Model-Centric Federated Machine Learning

AUTHORS, Institute xx, Country

Traditional Federated Machine Learning follows a server-domincated cooperation paradigm which narrows the application scenarios of federated learning and decreases the enthusiasm of data holders to participate.

CCS Concepts: • **Computer systems organization → Embedded systems**; *Redundancy*; Robotics; • **Networks** → Network reliability.

Additional Key Words and Phrases: datasets, neural networks, gaze detection, text tagging

ACM Reference Format:
Authors. 2018. Model-Centric Federated Machine Learning. *Proc. ACM Meas. Anal. Comput. Syst.* 37, 4, Article 111 (August 2018), 7 pages. https://doi.org/XXXXXXX.XXXXXXX

1 INTRODUCTION

Introduction: Federated Learning [27].

Four roles in FL systems design: the data owners, the model users, the coordinators, the auditors.

1.1 Related Surveys

In recent years, federated learning has become a buzzword in various fields, leading to the emergence of numerous FL studies. These works can be classified into three primary categories: FL systems design, FL appllications and FL toolkits. Extensive surveys are available to summarized the advancement of federated learning, as shown in Table 1. The initial architectures and concepts for FL systems were summaried by Yang *et al.* [49]. They categorized FL into horizontal FL, vertical FL and federated transfer learning based on the distribution characteristics of data, which are written in IEEE Standard 3652.1-2020 [43, 48]. Following this, an increasing number of surveys have emerged focusing on enhancing FL system design [5, 21, 26, 27, 53]. From the algorithmic perspective, personlized FL [23, 45] aims to learn personlized models for each client to address the challenge of statistical heterogeneity [33]. Besides, the privacy-perserving computing platforms and model aggregation protocols for FL systems also been widely studied and sumaried by [11, 31, 32, 51]. Furthermore, many advanced FL architectures had been proposed, such as asynchronous [46], decentralized and blockchain-based FL frameworks [36, 38, 58]. Given that federated learning technologies enable collaboration among distributed participants in model training and decision-making, this capability holds great promise in a wide range of application scenarios. For instance, multiple geogrphically distributed medical insitutions can enhace medication recommendation, drug-drug interaction prediction and medical image analysis in a collaborative manner without exchanging any sensitive data [6, 37, 41, 47]. The massive real-time data generated by IoT devices in smart cities [39, 55], industries [8], vehicles [10] has also sparked interest in exploring how FL technology can be used to deliver more advanced services such as intrusion detection, anomaly detection, fraud detection and network load prediction [3, 4, 14].

Author's address: Authors, Institute xx, City, Country, @mail.com.

2476-1249/2018/8-ART111 $15.00
https://doi.org/XXXXXXX.XXXXXXX

Table 1. Summary of existing FL surveys, SYS denotes FL Systems Design, APP denotes FL Applications, SDC denotes Server-Dominated Cooperation frameworks.

