Model-Centric Federated Machine Learning

AUTHORS, Institute xx, Country

Tranditional 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), 5 pages. https://doi.org/XXXXXXX.XXXXXXX

1 INTRODUCTION

Introduction: Federated Learning [14].

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.* [29]. They categorize 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 [24, 28]. Following this, an increasing number of surveys have emerged focusing on enhancing FL system design [4, 11, 13, 14, 31]. From the algorithmic perspective, personlized FL [12, 25] aims to learn personlized models for each client to address the challenge of statistical heterogeneity [18]. Besides, the privacy-perserving computing platforms and model aggregation protocols for FL systems also been widely studied and sumaried by [8, 16, 17, 30]. Furthermore, many advanced FL architectures had been proposed, such as asynchronous [26], decentralized and blockchain-based FL frameworks [19, 21, 34]. 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 [5, 20, 23, 27]. The massive real-time data generated by IoT devices in smart cities [22, 32], industries [6], vehicles [7] 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 [2, 3, 9].

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.* [29]	✓	✓	✓	✓	✓	✓	✓	✓
	Li *et al.* 2020 [14]	✓	✓	✓		✓	✓	✓	✓
	Zhang 2021*et al.* [31]	✓	✓	✓			✓	✓	✓
	Gupta *et al.* [10]	✓	✓	✓		✓	✓	✓	✓
	Xu *et al.* [26]	✓	✓	✓		✓	✓	✓	✓
	Li *et al.* 2021 [13]	✓	✓	✓	✓	✓	✓	✓	✓
	El *et al.* [8]			✓		✓	✓		✓
	Kulkarni *et al.* [12]	✓	✓				✓		✓
	Liu *et al.*[16]	✓		✓		✓	✓		✓
	Tan *et al.* [25]		✓				✓		✓
	Zhu *et al.* 2021 [33]		✓				✓		✓
	Ma *et al.* [18]	✓	✓	✓			✓		✓
	Aledhari *et al.* [4]	✓	✓				✓	✓	✓
	Kairouz *et al.* [11]	✓	✓	✓	✓	✓	✓	✓	✓
	AbdulRahman *et al.* [1]	✓	✓	✓	✓		✓	✓	✓
	Lim *et al.* [15]	✓	✓	✓	✓		✓	✓	✓
Healthcare	Xu *et al.* [27]	✓	✓	✓			✓	✓	✓
	Pfitzner *et al.*[20]	✓	✓	✓			✓	✓	✓
	Antunes *et al.* [5]		✓	✓				✓	✓
	Rieke *et al.* [23]		✓	✓		✓	✓	✓	✓
IoT	Zhang 2022*et al.* [32]	✓	✓				✓	✓	✓
	Boopalan *et al.* [6]	✓	✓	✓	✓	✓	✓	✓	✓
	Ramu *et al.* [22]	✓	✓	✓		✓	✓	✓	✓
	Du *et al.* [7]	✓	✓	✓	✓	✓	✓	✓	✓
Cybersecurity	Agrawal *et al.* [2]	✓	✓	✓		✓	✓	✓	✓
	Alazab *et al.* [3]			✓			✓	✓	✓
	Ghimire *et al.* [9]	✓		✓			✓	✓	✓
Blockchain	Nguyen *et al.* [19]	✓	✓	✓	✓	✓	✓	✓	✓
	Qu *et al.* [21]	✓	✓	✓	✓	✓	✓	✓	✓
	Zhu *et al.* 2022 [34]	✓	✓	✓	✓	✓	✓	✓	✓

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 and few-shot FL but goes beyond them. In this section, we will distinguish our survey by highlingting the similarities and differences between these related concepts.

Dcentralized FL.

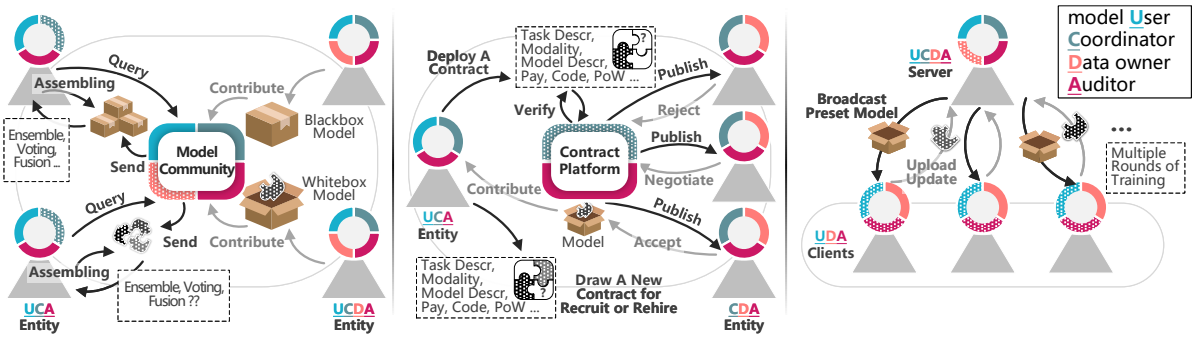
Blockchain-based FL.

Few-shot FL.

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.

REFERENCES

[1] 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

[2] 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

[3] 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

[4] 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

[5] 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

[6] 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

[7] 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

[8] 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

[9] 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

[10] 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

[11] 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

[12] 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

[13] 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

[14] 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.

[15] 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

[16] 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

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

[18] 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

[19] 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

[20] 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

[21] 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

[22] 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

[23] 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

[24] 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

[25] 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

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

[27] 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

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

[29] 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

[30] 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

[31] 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

[32] 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

[33] 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

[34] 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

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