IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, April 2023
Impact Factor: 7.301

Empowering Privacy-Preserving Machine Learning: A Comprehensive Survey on Federated Learning

I. Dwaraka Srihith[1]
[1]Alliance University, Bangalore
A. David Donald[2], **T. Aditya Sai Srinivas**[2], **G. Thippanna**[2]
[2]Ashoka Women's Engineering College, Kurnool
D. Anjali[3]
[3]G. Pulla Reddy Engineering College, Kurnool

Abstract: *As the need for machine learning models continues to grow, concerns about data privacy and security become increasingly important. Federated learning, a decentralized machine learning approach, has emerged as a promising solution that allows multiple parties to collaborate and build models without sharing sensitive data. In this comprehensive survey, we explore the principles, techniques, and applications of federated learning, with a focus on its privacy-preserving aspects.*

Keywords: Federated learning, Decentralized machine learning, Privacy-preserving machine learning, Collaborative learning.

REFERENCES

[1]. Kairouz, P., McMahan, H. B., Avent, B., Bellet, A., Bennis, M., Bhagoji, A. N., ... & Oh, S. (2019). Advances and open problems in federated learning. arXiv preprint arXiv:1912.04977.
[2]. Li, T., Sahu, A. K., Talwalkar, A., & Smith, V. (2020). Federated learning: Challenges, methods, and future directions. IEEE Signal Processing Magazine, 37(3), 50-60.
[3]. Bonawitz, K., Ivanov, V., Kreuter, B., Marcedone, A., McMahan, H. B., Patel, S., ... & Yurochkin, M. (2019). Towards federated learning at scale: System design. arXiv preprint arXiv:1902.01046.
[4]. Yang, Q., Liu, Y., Chen, T., & Tong, Y. (2019). Federated machine learning: Concept and applications. ACM Transactions on Intelligent Systems and Technology (TIST), 10(2), 1-19.
[5]. McMahan, H. B., Ramage, D., Talwar, K., & Zhang, L. (2017). Communication-efficient learning of deep networks from decentralized data. In Proceedings of the 20th International Conference on Artificial Intelligence and Statistics (pp. 1273-1282).
[6]. Sheller, M. J., Reina, G. A., & Edwards, B. (2018). Federated learning in medicine: facilitating multi-institutional collaborations without sharing patient data. Scientific Reports, 8(1), 1-7.
[7]. Li, Y., Zhang, K., & Yang, Y. (2020). Survey on secure federated learning. IEEE Access, 8, 212776-212787.
[8]. Konečnỳ, J., McMahan, H. B., Yu, F. X., Richtárik, P., Suresh, A. T., & Bacon, D. (2016). Federated learning: Strategies for improving communication efficiency. arXiv preprint arXiv:1610.05492.
[9]. Ramasubbareddy, Somula, Evakattu Swetha, Ashish Kumar Luhach, and T. Aditya Sai Srinivas. "A multi-objective genetic algorithm-based resource scheduling in mobile cloud computing." International Journal of Cognitive Informatics and Natural Intelligence (IJCINI) 15, no. 3 (2021): 58-73.
[10]. Hardy, M., Branson, K., & Zou, J. (2017). Federated learning for healthcare informatics. Journal of Healthcare Informatics Research, 1(3-4), 1-16.
[11]. Li, X., Li, B., & Li, Y. (2020). Federated learning: Challenges and opportunities. Future Generation Computer Systems, 102, 698-709.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, April 2023
Impact Factor: 7.301

[12]. Srinivas, T., G. Aditya Sai, and R. Mahalaxmi. "A Comprehensive Survey of Techniques, Applications, and Challenges in Deep Learning: A Revolution in Machine Learning." International Journal of Mechanical Engineering 7, no. 5 (2022): 286-296.

[13]. Yang, Q., Liu, Y., & Chen, T. (2019). Federated learning: A distributed machine learning approach for healthcare privacy and security. Journal of Medical Systems, 43(8), 1-9.

[14]. Zhang, Y., Yang, Q., Chen, T., & Liu, Y. (2020). Federated learning for mobile keyboard prediction. In Proceedings of the 26th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining (pp. 1771-1779).

[15]. Huang, L., Wang, T., & Xiao, Y. (2021). A survey of federated learning in smart cities. IEEE Communications Surveys & Tutorials, 23(1), 259-283.

[16]. Zhao, C., Yang, L., Li, J., & Zhang, Y. (2020). Federated learning based on blockchain: Challenges and opportunities. IEEE Access, 8, 26759-26772.

[17]. Srinivas, T. Aditya Sai, G. Mahalaxmi, R. Varaprasad, A. David Donald, and G. Thippanna. "AI in Transportation: Current and Promising Applications." IUP Journal of Telecommunications 14, no. 4 (2022): 37-57.

[18]. Kairouz, P., Oh, S., & Viswanath, P. (2021). Advances and open problems in federated learning. Communications of the ACM, 64(4), 82-89.

[19]. Bonawitz, K., Ivanov, V., Kreuter, B., Marcedone, A., McMahan, H. B., Patel, S., ... & Shin, M. (2019). Practical secure aggregation for privacy-preserving machine learning. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (pp. 1175-1191).

[20]. Hitaj, B., Ateniese, G., & Perez-Cruz, F. (2017). Deep models under the GAN: information leakage from collaborative deep learning. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (pp. 603-618).

[21]. McMahan, H. B., Ramage, D., Talwar, K., & Zhang, L. (2017). Learning differentially private recurrent language models. In International Conference on Learning Representations.

[22]. Konečný, J., McMahan, H. B., Yu, F. X., Richtárik, P., Suresh, A. T., & Bacon, D. (2016). Federated learning: Strategies for improving communication efficiency. arXiv preprint arXiv:1610.05492.

[23]. Li, J., Li, Q., Fang, B., Yang, C., Zhang, Z., & Wang, W. (2018). Federated learning for healthcare informatics. Journal of medical systems, 42(8), 1-7.