		Challenges					Contents		
Scenarios/Tasks	FL Surveys	Efficiency	Heterogeneity	Privacy	Incentive	Decentralized	SYS	APP	SDC
General	Yang *et al.* [49]	✓	✓	✓	✓	✓	✓	✓	✓
	Li *et al.* 2020 [27]	✓	✓	✓		✓	✓	✓	✓
	Zhang 2021*et al.* [53]	✓	✓	✓			✓	✓	✓
	Gupta *et al.* [15]	✓	✓	✓		✓	✓	✓	✓
	Xu *et al.* [46]	✓	✓	✓		✓	✓	✓	✓
	Li *et al.* 2021 [26]	✓	✓	✓	✓	✓	✓	✓	✓
	El *et al.* [11]			✓		✓	✓		✓
	Kulkarni *et al.* [23]	✓	✓				✓		✓
	Liu *et al.*[31]	✓		✓		✓	✓		✓
	Tan *et al.* [45]		✓				✓		✓
	Zhu *et al.* 2021 [57]		✓				✓		✓
	Ma *et al.* [33]	✓	✓	✓			✓		✓
	Aledhari *et al.* [5]	✓	✓				✓	✓	✓
	Kairouz *et al.* [21]	✓	✓	✓	✓	✓	✓	✓	✓
	AbdulRahman *et al.* [2]	✓	✓	✓	✓		✓	✓	✓
	Lim *et al.* [28]	✓	✓	✓	✓		✓	✓	✓
Healthcare	Xu *et al.* [47]	✓	✓	✓			✓	✓	✓
	Pfitzner *et al.*[37]	✓	✓	✓			✓	✓	✓
	Antunes *et al.* [6]		✓	✓				✓	✓
	Rieke *et al.* [41]		✓	✓		✓	✓	✓	✓
IoT	Zhang 2022*et al.* [55]	✓	✓				✓	✓	✓
	Boopalan *et al.* [8]	✓	✓	✓	✓	✓	✓	✓	✓
	Ramu *et al.* [39]	✓	✓	✓		✓	✓	✓	✓
	Du *et al.* [10]	✓	✓	✓	✓	✓	✓	✓	✓
Cybersecurity	Agrawal *et al.* [3]	✓	✓	✓		✓	✓	✓	✓
	Alazab *et al.* [4]			✓			✓	✓	✓
	Ghimire *et al.* [14]	✓		✓			✓	✓	✓
Blockchain	Nguyen *et al.* [36]	✓	✓	✓	✓	✓	✓	✓	✓
	Qu *et al.* [38]	✓	✓	✓	✓	✓	✓	✓	✓
	Zhu *et al.* 2022 [58]	✓	✓	✓	✓	✓	✓	✓	✓

As summarized in Table 1, most surveys extensively discuss the challenges of efficiency, heterogeneity, privacy in FL systems design, with the surveys from blockchain fileds offering the most comprehensive review. However, except for a few blockchain-based FL studies, most of the above surveys just present the same story from slightly different angles or backgrounds, i.e a server sets the model training task and delegate it to data holders to complete. This *server-domincated* cooperation framework is a narrow implementation of the FL systems. Therefore, this survey aim to fill the gap by investigating and surveying the associated tenchnologies that support more open and inclusive cooperation frameworks in FL systems, where all entities, whether they own the data or not, can benefit from it. The challenges investigated in this survey are not listed in the Table 1, to the best of our knowledge, this is the first survey that focuses on the cooperation frameworks of FL. In the following section, we will differentiate this survey from other related concepts in the field of FL.

1.2 Distinction of Our Survey

This survey focuses on exploring the innovative cooperation frameworks in FL, which will involve some FL concepts such as decentralized FL, blockchain-based FL, few-shot FL, ML related platforms and services but goes beyond them. In this section, we will distinguish our survey by highlingting the similarities and differences between these related concepts.

1.2.1 Dcentralized FL. ref: given the high scalability of modern edge computing networks, a single MEC server cannot manage to aggregate all updates offloaded from millions of devices. Therefore, there is an urgent need to develop a more decentralized FL approach without using a central server so as to solve security and scalability issues for enabling the next generation intelligent edge networks.

1.2.2 Blockchain-based FL.

1.2.3 Few-shot FL.

1.2.4 FL Systems. Federated learning, with its nature advantages in privacy-preserving decision sharing, has garnered significant attention in both industry and academia, leading to the rapid development of federated learning systems. The earliest attempt at the large-scale FL system was by Google, where FL was used to improve next-word prediction [18] and query suggesion [50] for Gboard applications. Subsequently, many novel FL systems have emerged to adapt to diverse federated training scenarios, such as Horizontal FL (e.g. TFF [1], FedLab [52], Felicitas [54]), Vertical FL or both (e.g. FATE [30], FedML [19], PaddleFL [34], FedTree [25]).

