A Comprehensive Study of Federated Learning Tools and Frameworks for Data-Sensitive Applications

Manu Narula[1], Jasraj Meena[2],Dinesh Kumar Vishwakarma[1]
Delhi Technological University, India[1]
Jawaharlal Nehru University, India[2]
Corresponding author: Manu Narula, Email: manunarula1996@gmail.com

Artificial intelligence depends upon various learning techniques to analyze and process data. Most of these techniques store data centrally or clone it to all training devices. While it presents no issue in standard applications, it quickly becomes a potential security risk when sensitive information gets involved in training, including a range of healthcare and finance utilities. Additionally, the data available for training of a Data Sensitive Application is often scattered across isolated data islands, either due to collaborative or competitive factors. Federated Learning (FL) provides a secure and efficient way to analyze such data. Due to the infancy of the technology, many tools and frameworks of FL are not well known and hence may not be used where their potential utility is maximum. This paper analyzes the various implementations and tools of FL and highlights their suitability for different scenarios with the DSAs.

Keywords: Federated Learning, Tools and Frameworks, Internet of Things, Distributed Learning

2025. In Puneet Kumar Gupta (ed.), *Computational Models for Intelligence and Automation*, 127–135. Computing & Intelligent Systems, SCRS, India. DOI: https://doi.org/10.56155/978-81-975670-1-8-12

1 Introduction

Artificial Intelligence (AI) has grown exponentially in every perceivable field, affecting daily life [7]. AI requires vast data to train models for effective performance and results. This data is usually stored centrally in one place or shared/copied, depending on the underlying learning technique. This transfers the control of all data to a third party, which the clients may not trust. However, this is not a significant concern for most AI applications like recommender systems, modeling utilities, etc. However, it is a concern for the applications when sensitive data is involved, like finance, healthcare, surveillance systems, etc. Moreover, the data required for these applications can be highly competitive and sensitive, thus cannot be centralized or shared without caveats, giving rise to data islands. It became a pivotal issue and limited the acceptance of traditional learning approaches in these applications as their efficiency suffers when trained over scattered data.

1.1 Federated Learning

To counter the requirements of Data-Sensitive Application (DSA), researchers turned to Federated Learning (FL) for private training and analysis. Google proposed FL in 2016, shifting focus from user data to model parameter vectors to train a global model [21]. The idea was extended to FL-based content suggestions and predictions in Android OS [12, 31].

At its core, FL can be seen as a modified form of Distributed Learning sharing similar architecture but implementing separate approaches for overall training. FL accounts for the distributed nature of data sources and accommodates training over multiple isolated entities, unlike distributed Learning, which manages a web of nodes to enforce parallel high-performance computing working over shared datasets [14]. In addition, FL helps alleviate the issue of data heterogeneity and system heterogeneity that is not accounted for in Distributed Learning.

1.2 Data-Sensitive Applications

A data-sensitive application is conceptualized as an implementation that depends on confidential data for its underlying AI, such as data related to individuals' social footprint [19]. Additionally, accuracy is paramount in these implementations, and faulty processing can result in invalid or dangerous outcomes. Some examples of DSA include Terminal diagnosis [15, 26] and Fraud detection [20, 22], etc. It is challenging to integrate encryption techniques during the training of such applications without affecting performance [24, 25]; this renders such measures of limited use. Another challenge in these applications is that one entity may not have sufficiently varied data for good-quality training in practical scenarios. Given the nature of the data involved, these entities are often reluctant to collaborate.

1.3 Motivation and Contribution

All currently available surveys focus on FL and its types in general, along with their applications in prominent and potential fields. Very few of them provide insights specifically for the DSA. Even fewer shine light on the actual frameworks and tools required or available to experiment with and integrate FL into application workflows. This paper evaluates FL as a secure learning medium for DSAs like healthcare and finance and highlights the popular tools and frameworks

available for FL. We discuss each of these technologies' advantages and shortcomings and the potential applications/scenarios for each. We also discuss possible future directions for budding researchers and enthusiasts. Our contributions are summarized as follows:

- To provide a comprehensive view of all the tools and frameworks available for integrating FL.
- To provide a categorical classification for state-of-the-art frameworks based on the optimal application area.
- To analyze the advantages and shortcomings of current FL tools and frameworks and suggest potential future directions.

