

Federated Learning: A Hype or a Trend?

Anna Wilbik^a

*Department of Advanced Computing Sciences (DACS),
Maastricht University, Maastricht, The Netherlands*

1 EXTENDED ABSTRACT

Federated learning is an emerging technology that attracts growing attention from academia and industry. Almost 3000 papers on this topic are already indexed in Web of Science, and almost half of them were published last year. Also many companies, from various industries, e.g. ICT, telecom, healthcare, manufacturing, finance are assessing the new possibilities.

Federated learning enables a collaboration between multiple parties to jointly train a machine learning model without exchanging the local data (by: Peter Kairouz and McMahan, 2021). Because the data are not exchanged between parties, it is considered a privacy preserving approach. The collaboration in learning is considered successful, if for at least one party the performance of the federated model is better than the performance of the local model (Li et al., 2019). It aims to help organizations in situations, when a single party does not have sufficient amount of data.


Federated learning has come a long way since it was first proposed by McMahan in 2016 (McMahan et al., 2017). Generally, FL can be divided into different scenarios based on how the data is partitioned or distributed among the data owners, i.e., horizontally or vertically. Horizontal federated learning is used when different parties collect the same features but from different subjects. A common example of horizontal federated learning is a group of hospitals collaborating to build a model that can predict a health risk for their patients, based on agreed data. Vertical federated learning is used when multiple parties share not the features, but the subjects, like e.g., a telecom company collaborating with a home entertainment company (cable tv provider), or an airline collaborating with a car rental agency.

Federated learning is still facing many challenges. For some issues, especially in the context of horizontal federated learning, here were proposed various approaches to deal with problems such as for instance algorithm convergence, communication over-

head, data heterogeneity, or security and privacy risks, especially in the context of adversary attacks. Yet, still those solutions are fragmented, and do not cover the whole spectrum of the problem, e.g. there are different, complementary strategies to deal with the non-iid data (Zhu et al., 2021). But there are also some basic challenges that needs some attention, such as supporting machine learning workflows including hyperparameter searches. Also currently most of the implemented federated learning methods employ the empirical risk minimization formulations. The tree-based methods, online learning, Bayesian learning are still not investigated. There may be needs for developments in the areas of other learning types, e.g., reinforcement learning, unsupervised and semi-supervised, active learning. Other challenges, like data alignment, are only partially recognized. Entity alignment is an important topic in vertical federated learning (e.g., Scannapieco et al., 2007)), while almost neglected in horizontal federated learning (Pekala et al., 2022). Moreover recent developments in XAI and ethical computing open additional possibilities in terms of addressing model fairness or assessing a party contribution to the model.

This vast research effort did not remained unnoticed, and the federated learning was added to the Gartner's Hype Cycle for Privacy in 2021 (Moore, 2021), see Figure 1. A hype cycle is a graphical representation of a common pattern that a technology goes through from conception to maturity and widespread adoption. The five stages in the hype cycle are Technology/Innovation Trigger, Peak of Inflated Expectations, Trough of Disillusionment, Slope of Enlightenment and Plateau of Productivity.

Federated learning is still at the first stage. Here the technology is at its infancy, with early proof-of-concept stories and significant publicity. However, often no usable products exist or the commercial viability is unproven. So far, Horizontal Federated Learning has been successfully deployed in google keyboard, where a mobile phone can better predict the next word typed by the owner (Hard et al., 2018). Moreover there were several suc-

^a  <https://orcid.org/0000-0002-1989-0301>

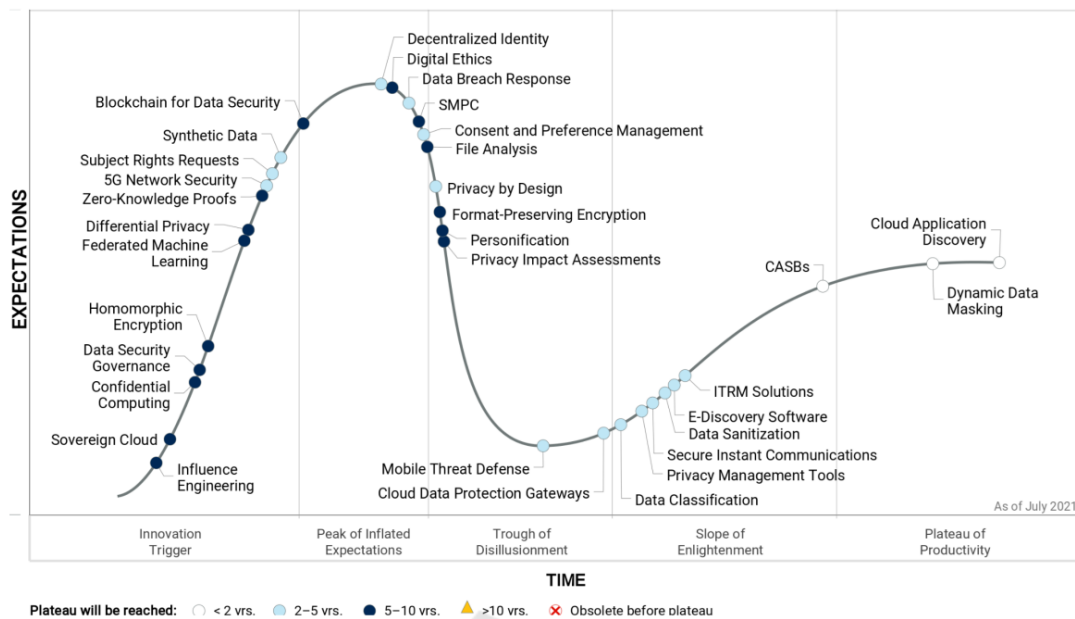


Figure 1: Gartner Hype Cycle for Privacy, 2021 (Moore, 2021).