More recently, Tensorflow Federated (TFF) [1] PySyft [59] PySyTFF[1] FATE [30] FedML [19] FedLab [52] PaddleFL [34] Flower [7]

Cross-device FL framework from Huawei [54]

We aim to provide an open and shared ecosystem where every user is free to collaborate on the training of machine learning models and where privacy is protected

1.2.5 As-a-Service Business Model. In the current context of Software-as-a-Service (SaaS) [9], there are several as-a-service cloud computing frameworks that encapsulate ML tasks as services and provides unified APIs for upper layer applications. For example, Model-as-a-Service (MaaS) [12, 29, 42, 44, 60] and Machine-Learning-as-a-Service (MLaaS) [17, 20, 22, 24, 40] encapsulate model execution and model development as services. The original concept of MaaS [12, 42] was to provide re-usable and fine-grained user interfaces and visualization tools of domain-specific models (e.g wealther model, oil spill detection model) for environmental decision support systems. Subsequently, this concept has been extended to the field of recommendation systems [60] and deep learning based systems [29, 44]. However, in contrast to the focus of this survey, the aforementioned MaaS framework does not involve any user collaboration but solely provides model inference APIs to users.

As the architectures of deep neural networks (DNNs) become increasingly complex, training and maintaining DNNs become more and more challenging [16]. To address this issue, cloud service providers have introduced MLaaS, which offers an integrated development environment as a service for constructing and operationalizing ML workflows, aiming to reduce the computational resources required. MLaaS enables users to upload their data for training [20, 40, 56] or inference [17], freeing them from the responsibility of managing hardware resources and implementation. Most MLaaS providers adopt a pay-by-query business model, such as Google Vertex AI[2], Microsoft Azure Machine Learning[3] and ChatGPT[4]. However, privacy protection can be compromised when users upload data to perform inference and training in the cloud. Moverover, under this model, users are not given the ability to contribute their own models to the repository or collaborate with others to enhance the diversity of available models. While there are some ongoing efforts to offer privacy-preserving MLaaS services using techniques such as Isolated Execution Environment [17, 35] and Homomorphic Encryption [13, 20], it

[1]https://blog.openmined.org/announcing-proof-of-concept-support-for-tff-in-pysyft-0-7/
[2]https://cloud.google.com/vertex-ai
[3]https://azure.microsoft.com/products/machine-learning/
[4]https://chat.openai.com/chat

Table 2. Summary of existing deep learning model repositories.

	DS Name	Model Architecture	Modality/Task	Tag	License	Input-Output	Batch Export	# of Models
Hugging Face[5]	✓	✓	✓	✓	✓	!	✗	133,641
Model Zoo[6]	✓	✓	✓	✓	✗	✗	✗	3,426
OpenVINO[7]	!	✓	✓	✗	!	!	✓	278
Tensorflow Hub[8]	✓	✓	✓	✓	!	!	✗	1,356
Pytorch Hub[9]	!	✓	✗	✗	✗	!	✗	49
NVIDIA NGC[10]	!	✓	✓	✓	!	!	✗	527

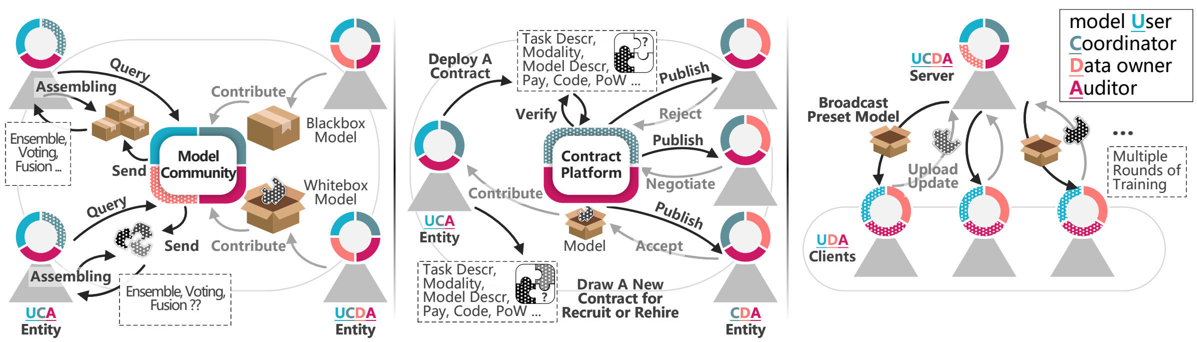
is worth noting that our focus is not solely on privacy. Rather, the FL framework we focus on emphasizes a collaborative framework where all entities involved have equal access to services and mutual benefits.