The rest of the paper is structured as follows: In section 2, we review the surveys available on FL and compare them with our proposed work. Section 3 investigates the various tools and frameworks available for FL development and integration. The paper is then concluded in section 4. Fig. 1 represents the structure of this manuscript.

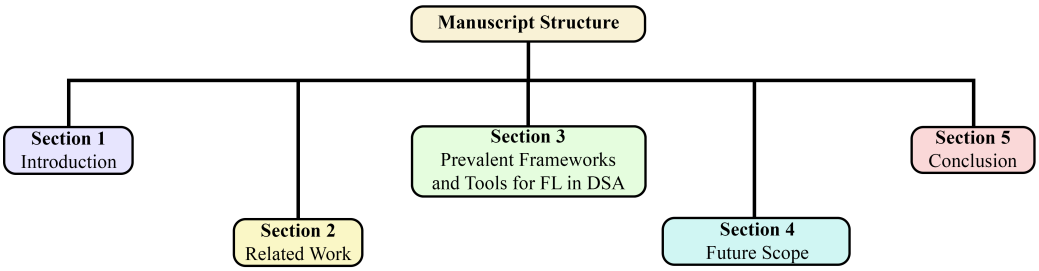

Figure 1: Structure of the manuscript.

2 Related Work

Federated Learning has attracted active research in recent years. Throughout our analysis, we came across many surveys and studies that explored the paradigm in many fields. Though many new works consider DSA, very few explore the tools and technology available for its integration. Li et al. [17] provided an in-depth view of the challenges and benefits of implementing FL, while also evaluating the reasons for the hype around the technology, Zhang et al. [32], Aledhari et al. [8], Bonawitz et al. [10], and Rodriguez Barroso et al. [28], following a general point of view. Authors in [18] take a more scrutinizing approach and focus on various present and potential concerns, flaws, and security threats of FL. Narula et al. [23] provided an elaborate systematic study of FL, detailing its types, challenges, tools, and frameworks concerning DSA. However, in the broader scope of their work, tools and frameworks made up a very small portion of the study. Most recently, Ciobotaru et al. [9] and Ali et al. [11] presented a survey on FL concerning Cancer screening and Automated Vehicles, respectively, but neither highlighted any tools to achieve the present integrations. An overview of these surveys is given in Table 1, highlighting the areas

covered and the challenges discussed in the respective works along with discussion of tools and frameworks.

Table 1: Comparison of Related Work Based on FL and DSA Aspects

Reference	FL	DSA	Advantages	Challenges	Tools	Frameworks
Li et al. [18]	✓	✗	✓	✓	✗	✗
Aledhari et al. [8]	✓	✗	✓	✓	●	●
Zhang et al. [32]	✓	✗	✓	✓	✗	✗
Li et al. [17]	✓	✗	✓	✓	●	●
Bonawitz et al. [10]	✓	✗	✗	✗	✗	✗
Rodriguez-Barroso et al. [28]	✓	✗	✓	✓	✗	✗
Narula et al. [23]	✓	✓	✓	✓	●	●
Ciobotaru et al. [9]	✓	●	✓	✓	✗	✗
Ali et al. [11]	✓	✗	✓	✓	✗	✗
Nuha et al. [?]	✓	✗	✓	✓	✗	✗
Our Work	✓	✓	●	●	✓	✓

✓ represents coverage, ✗ represents non-coverage, and ● represents partial coverage

3 Prevalent Frameworks and Tools

This subsection provides briefs about the popular tools and frameworks currently used on a large scale in the industry, including freelancing.

3.1 Tools and Frameworks for General FL Applications

3.1.1 Pysyft

In many scenarios, FL can be defined as Deep Learning with Multiparty Computation (MPC) that is sometimes secured with Differential Privacy (DP). This translates to a resource-hungry setup that can be difficult to implement and inefficient without proper management. Ryffel et al. [29] proposed the first standard that enabled FL to implement with support for both MPC and DP. The protocol is implemented through the PySyft framework, which is compatible with TensorFlow [6] and PyTorch [16] libraries, making it popular amongst developers.

3.1.2 TensorFlow Federated

TensorFlow Federated is an open-source framework for machine learning over decentralized data [30]. It is developed to promote open research and experimentation with FL. It enables users to simulate various predefined federated learning algorithms on their models and data, and can incorporate custom algorithms. A predefined set of models and algorithms also helps implement expanded FL applications, such as federated analytics.

