

DAFTAR PUSTAKA

- [1] R. Farishy, “The use of artificial intelligence in banking industry,” *International Journal of Social Service and Research*, vol. 3, pp. 1724–1731, 2023.
- [2] R. Towle and B. Mavleos, “Fraud in financial services: Leaning on generative ai to protect a rapidly expanding attack surface,” *Elastic Blog*, February 2024. [Online]. Available: <https://www.elastic.co/blog/financial-services-fraud-generative-ai-attack-surface>
- [3] M. Ibrahim, “Jos! transaksi qris tembus rp31,65 triliun, naik 149,46 persen,” *Infobanknews*, February 2024. [Online]. Available: <https://infobanknews.com/jos-transaksi-qris-tembus-rp3165-triliun-naik-14946-persen>
- [4] O. H. Fares, I. Butt, and S. H. M. Lee, “Utilization of artificial intelligence in the banking sector: A systematic literature review,” *Journal of Financial Services Marketing*, vol. 28, no. 4, pp. 835–852, 2022.
- [5] B. Hodges, “Banking-as-a-service: Fintechs walking the regulatory perimeter,” *Brooklyn Journal of Corporate, Financial & Commercial Law*, vol. 17, p. 127, 2023.
- [6] B. Gregory, “Why is my data playing hard to get?” *Astronomer Blog*, December 2016. [Online]. Available: <https://www.astronomer.io/blog/why-is-my-data-playing-hard-to-get/>
- [7] J. Boitnott, “Credit card fraud statistics,” *Self Financial — Data & Guides*, 2024. [Online]. Available: <https://www.self.inc/info/credit-card-fraud-statistics>
- [8] PYMNTS, “Seven in 10 financial institutions use ai and ml to combat fraud,” *PYMNTS.com*, March 2024. [Online]. Available: <https://www.pymnts.com/news/security-and-risk/2024/seven-in-10-financial-institutions-use-ai-and-ml-to-combat-fraud/>
- [9] H. He, Z. Wang, H. Jain, C. Jiang, and S. Yang, “A privacy-preserving decentralized credit scoring method based on multi-party information,” *Decision Support Systems*, vol. 166, p. 113910, 2023.
- [10] P. Kairouz, H. B. McMahan *et al.*, “Advances and open problems in federated learning,” *arXiv preprint arXiv:1912.04977*, 2019.
- [11] H. B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y. Arcas, “Communication-efficient learning of deep networks from decentralized data,” *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics*, pp. 1273–1282, 2017.
- [12] S. Truex, L. Liu, K.-H. Chow, M. E. Gursoy, W. Wei, and Y. Wu, “A hybrid approach to privacy-preserving federated learning,” *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, pp. 451–468, 2019.

- [13] L. Wang, R. Jia, and D. Song, "D2p-fed: Differentially private federated learning with efficient communication," *arXiv preprint arXiv:2006.13039*, 2020. [Online]. Available: <https://arxiv.org/abs/2006.13039>
- [14] A. Ponomareva, V. Nikolaenko, and D. Ivanov, "Clipping matters: Towards fair and accurate federated learning," in *Proceedings of the 40th International Conference on Machine Learning (ICML)*, 2023. [Online]. Available: <https://arxiv.org/abs/2303.07859>
- [15] M. Nasr, R. Shokri, and A. Houmansadr, "Comprehensive privacy analysis of deep learning: Passive and active white-box inference attacks against centralized and federated learning," *IEEE Symposium on Security and Privacy (SP)*, pp. 739–753, 2019.
- [16] M. Abadi, A. Chu, I. Goodfellow, H. B. McMahan, I. Mironov, K. Talwar, and L. Zhang, "Deep learning with differential privacy," *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, pp. 308–318, 2016.
- [17] R. C. Geyer, T. Klein, and M. Nabi, "Differentially private federated learning: A client level perspective," *arXiv preprint arXiv:1712.07557*, 2017.
- [18] A. Agarwal, A. T. Suresh, F. X. Yu, S. Kumar, and B. McMahan, "Communication-efficient federated learning using gradient descent optimization," *Advances in Neural Information Processing Systems*, pp. 4730–4740, 2018.
- [19] Y. Zhao, T. Li, L. Lai, A. K. Sahu, M. Zaheer, and A. Talwalkar, "Federated learning on non-iid data: A survey," *arXiv preprint arXiv:1806.00582*, 2018.
- [20] N. Papernot, S. Song, I. Mironov, A. Raghunathan, K. Talwar, and Ú. Erlingsson, "Scalable private learning with pate," *arXiv preprint arXiv:1802.08908*, 2018.
- [21] T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, "On the effectiveness of federated averaging in non-iid scenarios," *arXiv preprint arXiv:2006.04737*, 2020.
- [22] X. Sun, Y. Zhang, and L. Li, "Adaptive gradient clipping for improved training of federated learning with heterogeneous data," *Advances in Neural Information Processing Systems*, vol. 34, pp. 4861–4874, 2021.
- [23] J. Andrew, K. Lee, and E. Kim, "Hybrid clipping for privacy-preserving federated learning," *IEEE Transactions on Neural Networks and Learning Systems*, 2022.
- [24] S. Bhattacharyya, S. Jha, K. Tharakunnel, and J. Westland, "Data mining for credit card fraud: A comparative study," *Decision Support Systems*, vol. 50, no. 3, pp. 602–613, 2011.
- [25] F. Carcillo, A. Laurent, Y.-A. Le Borgne, G. Bontempi, and O. Caelen, "Combining unsupervised and supervised learning in credit card fraud detection," *Information Sciences*, vol. 557, pp. 317–331, 2021.
- [26] N. F. Aurna, M. D. Hossain, Y. Taenaka, and Y. Kadobayashi, "Federated learning-based credit card fraud detection: Performance analysis with sampling methods and deep learning algorithms," in *2023 IEEE International Conference on Cyber Security and Resilience (CSR)*, 2023, pp. 180–187.