Recently, Kourtellis *et al.* [22] propose Federated Learning as a Service (FLaaS) that provides high-level and extensible APIs aim to enabling 3rd-party applications to build collaborative, decentralized, privacy-preserving ML models. However, this approach also follows the traditional server-dominated cooperation framework, which falls under the scope of previous FL surveys[21, 27, 49].

1.3 FAIR in FL

FAIR Data Principles: Findable, Accessible, Interoperable, Reusable.

Three cooperation frameworks: query-based FL, contract-based FL, writ-based FL



(a) Query-based FML (b) Contract-based FML (c) Traditional FML

Fig. 1. Cooperation frameworks of FML.

ACKNOWLEDGMENTS

ACK.

[5]https://huggingface.co
[6]https://modelzoo.co/
[7]https://docs.openvino.ai/latest/model_zoo.html
[8]https://tfhub.dev/
[9]https://pytorch.org/hub/
[10]https://catalog.ngc.nvidia.com/models

REFERENCES

[1] Martín Abadi, Paul Barham, Jianmin Chen, Zhifeng Chen, Andy Davis, Jeffrey Dean, Matthieu Devin, Sanjay Ghemawat, Geoffrey Irving, Michael Isard, et al. 2016. Tensorflow: A system for large-scale machine learning. In *Proceedings of the 12th USENIX Symposium on Operating Systems Design and Implementation (OSDI)*. 265–283.

[2] Sawsan AbdulRahman, Hanine Tout, Hakima Ould-Slimane, Azzam Mourad, Chamseddine Talhi, and Mohsen Guizani. 2020. A survey on federated learning: The journey from centralized to distributed on-site learning and beyond. *IEEE Internet of Things Journal* 8, 7 (2020), 5476–5497. https://doi.org/10.1109/JIOT.2020.3030072

[3] Shaashwat Agrawal, Sagnik Sarkar, Ons Aouedi, Gokul Yenduri, Kandaraj Piamrat, Mamoun Alazab, Sweta Bhattacharya, Praveen Kumar Reddy Maddikunta, and Thippa Reddy Gadekallu. 2022. Federated learning for intrusion detection system: Concepts, challenges and future directions. *Computer Communications* (2022). https://doi.org/10.1016/j.comcom.2022.09.012

[4] Mamoun Alazab, Swarna Priya RM, M Parimala, Praveen Kumar Reddy Maddikunta, Thippa Reddy Gadekallu, and Quoc-Viet Pham. 2021. Federated learning for cybersecurity: concepts, challenges, and future directions. *IEEE Transactions on Industrial Informatics* 18, 5 (2021), 3501–3509. https://doi.org/10.1109/TII.2021.3119038

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

[6] Rodolfo Stoffel Antunes, Cristiano André da Costa, Arne Küderle, Imrana Abdullahi Yari, and Björn Eskofier. 2022. Federated learning for healthcare: Systematic review and architecture proposal. *ACM Transactions on Intelligent Systems and Technology (TIST)* 13, 4 (2022), 1–23. https://doi.org/10.1145/3501813

[7] Daniel J Beutel, Taner Topal, Akhil Mathur, Xinchi Qiu, Titouan Parcollet, Pedro PB de Gusmão, and Nicholas D Lane. 2020. Flower: A friendly federated learning research framework. *arXiv preprint arXiv:2007.14390* (2020).