3.1.3 Nvidia Clara

Nvidia Clara is a suite of computing solutions developed by Nvidia to empower AI in the medical domain [2]. The edge AI computing platform Nvidia EGX in Clara is designed to integrate APIs and SDK to support FL with relative ease in healthcare applications such as those discussed in [6], [7].

3.1.4 OpenFL

OpenFL is a community-driven open-source initiative developed to provide a plugin-type functionality for AI libraries in Python3 [4]. Like Pysyft, the OpenFL framework seamlessly integrates with both TensorFlow and PyTorch. The tool has extended Flash and HTML5 content support and is entirely portable.

3.1.5 FATE

FATE is another open-source project developed by Webank aimed at supporting a federated ecosystem of AI applications [1]. It provides a modular approach with ready-to-use libraries that simplifies the development process for new and learning developers. It supports MPC and big data protocols with FL-enabled libraries for graphics pipelines, interfaces, and scheduling.

3.1.6 Substra

Substra [5] is an open-source framework developed by Owkin and hosted by the Linux Foundation for AI. It doubles as a simulator for FL-based testing on a single-node setup and has a native web application to facilitate FL at a large scale.

3.1.7 IBM Federated Learning

IBM has been actively researching in the FL, developing new and innovative solutions [3]. Prominent achievements include optimizing and compressing models before uploading to the central FL server, which minimizes bandwidth utilization. Another pivotal example is the "DeTrust" framework, which employs consensus-based cryptography to securely transmit model parameter vectors.

3.1.8 PaddleFL

PaddleFL is based on PaddlePaddle, a deep learning platform developed by Baidu [27]. It supports both DP and MPC. It supports most state-of-the-art algorithms, such as FedAvg. But at the time, there is no support for Vertical FL algorithms. The development of PaddleFL is still in an early stage and wider support for new technologies may be added in future.

3.1.9 FedML

FedML is an FL framework with support for native benchmarking. Based on PyTorch, a team developed it at the University of Southern California [13]. Algorithms supported by FedML do not consider adversaries, but the support for DP is integrated as a safety measure. It supports simulation, distributed computing, and single-node implementation.

A summary of all popular Frameworks for FL is provided in Table 2.

4 Conclusion and Future Directions

In this section, we summarize our study while also suggesting a few potential research areas for future research

Table 2: Popular Frameworks for FL integration

Name	Open-Source	Pytorch support	Tensorflow support	Optimizable	Secure
Pysyft [29]	✓	✓	✓	✗	✓
TensorFlow Federated [30]	✓	✗	✓	✓	✓
Nvidia Clara [2]	✗	✓	✓	✓	✓
OpenFL [4]	✓	✓	✓	✓	✓
IBM Federated Learning [3]	✗	✗	✗	✗	✓
FATE [1]	✓	✓	✓	✓	✓
Substra [5]	✓	✓	✓	✓	✓
PaddleFL [27]	✓	✓	✓	✓	✗
FedML [13]	✓	✓	✓	✓	✗

✓ represents coverage, ✗ represents non-coverage, and ● represents partial coverage

4.1 Conclusion

Throughout this study, we go through the various tools and frameworks associated with the implementation of FL in various applications and utilities. We have provided a detailed summary of their capabilities, including integration and security optimizations. This summarized view aims to guide budding researchers with the most optimal tool for their objectives in the FL and distributed learning paradigm.

4.2 Future Directions

Most of the frameworks discussed in this work are aimed at delivering a simple and effective approach for the implementation of FL. However, whenever security is concerned, the frameworks present a substantial computational overhead that might not be feasible for resource-constrained networks such as those in the Medical field. Thus, further research should be aimed at providing security at minimal cost and in lightweight systems.

References

[1] Fate. https://fate.fedai.org/, 2023. Accessed: April 19, 2025.

[2] Federated learning powered by nvidia clara | nvidia technical blog. https://developer.nvidia.com/blog/federated-learning-clara/, 2023. Accessed: April 19, 2025.

[3] Ibm federated learning - ibm documentation. https://www.ibm.com/docs/en/cloud-paks/cp-data/4.8.x?topic=models-federated-learning, 2023. Accessed: April 19, 2025.

[4] Open federated learning (openfl) documentation. https://openfl.readthedocs.io/en/latest/, 2023. Accessed: April 19, 2025.

[5] Substra - open source federated learning software for healthcare research | owkin. https://www.owkin.com/substra, 2023. Accessed: April 19, 2025.