successful demonstrators of federated learning in hospitals (Deist et al., 2017) or in finance for transaction fraud detection (Zheng et al., 2020). We have explored the use of federated learning for processing IoT data to support decision making in business processes, building a concept model (Grefen et al., 2018) and a demonstrator (d’Hondt et al., 2019). In case of vertical federated learning, the technology seems to be even less mature, with a demonstrator in healthcare (Sun et al., 2021) and a developed platform (Liu et al., 2021) being the most advanced application examples.

But each emerging technology after initial bright start, reaches Peak of Inflated Expectations, after which comes a Trough of Disillusionment, where the interest gets smaller as experiments and implementations fail to deliver. Many “great” ideas and technologies, have not made through the Trough of Disillusionment, such as Emergent Computing, Mesh Networks, Dig Data to name just a few (Mullany, 2016).

The technology/innovation can only reach the fully mature stage of the Plateau of Productivity, if they can show their relevance. Whether federated learning can reach the full maturity, or will remain just a hype, depends on us. In my talk I will also discuss opportunities, we can unlock by embracing the relevance from the very beginning.

REFERENCES

- by: Peter Kairouz, E. and McMahan, H. B. (2021). Advances and open problems in federated learning. *Foundations and Trends® in Machine Learning*, 14(1):–.
- Deist, T. M., Jochems, A., van Soest, J., Nalbantov, G., Oberije, C., Walsh, S., Eble, M., Bulens, P., Coucke, P., Dries, W., et al. (2017). Infrastructure and distributed learning methodology for privacy-preserving multi-centric rapid learning health care: eurocat. *Clinical and translational radiation oncology*, 4:24–31.
- d’Hondt, T., Wilbik, A., Grefen, P., Ludwig, H., Baracaldo, N., and Anwar, A. (2019). Using bpm technology to deploy and manage distributed analytics in collaborative iot-driven business scenarios. In *Proceedings of the 9th International Conference on the Internet of Things*, pages 1–8.
- Grefen, P., Ludwig, H., Tata, S., Dijkman, R., Baracaldo, N., Wilbik, A., and D’hondt, T. (2018). Complex collaborative physical process management: a position on the trinity of bpm, iot and da. In *Working Conference on Virtual Enterprises*, pages 244–253. Springer.
- Hard, A., Kiddon, C. M., Ramage, D., Beaufays, F., Eichner, H., Rao, K., Mathews, R., and Augenstein, S. (2018). Federated learning for mobile keyboard prediction.
- Li, Q., Wen, Z., Wu, Z., Hu, S., Wang, N., and He, B. (2019). A survey on federated learning systems: vision, hype and reality for data privacy and protection. *arXiv preprint arXiv:1907.09693*.
- Liu, Y., Fan, T., Chen, T., Xu, Q., and Yang, Q. (2021). Fate: An industrial grade platform for collaborative learning

- with data protection. *Journal of Machine Learning Research*, 22(226):1–6.
- McMahan, B., Moore, E., Ramage, D., Hampson, S., and y Arcas, B. A. (2017). Communication-efficient learning of deep networks from decentralized data. In *Artificial Intelligence and Statistics*, pages 1273–1282. PMLR.
- Moore, S. (2021). Gartner says digital ethics is at the peak of inflated expectations in the 2021 gartner hype cycle for privacy.
- Mullany, M. (2016). 8 lessons from 20 years of hype cycles.
- Pekala, B., Dyczkowski, K., Szkola, J., and Wilbik, A. (2022). A method for improving the generation of linguistic summaries. In *2022 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)*.
- Scannapieco, M., Figotin, I., Bertino, E., and Elmagarmid, A. K. (2007). Privacy preserving schema and data matching. In *Proceedings of the 2007 ACM SIGMOD International Conference on Management of Data, SIGMOD '07*, page 653–664, New York, NY, USA. Association for Computing Machinery.
- Sun, W., Chen, Y., Yang, X., Cao, J., and Song, Y. (2021). Fedio: Bridge inner- and outer-hospital information for perioperative complications prognostic prediction via federated learning. In *2021 IEEE International Conference on Bioinformatics and Biomedicine (BIBM)*, pages 3215–3221.
- Zheng, W., Yan, L., Gou, C., and Wang, F.-Y. (2020). Federated meta-learning for fraudulent credit card detection. In *Proceedings of the Twenty-Ninth International Joint Conference on Artificial Intelligence (IJCAI-20)*.
- Zhu, H., Xu, J., Liu, S., and Jin, Y. (2021). Federated learning on non-iid data: A survey. *arXiv:2106.06843*.