[8] Parimala Boopalan, Swarna Priya Ramu, Quoc-Viet Pham, Kapal Dev, Praveen Kumar Reddy Maddikunta, Thippa Reddy Gadekallu, Thien Huynh-The, et al. 2022. Fusion of federated learning and industrial Internet of Things: A survey. *Computer Networks* (2022), 109048. https://doi.org/10.1016/j.comnet.2022.109048

[9] Pearl Brereton, David Budgen, Keith Bennnett, Malcolm Munro, Paul Layzell, Linda MaCaulay, David Griffiths, and Charles Stannett. 1999. The future of software. *Commun. ACM* 42, 12 (1999), 78–84. https://doi.org/10.1145/322796.322813

[10] Zhaoyang Du, Celimuge Wu, Tsutomu Yoshinaga, Kok-Lim Alvin Yau, Yusheng Ji, and Jie Li. 2020. Federated learning for vehicular internet of things: Recent advances and open issues. *IEEE Open Journal of the Computer Society* 1 (2020), 45–61. https://doi.org/10.1109/OJCS.2020.2992630

[11] Ahmed El Ouadrhiri and Ahmed Abdelhadi. 2022. Differential privacy for deep and federated learning: A survey. *IEEE Access* 10 (2022), 22359–22380. https://doi.org/10.1109/ACCESS.2022.3151670

[12] Gary N Geller and Woody Turner. 2007. The model web: a concept for ecological forecasting. In *2007 IEEE International Geoscience and Remote Sensing Symposium*. IEEE, 2469–2472. https://doi.org/10.1109/IGARSS.2007.4423343

[13] Craig Gentry. 2009. Fully homomorphic encryption using ideal lattices. In *Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing (STOC)*. 169–178. https://doi.org/10.1145/1536414.1536440

[14] Bimal Ghimire and Danda B Rawat. 2022. Recent advances on federated learning for cybersecurity and cybersecurity for federated learning for internet of things. *IEEE Internet of Things Journal* (2022). https://doi.org/10.1109/JIOT.2022.3150363

[15] Ruchi Gupta and Tanweer Alam. 2022. Survey on federated-learning approaches in distributed environment. *Wireless Personal Communications* 125, 2 (2022), 1631–1652. https://doi.org/10.1007/s11277-022-09624-y

[16] Xu Han, Zhengyan Zhang, Ning Ding, Yuxian Gu, Xiao Liu, Yuqi Huo, Jiezhong Qiu, Yuan Yao, Ao Zhang, Liang Zhang, et al. 2021. Pre-trained models: Past, present and future. *AI Open* 2 (2021), 225–250. https://doi.org/10.1016/j.aiopen.2021.08.002

[17] Lucjan Hanzlik, Yang Zhang, Kathrin Grosse, Ahmed Salem, Maximilian Augustin, Michael Backes, and Mario Fritz. 2021. Mlcapsule: Guarded offline deployment of machine learning as a service. In *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*. 3300–3309.

[18] Andrew Hard, Kanishka Rao, Rajiv Mathews, Françoise Beaufays, Sean Augenstein, Hubert Eichner, Chloé Kiddon, and Daniel Ramage. 2018. Federated learning for mobile keyboard prediction. *arXiv preprint arXiv:1811.03604* (2018).

[19] Chaoyang He, Songze Li, Jinhyun So, Xiao Zeng, Mi Zhang, Hongyi Wang, Xiaoyang Wang, Praneeth Vepakomma, Abhishek Singh, Hang Qiu, et al. 2020. FedML: A research library and benchmark for federated machine learning. In *NeurIPS 2020 Workshop on Scalability, Privacy, and Security in Federated Learning*.

[20] Ehsan Hesamifard, Hassan Takabi, Mehdi Ghasemi, and Rebecca N Wright. 2018. Privacy-preserving machine learning as a service. *Proc. Priv. Enhancing Technol.* 2018, 3 (2018), 123–142. https://doi.org/10.1515/popets-2018-0024

[21] Peter Kairouz, H Brendan McMahan, Brendan Avent, Aurélien Bellet, Mehdi Bennis, Arjun Nitin Bhagoji, Kallista Bonawitz, Zachary Charles, Graham Cormode, Rachel Cummings, et al. 2021. Advances and open problems in federated learning. *Foundations and Trends® in Machine Learning* 14, 1–2 (2021), 1–210. https://doi.org/10.1561/2200000083