[6] Martín Abadi, Paul Barham, Jianmin Chen, Zhifeng Chen, Andy Davis, Jeffrey Dean, Matthieu Devin, Sanjay Ghemawat, Geoffrey Irving, Michael Isard, et al. {TensorFlow}: a system for {Large-Scale} machine learning. In *12th USENIX symposium on operating systems design and implementation (OSDI 16)*, pages 265–283, 2016.

[7] Imran Ahmed, Gwanggil Jeon, and Francesco Piccialli. From artificial intelligence to explainable artificial intelligence in industry 4.0: a survey on what, how, and where. *IEEE Transactions on Industrial Informatics*, 18(8):5031–5042, 2022. https://doi.org/10.1109/TII.2022.3146552.

[8] Mohammed Aledhari, Rehma Razzak, Reza M Parizi, and Fahad Saeed. Federated learning: A survey on enabling technologies, protocols, and applications. *IEEE Access*, 8:140699–140725, 2020. https://doi.org/10.1109/ACCESS.2020.3013541.

[9] Asad Ali, Huang Jianjun, and Ayesha Jabbar. Recent advances in federated learning for connected autonomous vehicles: Addressing privacy, performance, and scalability challenges. *IEEE Access*, pages 1–1, 2025. https://doi.org/10.1109/ACCESS.2025.3562128.

[10] Kallista Bonawitz, Peter Kairouz, Brendan Mcmahan, and Daniel Ramage. Federated learning and privacy. *Communications of the ACM*, 65(4):90–97, 2022. https://doi.org/10.1145/3500240.

[11] Alexandru Ciobotaru, Cosmina Corches, Dan Gota, and Liviu Miclea. Deep learning and federated learning in breast cancer screening and diagnosis: A systematic review. *IEEE Access*, 2025. https://doi.org/10.1109/ACCESS.2025.3560211.

[12] Andrew Hard, Kanishka Rao, Rajiv Mathews, Swaroop Ramaswamy, Françoise Beaufays, Sean Augenstein, Hubert Eichner, Chloé Kiddon, and Daniel Ramage. Federated learning for mobile keyboard prediction (2018). *arXiv preprint arXiv:1811.03604*, 2018. https://doi.org/10.48550/arXiv.1811.03604.

[13] Chaoyang He, Songze Li, Jinhyun So, Xiao Zeng, Mi Zhang, Hongyi Wang, Xiaoyang Wang, Praneeth Vepakomma, Abhishek Singh, Hang Qiu, et al. Fedml: A research library and benchmark for federated machine learning. *arXiv preprint arXiv:2007.13518*, 2020. https://doi.org/10.48550/arXiv.2007.13518.

[14] Shuyan Hu, Xiaojing Chen, Wei Ni, Ekram Hossain, and Xin Wang. Distributed machine learning for wireless communication networks: Techniques, architectures, and applications. *IEEE Communications Surveys & Tutorials*, 23(3):1458–1493, 2021. https://doi.org/10.1109/COMST.2021.3086014.

[15] Sarfaraz Hussein, Pujan Kandel, Candice W Bolan, Michael B Wallace, and Ulas Bagci. Lung and pancreatic tumor characterization in the deep learning era: novel supervised and unsupervised learning approaches. *IEEE transactions on medical imaging*, 38(8):1777–1787, 2019. https://doi.org/10.1109/TMI.2019.2894349.

[16] Sagar Imambi, Kolla Bhanu Prakash, and GR Kanagachidambaresan. Pytorch. *Programming with TensorFlow: solution for edge computing applications*, pages 87–104, 2021. https://doi.org/10.1007/978-3-030-57077-4_10.

[17] Qinbin Li, Zeyi Wen, Zhaomin Wu, Sixu Hu, Naibo Wang, Yuan Li, Xu Liu, and Bingsheng He. A survey on federated learning systems: Vision, hype and reality for data privacy and protection. *IEEE Transactions on Knowledge and Data Engineering*, 35(4):3347–3366, 2021. https://doi.org/10.1109/TKDE.2021.3124599.

[18] Tian Li, Anit Kumar Sahu, Ameet Talwalkar, and Virginia Smith. Federated learning: Challenges, methods, and future directions. *IEEE signal processing magazine*, 37(3):50–60, 2020. https://doi.org/10.1109/MSP.2020.2975749.

