Issue 09,

[2] Emmanuel Ileberi, Yanxia Sun and Zenghui Wang; A machine learning based credit card fraud detection using the GA algorithm for feature selection (2022); Ileberi et al. Journal of Big Data.

[3] Bharat Kumar Padhi, Sujata Chakravarty, Bighnaraj Naik , Radha Mohan Pattanayak, and Himansu Das; RHSOFS: Feature Selection Using the Rock Hyrax Swarm Optimization Algorithm for Credit Card Fraud Detection System (2022); ;Sensors 2022, 22(23), 9321; (Online) https://doi.org/10.3390/s22239321

[4] Y. Fang, Y. Zhang, and C. Huang, "Credit Card Fraud Detection Based on Machine Learning," Computers, Materials & Continua, vol. 61, no. 1, pp. 185-195, 2019. [Online]. Available: http://www.techscience.com/cmc, doi:10.32604/cmc.2019.06144.

[5] S. Aggarwal, V. Nautiyal, G. Joshi, and N. Galhotra, "Credit Card Fraud Detection Using Machine Learning," International Journal of Innovative Science and Research Technology, vol. 8, no. 6, pp. 321, June 2023. [Online]. Available: www.ijisrt.com, ISSN: 2456-2165.

[6] K. Madkaikar, M. Nagvekar, P. Parab, R. Raikar, and S. Patil, "Credit Card Fraud Detection System," International Journal of Recent Technology and Engineering (IJRTE), vol. 10, no. 2, pp. [22], July 2021. [Online]. Available: https://www.ijrte.org, ISSN: 2277-3878.

[7] F. K. Alarfaj, I. Malik, H. U. Khan, N. Almusallam, M. Ramzan, and M. Ahmed, "Credit Card Fraud Detection Using State-of-the-Art Machine Learning and Deep Learning Algorithms," IEEE Access, vol. 10, pp. 1-1, 2022, Art no. 3166891, doi: 10.1109/ACCESS.2022.3166891.

[8] V. Sahaya Sakila, Sandeep M, Praveen Hari Krishna N, "Adversarial Attack on Machine Learning Models," International Journal of Innovative Technology and Exploring Engineering (IJITEE), vol. 8, no. 6S4, April 2019. ISSN: 2278-3075.

[9] Han Xu, Yaxin Li, Wei Jin, and Jiliang Tang, "Adversarial Attacks and Defenses: Frontiers, Advances and Practice," in Proceedings of the 26th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining (KDD '20), August 23–27, 2020, Virtual Event, USA, Computer Science and Engineering, Michigan State University. ACM, New York, NY, USA, 2 pages.

https://doi.org/10.1145/3394486.340646

[10] Anant Jain, "Breaking Neural Networks with Adversarial Attacks," Towards Data Science, available at: https://towardsdatascience.com/breaking-neural-networks-with-adversarial-attacks-f4290a9a45aa

[11] T. B. Brown, D. Mané, A. Roy, M. Abadi, and J. Gilmer, "Adversarial Patch," [Online]. Available: https://arxiv.org/pdf/1712.09665.pdf

[12] O. Kovalenko, "Credit Card Fraud Detection Using Machine Learning," SPD-Group, Project Manager, https://spd.tech/machine-learning/credit-card-fraud-detection/, viewed 02.01.2023.

[13] J. Lin, L. L. Njilla, and K. Xiong, "Secure machine learning against adversarial samples at test time," EURASIP Journal on Information Security, vol. 2022, no. 1, January 2022, Art. no. 1. doi: 10.1186/s13635-021-00125-2.

[14] Barreno, M., & Hinton, G. E. (2014). Elastic net regularization: A simple and effective method for sparse feature selection in high-dimensional data. *Journal of Machine Learning Research*, 15(1), 1671-1688.

[15] J. Goodfellow, J. Shlens, and C. Szegedy, "Explaining and harnessing adversarial examples," *arXiv preprint arXiv:1412.6572*, 2014. Available: https://arxiv.org/abs/1412.6572

[16] Moosavi-Dezfooli, S.-M., Fawzi, A., & Frossard, P. (2016). "DeepFool: A Simple and Accurate Method to Fool Deep Neural Networks." In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2016, pages 2574-2582 Available: https://arxiv.org/abs/1511.04599

[17] Chen, P.-Y., Zhang, H., Sharma, Y., Yi, J., & Hsieh, C.-J. (2017). "ZOO: Zeroth Order Optimization Based Black-box Attacks to Deep Neural Networks without Training Substitute Models." In *Proceedings of the 10th ACM Workshop on Artificial Intelligence and Security (AISec)*, 2017; Available: https://arxiv.org/abs/1708.03999

[18] Chen, P.-Y., Sharma, Y., Zhang, H., Yi, J., & Hsieh, C.-J. (2018). "EAD: Elastic-Net Attacks to Deep Neural Networks via Adversarial Examples." In *Proceedings of the AAAI Conference on Artificial Intelligence*, 2018 Available: https://arxiv.org/abs/1709.04114.

[19] Papernot, N., McDaniel, P., Wu, X., Jha, S., & Swami, A. (2016). "Distillation as a Defense to Adversarial Perturbations Against Deep Neural Networks." In *Proceedings of the IEEE Symposium on Security and Privacy (SP)*, 2016, pages 582-597; Available: https://arxiv.org/abs/1511.04508.

[20] Cohen, J., Rosenfeld, E., & Kolter, J. Z. (2019). "Certified Adversarial Robustness via Randomized Smoothing." In *Proceedings of the 36th International Conference on Machine Learning (ICML)*, 2019; Available: https://arxiv.org/abs/1902.02918.

[21] Global Risk Institute, “Adversarial machine learning: Risks and opportunities for financial institutions,” Global Risk Institute, Mar. 7, 2022. [Online]. Available: https://globalriskinstitute.org/publication/adversarial-machine-learning-risks-and-opportunities-for-financial-institutions/

[22] J. Ren and H. Wang, *Mathematical Methods in Data Science*, "Logistic Sigmoid," in *Computer Science*, ScienceDirect, 2023. Available: https://www.sciencedirect.com/topics/computer-science/logistic-sigmoid.

[23] M. Zhou, X. Gao, J. Wu, K. Liu, H. Sun, and L. Li, "Investigating White-Box Attacks for On-Device Models," ICSE '24: Proceedings of the IEEE/ACM 46th International Conference on Software Engineering, Article No. 152, pp. 1-12, 2024. doi: 10.1145/3597503.3639144.

[24] S. Kaviani and I. Sohn, "Black-Box Attack," Expert Systems with Applications, vol. 26, 2022.

[25] HYPR, "Hybrid Attack," Security Encyclopedia, Available: https://www.hypr.com/security-encyclopedia/hybrid-attack. [Accessed: 31-Mar-2025].