[22] Nicolas Kourtellis, Kleomenis Katevas, and Diego Perino. 2020. FLaaS: Federated learning as a service. In *Proceedings of the 1st workshop on distributed machine learning*. 7–13. https://doi.org/10.1145/3426745.3431337

[23] Viraj Kulkarni, Milind Kulkarni, and Aniruddha Pant. 2020. Survey of personalization techniques for federated learning. In *2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*. IEEE, 794–797. https://doi.org/10.1109/WorldS450073.2020.9210355

[24] Li Erran Li, Eric Chen, Jeremy Hermann, Pusheng Zhang, and Luming Wang. 2017. Scaling machine learning as a service. In *International Conference on Predictive Applications and APIs*. PMLR, 14–29.

[25] Qinbin Li, Yanzheng Cai, Yuxuan Han, Ching Man Yung, Tianyuan Fu, and Bingsheng He. 2022. FedTree: A Fast, Effective, and Secure Tree-based Federated Learning System. https://github.com/Xtra-Computing/FedTree/blob/main/FedTree_draft_paper.pdf.

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

[27] Tian Li, Anit Kumar Sahu, Ameet Talwalkar, and Virginia Smith. 2020. Federated learning: Challenges, methods, and future directions. *IEEE Signal Processing Magazine* 37, 3 (2020), 50–60.

[28] Wei Yang Bryan Lim, Nguyen Cong Luong, Dinh Thai Hoang, Yutao Jiao, Ying-Chang Liang, Qiang Yang, Dusit Niyato, and Chunyan Miao. 2020. Federated learning in mobile edge networks: A comprehensive survey. *IEEE Communications Surveys & Tutorials* 22, 3 (2020), 2031–2063. https://doi.org/10.1109/COMST.2020.2986024

[29] Hao Liu, Qian Gao, Jiang Li, Xiaochao Liao, Hao Xiong, Guangxing Chen, Wenlin Wang, Guobao Yang, Zhiwei Zha, Daxiang Dong, et al. 2021. Jizhi: A fast and cost-effective model-as-a-service system for web-scale online inference at baidu. In *Proceedings of the 27th ACM SIGKDD Conference on Knowledge Discovery & Data Mining*. Association for Computing Machinery, New York, NY, USA, 3289–3298. https://doi.org/10.1145/3447548.3467146

[30] Yang Liu, Tao Fan, Tianjian Chen, Qian Xu, and Qiang Yang. 2021. FATE: An industrial grade platform for collaborative learning with data protection. *The Journal of Machine Learning Research* 22, 1 (2021), 10320–10325.

[31] Ziyao Liu, Jiale Guo, Wenzhuo Yang, Jiani Fan, Kwok-Yan Lam, and Jun Zhao. 2022. Privacy-preserving aggregation in federated learning: A survey. *IEEE Transactions on Big Data (TBD)* (2022), 1–20. https://doi.org/10.1109/TBDATA.2022.3190835

[32] Lingjuan Lyu, Han Yu, and Qiang Yang. 2020. Threats to federated learning: A survey. *arXiv preprint arXiv:2003.02133* (2020).

[33] Xiaodong Ma, Jia Zhu, Zhihao Lin, Shanxuan Chen, and Yangjie Qin. 2022. A state-of-the-art survey on solving non-IID data in Federated Learning. *Future Generation Computer Systems* 135 (2022), 244–258. https://doi.org/10.1016/j.future.2022.05.003

[34] Yanjun Ma, Dianhai Yu, Tian Wu, and Haifeng Wang. 2019. PaddlePaddle: An open-source deep learning platform from industrial practice. *Frontiers of Data and Domputing* 1, 1 (2019), 105–115. https://doi.org/10.11871/jfdc.issn.2096.742X.2019.01.011

[35] Frank McKeen, Ilya Alexandrovich, Ittai Anati, Dror Caspi, Simon Johnson, Rebekah Leslie-Hurd, and Carlos Rozas. 2016. Intel® software guard extensions (Intel® SGX) support for dynamic memory management inside an enclave. In *Proceedings of the Hardware and Architectural Support for Security and Privacy 2016*. 1–9. https://doi.org/10.1145/2948618.2954331