[19] Hui Lin, Kuljeet Kaur, Xiaoding Wang, Georges Kaddoum, Jia Hu, and Mohammad Mehedi Hassan. Privacy-aware access control in iot-enabled healthcare: A federated deep learning approach. *IEEE Internet of Things Journal*, 10(4):2893–2902, 2021. https://doi.org/10.1109/JIOT.2021.3112686.

[20] Boliang Lv, Peizhe Cheng, Cheng Zhang, Hong Ye, Xianzhe Meng, and Xiao Wang. Research on modeling of e-banking fraud account identification based on federated learning. In *2021 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)*, pages 611–618. IEEE, 2021. https://doi.org/10.1109/ICMLA52953.2021.00064.

[21] Brendan McMahan, Eider Moore, Daniel Ramage, Seth Hampson, and Blaise Aguera y Arcas. Communication-efficient learning of deep networks from decentralized data. In *Artificial intelligence and statistics*, pages 1273–1282. PMLR, 2017.

[22] Delton Myalil, MA Rajan, Manoj Apte, and Sachin Lodha. Robust collaborative fraudulent transaction detection using federated learning. In *2021 20th IEEE International Conference on Machine Learning and Applications (ICMLA)*, pages 373–378. IEEE, 2021. https://doi.org/10.1109/DASC-PICom-CBDCom-CyberSciTech52372.2021.00105.

[23] Manu Narula, Jasraj Meena, and Dinesh Kumar Vishwakarma. A comprehensive review on federated learning for data-sensitive application: Open issues & challenges. *Engineering Applications of Artificial Intelligence*, 133:108128, 2024. https://doi.org/10.1016/j.engappai.2024.108128.

[24] Manu Narula, Jasraj Meena, and Dinesh Kumar Vishwakarma. Dynamic resource-aware federated framework for secure and sustainable learning in data sensitive applications. In *2024 IEEE 9th International Conference for Convergence in Technology (I2CT)*, pages 1–8. IEEE, 2024.

[25] Manu Narula, Jasraj Meena, and Dinesh Kumar Vishwakarma. Federated workload-aware quantized framework for secure learning in data-sensitive applications. *Future Generation Computer Systems*, 168:107772, 2025.

[26] Thang Ngo, Dinh C Nguyen, Pubudu N Pathirana, Louise A Corben, Martin B Delatycki, Malcolm Horne, David J Szmulewicz, and Melissa Roberts. Federated deep learning for the diagnosis of cerebellar ataxia: Privacy preservation and auto-crafted feature extractor. *IEEE Transactions on Neural Systems and Rehabilitation Engineering*, 30:803–811, 2022. https://doi.org/10.1109/TNSRE.2022.3161272.

[27] PaddlePaddle Developers. PaddlePaddle: An Open-Source Deep Learning Platform. https://github.com/PaddlePaddle/Paddle, 2024. Accessed: April 20, 2025.

[28] Nuria Rodríguez-Barroso, Daniel Jiménez-López, M Victoria Luzón, Francisco Herrera, and Eugenio Martínez-Cámara. Survey on federated learning threats: Concepts, taxonomy on attacks and defences, experimental study and challenges. *Information Fusion*, 90:148–173, 2023. https://doi.org/10.1016/j.inffus.2022.09.011.

[29] Theo Ryffel, Andrew Trask, Morten Dahl, Bobby Wagner, Jason Mancuso, Daniel Rueckert, and Jonathan Passerat-Palmbach. A generic framework for privacy preserving deep learning. *arXiv preprint arXiv:1811.04017*, 2018. https://doi.org/10.48550/arXiv.1811.04017.

[30] The TensorFlow Federated Authors. Tensorflow federated: Machine learning on decentralized data. https://www.tensorflow.org/federated, 2021. Accessed: April 20, 2025.

[31] Timothy Yang, Galen Andrew, Hubert Eichner, Haicheng Sun, Wei Li, Nicholas Kong, Daniel Ramage, and Françoise Beaufays. Applied federated learning: Improving google keyboard query suggestions. *arXiv preprint arXiv:1812.02903*, 2018. https://doi.org/10.48550/arXiv.1812.02903.

[32] Kaiyue Zhang, Xuan Song, Chenhan Zhang, and Shui Yu. Challenges and future directions of secure federated learning: a survey. *Frontiers of computer science*, 16:1–8, 2022. https://doi.org/10.1007/s11704-021-0598-z.