- [27] TensorFlow, “Tensorflow documentation,” 2025. [Online]. Available: <https://www.tensorflow.org/>
- [28] K. Team, “Keras documentation,” 2025. [Online]. Available: <https://keras.io/>
- [29] P. Team, “Pytorch documentation,” 2025. [Online]. Available: <https://pytorch.org/docs/stable/index.html>
- [30] S. learn Developers, “Scikit-learn documentation,” 2025. [Online]. Available: <https://scikit-learn.org/>
- [31] T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, “Federated optimization in heterogeneous networks,” *arXiv preprint arXiv:2003.00295*, 2020.
- [32] F. L. GmbH, “Flower framework documentation,” 2025. [Online]. Available: <https://flower.ai/docs/framework/index.html>
- [33] O. Community, “Pysyft documentation,” 2025. [Online]. Available: <https://github.com/OpenMined/PySyft>
- [34] C. Dwork, F. McSherry, K. Nissim, and A. Smith, “Calibrating noise to sensitivity in private data analysis,” *Journal of Privacy and Confidentiality*, vol. 7, no. 3, pp. 1–25, 2006.
- [35] F. McSherry, “Privacy integrated queries: an extensible platform for privacy-preserving data analysis,” *Proceedings of the 2009 ACM SIGMOD International Conference on Management of Data*, pp. 19–30, 2009.
- [36] A. Dal Pozzolo, O. Caelen, R. Johnson, and G. Bontempi, “Learned lessons in credit card fraud detection from a practitioner perspective,” *Expert Systems with Applications*, vol. 41, no. 10, pp. 4915–4928, 2014.
- [37] Q. Yang, Y. Liu, T. Chen, and Y. Tong, “Federated machine learning: Concept and applications,” *ACM Transactions on Intelligent Systems and Technology (TIST)*, vol. 10, no. 2, pp. 1–19, 2019.
- [38] T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, “Federated learning: Challenges, methods, and future directions,” *IEEE Signal Processing Magazine*, vol. 37, no. 3, pp. 50–60, 2020.
- [39] P. Kairouz, H. B. McMahan, B. Avent, A. Bellet, M. Bennis, A. N. Bhagoji, K. Bonawitz, Z. Charles, G. Cormode, R. G. D’Oliveira *et al.*, “Advances and open problems in federated learning,” *Foundations and Trends in Machine Learning*, vol. 14, no. 1-2, pp. 1–210, 2021.
- [40] A. Reisizadeh, A. Mokhtari, H. Hassani, A. Jadbabaie, and R. Pedarsani, “Fedpaq: A communication-efficient federated learning method with periodic averaging and quantization,” *arXiv preprint arXiv:2002.01029*, 2020.
- [41] V. Smith, C.-K. Chiang, M. Sanjabi, and A. Talwalkar, “Federated multi-task learning,” in *Proceedings of the 31st International Conference on Neural Information Processing Systems*, 2017, pp. 4427–4437.



- [42] K. Bonawitz, H. Eichner, W. Grieskamp, D. Huba, A. Ingerman, V. Ivanov, C. Kiddon, J. Konecny, S. Mazzocchi, B. McMahan, T. Van Overveldt, D. Petrou, D. Ramage, and J. Roselander, "Towards federated learning at scale: System design," *Proceedings of the 3rd Conference on Machine Learning and Systems (MLSys)*, 2019.
- [43] X. Chen, Z. S. Wu, and M. Hong, "Understanding gradient clipping in private sgd: A geometric perspective," in *Advances in Neural Information Processing Systems*, vol. 33, 2020, pp. 13 756–13 766.
- [44] Y. LeCun, L. Bottou, Y. Bengio, and P. Haffner, "Gradient-based learning applied to document recognition," in *Proceedings of the IEEE*, vol. 86, no. 11, 1998, pp. 2278–2324.
- [45] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "Imagenet classification with deep convolutional neural networks," in *Proceedings of the 25th International Conference on Neural Information Processing Systems (NIPS)*, 2012, pp. 1097–1105.
- [46] P. Chatterjee, D. Das, and D. B. Rawat, "Use of federated learning and blockchain towards securing financial services," *Cyber-Physical Systems*, 2023.
- [47] P. S. Foundation, "Python documentation," 2025. [Online]. Available: <https://docs.python.org/3/>
- [48] P. D. Team, "Pandas documentation," 2025. [Online]. Available: <https://pandas.pydata.org/>
- [49] N. Community, "Numpy documentation," 2025. [Online]. Available: <https://numpy.org/doc/>
- [50] M. D. Team, "Matplotlib documentation," 2025. [Online]. Available: <https://matplotlib.org/>
- [51] C. Dwork and A. Roth, *The Algorithmic Foundations of Differential Privacy*, ser. Foundations and Trends in Theoretical Computer Science. now Publishers, 2014, vol. 9, no. 3–4. [Online]. Available: <https://doi.org/10.1561/04000000042>
- [52] I. Mironov, "Rényi differential privacy," in *Proceedings of the 30th IEEE Computer Security Foundations Symposium (CSF '17)*. IEEE, 2017, pp. 263–275.
- [53] R. Geyer, T. Klein, and M. Nabi, "Client-level differentially private federated learning," *Advances in Neural Information Processing Systems*, vol. 31, 2018.