[36] Dinh C Nguyen, Ming Ding, Quoc-Viet Pham, Pubudu N Pathirana, Long Bao Le, Aruna Seneviratne, Jun Li, Dusit Niyato, and H Vincent Poor. 2021. Federated learning meets blockchain in edge computing: Opportunities and challenges. *IEEE Internet of Things Journal* 8, 16 (2021), 12806–12825. https://doi.org/10.1109/JIOT.2021.3072611

[37] Bjarne Pfitzner, Nico Steckhan, and Bert Arnrich. 2021. Federated learning in a medical context: A systematic literature review. *ACM Transactions on Internet Technology (TOIT)* 21, 2 (2021), 1–31. https://doi.org/10.1145/3412357

[38] Youyang Qu, Md Palash Uddin, Chenquan Gan, Yong Xiang, Longxiang Gao, and John Yearwood. 2022. Blockchain-enabled federated learning: A survey. *ACM Computing Surveys (CSUR)* 55, 4 (2022), 1–35. https://doi.org/10.1145/3524104

[39] Swarna Priya Ramu, Parimala Boopalan, Quoc-Viet Pham, Praveen Kumar Reddy Maddikunta, Thien Huynh-The, Mamoun Alazab, Thanh Thi Nguyen, and Thippa Reddy Gadekallu. 2022. Federated learning enabled digital twins for smart cities: Concepts, recent advances, and future directions. *Sustainable Cities and Society* 79 (2022), 103663. https://doi.org/10.1016/j.scs.2021.103663

[40] Mauro Ribeiro, Katarina Grolinger, and Miriam AM Capretz. 2015. MLaaS: Machine learning as a service. In *2015 IEEE 14th international conference on machine learning and applications (ICMLA)*. IEEE, 896–902. https://doi.org/10.1109/ICMLA.2015.152

[41] Nicola Rieke, Jonny Hancox, Wenqi Li, Fausto Milletari, Holger R Roth, Shadi Albarqouni, Spyridon Bakas, Mathieu N Galtier, Bennett A Landman, Klaus Maier-Hein, et al. 2020. The future of digital health with federated learning. *NPJ digital medicine* 3, 1 (2020), 119. https://doi.org/10.1038/s41746-020-00323-1

[42] Dumitru Roman, Sven Schade, Arne-Jørgen Berre, Nils Rune Bodsberg, and J Langlois. 2009. Model as a Service (MaaS). In *AGILE Workshop-Grid Technologies for Geospatial Applications*.

[43] IEEE Computer Society. 2021. IEEE Guide for Architectural Framework and Application of Federated Machine Learning. *IEEE Std 3652.1-2020* (2021), 1–69. https://doi.org/10.1109/IEEESTD.2021.9382202

[44] Tianxiang Sun, Yunfan Shao, Hong Qian, Xuanjing Huang, and Xipeng Qiu. 2022. Black-box tuning for language-model-as-a-service. In *Proceedings of the 39th International Conference on Machine Learning (ICML)*. PMLR, 20841–20855.

[45] Alysa Ziying Tan, Han Yu, Lizhen Cui, and Qiang Yang. 2022. Towards personalized federated learning. *IEEE Transactions on Neural Networks and Learning Systems (TNNLS)* (2022), 1–17. https://doi.org/10.1109/TNNLS.2022.3160699

[46] Chenhao Xu, Youyang Qu, Yong Xiang, and Longxiang Gao. 2021. Asynchronous federated learning on heterogeneous devices: A survey. *arXiv preprint arXiv:2109.04269* (2021).

[47] Jie Xu, Benjamin S Glicksberg, Chang Su, Peter Walker, Jiang Bian, and Fei Wang. 2021. Federated learning for healthcare informatics. *Journal of Healthcare Informatics Research* 5 (2021), 1–19. https://doi.org/10.1007/s41666-020-00082-4

[48] Qiang Yang, Lixin Fan, Richard Tong, and Angelica Lv. 2021. IEEE Federated Machine Learning. *IEEE Federated Machine Learning - White Paper* (2021), 1–18.

[49] Qiang Yang, Yang Liu, Tianjian Chen, and Yongxin Tong. 2019. Federated machine learning: Concept and applications. *ACM Transactions on Intelligent Systems and Technology (TIST)* 10, 2 (2019), 1–19. https://doi.org/10.1145/3298981

[50] Timothy Yang, Galen Andrew, Hubert Eichner, Haicheng Sun, Wei Li, Nicholas Kong, Daniel Ramage, and Françoise Beaufays. 2018. Applied federated learning: Improving google keyboard query suggestions. *arXiv preprint arXiv:1812.02903* (2018).

[51] Xuefei Yin, Yanming Zhu, and Jiankun Hu. 2021. A comprehensive survey of privacy-preserving federated learning: A taxonomy, review, and future directions. *ACM Computing Surveys (CSUR)* 54, 6 (2021), 1–36. https://doi.org/10.1145/3460427

[52] Dun Zeng, Siqi Liang, Xiangjing Hu, Hui Wang, and Zenglin Xu. 2021. Fedlab: A flexible federated learning framework. *arXiv preprint arXiv:2107.11621* (2021).

[53] Chen Zhang, Yu Xie, Hang Bai, Bin Yu, Weihong Li, and Yuan Gao. 2021. A survey on federated learning. *Knowledge-Based Systems (KBS)* 216 (2021), 106775. https://doi.org/10.1016/j.knosys.2021.106775

[54] Qi Zhang, Tiancheng Wu, Peichen Zhou, Shan Zhou, Yuan Yang, and Xiulang Jin. 2022. Felicitas: Federated Learning in Distributed Cross Device Collaborative Frameworks. In *Proceedings of the 28th ACM SIGKDD Conference on Knowledge Discovery and Data Mining*. 4502–4509. https://doi.org/10.1145/3534678.3539039

[55] Tuo Zhang, Lei Gao, Chaoyang He, Mi Zhang, Bhaskar Krishnamachari, and A Salman Avestimehr. 2022. Federated learning for the internet of things: applications, challenges, and opportunities. *IEEE Internet of Things Magazine* 5, 1 (2022), 24–29. https://doi.org/10.1109/IOTM.004.2100182

[56] Lingchen Zhao, Qian Wang, Cong Wang, Qi Li, Chao Shen, and Bo Feng. 2021. Veriml: Enabling integrity assurances and fair payments for machine learning as a service. *IEEE Transactions on Parallel and Distributed Systems* 32, 10 (2021), 2524–2540. https://doi.org/10.1109/TPDS.2021.3068195

[57] Hangyu Zhu, Jinjin Xu, Shiqing Liu, and Yaochu Jin. 2021. Federated learning on non-IID data: A survey. *Neurocomputing* 465 (2021), 371–390. https://doi.org/10.1016/j.neucom.2021.07.098

[58] Juncen Zhu, Jiannong Cao, Divya Saxena, Shan Jiang, and Houda Ferradi. 2022. Blockchain-empowered federated learning: Challenges, solutions, and future directions. *ACM Computing Surveys (CSUR)* (2022). https://doi.org/10.1145/3570953

[59] Alexander Ziller, Andrew Trask, Antonio Lopardo, Benjamin Szymkow, Bobby Wagner, Emma Bluemke, Jean-Mickael Nounahon, Jonathan Passerat-Palmbach, Kritika Prakash, Nick Rose, et al. 2021. PySyft: A library for easy federated learning. *Federated Learning Systems: Towards Next-Generation AI* (2021), 111–139. https://doi.org/10.1007/978-3-030-70604-3_5

[60] Guobing Zou, Bofeng Zhang, Jianxing Zheng, Yinsheng Li, and Jianhua Ma. 2012. MaaS: Model as a service in cloud computing and Cyber-I space. In *2012 IEEE 12th International Conference on Computer and Information Technology*. IEEE, 1125–1130. https://doi.org/10.1109/CIT.2012.228

Received 20 February 2007; revised 12 March 2009; accepted 5 June 2009